Flowmon solution for ISP

Flowmon is comprehensive solution for monitoring of network infrastructure, based on an observation of IP data flow (NetFlow/IPFIX). The technology provides overall view of network traffic within fixed, mobile or cloud infrastructure, details of every single communication as well as details about who, where, for how long, how often, using which protocol and which service, or amounts of data transferred during the communication. Flowmon is the only European solution using Network Behavioral Analysis (NBA) as identified by Gartner.

The solution consists of powerful dedicated probes, collectors and NBA based module Flowmon ADS (Anomaly Detection System), which detects both known and unknown security threats (attacks on network services, infected hosts, network traffic anomalies etc.). Flowmon solution may be extended by additional modules such as Data Retention module to fulfill governmental law requirements, Flowmon DDoS Defender for volumetric DDoS attack detection and mitigation and Flowmon Traffic Recorder module, which can be used for full packet capture of user defined network traffic flows.

Flow Monitoring – next generation network monitoring (NetFlow/IPFIX)

Network Behavior Analysis – next generation network security (NBA, NBAD)

DDoS protection – volumetric DDoS attack detection and mitigation

IP Data Retention – governmental law fulfillment

Flowmon Traffic Recorder – full packet capture (L2-L7)

As of today, internet service providers require next generation solutions, which provide faster and more comprehensive overview of network traffic and security of both their and their customer networks. Bandwidths are rapidly increasing – from 10Gbps, 40Gbps, 80Gbps up to 100Gbps and the only solution delivering overall network monitoring is IP flow monitoring.

Flowmon Networks, a.s., Brno, Czech Republic
+ 420 511 205 250 | info@flowmon.com

Benefits of Flowmon for ISP

- Real-time network traffic monitoring, improvement of security and detection of external and internal threats, long-term statistical analysis including computer/device details, applications and conversations, detailed monitoring of users and services, effective bandwidth capacity management.
- Long-term storage of network traffic statistics for law fulfillment.
- Quick, efficient and accurate network operational troubleshooting, identification of any kind of anomalies using automated alerting.
- Clear statements about network traffic, QoS monitoring, easier planning of infrastructure upgrades, peering control and supervision over the quality of service (SLA) are available thanks to qualified reporting.
- Monitoring and detection of anomalies within VoIP traffic (SIP).
- Detection of specific application usage based on NBAR2 standard.
- Clear visibility of peering process and optimization of peering policies which helps to control the network and achieve significant costs savings.
- Monitoring of IP flows between Autonomic Systems (AS).
- Monitoring of all inbound and outbound network traffic for the ISP.
- Verification whether load balancers are performing according to the proposed rules.
- Long-term statistics enable the status/performance ratio of the network to be compared before and after the upgrade of network elements.
- Flowmon provides information about the transmitted data or bandwidth enabling customer specific charging for services.

Security-as-a-Service Using Flowmon

Security-as-a-Service (SECaaS) is frequently demanded service by customers as well as DDoS protection, which ensures availability of datacenters´ services. Deploying tools for network visibility, traffic monitoring and analysis helps to provide such services and build added value requested by their customers. Extending Flowmon solution with Flowmon ADS and Flowmon DDoS Defender allows ISPs to offer services with added value to their customers.

Flowmon ADS utilizes sophisticated Network Behavior Analysis, an advanced artificial intelligence based on machine learning, it permanently observes and analyses data communication seeking anomalies and revealing suspicious behavior. Flowmon ADS detects events like network attack, network traffic anomalies, anomaly behavior of IP addresses, malware, outgoing spam and more.

Flowmon ADS allows customers to keep track of security incidents on their internet connectivity. The customer's Internet traffic is monitored with routers or Flowmon Probes, and the collected data is evaluated by sophisticated behavior analysis using Flowmon Threat Intelligence and methods detecting security risks. Service provider gives the customer regularly reports of the security risks in their network (detected attacks against computers in the customer network, scanning computers, spam generation, etc.), enabling them to react promptly and minimize their impact on users.

Flowmon ADS detects following events:

- Infected nodes in the network, communication with botnet command and control centers.
- Increased use of network services, suspicious communication in DNS traffic.
- Dictionary attacks to guess a username/password.
- Sending or attempting to send SPAM.
- Devices in the network attacking to the internet.

Flowmon Networks, a.s., Brno, Czech Republic
+ 420 511 205 250 | info@flowmon.com

Flowmon DDoS Defender is a scalable anti-DDoS solution leveraging statistics from routers or dedicated network probes for real-time detection of volumetric attacks led against customer's infrastructure. It provides the state of the art detection of DDoS, deep understanding of attack characteristics and a full-range of methods for successful attack mitigation. Network and security engineers can utilize a set of scripts, collaborate with a Scrubbing centre or with specialized out-of-band solutions to eliminate an attack.

Flowmon DDoS Defender allows to detect DDoS attack led against customer's network and successfully mitigate the attack and clean the customer's network traffic. Flowmon Collector equipped with DDoS Defender module continuously observes and profiles volumetric characteristics of network traffic to create and maintain dynamic baselines. In case of an unexpected increase of network traffic it triggers pre-configured actions including alerting (e-mail, syslog, SNMP trap), traffic diversion (policy based routing, border gateway protocol, remotely triggered black hole), execution of script or mitigation through specific out-of-band DDoS mitigation system. Flowmon DDoS Defender enables to define individual detection profiles that correspond with different IP ranges, subnets or network services.

Sample Use-Cases

Billing	Casablanca	Casablanca INT is leading provider of internet, data and voice services in Czech Republic as well as one of the largest data center in the country. Casablanca INT uses Flowmon solution for billing based on the traffic consumption by individual customers.
Data Retention	master data in motion	Master Internet is leading internet services and datacenter provider with their own cloud platform and provides server hosting services. Master Internet uses Flowmon solution for long-term storage of collected IP traffic information to fulfill Data Retention requirements.
Security Reporting	ČD-Telematika	ČD-Telematika is one of the largest providers of telecommunication services and ICT solutions in the Czech Republic. ČD-Telematika built based on Flowmon solution own reporting service called ČDT-Monitor. This service is offered for ČD-Telematika customers to automatically report on unusual network traffic patterns, network attacks or malware.
DDoS protection	ČD-Telematika	Great experiences with Flowmon products motivated ČD-Telematika to extend their solution with Flowmon DDoS Defender. ČDT-ANTIDDOS is service offered to ČD-Telematika customers for automatic DDoS attack protection based on Flowmon DDoS Defender module.
Managed Security Solution	Slovak Telekom	Slovak Telekom is a member of Deutsche Telekom Group and it is the largest multimedia and Internet operator in Slovakia. Slovak Telecom uses Flowmon solution to offer own service called Analyze NET to its customers. This service is implemented on Slovak Telecom datacenters and provides flow monitoring and network behavior analysis (NBA).

For more information contact Flowmon or Flowmon Partner.

Flowmon Networks, a.s., Brno, Czech Republic
+ 420 511 205 250 | info@flowmon.com