Flowmon Packet Investigator Models Specification

valid from 1.4.2020

Flowmon Packet Investigator	Lite FP-FPI-L	Standard FP-FPI-S	Business FP-FPI-B	Corporate FP-FPI-C	Enterprise FP-FPI-E
POČET LICENCOVANÝCH SOND	1	2	4	8	8
MONITOROVACÍ ROZHRANÍ	1/10GbE	1/10GbE	1/10GbE	1/10GbE	1/10/40/100GbE

Klíčové vlastnosti:

- **Záchyt paketů v plném rozsahu (PCAP)**
- **Adaptivní buffer pro ukládání paketů ke každému toku**
- **Analýza a diagnostika PCAP souborů**
- **Spuštění záchytu provozu pomocí Flowmon ADS (Anomaly Detection System)**
- **REST API pro nastavování záchytů provozu a přístup k PCAP souborům**

Záchyt paketů v plném rozsahu umožňuje nahrávání síťového provozu na všech Flowmon sondách nasazených v infrastruktuře. Záchyt paketů lze naplánovat na specifický čas a výsledkem je PCAP soubor, který je dostupný pro následnou analýzu. Flowmon Packet Investigator umožňuje zachytávat provoz na základě řady kritérií jako je IP adresa, CIDR, MAC adresa, protocol, port, VLAN tag, MPLS label nebo využitím jejich kombinací. Maximální objem dat, který je možný zachytit sondou a uložit na disk je 500Mb/s.

Adaptivní buffer pro ukládání paketů ukládá prvních N paketů na definovanou dobu ke každému toku do paměti, čímž umožňuje záchyt už probíhajících komunikací. Pakety uložené v paměti buffer jsou přidány k záchytům spuštěným požadavkem v modulu Flowmon Packet Investigator nebo na základě detekce události v modulu Flowmon ADS.

Analýza PCAP souborů umožňuje diagnostikovat a interpretovat informace z paketů zachycených modulem Flowmon Packet Investigator nebo nahraných do modulu uživatelem. Modul automaticky provádí expertní analýzu založenou na rozhodovacích stromech, sleduje odchylky od RFC specifikací pro podporované protokoly a jejich kombinace a jakékoliv odchylky či chybové kódy zaznamená. Výsledky analýzy jsou uživateli poskytnuty ve formě událostí s detailním popisem detekovaného problému. Modul navíc obsahuje vestavěnou expertntí znalost, díky které interpretuje zjištěné chyby a poskytuje návrh nápravných opatření. Analýza podporuje nejčastěji používané protokoly v podnikových sítích zahrnující protokoly pro síťovou konfiguraci, e-mailovou komunikaci, síťové úložiště a další protokoly. Seznam podporovaných protokolů je následující: DNS, DHCP, FTP, IMAP, IMF, POP, SIP, SLAAC, SMB, SMTP, IP, TCP, SLL, and HTTP. PCAP soubory je možné pořídit záznamem paketů na síti nebo nahráním existujících souborů do modulu.

Počet licencovaných sond lze zvýšit dokoupením licence pro další sondu. Pro více informací viz Flowmon ceník pro koncové uživatele.

Flowmon Networks a.s.
info@flowmon.com