Příloha č. 1 Smlouvy – Technická specifikace

NÁZEV VEŘEJNÉ ZAKÁZKY:

Nástroje pro analýzu a monitoring síťového provozu
(číslo projektu: CZ.31.1.01/MV/23_55/0000055)

Technická specifikace

Základní požadavky na dodávku a implementaci

Předmětem plnění veřejné zakázky (VZ) je dodávka a kompletní implementace Nástrojů pro analýzu a monitoring síťového provozu FTN, spočívající v nasazení řešení pro provozní, výkonnostní a bezpečnostní monitoring síťového provozu v hybridním prostředí s pokročilými analytickými funkcemi.
Plnění VZ bude obsahovat tyto základní komponenty a parametry:

- 2ks Monitorovací sonda s kapacitou 2x10Gbps (rozhraní SFP+) ve formě hardware appliance
- 2ks Monitorovací sonda s kapacitou 4x1Gbps (rozhraní SFP) ve formě hardware appliance
- 2ks Metalický TAP pro monitorování linky o rychlosti 1Gbps
- 2ks Monitorovací sonda s kapacitou 1x10Gbps ve formě virtuální appliance
- 1ks Kolektor s diskovou kapacitou 16TB a výkonem až 200 000 flows/s ve formě hardware appliance

- Všechny dodávané komponenty budou dodány včetně veškerého software a licencí potřebných k jejich provozu
- Součástí dodávky bude kompletní nastavení, implementace a instalace dodávaných komponent a software do stávající infrastruktury zadavatele, včetně zaškolení obsluhy
- Součástí dodávaného řešení bude záruka a podpora výrobce na všechny dodávané komponenty, včetně veškerého dodávaného potřebného software, po dobu minimálně 60 měsíců.
- Podléhají-li některé z dodávaných komponent či software časově omezenému licencování, musí být dodáno jeho předplatné v délce trvání min. 60 měsíců

Dodávané monitorovací sondy a TAP budou dodány ve dvou kusech (redundantně), jelikož budou nasazeny v režimu vysoké dostupnosti s tím, že každá sada těchto komponent bude umístěna v jiné, fyzicky oddělené lokalitě areálu Fakultní Thomayerovy nemocnice. Z důvodu zajištění bezpečnosti a bezpečného monitorování datové sítě, požaduje zadavatel, aby dodávaná zařízení zajišťující režim vysoké dostupnosti měla shodné technické parametry a výkon, aby mohla v případě výpadku jedné z lokalit převzít veškeré požadované funkce lokalita druhá.

Pro jednotlivé funkční vlastnosti a technické parametry požaduje zadavatel jejich doložení odkazy do příslušných dokumentů (technická specifikace, datový list, uživatelská dokumentace). Uchazeč předloží, jako součást nabídky, tuto dokumentaci ve **formátu PDF** pro aktuálně na trhu dostupnou verzi nabízeného řešení. Uchazeč odkáže na příslušné kapitoly uživatelské dokumentace pro požadované vlastnosti, které umožní zadavateli posoudit, zda a jakým způsobem, nabízené řešení požadavky splňuje, v případě nejasností si zadavatel vyhrazuje právo písemného doplnění a vysvětlení (potvrzení), jak jsou požadované parametry splněny.

Potvrzení o pětileté záruce

Součástí předávacích protokolů druhé etapy díla bude písemné potvrzení od výrobce dodávaných technologií, že na předmět plnění byla u výrobce zakoupena minimálně 5letá (60 měsíců) rozšířená záruka výrobce se zahájením opravy/výměny následující pracovní den s možností hlásit závadu 8 hodin denně v pracovní dny (označovaná zpravidla jako 8x5xNBD) platná od data zahájení zkušebního provozu. Doba dokončení výměny musí být provedena v maximální lhůtě 7 kalendářních dní od nahlášení závady. Tato záruka musí být poskytována na místě instalace pracovníky výrobce nebo dodavatele.

Požadavky na funkční vlastnosti a technické parametry dodávaných zařízení

1) Funkční vlastnosti

Následující tabulka specifikuje požadované funkční vlastnosti poptávaného řešení. Funkční vlastnosti se vztahují na systém jako celek, tedy ***dané vlastnosti musí splňovat jak sondy, tak kolektor***.

*Účastník vyplní u všech položek v následujících tabulkách, zda jeho nabízené řešení splňuje zadavatelem požadované parametry (**zapsáním ANO, nebo NE**) a dále vyplní (dle konkrétních položek v tabulce), jakým konkrétním způsobem požadované parametry naplňuje (**Skutečná hodnota, popis splnění požadavku**), uvede odkaz na dokumentaci dodávaného zařízení, ze které bude zřejmé, jak dodané zařízení požadavky splňuje (**Dokumentace odkaz**).*

Uvedené funkční parametry jsou minimální a účastník může nabídnout zařízení se shodnými nebo lepšími parametry.

Pro ověření parametrů v dokumentaci jsme stáhli aktuální podrobnou dokumentaci z webových stránek výrobce a přiložili ji k nabídce do VZ. V níže uvedených tabulkách jsou použity následující zkratky, které odkazují na jednotlivé dokumenty z přiložené dokumentace:

UG_FM	Flowmon 12.3.2 User Guide.pdf
UG_ADS	Flowmon ADS 12.2.1 User Guide.pdf
UG_APM	Flowmon APM 6.0.1 User Guide.pdf
UG_PI	Flowmon Packet Investigator 12.2.1 User Guide.pdf
MS_C	Flowmon Collector Models Specification.pdf
MS_P	Flowmon Probe Models Specification.pdf
MS_ADS	Flowmon ADS Models Specification.pdf
MS_APM	Flowmon APM Models Specification.pdf
MS_PI	Flowmon Packet Investigator Models Specification.pdf
D_TAP	Flowmon TAP Datasheet.pdf
PD_APM	Flowmon APM Storage Requirements.pdf
PD_FPI	Flowmon FPI Events Catalogue.pdf
PD_SaaSrec	Flowmon SaaS applications and platforms 2024-01-31.xlsx

Tabulka požadavků na Funkční vlastnosti

Požadované parametry	**Splněno (ANO/NE)**	**Dokumentace (odkaz)**
Podpora standardů NetFlow v5, NetFlow v9, IPFIX pro export i příjem statistik o síťovém provozu v souladu s příslušnými RFC pro dané standardy.	ANO	Popis: UG_FM s. 7, 8 Konfigurace: UG_FM s. 72, 73 Standardy: https://www.flowmon.com/en/solutions/network-and-cloud-operations/netflow-ipfix Kapitola List of Flow standards
Podpora pro spolehlivý a bezpečný přenos dat ve formátu IPFIX mezi sondami a kolektorem v souladu s RFC 7011.	ANO	UG_FM s. 72 (šifrování dle RFC 7011 sonda) UG_FM s. 141 (šifrování dle RFC 7011 kolektor)
Podpora pro nastavení času aktivní a neaktivní expirace toků (RFC 3954).	ANO	UG_FM s. 70
Monitorování v pasivním režimu (SPAN/TAP) a aktivním režimu (GRE/ERSPAN).	ANO	Popis SPAN/TAP UG_FM s. 17 Popis/Konfigurace GRE/ERSPAN UG_FM s. 73-75
Deduplikace paketů na úrovni monitorovacích portů.	ANO	Popis: UG_FM s. 80 Konfigurace: UG_FM s. 74
Monitorování MAC adres.	ANO	Popis: UG_FM s. 75,

		Konfigurace: UG_FM s. 74
Monitorování VLAN tagů.	ANO	Popis: UG_FM s. 75, Konfigurace: UG_FM s. 74
Monitorování výkonnostních parametrů sítě: ● round trip time, ● server response time, ● TCP retransmise.	ANO	Popis: UG_FM s. 75, Konfigurace: UG_FM s. 74
Monitorování odezvy aplikací pro protokoly HTTP, HTTPS (s možností dešifrování provozu na základě privátního klíče), MS SQL, PostgreSQL a MySQL. V rámci monitorování odezvy aplikací jsou k dispozici následující metriky: ● network transport time (doba přenosu požadavku a odpovědi), ● application response time (odezva aplikační transakce).	ANO	Popis: UG_APM s. 6 UG_APM s. 42-43
Identifikace a extrakce metadat z aplikačního protokolu HTTP.	ANO	Popis: UG_FM s. 76 Konfigurace: UG_FM s. 74
Identifikace a extrakce metadat z aplikačního protokolu SSL/TLS vč. TLS 1.3.	ANO	Popis: UG_FM s. 77 Konfigurace: UG_FM s. 74
Identifikace a extrakce metadat z aplikačního protokolu DNS.	ANO	Popis: UG_FM s. 76 Konfigurace: UG_FM s. 74
Identifikace a extrakce metadat z aplikačního protokolu DHCP.	ANO	Popis: UG_FM s. 76 Konfigurace: UG_FM s. 74
Identifikace a extrakce metadat z aplikačního protokolu Samba.	ANO	Popis: UG_FM s. 76 Konfigurace: UG_FM s. 74

Identifikace a extrakce metadat z aplikačního protokolu SMTP.	ANO	Popis: UG_FM s. 76 Konfigurace: UG_FM s. 74
Identifikace a extrakce metadat z aplikačního protokolu QUIC.	ANO	Popis: UG_FM s. 77 Konfigurace: UG_FM s. 74
Uživatelsky definované šablony pro export statistik o síťovém provozu ve formátu IPFIX, pomocí kterých je možné definovat exportované atributy. Uchazeč předloží přehled všech podporovaných atributů (tzv. IPFIX Enterprise Extensions). Zadavatel požaduje možnost exportovat v IPFIX výkonnostní parametry sítě i metadata z aplikačních protokolů.	ANO	UG_FM s. 71–80 UG_FM s. 138–140 UG_FM s. 162–182
Systém umožní vizualizaci statistik o provozu datové sítě v 5 minutových, 1 minutových nebo 30 sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu datových toků.	ANO	Popis: UG_FM s. 188 – 190 Konfigurace: UG_FM s. 193 – 194
Systém zobrazuje výkonnostní metriky v grafech provozu společně s volumetrickými statistikami a to vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty volumetrických i výkonnostních metrik.	ANO	UG_FM s. 243 – 244
Systém umožňuje zpracovávat dotazy na dlouhé časové intervaly s délkou minimálně 1 měsíc bez nutnosti dotaz rozdělit dotaz na menší časové intervaly. Spuštění a vykonání dotazu není limitováno délkou časového intervalu nebo maximální dobou vykonávání dotazu. Dotazy, které se vykonávají dlouhou dobu, běží na pozadí a výsledky si uživatel může zobrazit, jakmile je dotaz dokončen a výsledky jsou dostupné.	ANO	UG_FM s. 243-250
Systém umožňuje filtrovat s využitím libovolných atributů flow statistik včetně aplikačních metadat nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnout do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace).	ANO	UG_FM s. 243-250 UG_FM s. 201 a dále

Systém umožňuje agregovat síťové statistiky podle libovolných atributů a sumarizovat podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.).	ANO	UG_FM s. 247-248
Systém nabízí konfigurační šablony pro typické scénáře použití, například monitorování SaaS aplikací, analýza aplikačních protokolů apod. Tyto konfigurační šablony jsou vestavěné, poskytované výrobcem a pravidelně aktualizované. Jejich aplikace provede nastavení systému pro dané scénář použití.	ANO	UG_FM s. 303-308
Systém automaticky rozpozná každý zdroj flow dat, který mu tato data zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow dat automaticky zobrazuje graf průběhu provozu a umožňuje následně automaticky identifikovat ztrátu nebo významný pokles dat z daného zdroje.	ANO	UG_FM s. 141 UG_FM s. 183 - 188
Systém podporuje obohacování statistik o síťovém provozu o uživatelské identity z externích zdrojů. Jako transportní protokol slouží syslog, který do systému doručuje informace o identitě uživatele pro danou IP adresu. Systém následně obohacuje každý jednotlivý datový tok o identitu uživatele pro zdrojovou i cílovou adresu, pokud je tato informace dostupná. Současně je možné zpracovávat uživatelské identity z více zdrojů, v systému je možné uživatelsky definovat parsovací pravidla pro syslog zprávy pro rozšiřování podporovaných zdrojů uživatelských identit.	ANO	UG_FM s. 53-55
Systém nabízí funkcionalitu detekce útoků, bezpečnostních incidentů a anomálií kombinací tradičního IDS pro identifikaci známých útoků a hrozeb základě signatur s moderní behaviorální analýzou pro detekci neznámých/nových útoků na základě analýzy chování. Detekčních schopnosti pokrývají jednotlivé taktiky dle MITRE ATT&CK framework (uvedeny anglicky): Reconnaissance, Initial Access, Execution, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact. Před detekcí anomálií na základě behaviorální analýzy je možné aktivovat deduplikaci datových toků pro zpřesnění detekce v případě, že síťový provoz prochází větším počtem měřících bodů.	ANO	UG_ADS s. 77-131
Součástí událostí jsou relevantní artefakty (síťová komunikace, na základě které byla událost	ANO	UG_ADS s. 144-157 UG_ADS s. 71 – 72 (nastavení záchytu provozu)

detekována ve formě datových toků i záchytu provozu v plném rozsahu - PCAP) s možností podrobnější analýzy a související události. K jednotlivým externím IP adresám jsou dostupné odvozené informace minimálně v rozsahu geolokace a identifikace SaaS aplikace nebo platformy, jejíž je aplikace součástí. Systém automaticky rozpoznává minimálně 1000 nejběžnějších SasS aplikací a platforem.		Rozpoznávané aplikace (aktuální seznam k datu vypracování nabídky): PD_SaaSrec
Systém pomáhá prioritizovat práci bezpečnostního analytika a poskytuje mu souhrnné informace o nejvýznamnějších událostech, nových incidentech (nebyly zaznmenány v předchozím období), rizikových stanicích a trendech. Předpokládá se využití prostředků umělé inteligence a asistované analýzy, nikoliv prostou prioritizaci událostí na základě severity. Systém automaticky provádí scoring jednotlivých zařízení v síti z hlediska jejich chování a sestavuje přehled zařízení seřazených podle dosaženého score.	ANO	UG_ADS s. 139-140 (Sekce shrnutí)
Výrobce poskytuje automatické, pravidelné aktualizace databáze známých indikátorů kompromitace (tzv. threat intelligence) a databáze signatur. Aktualizace probíhají minimálně jednou denně. Uživatel může nad rámec indikátorů kompromitace poskytovaných výrobcem doplnit vlastní indikátory kompromitace bez nutnosti použití specializovaných datových formátů, tj. prostřednictvím CSV nebo TXT souborů. Indikátory kompromitace je možné získávat automaticky ze systému MISP bez nutnost skriptování (nativní vlastnost produktu).	ANO	UG_ADS s. 33-42
Události je možné automaticky exportovat do systémů typu log management nebo SIEM prostřednictvím protokolu syslog ve standardizovaném formátu CEF.	ANO	UG_ADS s. 68-69
Na základě události je možné automaticky spustit záchyt provozu v plném rozsahu jehož výsledkem je soubor ve formátu PCAP. Záchyt provozu je cílený (pouze provoz přímo související s událostí) a nabízí krátkodobý paměťový buffer pro získání provozu, který bezprostředně předcházel detekci události.	ANO	UG_ADS s. 71-72
Systém podporuje pokročilé dashboardy s libovolným počtem pohledů na data. Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat). Existují předdefinované dashboardy od výrobce pro	ANO	UG_FM s. 275-290

typické scénáře použití, seznam předdefinovaných dashboardů je možné uživatelsky rozšiřovat.		
Systém nabízí předdefinovanou sadu reportů s možností plné konfigurace uživatelem. Reporty jsou obsahově ekvivalentní s dashboardy a umožňují zobrazit veškeré informace, které je možné zobrazit na dashboardu. Reporty jsou dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště.	ANO	UG_FM s. 290-296
Systém nabízí REST API, které pokrývá přístup k datům i konfiguraci. REST API je plnohodnotně dokumentované a oficiálně podporované výrobcem.	ANO	https://restapi.docs.flowmon.com/
Systém nabízí management aktivních relací (uživatelů připojených k systému) prostřednictvím grafického uživatelského rozhraní, REST API a konzole SSH. Administrátor systémů může jednotlivé relace ukončit. V rámci nastavení bezpečnostní politiky je možné konfigurovat session timeout pro grafické uživatelské rozhraní a REST API nezávisle na sobě.	ANO	UG_FM s. 67-68 UG_FM s. 134-135
Systém nabízí integraci LDAP/AD pro autentizaci a autorizaci uživatelů.V rámci konfigurace je možné prostřednictvím uživatelského rozhraní manuálně mapovat skupiny v rámci LDAP/AD na role v systému.	ANO	UG_FM s. 55-60

2) Technické a výkonnostní parametry dodávaných zařízení

Uvedené technické parametry jsou pro každou dodávanou komponentu (každý kus) minimální a účastník může nabídnout zařízení se shodnými nebo lepšími parametry.

*U dodávaných komponent vyplní účastník v tabulkách **navíc konkrétní nabízený typ komponenty** (včetně označení případného software nutného pro provoz komponenty) **a výrobce komponenty**.*

2 kusy … Monitorovací sonda 2x10Gbps (hardware appliance)

Zadavatel požaduje monitorovací sondu ve formě ***hardware appliance***, specializované zařízení v provedení tzv. rack-mount serveru vybavené síťovými rozhraními pro příjem kopie síťového provozu z tzv. mirror portů nebo TAPů, musí umožňovat generování metadat o síťovém provozu a jejich odesílání na tzv. kolektor.

Tabulka požadavků na Monitorovací sondu 2x10Gbps (hardware appliance)

Konkrétní typové označení a název nabízené komponenty		**Flowmon Probe IFP-20000-SFP+**		
Výrobce nabízené komponenty		**Progress Software Corporation**		
Požadované parametry	**Požadovaná hodnota**	**Splněno (ANO/NE)**	**Skutečná hodnota**	**Dokumentace (odkaz)**
Monitorovací port s propustností 10Gbps a rozhraním SFP+	2	ANO	2	MS_P
Výkon v milionech paketů za vteřinu na 1 monitorovací port	1,48	ANO	1,5	MS_P
Výkon v milionech paketů za vteřinu na celé zařízení	2,96	ANO	3	MS_P
Počet souběžných spojení na síťové/transportní vrstvě na 1 monitorovací port v milionech	1	ANO	2*	MS_P
Počet souběžných spojení na síťové/transportní vrstvě na celé zařízení v milionech	2	ANO	4*	MS_P
Export dat ve formátu IPFIX na více cílů současně	5	ANO	Není omezeno	UG_FM s. 71-73
Paměťový buffer až do minut	10	ANO	Není omezeno	UG_PI s. 10-11 Doporučeno max. 15
Paměťový buffer až do počet paketů per tok	20	ANO	Není omezeno	UG_PI s. 10-11 Doporučeno max. 100
Velikost zařízení/provedení	1U	ANO	1U	MS_P
Napájení	1x230V	ANO	1x230V	MS_P

*Jedná se o hodnotu „Flow Cache“ v dokumentu MS_P, počet souběžných spojení odpovídá až dvojnásobnému počtu záznamů ve flow cache.

2 kusy ... Monitorovací sonda 4x1Gbps (hardware appliance)

Zadavatel požaduje monitorovací sondu ve formě ***hardware appliance***, specializované zařízení v provedení tzv. rack-mount serveru vybavené síťovými rozhraními pro příjem kopie síťového provozu z tzv. mirror portů nebo TAPů, musí umožňovat generování metadat o síťovém provozu a jejich odesílání na tzv. kolektor.

Tabulka požadavků na Monitorovací sondu 4x1Gbps (hardware appliance)

Konkrétní typové označení a název nabízené komponenty	**Flowmon Probe IFP-4000-SFP**

Výrobce nabízené komponenty		**Progress Software Corporation**		
Požadované parametry	**Požadovaná hodnota**	**Splněno (ANO/NE)**	**Skutečná hodnota**	**Dokumentace (odkaz)**
Monitorovací port s propustností 1Gbps a rozhraním SFP	4	ANO	4	MS_P
Výkon v milionech paketů za vteřinu na 1 monitorovací port	0,74	ANO	1,48	MS_P
Výkon v milionech paketů za vteřinu na celé zařízení	2,96	ANO	3	MS_P
Počet souběžných spojení na síťové/transportní vrstvě na 1 monitorovací port v milionech	0,25	ANO	0,25*	MS_P
Počet souběžných spojení na síťové/transportní vrstvě na celé zařízení v milionech	1	ANO	1*	MS_P
Export dat ve formátu IPFIX na více cílů současně	5	ANO	Není omezeno	UG_FM s. 71-73
Paměťový buffer až do minut	10	ANO	Není omezeno	UG_PI s. 10-11 Doporučeno max. 15
Paměťový buffer až do počet paketů per tok	20	ANO	Není omezeno	UG_PI s. 10-11 Doporučeno max. 100
Velikost zařízení/provedení	1U	ANO	1U	MS_P
Napájení	1x230V	ANO	1x230V	MS_P

*Jedná se o hodnotu „Flow Cache“ v dokumentu MS_P, počet souběžných spojení odpovídá až dvojnásobnému počtu záznamů ve flow cache.

2 kusy ... Metalický TAP

TAP (Test Access Point) je rozbočovač síťového provozu, musí umožňovat replikovat provoz linky do monitorovacích systémů a analyzátorů síťového provozu.

Tabulka požadavků na Metalický TAP

Konkrétní typové označení a název nabízené komponenty		**Tap P1GCCB**		
Výrobce nabízené komponenty		**Progress Software Corporation**		
Požadované parametry	**Požadovaná hodnota**	**Splněno (ANO/NE)**	**Skutečná hodnota**	**Dokumentace (odkaz)**

Podpora pro metalický ethernet pro rychlosti v Mbps	1000	ANO	10/100/ 1000	D_TAP
Počet výstupních rozhraní (rozdělení RX a TX směru provozu)	2	ANO	2	D_TAP

2 kusy ... Monitorovací sonda 1x10Gbps (virtual appliance)

Zadavatel požaduje monitorovací sondu ve formě ***virtuální appliance*** (Z důvodu kompatibility stávajícího provozovaného virtuálního prostředí zadavatele)**,** software vybavený síťovými rozhraními pro příjem kopie síťového provozu z virtuálních mirror portů (případně ERSPAN), musí umožňovat generování metadat o síťovém provozu a jejich odesílání na tzv. kolektor.

Tabulka požadavků na Monitorovací sondu 1x10Gbps (virtual appliance)

Konkrétní typové označení a název nabízeného software, který zajišťuje funkcionalitu *virtuální appliance*		**Flowmon Probe IFP-10000-VA**		
Výrobce nabízené komponenty		**Progress Software Corporation**		
Požadované parametry	**Požadovaná hodnota**	**Splněno (ANO/NE)**	**Skutečná hodnota**	**Dokumentace (odkaz)**
Monitorovací port (virtuální) s propustností 10Gbps	1	ANO	1	MS_P
Výkon v milionech paketů za vteřinu na 1 monitorovací port	0,5	ANO	0,7	MS_P
Počet souběžných spojení na síťové/transportní vrstvě na 1 monitorovací port v milionech	0,5	ANO	2*	MS_P
Export dat ve formátu IPFIX na více cílů současně	5	ANO	Není omezeno	UG_FM s. 71-73
Paměťový buffer až do minut	10	ANO	Není omezeno	UG_PI s. 10-11 Doporučeno max. 15
Paměťový buffer až do počet paketů per tok	20	ANO	Není omezeno	UG_PI s. 10-11 Doporučeno max. 100
Minimální podporovaná verze VMWare (Z důvodu kompatibility stávajícího	6.7	ANO	5.5 a vyšší	MS_P

virtuálního prostředí zadavatele)				

*Jedná se o hodnotu „Flow Cache“ v dokumentu MS_P, počet souběžných spojení odpovídá až dvojnásobnému počtu záznamů ve flow cache.

1 kus ... Kolektor

Zadavatel požaduje kolektor ve formě ***hardware appliance,*** specializované zařízení v provedení tzv. rack-mount serveru vybavené dostatečnou diskovou kapacitou pro dlouhodobé uložení metadata o síťovém provozu ve formátu NetFlow/IPFIX a kompatibilních. Kolektor musí zajišťovat normalizaci, uložení, zpracování, vizualizaci a konsolidovaný reporting agregovaných informací o monitorovaném síťovém provozu z libovolného počtu sond, routerů a dalších zařízení, která metadata o síťovém provozu poskytují.

Tabulka požadavků na Kolektor

Konkrétní typové označení a název nabízené komponenty		**Flowmon Collector IFC-R10-16000PRO**		
Výrobce nabízené komponenty		**Progress Software Corporation**		
Požadované parametry	**Požadovaná hodnota**	**Splněno (ANO/NE)**	**Skutečná hodnota**	**Dokumentace (odkaz)**
Disková kapacita v TB	16	ANO	16	MS_C
Maximální výkon (zatížení) v flows/s až do	200 000	ANO	300 000	MS_C
Běžný výkon (zatížení) v flows/s až do	100 000	ANO	160 000	MS_C
Zpracování flows/s pro detekci anomálií a incidentů až do	10 000	ANO	20 000	MS_ADS
Minimální doba retence bezpečnostních událostí (měsíců)	18	ANO	Není omezeno	UG_ADS s. 15
Oddělené zpracování dat pro detekci anomálií včetně konfigurace detekčních algoritmů, vlastních pravidel a base lines	4	ANO	20	MS_ADS
Cílů exportu událostí protokolem syslog s možností exportovat různé události na různé cíle	10	ANO	Není omezeno	UG_ADS s. 68-69
Záznam provozu ve formátu	400	ANO	500	MS_PI

PCAP na disk až do Mbps				
Monitorování výkonu a odezvy aplikací, počet transakcí za minutu	10 000	ANO	15 000	MS_APM
Minimální doba retence aplikačních transakcí (měsíců)	6	ANO	Není omezeno	PD_APM UG_FM s. 89-90 Podle nastavení správce kvót
Ochrana dat při selhání disku, minimálně	RAID 5	ANO	RAID 10	MS_C
Velikost zařízení/provedení	1U	ANO	1U	MS_C
Napájení (vč. hot swap)	2x230V	ANO	2x230V	MS_C

3) Požadavky na vybrané příklady použití

Následující příklady použití navazují na výše požadované funkční a technické vlastnosti jednotlivých komponent a podrobně specifikují, jakým způsobem plánuje zadavatel poptávaný systém využít jako celek.
Příklady použití jsou popsány podrobně tak, aby bylo možné vyhodnotit soulad nabízeného řešení se záměrem zadavatele. Uchazeč posoudí každý jednotlivý případ použití systému jako celku a do tabulky uvede “ANO” nebo “NE” tak, aby bylo zřejmé, že jeho nabízené řešení splňuje požadavky na jednotlivé příklady použití.
Hodnota “ANO” pro daný příklad použití znamená, že daný případ použití je splněn úplně a bezvýhradně ve všech uvedených bodech. Uchazeč dále doloží soulad pro každý případ použití odkazem do uživatelské dokumentace.

Zálohování a obnova logů o aktivitě na síti

Zákon o kybernetické bezpečnosti ukládá povinným subjektům uchovávat logy po dobu až 18 měsíců. Za účelem archivace logů o síťové komunikaci je požadována následující funkcionalita nabízeného řešení:

- K řešení je možné připojit standardizované datové úložiště (např. Samba, NFS, S3).
- Objem zálohovaných dat není licenčně omezen a je limitován pouze kapacitou úložiště.
- Data, která jsou předmětem zálohování je možné definovat pomocí libovolné kombinace atributů záznamů o síťovém provozu. Takových definic je možné vytvořit větší počet, bez explicitního omezení.
- Zálohování dat probíhá pravidelně, minimálně jednou za 24 hodin.
- Zálohovaná data je možné v případě potřeby obnovit tak, aby tato data bylo možné analyzovat standardními prostředky řešení identicky jako data, která jsou standardně v systému dostupná.

- Při obnově dat je možné zvolit, která data a za jaký časový interval (minimálně s denní granularitou), budou obnovena.

Výše specifikovaná funkcionalita je standardně dostupná prostřednictvím uživatelského rozhraní produktu, nevyžaduje použití produktu třetí strany, nevyžaduje použití příkazové řádky ani dodatečného skriptování.

Podpora pro tzv. FlowLogs

Nabízené řešení musí být připravené na monitoring datového provozu v prostředí AWS nebo Azure s využitím technologie tzv. FlowLogs. Požadována je nativní podpora pro VPC FlowLogs v případě AWS a NSG FlowLogs v případě Azure. Požadované vlastnosti:

- Řešení podporuje nativní API AWS a Azure pro získávání příslušných FlowLogs z prostředí public cloud, která jsou periodicky (minimálně jednou za 5 minut) získávána z prostředí public cloud.
- Získávaná data ve formátu FlowLogs jsou normalizována a zpracována stejným způsobem jako statistiky o síťovém provozu ve formátu NetFlow/IPFIX s jednotným způsobem vizualizace, reportingu a manuální analýzy.
- Automaticky identifikuje zdroje dat z prostředí AWS a Azure a tyto zdroje pojmenuje podle příslušného pojmenování v prostředí AWS, resp. Azure bez nutnosti manuální konfigurace.
- Neexistují žádná omezení na místo nasazení (on-premise, public cloud) nebo omezení na kombinace zdrojů dat, řešení podporuje současně sběr dat z AWS, Azure, vlastních senzorů i flow dat z aktivních prvků.
- Výše specifikovaná funkcionalita je standardně dostupná prostřednictvím uživatelského rozhraní produktu, nevyžaduje použití příkazové řádky ani dodatečného skriptování.

Výše specifikovaná funkcionalita je standardní součástí produktu a nevyžaduje nasazení dalšího software, virtuální nebo fyzické appliance např. pro konverzi dat.

Pokročilé zpracování flow dat

Nabízené řešení umožní přijímat data ve formátu NetFlow/IPFIX nejen z vlastních senzorů, ale i ze systémů třetích stran. Tato data je následně možné předávat do systémů třetích stran včetně duplikace, filtrování a konverze formátu. Požadované vlastnosti:

- Přijímaná data ve formátu NetFlow/IPFIX je možné duplikovat na libovolný počet cílů.
- Přijímaná data ve formátu NetFlow/IPFIX je možné pro konkrétní cíl libovolně konvertovat mezi formáty, konkrétně NetFlow verze 5, NetFlow verze 9, IPFIX.
- Přijímaná data ve formátu NetFlow/IPFIX je možné pro konkrétní cíl filtrovat, minimálně na základě zdrojových a cílových IP adres nebo sítí, VLAN tagů a L4 protokolů.
- Výše specifikovaná funkcionalita je standardně dostupná prostřednictvím uživatelského rozhraní produktu, nevyžaduje použití příkazové řádky ani dodatečného skriptování.

Výše specifikovaná funkcionalita je standardní součástí produktu a nevyžaduje nasazení dalšího software, virtuální nebo fyzické appliance.

Monitorování výkonu a odezvy aplikací proti definovanému SLA

Nabízené řešení umožní monitorovat skutečnou odezvu aplikací z pohledu uživatele, tj. monitorovat transakce jednotlivých uživatelů v reálném čase bez nutnosti instalovat softwarové agenty na servery nebo koncové stanice. Požadované vlastnosti:

- Podpora webových (HTTP) a databázových aplikací (MSSQL, PostgreSQL, MySQL).
- Systém umožňuje pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně vyhodnocuje všechny uživatelské transakce a stanovuje celkový index výkonu aplikace na základě plnění SLA.
- 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.
- Systém nabízí flexibilní možnosti definice aplikace pro monitoring. Minimálně v rozsahu IP adresy, porty, host, URL, název databáze, vč. regulárních výrazů pro jejich definici.
- Pro každou webovou transakci jsou dostupné detaily minimálně v rozsahu URL, parametry, user agenty, objem přenesených dat, návratová hodnota, cookie.
- 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.
- Systém umožňuje filtrovat nad seznamem agregovaných transakcí pomocí kritérií (např. výkonnostní index aplikace, počet chyb, celkový objem přenesených dat a další). Díky tomu lze získat informace o tom, jaké části aplikace jsou nejpomalejší, vykazují nejvíce chyb atd.
- 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.

Systém automaticky reportuje přehled transakcí, které mají největší negativní dopad na výkon aplikace jako celku a jejichž zlepšení by zvýšilo odezvu aplikace. Tento přehled je možné získat formou reportu nebo zobrazení na dashboardu.

Modelování topologie

Nabízené řešení umožní vytvářet libovolné logické nebo fyzické topologie a na tyto topologie mapovat síťový provoz, resp. libovolně filtrovaný síťový provoz. Účelem je modelovat a vizualizovat prostředí datové sítě, význačné systémy a zobrazovat jejich síťový provoz a vytížení. Požadované vlastnosti:

- Uživatel může vytvořit prostřednictvím integrovaného grafického editoru libovolný počet topologií, které se skládají z uzlů reprezentujících routery, switche, servery nebo služby a tyto uzly jsou propojené hranami, které reprezentují datový provoz mezi definovanými uzly.

- Na hrany je možné mapovat libovolný datový provoz nebo jakoukoliv jeho podmnožinu určenou filtrem. Filtrovat provoz je možné na základě jakéhokoliv parametru statistik o síťovém provozu.
- Pro každou hranu je možné stanovit libovolnou propustnost (kapacitu) a to v režimu symetrické datové linky nebo asymetrické datové linky. Pro každou hranu je možné stanovit způsob výpočtu utilizace průměrem nebo 95-percentilem.
- Pro každou topologii je možné stanovit barevnou škálu utilizace a citlivosti, tj. od jaké utilizace systém signalizuje zvýšené zatížení.

Topologii je možné vizualizovat v podobě grafu nebo tabulky, kde jsou jednotlivé hrany seřazené podle utilizace. Obě formy vizualizace je možné kombinovat na dashboardu a v reportech.

Záchyt provozu s krátkodobým bufferem

Nabízené řešení umožňuje selektivní záznam datového provozu v plném rozsahu ve formátu PCAP pro následnou analýzu. Zároveň je k dispozici krátkodobá paměť pro datový provoz, který bezprostředně předcházel spuštění záchytu provozu. Záchyt je integrován se systémem detekce anomálií a umožňuje v případě signifikantní detekce provoz automaticky zaznamenat. Požadované vlastnosti:

- Centrální řízení záchytu na všech monitorovací sondách, selektivní výběr záchytu pouze na vybraných sodnách a vybraných monitorovacích rozhraní.
- Filtrování provozu pro záchyt na základě IP adres, portů, protokolu, MAC adres, VLAN tagů a jejich libovolné kombinace pomocí logických spojek ANO, OR, NOT (negace).
- Záchyt provozu je možné spustit okamžitě nebo načasovat na definovanou dobu.
- Krátkodobý buffer umožní uchovat v paměti po dobu minimálně 600 sekund nejméně 20 paketů z každého spojení. Tato data jsou k dispozici při spuštění záchytu provozu s datem zahájení v minulosti.
- Výsledné soubory ve formátu PCAP jsou uchovány v systému a jsou rotovány při dosažení definované velikosti a při dosažení definovaného stáří ve dnech.
- Záchyt provozu je možné automaticky spustit ze systému detekce anomálií na základě definovaných pravidel. V rámci pravidla je možné definovat typ události, zdroj dat, filtr pro IP adresy, které jsou původcem události a filtr pro IP adresy, které jsou cílem události. Zároveň je možné omezit maximální počet záchytů, tak byl nemohlo dojít k přetížení systému v případě špatné konfigurace.

Výše specifikovaná funkcionalita je standardně dostupná prostřednictvím uživatelského rozhraní produktu, nevyžaduje použití produktu třetí strany, nevyžaduje použití příkazové řádky ani dodatečného skriptování.

Automatická analýza záchytů provozu ve formátu PCAP

Nabízené řešení umožňuje automaticky analyzovat obsah záchytu provozu ve formátu PCAP s cílem identifikovat příčiny provozních a výkonnostních problémů bez nutnosti manuální analýzy v nástroji typu Wireshark a bez specifických znalostí v oblasti paketové analýzy. Požadované vlastnosti:

- Analýza je k dispozici jak pro PCAP pořízené přímo systémem, tak pro PCAPy pořízené externě a uploadované do systému.
- Analýza pokrývá minimálně následující protokoly: ARP, IP, TCP, ICMP, DHCP, DNS, NTP, SMTP, SAMBA, SSL/TLS.
- Systém musí identifikovat minimálně následující situace.
- Následuje přehled požadované minimální funkcionality automatické analýzy pro jednotlivé protokoly:
    - ARP: gratuitous ARP, ARP sweep, duplicitní ARP adresa.
    - DHCP: chybějící iniciální DHCP paket, chybějící DHCP ACK, velký počet DHCP requestů od jediného klienta, velký počet DHCP discover paketů, DHCP server neposkytuje konfigurační parametry, chybějící DHCP request, chybějící DHCP ACK nebo DHCP NACK.
    - DNS: chybějící odpověď DNS serveru, chybná odpověď DNS serveru, zvýšená doba odezvy pro DNS překlad, nekonzistentní odpovědi DNS serveru na stejný dotaz různým klientům.
    - ICMP: překročení TTL, cílový host nebo síť není dostupná, vyžadována fragmentace, cílový port není dostupný.
    - IP: duplicitní IP adresa, použití link local IP adresy.
    - NTP: chybějící odpověď NTP serveru, nevyžádané odpovědi NTP serveru, chybná autentizace klienta k NTP serveru, neočekávaná hodnota "stratum", chybný čas nebo časová zóna.
    - SAMBA: Samba spojení nebylo korektně vytvořeno, Samba server odmítl připojení ke stromu, pokus o negociaci Samba verze 1, Samba server odmítl připojení k prostředku.
    - SMTP: SMTP server neodpověděl klientovi, SMTP server není připraven pro příjem požadavků, chybějící EHLO/HELO, slabá autentizace klienta k serveru, neúspěšná autentizace, klient se nepokusil odeslat žádný email, chyba při přenosu emailu.
    - TCP: odmítnutí TCP spojení, pomalá relace díky retransmisím, pomalá relace díky plnému přijímacímu bufferu, pomalá relace díky malému MSS, pomalá relace díky ztrátám segmentů.
    - SSL/TLS: šifrování nebylo korektně navázáno.
- Výsledkem analýzy je přehledná struktura obsahu PCAP s vyznačenými nálezy, které obsahují vysvětlení a doporučení pro řešení problému. Nálezy jsou minimálně dvou úrovní - varování a chyba.
- Protokoly nejsou analyzovány izolovaně, systém rozumí jejich vzájemným vazbám, například situace, kdy klient není schopen odeslat email protokolem SMTP může souviset s nefunkčním překladem DNS jména na IP adresu. Systém musí tuto situaci rozeznat a správně vyhodnotit.
- Požadovanou funkcionalitu není možné splnit konstatováním, že informace z výše uvedených protokolů jsou k dispozici v monitorovaných datech. Systém musí provádět automatickou analýzu souborů ve formátu PCAP a uživateli prezentovat výsledky analýzy.

Výše specifikovaná funkcionalita je standardně dostupná prostřednictvím uživatelského rozhraní produktu, nevyžaduje použití produktu třetí strany, nevyžaduje použití příkazové řádky ani dodatečného skriptování.

Tabulka požadavků na vybrané příklady použití

Odpovídající případ použití	Splněno (ANO/NE)	Dokumentace (odkaz)
Zálohování a obnova logů o aktivitě na síti	ANO	UG_FM s. 45-46 (konfigurace úložiště) UG_FM s. 197-201 (vlastní funkce zálohování a obnova)
Podpora pro tzv. FlowLogs	ANO	UG_FM s. 150-163
Pokročilé zpracování flow dat	ANO	UG_FM s. 141-144
Monitorování výkonu a odezvy aplikací proti definovanému SLA	ANO	UG_APM 31-45
Modelování topologie	ANO	UG_FM s. 297-303
Záchyt provozu s krátkodobým bufferem	ANO	UG_PI s. 9-13
Automatická analýza záchytů provozu ve formátu PCAP	ANO	UG_PI s. 19-29 PD_FPI

4) Další požadavky

Tabulka požadavků na záruční podporu

Požadované parametry	Splněno (ANO/NE)	Popis splnění požadavku
Záruka a záruční podpora výrobců všech dodávaných komponentů na úrovni 8x5xNBD – Minimálně 60 měsíců	ANO	Záruka a záruční podpora výrobce všech dodávaných komponentů na úrovni 8x5xNBD – po dobu 60 měsíců
Součástí záruky musí být přímý přístup zadavatele k technické podpoře výrobce zařízení – Minimálně 60 měsíců. Účastník uvede internetovou adresu, kde bude možné uplatnit přímou podporu výrobce zařízení.	ANO	support.kemptechnologies.com

Tabulka požadavků na ostatní služby

Požadované parametry	Splněno (ANO/NE)	Popis splnění požadavku
Implementace, instalace a nastavení dodávaných komponent, v minimálním rozsahu 15MD (jde o kvalifikovaný odhad, v případě vyšší pracnosti není uchazeč oprávněn účtovat MD navíc)	ANO	Implementace, instalace a nastavení dodávaných komponent v plném rozsahu funkčnosti
Zaškolení obsluhy - v rozsahu minimálně 5MD	ANO	Zaškolení obsluhy v rozsahu 5 MD