# DDOS PROTECTION FOR HIGH-SPEED NETWORKS

*DDoS attacks are one of the most harmful problems that current networks can encounter. At the same time, they are tricky to detect and effectively protect from, which makes them a real nightmare of online service providers and large network owners. To tackle this type of attacks, Flowmon Networks and F5 Networks have joined forces and developed a DDoS protection solution that is flexible, scalable, affordable, and arguably the fastest on the market.*

## WHY ARE DDOS ATTACKS SO HARMFUL?

Because 1) they're very difficult to prevent, 2) they have massive consequences. The nature of DDoS attacks makes it practically impossible to put a reliable “outer walls” protection in place, in other words, the attacks cannot be prevented – only detected and stopped early on, before harm is done. This is complicated by the number and seemingly legitimate nature of the attacking devices and by the fact that the attackers, evolving their techniques, are always a step ahead.

What is at stake? In case of online services, each downtime is very noticeable to customers and often gets media attention, too. Companies lose productivity, credibility, reputation, and money – whether in direct revenue loss, service unavailability compensations, or fixing the infrastructure. *Ponemon Institute’s Cyber Security on the Offense: A Study of IT Security Experts* states that the average amount of downtime following a DDoS attack is 54 minutes and the average cost for each minute of downtime is about $22,000, making for a whopping total of over a million dollars per average downtime, and that is just the direct loss.

## HOW CAN LARGE NETWORKS BE PROTECTED?

There are two basic types of DDoS protection: **in-line** and **out-of-band**. In-line devices are essential for the “last mile” protection from sophisticated attacks on the application layer, and irreplaceable in smaller networks. On their own, however, they are not sufficient as they are vulnerable to in-line overload and outages, plus installing them across large networks is also quite costly. Administrators of large high-speed networks cannot rely on protecting each individual uplink with a dedicated in-line device – instead, they need an efficient and economical **out-of-band** solution based on IPFIX/NetFlow data analysis, fast attack detection, and safe out-of-band mitigation. And that is exactly what the integrated Flowmon & F5 solution delivers.

## BENEFITS

### Automation

***Flowmon DDoS Defender*** *detects an attack within seconds, extracts the characteristics and orchestrates the mitigation via* ***F5 BIG-IP Advanced Firewall Manager****. No manual inputs are required.*

### Adaptability

*The integrated solution can be easily deployed within existing infrastructure and scale to fit a network of any size. Out-of-band service can effectively protect multiple uplinks at once and keep resistant to in-line outages.*

### Cost savings

*Our scalable out-of-band solution can cover whole networks, meaning that separate uplinks and network segments do not need separate protection. This cuts both initial and maintenance costs, and the savings are significant!*

> ***“DDoS attacks have seen an almost yearly evolution with the most recent focus being IoT. Enterprises should look into mitigation options as a way to protect and defend against these attacks.”***
>
> **Gartner**

## HOW DOES THE FLOWMON & F5 SOLUTION WORK?

As mentioned, there is no way to prevent a DDoS attack from happening, so detecting and stopping it at its earliest stage is key. The steps are as follows:

1. Collect detailed network statistics from routers or dedicated network probes.
2. Analyze the data to identify a starting attack and distinguish malicious traffic from legitimate.
3. Block or divert malicious traffic to protect the network.

Flowmon uses its **Collector** for data flow collection (1) and the **DDoS Defender** module for analysis (2), while F5 provides its **BIG-IP Advanced Firewall Manager** to execute the traffic diversion (3).

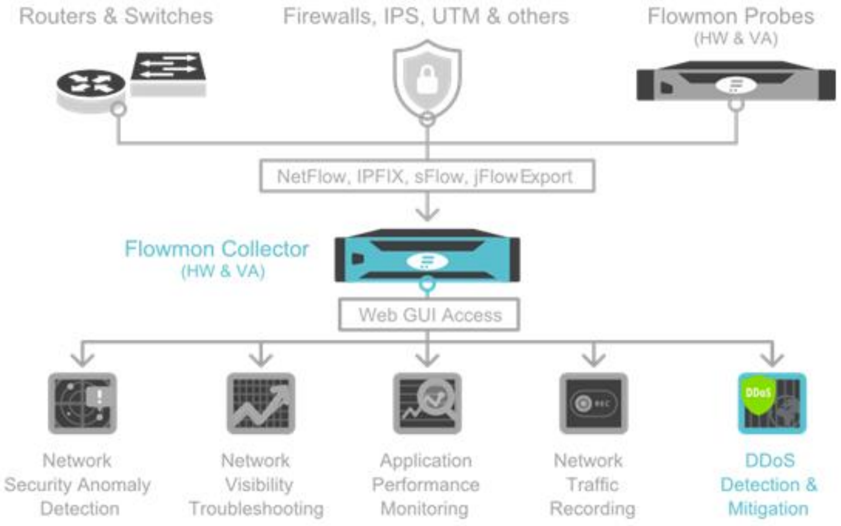
### Flowmon Collector and DDoS Defender

The heart of the Flowmon solution is **Flowmon Collector**, designated to gather network traffic data, analyze it, and provide detailed statistics and reports.

The Collector is complemented by the **Flowmon DDoS Defender** module, employing advanced threat intelligence to analyze flow data from the Collector to specifically detect volumetric (flood-based) attacks and bandwidth consumption. The data is processed in 30s batches, allowing for attack detection in under a minute, which is as fast as it gets.

In case of an unexpected increase of network traffic, Flowmon collects detailed information for later reference, such as top ten source IP addresses, subnets, autonomy systems and countries, L4 protocols and interfaces. At the same time, it triggers actions to start attack mitigation. The actions can be configured for various network segments, services or users individually, and can include:

- alerting admins (via e-mail, syslog, SNMP trap),
- diverting the traffic (via policy-based routing, border gateway protocol, remotely triggered black hole),
- executing scripts,
- re-routing the attack to a specific out-of-band DDoS mitigation system – in this case, F5.


Routers & Switches
Firewalls, IPS, UTM & others
Flowmon Probes
(HW & VA)
NetFlow, IPFIX, sFlow, jFlow Export
Flowmon Collector
(HW & VA)
Web GUI Access
Network Security Anomaly Detection
Network Visibility Troubleshooting
Application Performance Monitoring
Network Traffic Recording
DDoS Detection & Mitigation

### F5 BIG-IP Advanced Firewall Manager

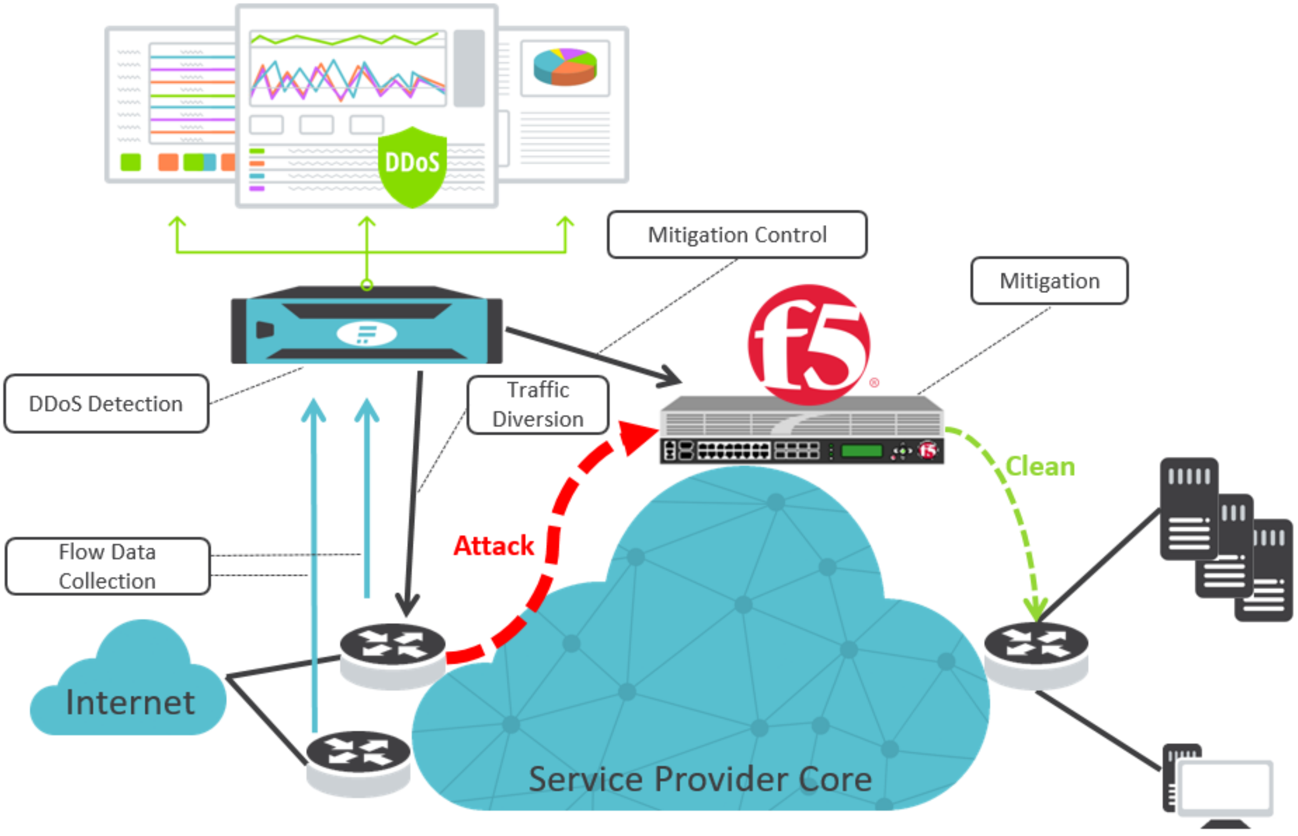
The BIG-IP AFM (Advanced Firewall Manager) by F5 employs threat intelligence and flexible mitigation options to effectively react to volumetric attacks on network and transport layers. It can create a dynamic attack signature and stop or re-route malicious traffic, scrubbing the attack and enabling legitimate traffic to continue unaffected.

### The Combined Protection

As the above description of the individual components suggests, both Flowmon and F5 can detect and mitigate a DDoS attack. However, together they offer enhanced protection that allows the components to do what each does best, and double up in critical points.

**Flowmon** ensures reliable data collection and analysis, very fast attack detection, and resistance to in-line outages. **F5** provides an out-of-band mitigation device able to clean any detected attack. Both products are seamlessly integrated into a complete, robust solution that can take fully automatic care of DDoS protection, using combined mitigation strategies for best results.

A notable benefit for large networks is great scalability of the joint solution – it can be easily added to existing infrastructure and adapted to any network size and complexity. Multiple uplinks and separate network segments can be effectively protected by a single device, which ensures significant cost savings. The joint Flowmon and F5 solution is therefore a perfect choice for even the largest networks with multiple peering partners and bandwidth of tens of gigabits per second, such as ISPs and backbone operators.



## F5 NETWORKS

F5 Networks helps organizations seamlessly scale cloud, data center and software-defined networking deployments to successfully deliver applications to anyone, anywhere, at any time.

www.f5.com

F5 Networks, Inc.
401 Elliott Avenue
Seattle, WA 98119-4017
USA

## FLOWMON NETWORKS

Flowmon Networks enables businesses to manage and secure their computer networks confidently. Flowmon's unique monitoring technology and behavior analytics offer perfect network traffic visibility, which helps enhance network and application performance and deal with modern cyber threats.

www.flowmon.com

Flowmon Networks a. s.
Sochorova 3232/34
616 00 Brno
Czech Republic