

Případové studie

Nasazení řešení FlowMon přináší četné výhody a snížení finančních nákladů na správu sítě pro všechny – malé, střední a velké společnosti, vládní organizace, akademické organizace i poskytovatele internetu. Zatímco v menších sítích naleznou využití sondy s vestavěným kolektorem a dohledovými nástroji, ve větších sítích se uplatní škálovatelná architektura celého řešení založená na autonomních sondách a výkonných kolektorech. Níže jsou uvedeny některé z úspěšných případů nasazení řešení FlowMon v rámci různých organizací.

Zvýšení bezpečnosti sítě

Detailní pohled do síťového provozu poskytnutý řešením FlowMon umožňuje účinnou detekci anomálií v síťovém provozu, odhalení nesprávných konfigurací (např. omylem využívaný neaktualizovaný autentizační server) a detekci DOS/DDOS, SYN SCAN a jiných útoků. Odhalením těchto bezpečnostních problémů přispívá řešení FlowMon k nápravě těchto incidentů, bezproblémovému chodu a vyšší dostupnosti počítačové sítě.

Detekce vnějších i vnitřních útoků

Zatímco v minulosti znamenaly největší nebezpečí vnější útoky, v dnešní době přichází více než 50% útoků z vnitřní sítě. Nasazení řešení FlowMon umožňuje detekovat oba typy útoků a účinně se bránit proti takzvanému „vnitřnímu nepříteli“. Příkladem je okamžitá detekce problémového uživatele se zavírovaným notebookem, který po připojení k místní síti zahltl celou síť organizace a snížil dostupnost všech síťových služeb.

Rychlé a efektivní řešení problémů

Pohled do síťového provozu v reálném čase a s uložením dlouhodobé historie komunikací umožňuje rychle a efektivně řešit problémy typu zahlcení sítě či zvýšení dob odezvy síťových služeb. Klíčové je zejména okamžité dohledání problémového místa v síti a změření času odezvy serverů či služeb. Jedním z příkladů využití bylo vyřešení problémů se zahlcením sítě, kdy bylo odhaleno, že při zálohování se data omylem místo po zálohovacích linkách přenášela produkční sítí.

Dohled nad sítí a službami

Dohledový systém pro kontrolu dostupnosti serverů a služeb informuje administrátory o problémech dříve, než na ně upozorní uživatelé či zákazníci. Systém integrovaný na sondách či kolektorech umožňuje sledování vytiženosti aktivních prvků a serverů, kontrolu dostupnosti služeb (webové, emailové či jiné služby) a podporuje široké možnosti uživatelských upozornění. Předchází tak stížnostem, ulehčuje správu sítě a omezuje ztráty vzniklé nedostupností sítě a služeb.

Dohledání bezpečnostních incidentů

V dnešní době jsou častým problémem různé bezpečnostní incidenty jako stahování nelegálního obsahu, nezákonné sdílení dat či útoky ze zavírovaných nebo jinak napadených serverů.

Různé organizace zabývající se odhalováním těchto přestupků vyžadují dohledání a potrestání viníků. Řešení FlowMon dává správci možnost dohledat problémovou komunikaci či počítač a potvrdit nebo vyvrátit oprávněnost stížnosti. Dle výsledného zjištění pak může či nemusí následovat potrestání viníka.

Nedostatečný výkon směrovačů

Vysoce zatížené páteřní linky bývá často problém monitorovat z důvodu nedostatečného výkonu směrovačů pro výpočet síťových statistik (zejména při probíhajících útocích). Nasazením výkonných hardwarově akcelerovaných FlowMon sond je možné generovat statistiky za všech podmínek (DDOS útoky aj.) a zaručit zpracování každého paketu. Směrovačům je tímto způsobem snížena zátěž (až 40% směrovacího výkonu) a díky tomu je možné odložit upgrade stávající síťové infrastruktury.

Monitorování aktivit uživatelů a využití internetu

Různé výzkumné studie prokazují, že někteří zaměstnanci tráví více než polovinu pracovní doby na internetu, hrají online hry či sledují multimediální kanály. Přestože řešení FlowMon není primárně určeno pro sledování uživatelů, snadno jej lze využít k prokázání výše zmíněných aktivit. Při nasazení tohoto řešení se navíc ukazuje, že pouhým upozorněním zaměstnanců na systém, který je schopný odhalit veškerou jejich síťovou aktivitu, se sníží zneužití internetu a sítě obecně o více než 80%.

Dlouhodobé trendy a plánování kapacit

Detailní statistiky o síťovém provozu výrazně usnadňují plánování kapacit sítě a datových linek, ukazují dlouhodobé trendy, identifikují kritická místa v síti, znázorňují požadavky jednotlivých služeb na kapacitu sítě a pomáhají efektivně předcházet zahlcením a kolapsům. Přesná znalost složení síťového provozu dále umožňuje efektivně optimalizovat stávající infrastrukturu, předejit zbytečným nákladům za modernizaci a celkově tedy minimalizovat cenu síťových operací při maximalizaci výkonu, kapacity a dostupnosti sítě.

Účtování a fakturace

Znalost složení síťové komunikace umožňuje využít řešení FlowMon pro účtování a fakturaci za přenesená data mezi poskytovateli datových linek a internetového připojení nebo pro rozúčtování nákladů mezi pobočkami jedné organizace. Příkladem úspěšného nasazení je webový portál poskytovatele internetového připojení, který uživatelům zobrazuje aktuální FUP limity a statistiky využití linky.

Dodržování vyhlášky o elektronické komunikaci

Evropský zákon o sledování elektronické komunikace a česká vyhláška č. 485/2005 ukládají provozovatelům veřejných komunikačních sítí povinnost uchovávat údaje o elektronické komunikaci typu kdo komunikoval s kým, jak dlouho a kolik přenesl dat. Přesně tyto statistiky poskytuje řešení FlowMon a umožňuje tak operátorům splnění tohoto bodu zákona.