OVERVIEW

High-Performance DDoS Protection

KEY BENEFITS

- Seamless detection and mitigation of volumetric DDoS attacks
- Full network visibility, traffic analysis, and attack detection
- Highest performance to support service providers, backbone operators, and large enterprises

To drive business success, modern ISPs, backbone operators, and large enterprises must protect their high-speed networks and mitigate today's volumetric DDoS attacks. If a DDoS attack is successful, then the Internet pipes are choked off. This bandwidth starvation causes service degradation, and eventually, service disruption for enterprise customers or employees. By detecting these volumetric DDoS attacks and helping with subsequent mitigation, Flowmon DDoS Defender and F5® DDoS Hybrid Defender (DHD) deliver powerful, comprehensive protection.

CHALLENGES

The continuing rise in both, the frequency and size of DoS/DDoS attacks is highlighted by the latest major security reports. According to Neustar's *Worldwide DDoS Attacks & Cyber Insights Research Report*, the average cost of a DDoS attack on a business is $2.5 million with some businesses reporting that revenue losses of $250,000 an hour are not uncommon.

In addition, the attack landscape is changing every day, and attackers are deploying new techniques to increase the magnitude of attacks and make them more difficult to mitigate. Consider the latest attacks launched by Internet of Things (IoT)-powered Mirai botnets, which were composed of hundreds of thousands of compromised devices. And because a successful attack can disrupt service for millions of customers, service providers and backbone operators must focus on detecting these attacks—and mitigating them before they reach the network.

SOLUTION

Service providers, backbone operators, and large enterprises can solve the problems of ever-growing DDoS attacks using the combined capabilities of Flowmon DDoS Defender and DDoS Hybrid Defender.

Flow monitoring and attack detection

Network visibility, traffic analysis, and attack detection and mitigation are the keys to fighting DDoS attacks in backbones—as close to the attack source as possible. Leveraging network traffic statistics from routers or dedicated network probes allows organizations to detect attacks, understand their characteristics, and start successful mitigation.

Powerful DDoS mitigation

For customers using flow data to detect an attack, network traffic must be diverted to a specific out-of-band DDoS mitigation appliance, a proecess that is streamlined by the deep integration of Flowmon and F5 technology. After an attack is detected, the solution creates a dynamic attack signature, which automatically launches a virtual server and allows DDoS Hybrid Defender to perform mitigation immediately after redirection—while allowing legitimate traffic to continue unaffected.

That's where DDoS Hybrid Defender comes in, performing DDoS mitigation for diverted traffic. The deep threat intelligence services and flexible mitigation options offered by DDoS Hybrid Defender help organizations defend against DDoS attacks at all network layers, stopping them before they cause real damage. DDoS Hybrid Defender scales quickly and easily to shut down high-capacity DDoS attacks that can overwhelm applications, intrusion detection and prevention systems, firewalls, and even networks.

LEARN MORE

- DDoS Hybrid Defender

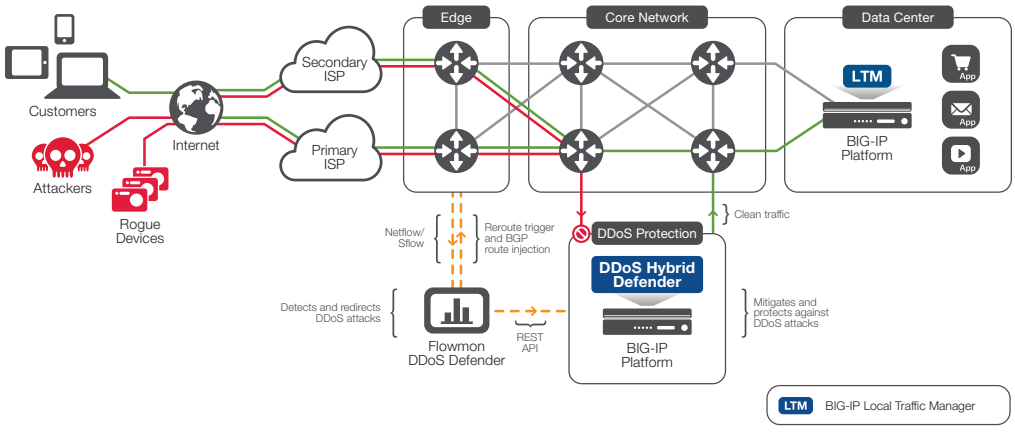

Figure 1: F5 and Flowmon solutions provide powerful DDoS detection and mitigation.

Working seamlessly together, Flowmon and F5 form a complex attack detection and mitigation ecosystem focused on volumetric attacks. The joint solution utilizes a high degree of automation, ensuring the fastest mean time to resolution while freeing network administrators from manual drudgery.

DC0318 | OV-SEC 211113605 | 0318