

FlowMon – inovace v oblasti monitorování a bezpečnosti počítačových sítí

Úvod

Spolehlivá a dobře zabezpečená počítačová síť je klíčem pro úspěšné fungování každé organizace. 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). Následující článek popisuje, jak takovým situacím úspěšně předcházet a čelit za pomoci moderních monitorovacích technik na bázi NetFlow.

Dlouhá léta byl synonymem pro monitorování a dohled nad počítačovou sítí protokol SNMP. Současná doba, kdy na dostupnosti a správné funkci počítačové sítě závisí fungování většiny organizací, si však žádá modernější a efektivnější prostředky. Ty musí 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 pětici 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.

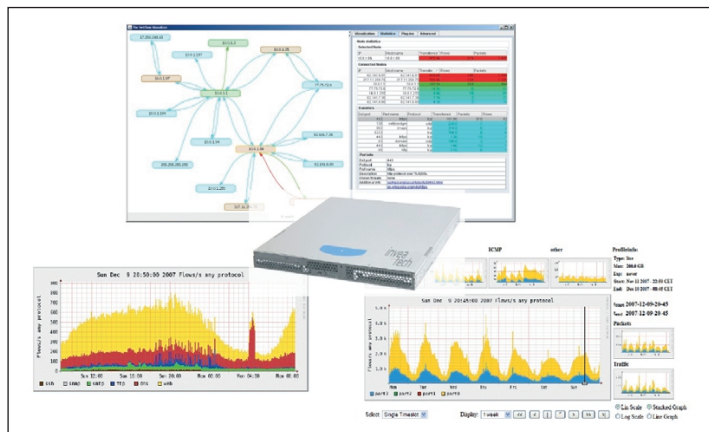
Zatímco SNMP statistiky poskytují jenom souhrnné informace o provozu a neumožňují vidět, co se v síti doopravdy děje (jaké je rozložení provozu, kdo síť nejvíce zatěžuje), NetFlow statistiky poskytují detailní informace o tom, kdo komunikoval s kým, kdy, jak dlouho, jak často, nad kterým protokolem a 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

a hardwarově akcelerované modely pro kritické a vysoce vytížené linky. Sondy jsou dostupné pro metalická i optická rozhraní a nabízejí až 4 monitorovací porty na zařízení. Výhodou proti konkurenčním produktům je garantované zpracování všech dat bez ztráty paketu a integrace NetFlow kolektoru přímo na sondách.

FlowMon monitorovací centrum

NetFlow data generovaná sondou jsou zaslána na integrovaný, nebo na externí kolektor. Jako kolektor lze využít libovolnou aplikaci třetích stran nebo předem konfigurovanou aplikaci – FlowMon monitorovací centrum. Vestavěná verze tohoto nástroje integrovaná přímo na sondě je určená pro rychlé seznámení



Obr. 1 FlowMon sonda a způsoby vizualizace síťového provozu

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 a. s. (www.invea.cz), 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 Gbit/s, kolektory pro uložení, zobrazení a analýzy síťových statistik a další rozšiřující moduly (detekce anomálií, dohled nad sítí, inteligentní hlášení).

Sondy FlowMon

Sondy FlowMon reprezentují výkonné monitorovací zařízení určená pro ethernetové sítě v rozsahu přenosových rychlostí od 10 Mbit/s do 10 Gbit/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. Vlastní připojení sondy do sítě se realizuje pomocí mirror portu směrovače či přepínače, nebo přímým vložením do linky s využitím optického nebo metalického rozbočovače.

Řada produktů FlowMon sond zahrnuje standardní modely pro běžné sítě

s technologií NetFlow a nabízí kompletní řešení pro menší a střední sítě. Samostatná verze realizovaná na vyhrazeném serveru naopak nabízí maximální výkon a profesionální řešení pro sběr dat z více sond ve větších sítích.

Přístup k uloženým NetFlow datům je realizován přes zabezpečené webové rozhraní. Intuitivní ovládání FlowMon monitorovacího centra umožňuje zobrazovat síťové statistiky v podobě grafů a tabulek s různým časovým rozlišením, generovat takzvané top N statistiky, filtrovat data dle 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 dostupné funkce dále rozšířit například o SNMP dohled nad sítí nebo automatickou detekci anomálií.

Závěr

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, ochránit investice do síťové infrastruktury, zvýšit spolehlivost a dostupnost sítě a maximalizovat spokojenost jejich uživatelů a zákazníků.

Ing. Jiří Tobola
Obchodní ředitel INVEA-TECH a. s.