Kdy je správci sítě doopravdy horko?

ZDENĚK TLUSTÝ

Správci datové sítě se mají! Většinou je nic moc nerozhodí. Když správně funguje klimatizace v serverovně, tak je nevyvede z míry ani horké počasí. S poznámkou „jdu udělat pořádek v kabelech“ se odporoučí do příjemně vychlazeného místa. Sice si všichni myslíme, že největší úpravy infrastruktury se provádějí o letních prázdninách z důvodu okurkové sezony a hromadných dovolených, ale skutečná příčina může být jinde. Tolerujeme jim to, protože víme, že ve chvíli nouzové situace postaví celou síť na nohy. Snaží se co nejrychleji opět vše zprovoznit.

K odstranění závady ovšem musí nejdřív vědět, co ji způsobilo. S rostoucí složitostí sítí přestal na diagnostiku stačit jednoduchý nástroj typu ping, kterým se z jednoho uzlu kontrolovala dostupnost sousedního zařízení. Vznikla potřeba nasadit složitější řešení. Momentálně je na trhu obrovské množství různých monitorovacích nástrojů se širokým spektrem funkcionalit. Od základních, které pouze sledují síťovou dostupnost jednotlivých zařízení, přes sofistikované, které sbírají informace o událostech z různých prvků a navzájem je korelují, až po nástroje umožňující globální přehled i detailní zobrazení jednotlivých síťových komunikací.

Úplným minimem monitorovacích nástrojů je zobrazení síťové dostupnosti jednotlivých uzlů. Obvykle je vidět aktuální stav sítě a uchovávají se i historické údaje. Bohužel vám tyto nástroje neřeknou, že se někde blíží pohroma. Na druhou stranu jsou velmi snadno dostupné a nasazení je relativně jednoduché.

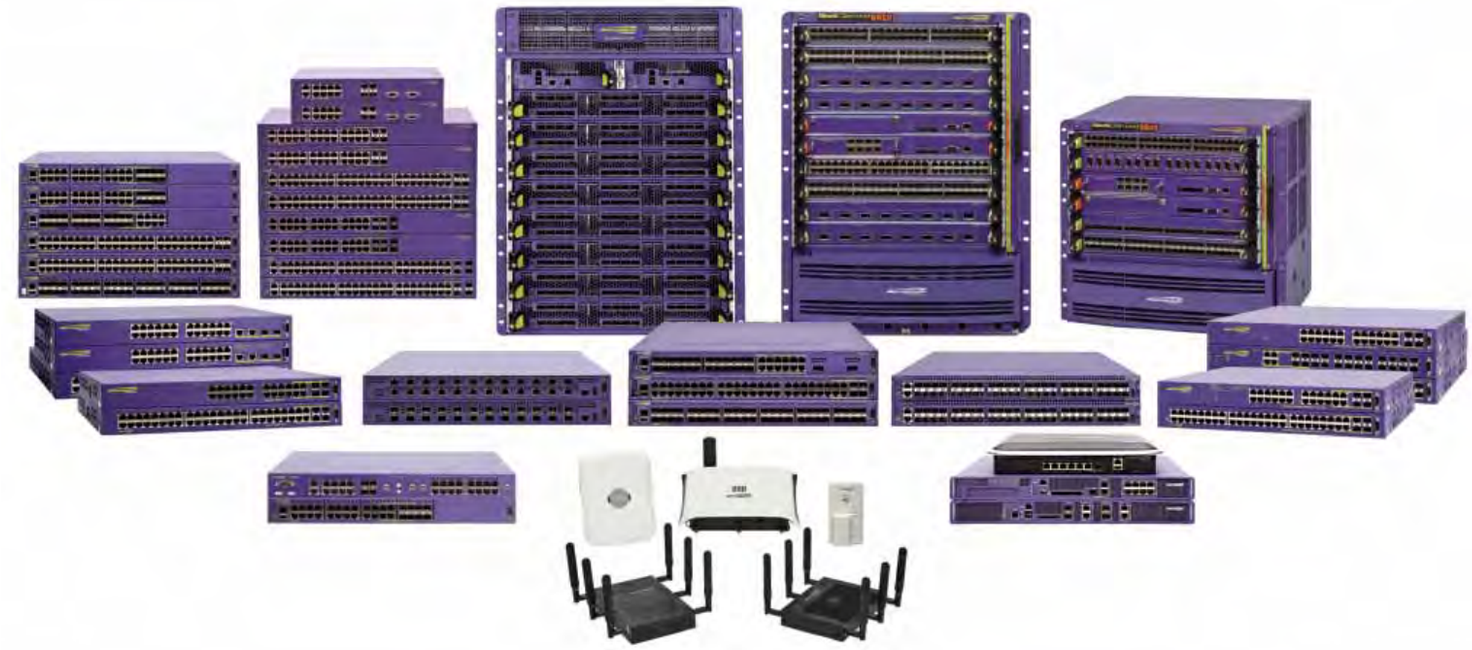
Sběr informací

Vedle základních nástrojů se staly velmi populárním pomocníkem produkty typu SIEM. Ty dokážou sbírat informace z mnoha zařízení v síti a navzájem mezi nimi provádět korelaci. Některé dokonce dokážou čerpat informace i ze speciálních sond, které analyzují přenášená data v síti a rozumí i konkrétním aplikacím. Díky velkému množství zdrojů má toto řešení dobrý přehled o celkovém zdraví sítě. Z jednotlivých zařízení může dostávat různé střípky, které v součtu mohou být vyhodnoceny jako potenciální hrozba pro celou infrastrukturu. Pak je možné podniknout opatření ještě před reálným dopadem na provoz. Řešení typu SIEM se primárně používají spíše pro zvýšení bezpečnosti než pro snížení rizik běžného provozu. Korelace se často neprovádí okamžitě, ale až s nějakým zpožděním. Rovněž cena je vyšší a nasazení vyžaduje daleko více práce. Ovšem odměnou je sofistikovaný nástroj na monitorování událostí. Každé ráno si tak může správce sítě prohlédnout zprávu, co nebezpečného se minulý den v síti odehrálo, a podle toho učinit příslušné kroky.

Před nedávnem se objevil další nástroj pro monitorování sítě, který si rychle získává popularitu. Jde o behaviorální analýzu. Myšlenka je elegantní: „budeme sledovat, co se v síti děje, a když se objeví něco neobvyklého, tak to ohlásíme“. Jako sondy sledující provoz mohou sloužit i běžná síťová zařízení v infrastruktuře, jako je přepínač nebo směrovač. Případně lze použít i speciální zařízení pro sledování provozu. Druhý způsob je obvykle zvolen u instalací, kde přepínače nejsou schopny trvale sledovat všechny komunikace a provádí určité statistické vzorkování (jako je tomu například u standardu sFlow). Nikdo nechce, aby mu kvůli statistickému výběru utekla právě ta jedna jediná důležitá informace, která ho může upozornit na hrozící riziko. Proto se nejčastěji používají standardy NetFlow nebo IPFIX. Ty posílají informace o každém spojení. Analyzátor těchto dat pak všechno zpracuje a porovná s historií. Pokud najde něco, co neodpovídá typickému vzorci chování, tak na to správce upozorní. Podobně jako u SIEM se tento nástroj spíše používá pro odhalení bezpečnostních hrozeb než jako pomocník v zajištění hladkosti provozu. Díky zpětné analýze dat se opět nedíváme na online informace. Cena velmi záleží na způsobu nasazení a počtu sond. Zpravidla je ale nižší než u SIEM a nasazení rovněž bývá jednodušší.

Analýza síťového provozu

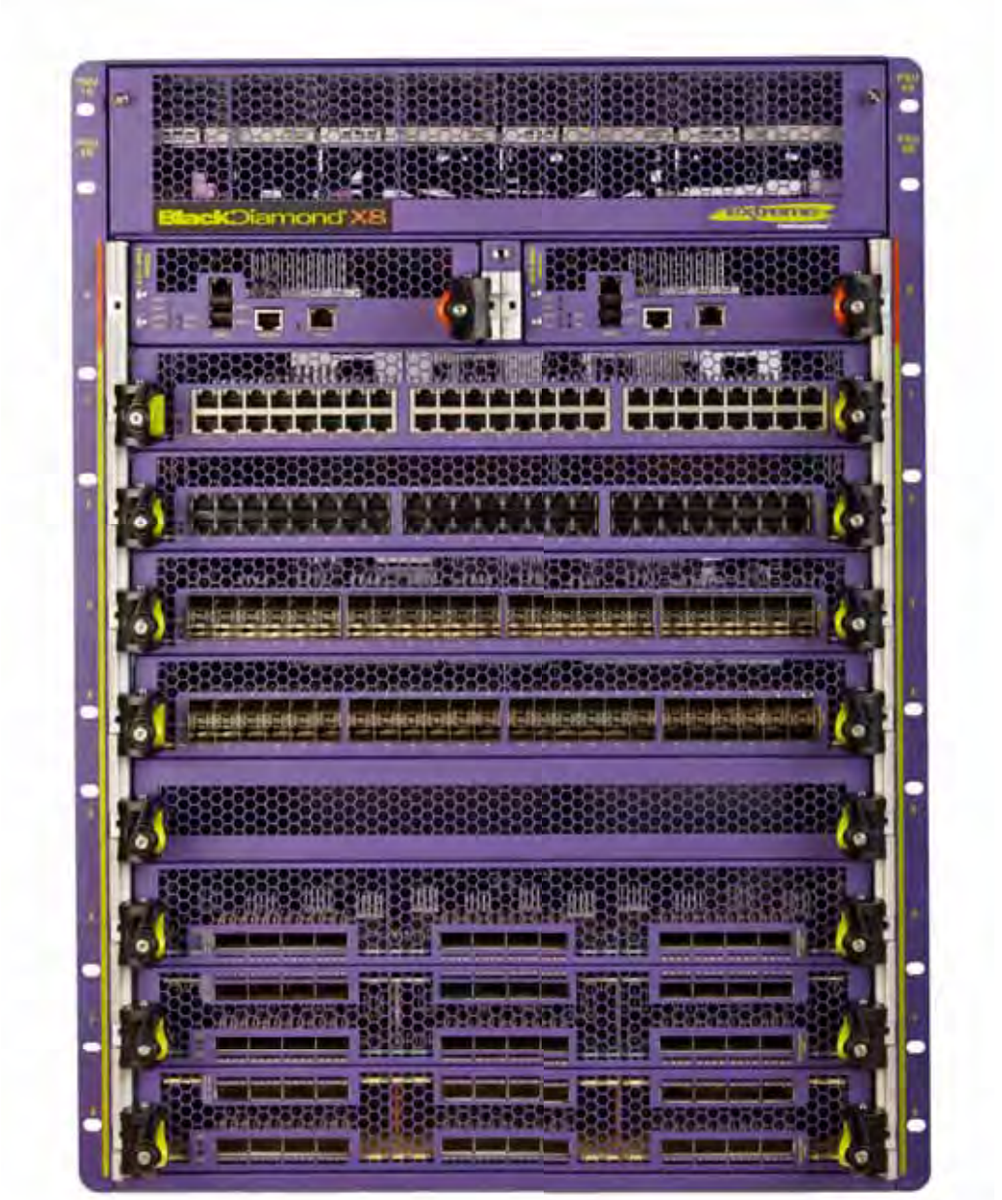
Nejnovějším výkřikem ve sledování sítí je monitorování provozu včetně analýzy přenášených aplikací a dalších doplňkových informací. Tato metoda rovněž využívá síťových přepínačů jako sond, které zasílají



informace pro analýzu, ale je navíc rozšířená o další důležité podrobnosti. Jednou z nich je informace o konkrétní aplikaci, která je přenášena, dalším velmi důležitým detailem je informace o uživateli. Představte si tedy, že dostanete do ruky nástroj, který je vám schopen poskytnout nejenom statistické informace v podobě délky spojení, objemu přenesených dat, zdrojové a cílové IP adrese, případně TCP/UDP portu, ale i konkrétní jméno aplikace, která toto spojení navázala, jaké bylo zpoždění na síti, jaké zpoždění měla aplikace na serveru a v neposlední řadě i informaci o uživateli, včetně jeho polohy a typu použitého zařízení. V tu chvíli máte k dispozici daleko mocnější nástroj pro kontrolu sítě. Tento je od začátku určen primárně k usnadnění správy, nikoliv jako bezpečnostní řešení. Data jsou dostupná téměř online, což velmi pomáhá při okamžitém hledání příčiny problému. Typickým příkladem usnadnění práce může být situace, kdy na helpdesk zavolá uživatel s problémem s dostupností informačního systému. Místo složitého pátrání stačí jedno kliknutí a správce hned vidí, že problém se týká pouze tohoto konkrétního uživatele, který má dlouhé odezvy na síťové úrovni, a všichni ostatní uživatelé pracují naprosto normálně. Následně si u daného uživatele zjistil, že je připojen přes bezdrátovou síť v konkrétním místě, o kterém ví, že tam je špatné pokrytí. Další důležitá informace je, že pracuje na svém tabletu, a o tabletech je všeobecně známo, že mají horší antény než notebooky. Místo běžného šoku, který je s telefonátem typu „nefunguje informační systém“ obvykle spojen, tak může volající dostat naprosto přesnou odpověď. Ta by mohla být v podobě doporučení na změnu místa, odkud přistupuje, a výměny tabletu za notebook. Vedle toho může správce opět požádat držitele financí o výměnu dotčeného bezdrátového přístupového bodu za výkonnější, protože si stěžoval další pracovník. Z jedné univerzity, která tento systém monitorování již nasadila, je další příklad. Tamější uživatelé si dlouho stěžovali na pomalost informačního systému. Správci si s tím nevěděli rady. Navyšovali výkon na serveru, kontrolovali rychlost databáze a aplikačního kódu, ale nic nepomohlo. Po nasazení tohoto pokročilého sledování sítě najednou objevili skutečnou příčinu. Jejich aplikace ke svému provozu používala DNS služby jiného serveru, který měl výkonnostní problémy a odpovídal se zpožděním. Zde pomohla možnost hlídání délky síťové a aplikační odezvy objevit zapeklitou příčinu, která byla úplně mimo původně podezřelý server. A takto bychom mohli pokračovat. Největší výhodou je, že často ani k nahlášení problémů vůbec nedojde. Správce sítě ví s předstihem, že nějaký server bude mít výkonnostní problémy, a lze tak naplánovat upgrade tohoto serveru ještě před vyčerpáním trpělivosti uživatelů. Rovněž je velmi snadné se podívat na statistiku zatížení sítě a dle ní naplánovat vhodný okamžik pro odstávku.

Síť jako nástroj

Typickým uživatelem tohoto řešení jsou pokroková správci sítě, kteří síť chápou jako nástroj pro dosažení cílů firmy. Pokud jsou k firmě skutečně upřímní, tak musí často přiznat, že některé investice lze odložit bez negativního dopadu na provoz. Za použití analýzy přenášených dat, kterou tento systém monitorování poskytuje, mohou snadno zjistit, co jim vytěžuje kapacitu. Jestliže vidí, že polovinu tvoří mimopracovní provoz v podobě sociálních sítí, jako je Facebook, Google+, Twitter nebo Instagram, tak je jasné, že síť není potřeba obměňovat. Stačí omezit tyto služby a síť může ještě nějakou dobu fungovat se současným vybavením. A vedlejším efektem může být růst produktivity dotčených pracovníků.



Z pohledu managementu znamená tento způsob kontroly provozu snížení nákladů na investice, provoz a údržbu. Po reálném nasazení v nemocnici v Německu zjistili, že jim klesl počet zadaných tiketů v helpdeskovém systému na třetinu původního počtu. Najednou byli schopni lépe a rychleji identifikovat příčinu problému a nebylo potřeba hlásit problém správci aplikace, správci serveru a správci sítě s tím, aby se podívali, jestli náhodou není chyba u nich. I přes rostoucí velikost a komplexnost infrastruktury bylo možné zachovat stejný počet pracovníků podpory.

Může se to zdát nečekané, ale o tento způsob analýzy provozu mají zájem i marketingové agentury. Po reálném nasazení na sportovních stadionech měly k dispozici velmi hodnotné údaje. Zjistily, že se přes 16 % návštěvníků připojilo nějakým mobilním zařízením. Tito fanoušci nejvíce přistupovali na sociální sítě Facebook, Instagram a Twitter. Na základě toho může marketingová agentura přesně určit média, kam umisťovat informace a reklamu. Ví, kde jsou příjemci jejich obsahu aktivní. Rovněž se zjistilo, že 80 % návštěvníků používalo jeden operační systém. Je tedy jasné, že při vývoji aplikace na online prodej lístků dostane tento systém přednost, protože se tím pokryje nejvíce zákazníků. Podobné informace mají velkou hodnotu i pro majitele obchodních center, pořadatele koncertů a dalších společenských akcí.

Tato a další data získaná z analýzy provozu nejsou pouhá suchá statistická čísla, ale mají reálné využití. Jsou schopna ušetřit, nebo dokonce vydělat peníze.

Analýza jako služba

Někteří reselleři a integrátoři mohou tuto technologii využít i jako nástroj pro podnikání. Mohou svým zákazníkům nabídnout tuto analýzu jako službu. Například v podobě provedení již zmiňované analýzy, následované doporučeními a nabídkou jejich realizace. Po určité době je vhodné toto celé zopakovat.

Pokud někdo poskytuje službu provozu datového centra pro své klienty, tak i pro něj může být tento nový trend velkou příležitostí. V konkurenčním prostředí slibuje novým zákazníkům každý provozovatel téměř modré z nebe. Pro zákazníka se pak stávají nabídky nepřehlednými, až se nakonec upne k jemu pochopitelnému rozlišení nabídek. A tím je cena. Nyní je k dispozici nástroj, díky kterému lze zákazníkovi seriózně nabídnout kvalitu služby: Je možné mu slíbit, že maximální délka odezvy webové aplikace bude 100 ms, libovolného informačního systému 200 ms a u pošty 500 ms, protože existuje jednotný nástroj pro měření těchto parametrů, který je aplikačně nezávislý. Tím se myslí, že je možné nabídnout provoz libovolné aplikace a bez potřeby instalovat nějaký dodatečný software na servery lze provádět měření. Zákazník má možnost jasně si ověřit, že právě tento poskytovatel má lepší služby, a proto je jeho vyšší cena oprávněná.

Lze tedy říci, že monitorování provozu sítě včetně analýzy přenášených aplikací a dalších doplňkových informací je moderní trend, který má dveře otevřené k mnoha zákazníkům. Od běžných provozů, přes marketingové agentury až po integrátory. Asi největším oříškem bude překonat prvotní ostych některých správců sítě, kterým nově manažeři snadno uvidí do přenášených dat. Obava, že by mohli přijít o peníze na rozvoj sítě, když se přijde na to, že má infrastruktura rezervy, může být značná. Ti, kteří pochopí, že díky tomuto nástroji naopak budou moci své investice a úsilí přesně zaměřit pouze na problémové body, a tím společnosti ušetřit, si ho velmi rychle oblíbí. Pořizovací cena tohoto analytického nástroje je nízká a nasazení je obvykle velmi snadné.

Co čeká síťaře

Objevují se i náznaky, že by mohla síť využívat informací z této detekce aplikací, uživatelů a jejich zařízení přímo k uzpůsobování jednotlivých přenosů. Koncept, kdy je možné nějakým způsobem řídit jednotlivé komunikace dle přenášené aplikace, uživatele a jeho zařízení, je momentálně vlastní pouze UTM nebo Next Generation firewallům. A to nejsou zařízení, která jsou umístěná v centru sítě a jsou schopná zvládnout provoz v řádu terabitů. Ale toto je zatím hudba budoucnosti.

Správci sítě mají těžký život. Lidé je viní ze spousty problémů, za které správci ani nemohou. A když nastane výpadek, tak musí vše rychle opravit. Jestliže k zjištění původu problému nemají dostatečné informace, tak i jim začne být opravdové horko a začnou se potit. Proto tu s námi jsou monitorovací nástroje, aby jim jejich práci zpříjemnily.

Zdeněk Tlustý pracuje ve společnosti Veracomp na pozici business development manager technologie Extreme Networks