

## FLOWMON

# Nový přístup k monitorování a bezpečnosti počítačových sítí

JIŘÍ TOBOLA, PAVEL ČELEDA

Již krátkodobý výpadek sítě znamená narušení infrastruktury společnosti a může způsobit škody v řádech milionů korun, poškození dobrého jména společnosti a nespokojenost nebo dokonce ztrátu zákazníků. Podobné problémy přináší i „pouhé“ ne zcela správné fungování počítačové sítě projevující se například sníženou dostupností a pomalou odezvou kritických aplikací (podnikové systémy, VoIP).

Dlouhá léta byl synonymem pro monitorování a dohled nad počítačovou sítí protokol SNMP. Současná doba, kdy na dostupnosti a správné funkcionalitě počítačové sítě závisí fungování většiny organizací, si však žádá modernější a efektivnější prostředky. Ty musejí v reálném čase poskytovat detailní statistiky o síťovém provozu, které jsou klíčové pro efektivní správu a účinné zabezpečení počítačových sítí. Právě takové statistiky nabízí technologie NetFlow.

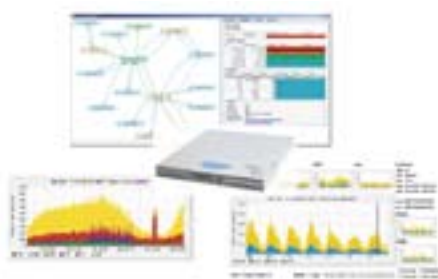
## Monitorování na bázi NetFlow

NetFlow je v současnosti nejrozšířenější průmyslový standard pro měření a monitorování počítačových sítí na základě IP toků. Tok je v terminologii NetFlow definován jako sekvence paketů se shodnou pěticí údajů: cílová/zdrojová IP adresa, cílový/zdrojový port a číslo protokolu. Pro každý tok je zaznamenávána doba jeho vzniku, délka jeho trvání, počet přenesených paketů a bajtů a další údaje. V tradiční NetFlow architektuře jsou statistiky vytvářeny pomocí směrovačů a odesílány na kolektory (datová úložiště) k dalšímu zpracování, vizualizaci a analýzám.

Zatímco SNMP statistiky poskytují jenom souhrnné informace o provozu a neumožňují vidět, co se v síti doopravdy děje (jaké je rozložení provozu, kdo síť nejvíce zatěžuje), NetFlow statisticky poskytují detailní informace o tom, kdo komunikoval s kým, kdy, jak dlouho, jak často, nad kterým protokolem a kolik bylo přeneseno dat. Tyto statistiky umožňují sledování vytížení sítě v reálném čase, monitorování aktivit uživatelů i služeb, optimalizaci síťové infrastruktury, sledování reálného využití internetu, dodržování vyhlášky o elektronické komunikaci, či odhalování a prokazování bezpečnostních incidentů. Tím šetří finance vynaložené na správu počítačových sítí, usnadňují práci síťových administrátorů a zvyšují spokojenost koncových uživatelů a zákazníků.

V minulosti bránila rozšíření monitorovacích systémů na bázi NetFlow jejich vysoká pořizovací cena a dostupnost pouze pro omezený počet směrovačů. Tyto nevýhody odstranila česká společnost

Invea-tech, která uvedla na trh kompletní, cenově dostupné řešení FlowMon pro monitorování sítí s využitím technologie NetFlow. Portfolio produktů FlowMon zahrnuje výkonné autonomní sondy pro všechny typy sítí až do rychlosti 10 Gb/s, kolektory pro uložení, zobrazení a analýzy síťových statistik a další rozšiřující moduly (detekce anomálií, dohled nad sítí, inteligentní reporting).



## Řešení FlowMon

Sondy FlowMon reprezentují výkonná monitorovací zařízení určená pro ethernetové sítě na rychlostech od 10 Mb/s do 10 Gb/s. Sondy sledují komunikaci na síti, vytvářejí statistiky plně kompatibilní s NetFlow standardem a odesílají je na vestavěný či externí kolektor. Sondy se typicky umísťují na vstupní a výstupní body sítě, kritická místa či linky s největšími přenosy dat. Připojení sond do sítě se realizuje pomocí mirror portu směrovače/přepínače, nebo přímým vložením do linky s využitím optického nebo metalického rozbočovače (TAPu). Řada produktů FlowMon zahrnuje standardní modely sond pro běžné sítě a hardwarově akcelerované modely pro kritické a vysoce vytížené linky. Výhodou proti konkurenčním produktům je garantované zpracování všech dat bez ztráty paketu.

NetFlow data generovaná sondou jsou zasílána na integrovaný, nebo na externí kolektor. Jako kolektor lze přitom využít libovolnou aplikaci třetí strany, nebo FlowMon monitorovací centrum, které tvoří součást kompletního FlowMon řešení. Vestavěná verze tohoto nástroje – integrovaná při-

mo na sondách – je určená pro rychlé seznámení s technologií NetFlow a nabízí kompletní řešení pro menší a střední sítě. Samostatná verze realizovaná na vyhrazeném serveru nabízí maximální výkon a nalezne využití jako profesionální řešení pro sběr dat z více sond ve větších sítích.

### Základní vlastnosti produktů FlowMon

- Výkonné NetFlow sondy a kolektory,
- zpracování dat v reálném čase bez ztráty paketů až pro 10 Gb/s Ethernet sítě,
- snadná instalace do stávající infrastruktury sítě,
- jednoduchá správa přes intuitivní webové rozhraní,
- monitorování provozu na síti v reálném čase,
- detailní sledování uživatelů, služeb a využití internetu,
- efektivní řešení problémů a plánování kapacity sítě,
- účtování a fakturace na základě přenesených dat,
- zvýšení bezpečnosti sítě a možnost odhalení vnějších i vnitřních útoků.

FlowMon monitorovací centrum je plně přístupné přes zabezpečené webové rozhraní. Ovládání je intuitivní a umožňuje zobrazovat síťové statistiky v podobě grafů a tabulek s různým časovým rozlišením, generovat top N statistiky, filtrovat data podle požadovaných kritérií, tvořit uživatelské profily, provádět bezpečnostní analýzy, nebo nastavovat generování automatických upozornění na požadované události, např. porušení bezpečnostní politiky. Pomocí rozšiřujících modulů je možné funkcionalitu dále rozšířit například o SNMP dohled nad sítí nebo automatickou detekci anomálií. FlowMon řešení nabízí vysokou flexibilitu a nezávislost na stávající síťové infrastruktuře. Výhodou je také integrace NetFlow kolektoru přímo na sondách.

### SHRNUTÍ

Řešení FlowMon je vhodným prostředkem pro trvalé monitorování firemní počítačové sítě. Nasazení tohoto pokročilého monitorovacího systému založeného na sledování toků umožňuje organizacím předcházet ztrátám v důsledku nedostupnosti sítě, snižovat náklady na provoz a zabezpečení sítě, zvýšit spolehlivost a dostupnost sítě a maximalizovat spokojenost jejich uživatelů a zákazníků.

**Ing. Pavel Čeleda, Ph.D.**, je vedoucím vývoje aplikací ve společnosti INVEA-TECH. Kontaktovat ho můžete na adrese [celeda@invea.cz](mailto:celeda@invea.cz). **Ing. Jiří Tobola** je obchodním ředitelem společnosti INVEA-TECH. Kontaktovat ho můžete na adrese [tobola@invea.cz](mailto:tobola@invea.cz)