Flowmon 8.01 and Flowmon DDoS Defender 3.0 News

Flowmon 8.01 builds on the new architecture of flow data storage introduced with Flowmon 8.0 release. Thanks to the architecture evolution, Flowmon 8.01 significantly improves granularity of flow collection to 30 seconds. In addition, several GUI improvements and other useful features are introduced. Concurrently to Flowmon 8.01 was released Flowmon DDoS Defender 3.0. It benefits from improved data granularity and brings mitigation using BGP Flowspec.

---

At-a-glance insight

- 30s profile granularity
- Pipelined processing of flows
- Floating menu
- TACACS+ authentication

DDoS Defender 3.0

- Near real-time attack detection
- BGP Flowspec Support
- Automatic detection of attacked IPs/subnets
- Preferred subnets for mitigation

New customer stories

Check out our new Success Stories of customers relying on Flowmon.

---

30s profiles granularity and stream processing of flow data

Flowmon 8.01 is coming with stream processing of flow data which enables to profile flow data with 30s granularity. New type of profile enables to show traffic statistics per 30s slices in traffic chart and run analysis on top of that. Flowmon 8.01 brings significant increase of profile's granularity. In addition to well-known 5 min profiles, user can create 30s profiles as well.

Decrease of granularity takes effect in use-cases beyond network traffic monitoring. Especially use-cases where reduction of reaction time is desired:

- Network behavior analysis and anomaly detection
- DDoS detection
- Alerting of operational and security issues

Note that all previous profiles stay without change, which means 5 min.
Floating Menu
New fresh floating collapsible left menu is available. User has all items by hand even if the menu is collapsed.

In addition, Profiles drop down menu can be used for filtering menu content:
Other news and features

Flowmon Monitoring Center

- Reports can be sent to multiple e-mail addresses
- Traffic chapter in Reports can be newly configured to display selected charts only
- Flow source availability can be monitored by SNMP

Flowmon Configuration Center

- Support for TACACS+ directory service for user login
- Alert icon - error can be reported by syslog or SNMP trap if configured
- Aggregation function (AVG, MAX) can be selected for graph in Profiles and Analysis
- Query parameters can be displayed for advanced analysis result
- Form for change of displayed channels in Analysis was improved

Flowmon Networks © 2016 www.flowmon.com
Flowmon DDoS Defender 3.0

Reduction of detection time
DDoS Defender 3.0 takes advantage from 30s profiles described in Flowmon 8.01 and detects DDoS attacks in sub 60s timeframe which is on the edge of flow-based detection.

BGP Flowspec Support
In addition to reduction of detection time, DDoS Defender 3.0 supports BGP Flowspec. This technology enables to mitigate volumetric attacks without the use of scrubbing center in place. DDoS Defender provides dynamic signature of the attack for the routers with BGP Flowspec capabilities and routers mitigate the attack.

Picture shows an example of DDoS mitigation using Flowmon DDoS Defender and BGP Flowspec. Flowmon DDoS Defender permanently collects flow data from border routers and evaluates the traffic patterns. When a DDoS attack occurs, DDoS Defender sends specific route advertisement via BGP Flowspec. It includes dynamic signature of the attack and the action which should be performed by the router for specified traffic. In this case, there was a command to drop the traffic corresponding to the characteristics of the attack.

BGP Flowspec enables to use various types of flow specification used for dynamic signature of the attack. For detailed information, see [RFC 5575](http://example.com/rfc5575) document. Flowmon DDoS Defender 3.0 uses following attributes and their combination to create dynamic signature of the attack:

- Destination Prefix
- Source Prefix
- IP Protocol
- Destination port
- ICMP type
- ICMP code
In case of an attack detection a user is alerted and provided with an attack details. User can trigger a mitigation by providing a Flowspec rule to a router or mitigation can be triggered automatically when attack is detected. The Flowspec rules (attack’s signature) for injection are based on attack statistics from the first 30s of attack. The rules can be created for destination network, source network, destination port, source port and L4 protocol. For specified segments, various types of action can be taken:

Selected Flowspec action can provide mitigation or other actions in accordance with router configuration.

**Other news**

- Automatic detection of attacked IPs/subnets for more precise mitigation
- Preferred subnets for mitigation can be set up to precision 1.2.3.4/32
- Ability to reset baseline for given segment
- Besides the automatic maximal bandwidth configuration there is a new option to manual setting of maximal bandwidth for given segment
- Attack can be marked/unmarked as a false positive to include false alarm traffic to baselines
- A user comment can be added to each attack to store related details