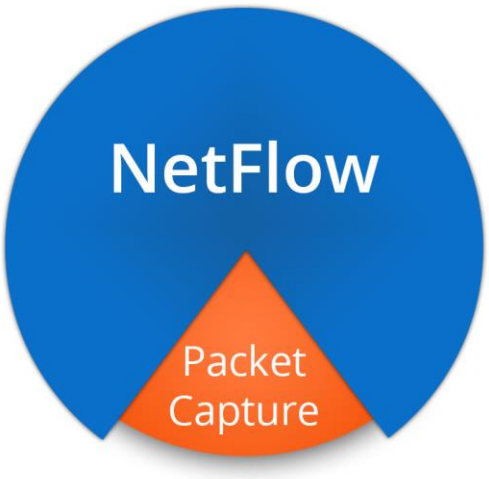
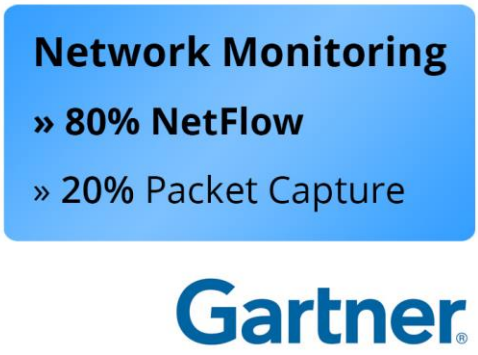
Moderní řešení pro viditelnost do síťového provozu

Účel dokumentu

Zajištění stabilní počítačové sítě a kontroly nad síťovými aplikacemi patří v situaci, kdy téměř veškerá komunikace probíhá na sdílené síťové infrastruktuře, mezi kritické úlohy organizace. Manažeři zodpovědní za správu sítě musí čelit dynamickému prostředí s rostoucím počtem aplikací, narůstajícím množstvím přenášených dat, mobilními koncovými stanicemi, často pod správou zaměstnanců (BYOD), virtualizací, distribuovanou infrastrukturou a cloudovými službami. Tyto nové koncepty kladou nové nároky na stabilitu a správu počítačové sítě a její schopnost zajišťovat vykonávání klíčových procesů organizace i rutinního provozu.

Je zřejmé, že oddělení správy sítě potřebují nové a výkonné nástroje pro efektivní vykonávání své práce. Cílem těchto nástrojů je poskytnout potřebnou viditelnost do dění v síti na úrovni komunikací jednotlivých zařízení i sítě jako celku a kontrolu nad aplikacemi v síti. Díky tomu umožňují snížit dobu mezi výskytem problému v síti a jeho vyřešením, případně problémům se sítí a aplikacemi proaktivně předcházet.





Tento dokument popisuje:

- Hlavní výzvy v oblasti správy sítě a analýzy síťového provozu
- Architekturu řešení pro pokročilou analýzu síťového provozu
- Přínosy moderních technologií pro monitorování toků
- Popis propojení řešení Cisco a Flowmon Networks

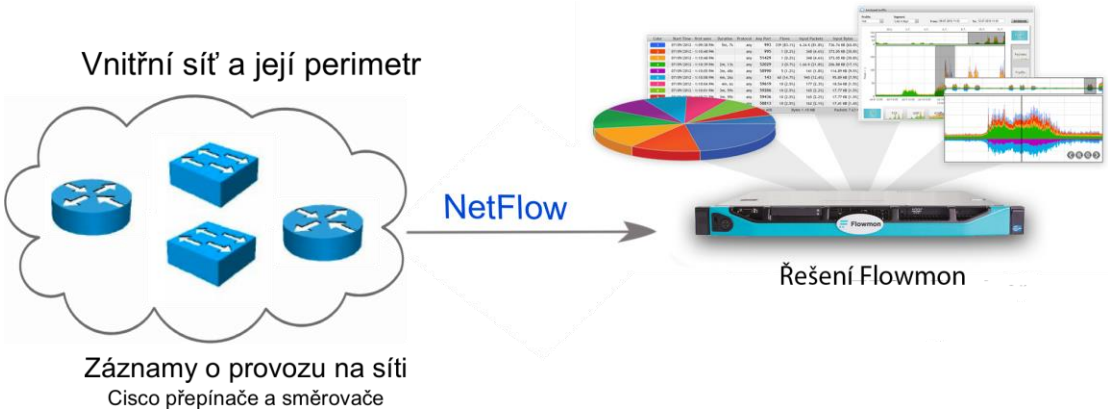
Výzva

Přenosové rychlosti v rámci firemních síti i WAN v řádech jednotek nebo desítek gigabitů umožňují organizacím i zaměstnancům přenášet obrovské objemy dat jak na úrovni vnitřní sítě, tak při komunikaci do internetu. Řada služeb je poskytována prostřednictvím cloudu nebo pomocí distribuované infrastruktury, jako přístupový bod jsou často využívána mobilní zařízení, organizace nasazují nové systémy, z nichž řada je kritická z pohledu chodu organizace. Koncept BYOD způsobuje, že do firemní sítě jsou připojena zařízení, která nejsou pod kontrolou správy sítě a která do sítě zanášejí nepovolené aplikace či spotřebovávají značnou část kapacity sítě.
Pokud má mít v této situaci oddělení pro správu sítě potřebnou kontrolu nad děním v síti, potřebuje adekvátní nástroje. Široce používaná technologie SNMP monitorování je z pohledu viditelnosti do dění v síti nedostatečná. Technologie zachytávání provozu je z pohledu dlouhodobého monitorování celé sítě nepoužitelná. Správa sítě potřebuje detailní informace nejen o tom, jaké objemy dat se v síti přenášejí, ale také které stanice tato data generují, kam je posílají, o jaký druh provozu či konkrétní aplikace se jedná a zda tyto přenosy neznamenají ohrožení stability a bezpečnosti sítě. Podobný pohled je nutné mít na úrovni aplikací, které organizace používá, nebo které se naopak v síti organizace vyskytují. Tyto informace je nutné mít k dispozici pro celou síť, tedy pro každé jednotlivé zařízení připojené do sítě, a to jak v reálném čase, tak dlouhodobě zpět. S ohledem na množství takto zachycených dat je zároveň nutná určitá míra automatického zpracování a detekce incidentů v síti.

Architektura řešení

Řešení pro pokročilou analýzu síťového provozu kombinuje níže uvedené prvky pro zajištění kompletní viditelnosti do sítě a efektivní zpracování nasbíraných dat:

- Viditelnost provozu uvnitř sítě zajišťují Cisco aktivní prvky se schopností generovat kompletní (nevzorkované) NetFlow záznamy o komunikaci v síti (podporují switche a routery společnosti Cisco). Viditelnost aplikací a sledování výkonových ukazatelů zajišťují stejné prvky pomocí technologie Cisco AVC a standardu Cisco NBAR 2.
- Uchovávání informací o provozu v síti, jejich zpracování, analýzu a reporting provádí Flowmon kolektor společnosti Flowmon Networks, podporující Cisco standardy NetFlow v5, v9, NBAR2, AVC ale i obecné protokoly IPFIX či sFlow.



Díky možnosti řešení Flowmon zpracovávat NetFlow a NBAR2 nebo AVC informace z Cisco přepínačů a směrovačů lze využít prvky Cisco v síti zákazníka, které export těchto dat podporují. Toto zapojení snižuje pořizovací náklady a zhodnocuje investici zákazníka do Cisco infrastruktury.

Přínosy řešení

Řešení pro pokročilou analýzu síťového provozu je zaměřeno na poskytnutí detailního vhledu do interní sítě a odhalování provozních a bezpečnostní incidentů v síti. Klíčové přínosy řešení jsou:

- Detailní evidence informací o provozu v interní síti organizace
- Zjednodušení a zrychlení procesu řešení problémů se sítí
- Kontrola nad aplikačním provozem v síti (application awareness)
- Podrobné sledování výkonových parametrů datové sítě
- Detekce vybraných provozních a bezpečnostních událostí na úrovni sítě
- Možnost včasného odhalení problémů v síti a předcházení incidentům
- Pravidelný reporting o stavu sítě, možnost plánování kapacit sítě
- Zefektivnění správy sítě, snížení pracnosti pro správu sítě
- Zvýšení dostupnosti a stability sítě
- Možnost využít stávající Cisco infrastrukturu v síti

Analýzu NetFlow dat doporučuje kromě společnosti Cisco jako klíčovou technologii pro zvýšení dostupnosti a stability sítě také analytická skupina Gartner.

Komponenty řešení

Generování informací o provozu napříč celou sítí

Nová funkcionalita Cisco Catalyst switchů a routerů umožňuje integrované monitorování provozu v síti – od uživatelských stanic, přes servery až po mobilní zařízení. Nativní export NetFlow dat bez dopadu na výkonnost daného zařízení zajišťují switche Cisco Catalyst 3560-X, 3750-X, 3850, 4500, 6500, Cisco Nexus a všechny routery společnosti Cisco.

Agregace, evidence a analýza NetFlow dat

Analýzu NetFlow dat zajišťuje řešení Flowmon společnosti Flowmon Networks. Flowmon zpracovává data v reálném čase a poskytuje tak možnost okamžité reakce na nežádoucí události v síti. Umožňuje také ukládání dlouhodobé historie informací o provozu v síti a poskytuje tak potřebné podklady pro analýzu i několik měsíců zpětně.

Primární komponenta Flowmon řešení:

- Flowmon kolektor – slouží k agregaci a uchovávání NetFlow dat z neomezeného počtu zdrojů. Poskytuje moderní reportovací a analytické nástroje nad provozem v síti a aplikačním provozem.

Doplňkové komponenty Flowmon řešení zahrnují:

- Flowmon sondy – specializovaná zařízení pro generování NetFlow dat včetně identifikace aplikací, sledování výkonových charakteristik nebo analýzy VoIP provozu v prostředí, kde není možné tato data generovat pomocí stávající Cisco infrastruktury.

Řešení Flowmon je dostupné jako fyzické nebo virtuální appliance.

Proč řešení pro pokročilou analýzu síťového provozu?

Unikátní kombinace Cisco prvků se schopností generovat NetFlow záznamy a řešení Flowmon pro zpracování těchto dat umožňuje zkrácení doby nutné pro řešení problémů v síti, zvyšuje stabilitu sítě, zajišťuje potřebnou kontrolu nad aplikacemi v síti a snižuje provozní náklady na správu sítě. Pro zákazníky využívající Cisco prvky ve své infrastruktuře jsou navíc náklady na implementaci a provoz tohoto řešení minimální.

Pro více informací

Pro více informací prosím kontaktujte svého Cisco nebo Flowmon Networks partnera.

Cisco Systems (Czech Republic) s.r.o.
V Celnici 10
117 21 Praha 1
Czech Republic
www.cisco.com

Flowmon Networks, a.s.
U Vodárny 2965/2
616 00 Brno
Česká republika
www.flowmon.com