Sampling and its impact on Flowmon

Flowmon is flow-based (NetFlow/IPFIX/sFlow) solution for network visibility, traffic monitoring, reporting, analysis and anomaly detection. It is composed of optional Probes to accurate generate flow-based statistics even in high performance networks, Collector to store, visualize and report on traffic characteristics using flow data and software modules for additional features like Flowmon ADS (network behavior analysis, automatic detection of security and operational issues as well as network anomalies), Flowmon APM (application performance monitoring to provide agent-less user and transaction aware visibility and reporting on application performance) and Flowmon Traffic Recorder to provide on-demand packet capture and full packet traces.

In ISP or datacenter environment is common to leverage flow capabilities of routers to provide statistics on network traffic. Usually sampling on packet level when flows are being generated is utilized. This sampling is referred to as a sampling o packet level and it changes the original characteristics to of network traffic itself. On the other hand sampling on flow level means that the traffic is measured 1:1 and only limited number of flows is exported/processed.

Flowmon Collector works with both sampling methods on any sampling levels without limitations. Sampling is not an issue for common Collector use-cases like reporting on traffic volume or traffic structure or alert on increase of traffic volumes. Flowmon ADS feature is limited when sampling on packet level is in place due to changes of original traffic characteristics. On the other hand, sampling on flow level does not limit any features as the original character of network traffic is preserved and anomalies or attacks in terms of important issues for Telcos, ISPs or operators of backbone networks are massive and still visible.

Limitations of Flowmon ADS with packet level sampling

Flowmon ADS is based on various detection methods focused on different network anomalies and issues. Sampling on packet level has impact on the accuracy of these detection methods. There are detection methods resistant to sampling on packet level where sampling does not mean any limitation or inaccuracy. On the other hand there are methods which are sensitive in term of sampling on packet level. Sensitivity to sampling does not mean that these methods will not work at all but they are affected by packet sampling in terms of false positives or false negatives.

Methods resistant to packet sampling:

ANOMALY – this method predicts network behavior in various parameters (amount of data, number of active hosts, etc.) based on the current and historical network behavior. This method works also when packet sampling is in place as the method is based on statistic algorithms.

SCANS – method is focused on various types of port scans based on TCP flags. Packet sampling does not affect the method as scans on the backbone level are massive and method sensitivity can be adjusted based on the packet sampling levels.

BLACKLIST – this method leverages the knowledge of worldwide known botnet command and control centers, attackers and other malicious IP addresses to identify infected devices or suspicious communication. It is possible to provide own blacklist to customize the detection. Sampling is not an issue and the results of this method are reliable.

TELNET – this method is focused on finding to many telnet (tcp/23) connections and sampling on packet level is no issue as it is possible to adjust the sensitivity of this method.

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

OUTSPAM – method is focused on detection of unexpected mail traffic usually related to SPAM. Dynamic baseline is in place and deviations from that baseline are reported.

L3ANOMALY, HONEYPOT – method detects communication of IP addresses that should not appear in the monitored network or communication towards IPs that are not in use, e.g. IPs where no DNS records point to. Packet sampling is not an issue for results of this method.

HIGHTRNSF, MULTICAST – detection of high volumes of transferred data or connections towards multicast IP addresses. Sampling on packet level is no issue as it is possible to adjust the sensitivity of this method.

Methods with limited usability when packet sampling is in place:

SSHDICT, RDPDICT, HTTPDICT – these methods are focus on attacks against authentication on websites or SSH and RDP service. Both methods are based on decision trees that inspect each and every single flow and expect accurate data.

SIP – methods focused on SIP (*SIPSCAN, SIPFLOOD, SIPROXY*) can be used only with data generated by Flowmon Probes as VoIP-related information is missing in traditional flow statistics.

DOS, REFLECTDOS – both methods focus on specific DDoS attacks that are usually undetectable by traditional volumetric approach. For detection of volumetric attacks please use the alerting feature in Flowmon Monitoring Center where absolute or relative thresholds can be used.

DNSANOM, DNSQUERY, ICMPANOM – methods are focused on various anomalies in DNS and ICMP traffic, packet sampling usually means inaccuracy.

SRVNA – method is focused on detection of unavailable network services. This method needs to see both directions of the network traffic so the results when packet sampling is in place are usually inaccurate.

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