# Obnova systém pro analýzu datových toků

Jihomoravský kraj (dále jen „JMK“) aktuálně disponuje systémem pro analýzu datových toků. Tento systém je složen s HW a SW prvků jenž umožňují základní analýzu a detekci síťových a bezpečnostních anomálií a útoků. Tento systém je složen s následujících součástí:

- 1x IFP-10000-SFP+ FlowMon Probe 10000 SFP+
- 1x IFC-3000-VA INVEA, FlowMon, Collector, IFC-3000-VA
- 1x Synology RS814 + Rack Station
- 1x Synology Rail Kits Sliding (posuvné), RKS1314
- 2x HDD 3TB WD3000FYYZ64MB SATAIII/600 7,2k RAID

Cílem veřejné zakázky „obnova systému pro analýzy datových toků“ je obnova výše uvedených zařízení s tím že musí být možné přenést nastavení, filtru a zaznamenaných dat na nově pořizovaný systém.

## Požadavky – sonda

- 1U rack mount zařízení, snadná instalace do stávající síťové infrastruktury, nezávislost na stávající síťové infrastruktuře, pasívní zařízení – neviditelné z pohledu vrstev L2 a L3
- dva plnohodnotné administrativní porty 10/100/1000 Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat,
- 1X monitorovací rozhraní 10Gb/s
- celkový výkon zařízení minimálně 10 Mp/s
- detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik, podpora monitorování MAC adres, VxLAN a GRE tunelů
- podpora vzorkování na úrovni paketů i toků,
- podpora filtrování a export datových toků na základě AS,
- zabezpečená vzdálená správa, dohled a konfigurace výhradně přes zabezpečené protokol – SSH, HTTPS,
- vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance)
- podpora standardů NEL a NSEL
- podpora pro export informací o detekovaných aplikacích dle NBAR2 standardu
- podpora pro export informací z HTTP provozu – včetně položek typu URL, hostname,
- podpora pro export informací z DNS provozu
- podpora pro export VoIP SIP statistik (jitter, latence, ztrátovost),
- podpora pro export informací z SMB provozu,
- podpora pro export informací z DHCP provozu,
- podpora pro export informací z MSSQL, MySQL a PostgreSQL provozu,
- podpora pro export informací z SSL/TLS provozu,
- instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.
- časová synchronizace zařízení proti centrálnímu zdroji času na síti,
- možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232),
- podpora autentizace vůči LDAP (Active Directory)

- monitorování výkonnostních parametrů sítě (Network Performance Monitoring – NPM)
- Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety.
- drill-down – možnost dohledat každý jednotlivý tok zaznamenaný sondami
- detekce aktivních zařízení na sítí - pro podporu konceptu BYOD
- podpora geolokace na základě IP adresy,
- top N statistiky, vytváření profilů, pokročilý reporting (online, email, PDF, CSV…), grafy, dashboardy
- pokročilý alerting definovaných událostí (email, SNMP Trap, syslog),
- řízení uživatelského přístupu
- plná zákaznická podpora v českém jazyce a české uživatelské rozhraní,
- Poskytnutí updatů a upgradů SW komponent v případě jejich uvolnění na 36 měsíců
- Telefonická a e-mailová podpora v českém jazyce v pracovní době (8x5) na 36 měsíců

## Požadavky – kolektor

- 1U rack mount server, snadná instalace do stávající síťové infrastruktury,
- Systémová architektura x86_64
- Minimálně 32 CPU jader (včetně HT)
- Minimálně 64 GB RAM
- Minimálně 2x 1 Gb/s Ethernet rozhraní pro vzdálenou správu a přenos flow záznamů
- Hardwarový diskový řadič s podporou RAID 5 včetně SMART detekce
- Minimálně 3TB celková kapacita pevných disků typu SSD s podporou funkce Hot Swap
- Minimálně dva napájecí zdroje typu Hot Plug
- Podpora zpracování protokolů pro export síťových toků (minimálně NetFlow v5, NetFlow v9, IPFIX, jFlow, sFlow)
- Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, databáze aktivních zařízení na síti vč. identifikace zařízení
- Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.
- Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.
- Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety.
- detekce aktivních zařízení na sítí - pro podporu konceptu BYOD
- podpora geolokace na základě IP adresy,
- top N statistiky, vytváření profilů, pokročilý reporting (online, email, PDF, CSV…), grafy, dashboardy
- pokročilý alerting definovaných událostí (email, SNMP Trap, syslog),
- řízení uživatelského přístupu
- plná zákaznická podpora v českém jazyce a české uživatelské rozhraní,
- Poskytnutí updatů a upgradů SW komponent v případě jejich uvolnění na 36 měsíců
- Telefonická a e-mailová podpora v českém jazyce v pracovní době (8x5) na 36měsíců

## Požadavky – na záchyt síťového provozu

- Systém zachycuje síťový provoz v plném rozsahu (vrstvy L2-L7) a záznamy zachyceného síťového provozu ukládá v souboru s formátem PCAP, který je možno stáhnout z

webového uživatelského prostředí pro následnou analýzu v programu třetí strany (např. Wireshark).

- Je nutné mít možnost záchytu síťového provozu v sítích s rychlostmi až 10Gb/s.
- Centrální ovládání z kolektoru, možnost definovat sondy a monitorovací porty.
- Možnost definování filtrů na zachycení části síťového provozu. Kritéria filtrace parametry z vrstev L2-L4 a L7
- Možnost filtrování síťového provozu podle VLAN tagů. MPLS značky.
- Možnost filtrovat síťový provoz podle IPv4, IPv6 adresy, čísla sítě a masky´
- Možnost filtrovat síťový provoz podle portů TCP, UDP a SCTP
- Možnost filtrovat síťový provoz VoIP hovorů používající SIP a H.323 protokoly
- Možnost definovat časový interval, ve kterém se bude síťový provoz zachytávat
- Možnost definovat skupinu uživatelů, která má přístup ke stažení záznamu.
- Záchyt síťového provozu je možné spustit automaticky na základě detekce události systémem pro automatické vyhodnocování NetFlow dat
- Automatická rotace starých dat pro uvolnění místa na disku pro nové záchyty síťového provozu.
- plná zákaznická podpora v českém jazyce a české uživatelské rozhraní
- Poskytnutí updatů a upgradů SW komponent v případě jejich uvolnění na 36 měsíců

### Implementace

- Přenesení stávajícího prostředí
- Vytvoření produkčního prostředí a integrace s prostředím technologického centra kraje
- Tvorba dokumentace.
- zaškolení administrátorů.

## Upřesnění technické specifikace

### Požadavky na implementaci, školení a technickou podporu

Vybraný dodavatel provede kompletní implementaci. V průběhu implementace bude prováděno testování jednotlivých komponent.

Dodavatel bude při implementaci dodržovat zásady projektového řízení.

Součástí implementace bude odpovídající školení administrátorů.

Dodavatel prokáže odborné předpoklady pro implementaci a zkušenosti s implementovanými technologiemi.