Příloha č. 1 – Specifikace předmětu plnění

1. Požadavky na zdroje NetFlow/IPFIX dat (sondy)

Sondy umožňují analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP). Mimo objemových charakteristik provozu poskytují sondy rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti. Díky tomu přináší sonda komplexní přehled a detailní informace o dění v síti a usnadňuje tak řešení síťových problémů, správu a optimalizaci sítě a zvyšuje její bezpečnost.

Uživatelsky definované šablony	Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX pomoci kterých lze definovat exportované atributy.
Detekce aplikací	Detekce aplikací dle standardu NBAR2.
Monitorování a analýza HTTP provozu	Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname, stavový kód HTTP, dotazovací metoda. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX).
Profilování zařízení v síti	Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (IPFIX).
Zabezpečená vzdálená správa	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí.
Podpora spolehlivého a šifrovaného exportu toků dle standardu	Zařízení umožňuje exportovat statistiky o síťovém provozu (toky) pomocí spolehlivého a zabezpečeného komunikačního kanálu dle standardu RFC 7011.
Zpracování datového provozu	Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor.
Dohled	Sondu je možné integrovat do dohledového systému jako monitorované zařízení pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP.
Vestavěný kolektor	Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru.
Časová synchronizace	Časová synchronizace zařízení proti centrálnímu zdroji času na síti.
Podpora příkazové řádky	Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.

Požadavky na kolektory NetFlow dat

Kolektory jsou zařízení (datová úložiště) s vysokou diskovou kapacitou určená pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat. Kolektory jsou připraveny pro hybridní sítě a podporují sběr nativních cloudových VPC flow logů. Zobrazení uložených flow dat a jejich analýza (vyhledávání, agregace, výpisy aj.) probíhá na kolektoru prostřednictvím zabezpečeného webového rozhraní. Uložená data a výsledky analýz jsou dostupná ve formě dlouhodobých grafů a top statistik s možností zobrazení dat až na úrovni jednotlivých komunikací (jednotlivé NetFlow/IPFIX záznamy). Kolektor poskytuje funkce reportování statistik i monitorování výkonu aplikací a systém notifikací v případě výskytu definované události/anomálie.

Název požadavku	**Popis požadavku**
Ukládání flow statistik	Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce.
Granularita vizualizace	Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5 minutových, 1 minutových nebo 30 sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků.
Podpora standardů datových toků	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. Podpora VPC flow logů z AWS, Azure a GCP.
Hlavní funkcionalita	Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení.
Monitoring informací z aplikační vrstvy	Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS).
Spolehlivý a šifrovaný přenos IPFIX dat	Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011.
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).
Předdefinované dashboardy	Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu. Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů.
Sdílené dashboardy	Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat).
Vizualizace statistických dat	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů,

	toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem.
Vizualizace výkonnostních metrik sítě	Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami.
Vizualizace výkonnostních metrik sítě	Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru.
Analýza dat a ad hoc výstupy	Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV.
Reporting	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště.
Řízení uživatelského přístupu	Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem).
Top N statistiky	Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.

2. Požadavky na monitorování výkonu aplikací

Systém na monitorování výkonu aplikací poskytuje informace o skutečné odezvě aplikace z pohledu uživatele (tzv. user experience) a to pro všechny uživatele a všechny jejich uživatelské transakce v reálném čase. Systém umožňuje transparentně (bez vlivu na aplikaci a infrastrukturu) a bez instalace softwarových agentů monitorovat provoz aplikace, vyhodnocovat její výkon a reportovat/notifikovat o stavu aplikace. Monitoring probíhá na úrovni uživatel – aplikační server a aplikační server – databázový server. Hlavní metriky jsou doba odezvy a čas na transportní vrstvě, což umožňuje odlišit zpoždění dané zpracováním požadavku od zpoždění přenou dat na síti. Výkon aplikace je možné vyjádřit prostřednictvím ukazatele na bázi tzv. appdexu[1], vypočteného na základě uživatelsky definovaného SLA. Díky tomu je možné přesně identifikovat místa a příčiny problému a tím výrazně zrychlit čas potřebný k jejich nápravě a snížit náklady na správu aplikací.

[1] https://en.wikipedia.org/wiki/Apdex

Název požadavku	Popis požadavku
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Vizualizuje stav aplikace pomocí indexu výkonu aplikace, počtu transakcí a dalších informací ve formě grafů a tabulek. Umožňuje analyzovat stav jednotlivých částí aplikace a transakcí.
Uživatelsky definovatelný dashboard	Uživatelsky definovatelný dashboard pro okamžitou vizualizaci stavu aplikace pomocí widgetů. Možnost přizpůsobení a vkládání vybraných widgetů uživatelem, např. index výkonu aplikace, 5 nejpomalejších transakcí, souhrnné informace a další statistiky vztažené k definovatelnému časovému intervalu (předcházejících x hodin/dnů).
Reporting odezvy aplikace	Systém reportuje pro definované aplikace a každou uživatelskou transakci realizovanou nad aplikací dobu odezvy aplikace a čas na transportní vrstvě. Díky tomu je možné odlišit zpoždění sítě od zpoždění aplikace.
Bez-agentní monitoring	Systém monitoruje aplikace bez nutnosti instalovat jakýkoliv SW na servery nebo klientské stanice.
Transparentní monitoring	Systém monitoruje aplikace bez jakéhokoliv vlivu na aplikaci nebo síťovou infrastrukturu.
Architektura systému	Systém je možné nasadit samostatně na jedné sondě, nebo na více sondách s centrální správou a webovým uživatelským rozhraním na kolektoru.
Monitoring na úrovni uživatel – aplikační server	Systém umožňuje monitorovat komunikaci mezi klienty aplikace a aplikační serverem na bázi protokolu HTTP a HTTPS. V případě použití protokolu HTTPS podporuje automatické dešifrování komunikace se znalostí privátního klíče pro šifrovací protokoly, které toto umožňují.
Monitoring na úrovni aplikační server – databázový server	Systém umožňuje monitorovat komunikaci mezi aplikačními servery a databázovými servery Oracle , MSSQL, Postgre SQL, MySQL MariaDB.
Definice SLA a index výkonu aplikace	Systém umožňuje pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně vyhodnocuje všechny transakce a stanovuje celkový index výkonu aplikace na základě plnění SLA.
Konfigurace aplikací	Systém nabízí flexibilní možnosti definice aplikace pro monitoring. Minimálně v rozsahu IP adresy, porty, host, URL vč. regulárních výrazů pro jejich definici.

Korelace	Systém umožňuje korelovat zpoždění na úrovni uživatelské transakce na aplikačním serveru a transakce mezi aplikačním a databázovým serverem. Pro každou uživatelskou transakci je možné zobrazit SQL transakce, které byly v rámci uživatelské transakce vykonány.
Skupiny	Systém umožňuje definovat skupiny pro sledování metrik pouze pro zvolenou podmnožinu transakcí (např. skupina pro PHP soubory, multimediální soubory, část klientů a uživatelů).
Přepočítávání historických statistik	Systém přepočítává historické statistiky pro nově vytvořené skupiny.
Reporting	Systém umožňuje vytvářet reporty dostupné prostřednictvím webového GUI, ve formátu PDF. Reporty je možné automaticky odesílat e-mailem.
Notifikace	Jako reakci na snížení indexu výkonu aplikace, případně další metriky umožňuje systém odeslat e-mail, syslog zprávu, SNMP trap, nebo spustit skript.
Detaily HTTP transakcí	Pro každou transakci jsou dostupné detaily minimálně v rozsahu URL, parametry, user agenty, objem přenesených dat, návratová hodnota, cookie.
Detaily databázových transakcí	Pro každou transakci jsou dostupné detaily minimálně v rozsahu SQL dotazu v plném rozsahu, velikost dotazu a odpovědi, typ SQL dotazu, čas vzniku dotazu i odpovědi a doba odezvy.
Filtrace agregovaných transakcí	Systém umožňuje filtrovat nad seznamem agregovaných transakcí pomocí kritérií (např. APM, index, počet chyb, celkový objem přenesených dat a další). Díky tomu lze získat informace o tom, jaké části aplikace jsou nejpomalejší, vykazují nejvíce chyb, atd.
Filtrace jednotlivých transakcí	Systém umožňuje filtrovat nad seznamem jednotlivých transakcí pomocí různých kritérií (např. IP adresa uživatele, doba odezvy, SLA, uživatelské jméno, začátek a konec transakce a další). Díky tomu lze získat informace o tom, jaká skupina uživatelů komunikovala s aplikací, jaká byla odezva aplikace, pro jaké uživatele a transakce byla aplikace nedostupná, atd.
CSV export	Systém umožňuje exportovat informace o transakcích ve formátu CSV.
Odvozené metriky	Systém sleduje další odvozené metriky jako je průměr, medián, 99-percentil a 95-percentil doby odezvy aplikace, zobrazuje přehled nejpomalejších transakcí, počet uživatelů současně pracujících s aplikací, počet transakcí dle splnění SLA, struktura chybových kódů.