SCALABLE OUT-OF-PATH DDOS PROTECTION

Today, both customers and businesses depend on the internet as a single channel for service delivery. ISPs, enterprises and data centers need to maintain high availability to continually deliver quality services. Downtime means an immediate drop in productivity and revenue loss. Even partial service speed degradation can lead to loss of reputation and loss of customer base.

Flowmon Networks and A10 Networks have introduced joint out-of-path DDoS protection. Flowmon leverages flow data for fast volumetric DDoS detection while A10 adds surgical mitigation capabilities.

COST OF DOWNTIME

Ponemon Institute's *Cyber Security on the Offense: A Study of IT Security Experts* estimates that the average cost of a single minute of downtime is $22,000 with the average downtime of 54 minutes. Meaning businesses can easily lose over $1 Million as a direct result of a single attack (not accounting for subsequent loss in revenue due to the damaged reputation). Gartner offers a handy tool for downtime cost estimation: Downtime Cost Calculator. Companies who understand outage cost estimations can better plan their investments.

IoT BOTNET

In 2016 a massive DDoS attack brought down large internet services, such as GitHub, Reddit, Twitter and Amazon for several hours. This was done by employing a massive botnet consisting of hundreds of thousands of IoT (Internet of Things) devices infected by Mirai malware and attacking the DNS provider Dyn. This affected many downstream clients. Instead of targeting individual online services it showed how effective it was to attack the DNS service. IoT devices used for the attack often have poor security and are easy to infect, for example, they often keep default passwords.

BENEFITS

Automation

Flowmon DDoS Defender detects an attack within seconds, extracts the characteristics and orchestrates the mitigation via A10 TPS/aGalaxy. No manual inputs are required.

Machine learning

Advanced machine learning techniques create baselines and adaptive thresholds. The joint solution takes advantage of open API when configuring A10 for mitigation.

Volumetric attacks

These attacks are aimed to flood and saturate a victim's Internet connection, thus rendering services unavailable. Volumetric attacks make up roughly 99% of the overall attack traffic. It is far more trivial for the attacker to launch a volumetric attack, because it does not require a lot of skill.

> “ ***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**

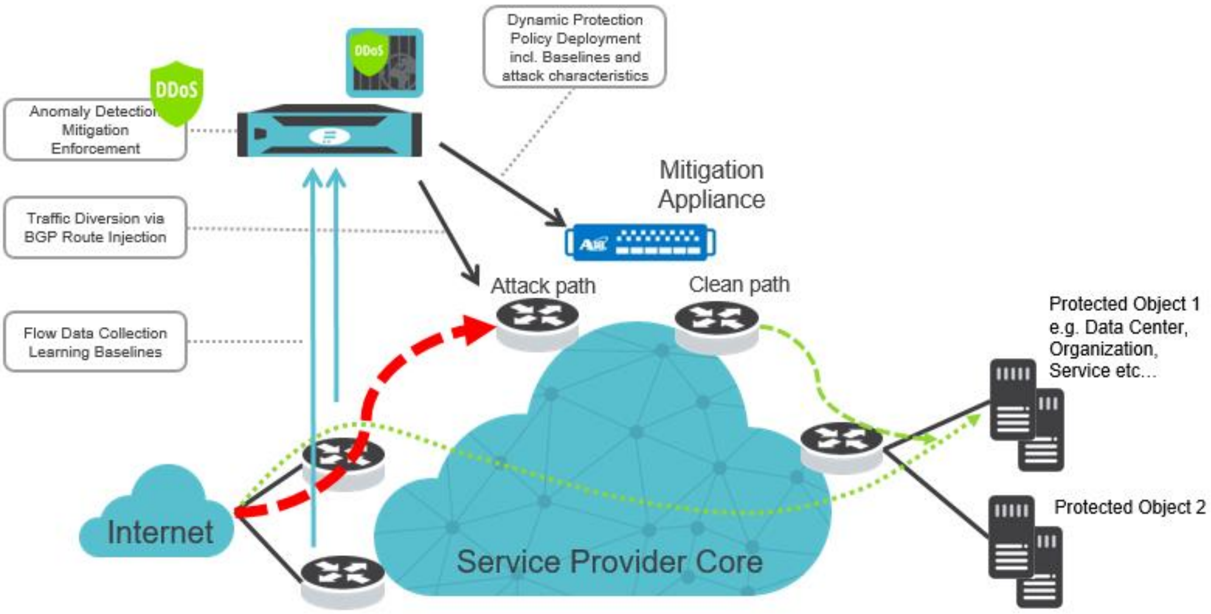
INTEGRATED SOLUTION

Flow-based DDoS attack detection combined with multi-layer out-of-path or cloud mitigation is a cost-effective alternative to traditional DDoS protection. The partnership between Flowmon and A10 Networks brings easy integration of detection and mitigation capabilities.

In a nutshell, Flowmon offers fast DDoS attack detection and provides dynamic attacks characteristics for mitigation. A10 carries out traffic redirection and mitigates the attack using advanced techniques.

Out-of-path DDoS detection and mitigation offers a cost effective way to deal with DDoS attacks. The out-of-path approach scales mitigation to a fraction of the ingress traffic, bringing significant savings. Flowmon permanently collects flow data and provides additional benefits such as enhanced network visibility, visualization, easier and faster network troubleshooting, reporting and alerting. Functionality, the solution can be further extended by Flowmon modules for anomaly detection, application performance monitoring and traffic recording.

When Flowmon detects a DDoS attack, it configures a zone in the A10 Threat Detection System (TPS) or aGalaxy with an API call. This includes dynamic attack signature and traffic baselines. Based on the detection, traffic is redirected via BGP route injection into the A10 appliance which mitigates the attack through different levels of escalations. Cleaned traffic is sent to downstream routers. This enables legitimate traffic to continue unaffected. Once Flowmon detects that an attack has ended, it removes the zone configuration through an API call, and the traffic route is returned to normal.



FLOW DATA MONITORING

Enhanced network visibility is a prerequisite to comprehensive traffic analysis needed for fast and reliable attack detection. Flow data monitoring is employed to get a deep insight into network traffic. Flow-based monitoring provides detailed information on communication: IP addresses, ports, time characteristics, protocol, the number of packets and data volume.

These statistics enable real-time monitoring of network utilization and data transfers. Various industrial standards exist for flow data monitoring: NetFlow v5/v9, jFlow, sFlow, NetStream and IPFIX.

FLOWMON ARCHITECTURE

Flowmon provides the following components for advanced DDoS protection:

Flowmon Collector

Aggregation and storage of flow data in all major industrial formats from thousands of flow sources. The collector provides full-featured tools to analyze and report on network traffic including deep drill-down.

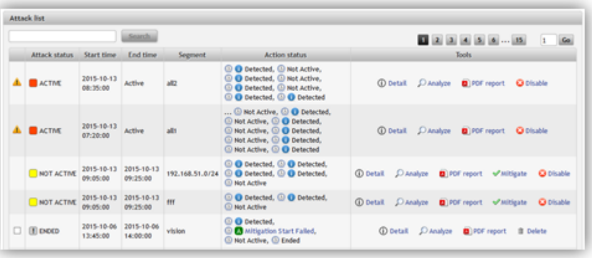
Flowmon DDoS Defender

Scalable multi-tenant DDoS detection module for Flowmon Collector using dynamic baselines and adaptive thresholds to detect various types of volumetric attacks and bandwidth consumption.

Flowmon Collector equipped with DDoS Defender module observes and profiles volumetric characteristics of network traffic to create and maintain dynamic baselines. DDoS Defender takes advantage of stream processing of flow data which enables to profile traffic with 30s granularity. It allows to manually or automatically initiate the mitigation process.

In case of an unexpected increase in network traffic it triggers configurable actions that include alerting (email, syslog, SNMP trap), traffic diversion (policy based routing, border gateway protocol, BGP Flowspec, remotely triggered black hole), execution of scripts or mitigation through a specific out-of-band DDoS mitigation system or to a Scrubbing Center. After the end of the attack, reports can be generated to give an overview and details of the DDoS attack.

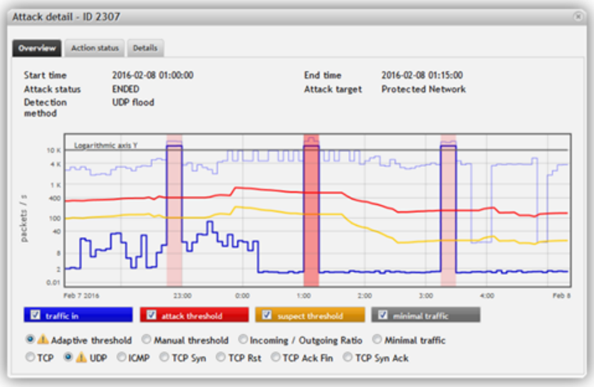
Flowmon DDoS Defender enables a way to define protected segments - corresponding to IP ranges, subnets or network services. For each segment, a set of baselines is learned from monitored traffic. Both adaptive and manual thresholds are supported. Adaptive thresholding is a fully automated approach eliminating the need to manually set baselines. In the event that a DDoS attack is detected, all the attack characteristics including attack type and status, top source 10 IP addresses, subnets, autonomy systems and countries, L4 protocols, TCP flags and interfaces are part of the attack details.



Attack list

Search 1 2 3 4 5 6 ... 15 1 Go

	Attack status	Start time	End time	Segment	Action status	Tools
⚠	🟥 ACTIVE	2015-10-13 08:35:00	Active	all2	Detected, Not Active, Detected, Not Active, Detected, Not Active, Detected, Detected	Detail Analyze PDF report Disable
⚠	🟥 ACTIVE	2015-10-13 07:20:00	Active	all1	... Not Active, Detected, Not Active, Detected, Not Active, Detected, Not Active, Detected, Not Active, Detected	Detail Analyze PDF report Disable
	🟨 NOT ACTIVE	2015-10-13 09:05:00	2015-10-13 09:25:00	192.168.51.0/24	Detected, Detected, Detected, Detected, Not Active	Detail Analyze PDF report ✓Mitigate Disable
	🟨 NOT ACTIVE	2015-10-13 09:05:00	2015-10-13 09:25:00	fff	Detected, Detected, Not Active	Detail Analyze PDF report ✓Mitigate Disable
□	ENDED	2015-10-06 13:45:00	2015-10-06 14:00:00	vision	Detected, Mitigation Start Failed, Not Active, Ended	Detail Analyze PDF report Delete



Attack detail - ID 2307

Overview | Action status | Details

Start time 2016-02-08 01:00:00
Attack status ENDED
Detection method UDP flood
End time 2016-02-08 01:15:00
Attack target Protected Network

● ⚠ Adaptive threshold ○ Manual threshold ○ Incoming / Outgoing Ratio ○ Minimal traffic
○ TCP ● ⚠ UDP ○ ICMP ○ TCP Syn ○ TCP Rst ○ TCP Ack Fin ○ TCP Syn Ack

MITIGATION WITH A10

The A10 Thunder Threat Protection System (TPS) product line provides high-performance (up to 300 Gbps in a single appliance), network-wide protection against DDoS attacks, and it ensures service availability against a variety of volumetric, protocol, resource and other sophisticated attacks (including application and IoT-based assaults). Automatic mitigation policies escalate suspect traffic through progressively tougher countermeasures to minimize legitimate traffic drops.

Complex application attacks (e.g., HTTP, DNS, etc.) are mitigated with advanced parallel processing across a large number of CPU cores to distinguish legitimate users from attacking botnets. The solution takes advantage of hardware acceleration for highly scalable flow distribution and hardware DDoS protection capabilities.

Thunder TPS offers a variety of authentication techniques, amplification and flood attack mitigation. It can also filter spoofed traffic and can apply a highly granular, multi-protocol rate limiting to prevent sudden surges of illegitimate traffic that can overwhelm a network and server resources. It is possible to apply limits per connection, defined by bandwidth or packet rate.

Protocol attacks, such as SYN floods, ping of death, and IP anomalies, are aimed at exhausting a victim’s protocol stack so it cannot respond to legitimate traffic. Thunder TPS protects the largest, most-demanding network environments. Thunder TPS offloads common attack vectors to specialized hardware. FPGA detects and mitigates more than 60 common attack vectors in hardware without impacting the performance of the data CPUs used for processing more complex application-layer attacks. For example, SYN requests can be validated.

Application attacks such as Slowloris, HTTP GET flood or SSL-based attacks specifically exploiting a weakness in an application’s function or try to make it unavailable. Embedded SSL security processors offload CPU intensive tasks and mitigate SSL/TLS-based attacks to maintain high-performance system scaling, even for multi-vector attacks. Lastly, Thunder TPS is extremely efficient. It delivers high performance in a small form factor to reduce OPEX with significantly lower power usage, rack space and cooling requirements.

DDoS Protection Cloud protects your organization when volumetric attacks grow past your internet bandwidth capacity. It works in concert with Thunder TPS and is delivered as a service orchestrated by A10’s DDoS Security Incident Response Team (DSIRT).

In addition to TPS, the aGalaxy platform is supported for the mitigation.

A10 NETWORKS

A10 Networks enables intelligent automation with machine learning to ensure business critical applications are protected, reliable and always available. A10 Networks is based in San Jose, California, and serves customers globally with offices in United States, UAE, Levant, Japan, China, Korea, Taiwan, Germany, France, The Netherlands and the United Kingdom. A10 currently has over 800 employees.

https://www.a10networks.com

FLOWMON NETWORKS

Flowmon Networks empowers businesses to manage and secure their computer networks confidently. Through our high performance network monitoring technology and lean-forward behavior analytics, IT pros worldwide benefit from absolute network traffic visibility to enhance network and application performance and deal with modern cyber threats. Driven by a passion for technology, we are leading the way of NetFlow/IPFIX network monitoring that is high performing, scalable and easy to use.

https://www.flowmon.com