Flowmon Packet Investigator Models Specification

valid from 1.12.2020

Flowmon Packet Investigator	Lite FP-FPI-L	Standard FP-FPI-S	Business FP-FPI-B	Corporate FP-FPI-C	Enterprise FP-FPI-E
LICENSED PROBES	1	2	4	8	8
MONITORING PORTS	1/10GbE	1/10GbE	1/10GbE	1/10GbE	1/10/40/100GbE
HW REQUIREMENTS*	1 CPU and 4GB RAM per running PCAP analysis				

* The hardware requirements are based on the number of analyses executed in parallel for all users. A single analysis runs on a single CPU core. Memory utilization is up to 4GB of RAM for a single running analysis of a PCAP of reasonable size and structure. The reference PCAP file has the following characteristcs: a mixture of supported protocols, 100MB file size, 150k packets, 10k flows.

The FPI is designed to perform root-cause analysis on packet traces captured selectively when specific troubleshooting, such as client-server compatibility, protocol mismatch, or network failure, is required. For a smooth analysis and clear results, it is recommended to limit the scope of the capture to a minimal set of full-packet data required to diagnose the issue. It is not recommended to run analysis on PCAP files larger than 100MB. The memory consumption and processing time depends on the PCAP's characteristics and procotol mixture, e.g. a PCAP composed of 1 million DNS packets of a total size of 200MB will take around 20 minutes to process while consuming up to 8GB of RAM.

The memory requirement refers to the memory consumed by the Packet Investigator only. The total memory required for the Flowmon appliance depends on the appliance type, and other software modules installed with respect to corresponding appliance or module specification.

Key features:

- **Full packet capture in PCAP format**
- **Rolling capture buffer**
- **PCAP analysis & diagnostics**
- **Triggered capture via Flowmon ADS (Anomaly Detection System)**
- **REST API controlled traffic recording and access to PCAP files**

Full packet capture provides the ability to record network traffic on the fly on all the Flowmon Probes deployed over the infrastructure. Packet recording can be scheduled for a specific time and result in a set of PCAP files for subsequent analysis. Flowmon Packet Investigator provides various traffic filtering criteria such as IP address, CIDR, MAC address, protocol, port, VLAN tag, MPLS label, and their combinations. Maximum data volume, which can be recorded from the traffic and stored on disk, is 500Mbps.

Rolling buffer stores the first N packets for each flow for a defined period in the memory buffer, which allows it to capture communications that have already started. Packets stored in the rolling buffer are included in the recording triggered either by Flowmon Packet Investigator or an event detected by Flowmon ADS module.

PCAP analysis diagnoses and interprets full packet data recorded by Flowmon Packet Investigator or uploaded by the user. The module automatically performs an expert decision-tree analysis, looking for deviations from the RFC specifications of the respective protocols and their combinations, and records any error codes or other failures. The results of the analysis are provided in the form of events with a detailed description of detected issues. Moreover, the module also contains in-built expertise with interpretations of error codes and suggestions for remedial actions. PCAP analysis supports the most commonly used enterprise network protocols for network configuration, network storage, e-mail, and other protocols. List of currently supported protocols is the following: DNS, DHCP, FTP, IMAP, IMF, POP, SIP, SLAAC, SMB, SMTP, IP, TCP, SSL, and HTTP. PCAP files can be recorded in the network or uploaded from existing data.

The number of licensed probes can be increased by purchasing a license for an additional Probe. For more information, see Flowmon Price List for end users.

Flowmon Networks a.s.
info@flowmon.com