Příloha č. 2 - Technická specifikace

Použité zkratky:
KKN – Karlovarská krajská nemocnice a.s. – nebo zadavatel nebo objednatel nebo provozovatel
KV – Karlovy Vary
CH - Cheb

Tento návrh specifikuje technické parametry, které v souladu s podmínkami dotačního programu zajišťují vybudování robustní, škálovatelné a bezpečné infrastruktury nezbytné pro provoz nemocničního prostředí a lékařských přístrojů a systémů.

1. Popis výchozího stavu

1.1. Popis lokalit

(1) Z pohledu IT je pro Zadavatele nejvýznamnější lokalitou areál nemocnice Karlovy Vary. V této lokalitě jsou umístěny jak ICT technologie pro nemocnici KV, tak i sdílené technologie pro nemocnici CH. Provoz ICT je zajišťován vlastními zaměstnanci Zadavatele ve spolupráci s externími specializovanými firmami.

(2) Projekt bude realizován v těchto lokalitách:

(a) Areál nemocnice Karlovy Vary (dále také jen „KV“) na adrese Bezručova 1190/19, 360 01 Karlovy Vary.

(b) Areál nemocnice Cheb (dále také jen „CH“) na adrese K Nemocnici 1204/17, 350 02 Cheb.

1.2. Popis stávajícího HW prostředí

(1) Pro provozování ICT technologií má Zadavatel v každé lokalitě vybudovány serverovny, které jsou mezi sebou propojeny optickou trasou Regionální komunikační infrastruktury (dále RKI). RKI je WAN na bázi optických vláken propojující významné úřady a veřejné organizace v kraji včetně všech lokalit Zadavatele. Přenosová kapacita páteřních spojů RKI je 1 Gb/s. RKI je vlastněná Karlovarským krajem a je jím, ve spolupráci s externími partnery, provozována a rozvíjena.

(2) RKI je provozována na technologiích HP, klíčovými prvky jsou 2 centrální šasi HP 7500, jako koncové a uzlové přepínače jsou využívány prvky řady HP 5500 a HP 5800. Stávající prvky musí být využity v návrhu nové infrastruktury.

(3) Každá serverovna je v uzamykatelném prostoru, je vybavena redundantními klimatizacemi. V serverovně je nainstalováno prostorové čidlo požáru, jeden centrální RACK se zhášecím systémem a ručním hasicím přístrojem. Pro případ dlouhodobého výpadku elektrické energie je k dispozici dieselagregát.

(4) Serverovna KV i CH je dostatečně kapacitní pro umístění navrhovaných technologií.

(5) Serverová infrastruktura KKN je tvořena kombinací tří fyzických serverů HPE v Karlových Varech a tří fyzických serverů HPE v Chebu. Všechny servery jsou virtualizovány technologií Hyper-V. Jako operační systém jsou využívány Windows a Linux. Virtualizovaná disková pole jsou značky HP VSA propojena se servery iSCSI 10Gb/s.

(6) Síťová infrastruktura KKN je tvořena přepínači HP/HPE řad 1xxx, 25xx, 4xx a 5xxx, převážně s operačním systémem Comware. V obou lokalitách je vybudované kompletní propojení všech pavilónů pomocí optické sítě na 1GB, páteřní spoje mají kapacitu 10Gb. Přepínače jsou centrálně monitorovány a spravovány systémem HPE Intelligent Management Center (IMC).

(7) Bezdrátová část sítě je vybudována převážně z prvků UBIQUITI UniFi AP AC Pro s centrálním kontrolerem.

(8) Síť KKN je staticky segmentována.

(9) Zálohování a obnova dat v KKN je řešeno pomocí centrálního zálohování na NAS úložiště v KV propojení optickou linkou 10Gb na centrální switch.

(10) Přístup na internet je zajištěn 700 Mb bezdrátovou linkou v obou lokalitách. Zabezpečení přístupu k internetu využívá dvojici firewallů Fortinet FortiGate FG-240D v KV a jedním firewallem FortiGate FG-100E v CH.

(11) Zadavatel má implementovány adresářové služby Active Directory. Pro jmenné a adresní síťové služby (DNS a DHCP) je využívána služba Windows Serveru.

(12) Koncové stanice (počítače), celkem je cca 750 PC v lokalitě KV a cca 240 PC v lokalitě CH.

(13) Tiskové prostředí je tvořeno v KV převážně síťovými tiskárnami v celkovém počtu 290 kusů, v CH přávážně síťovými tiskárnami v celkovém počtu cca 180 kusů. Typové řady HP, nebo Brother.

(14) Serverová a sítová infrastruktura je vybudována jako redundantní a v současné době jsou implementovány technologie umožňující automatické překlenutí odstávky (plánované i neplánované) klíčového prvku s žádným nebo minimálním (v řádu jednotek minut) výpadkem služeb.

1.3. Popis stávajícího SW prostředí

(1) Síťové služby Zadavatele jsou provozovány na platformě Microsoft Windows převážně ve verzi 2016 a Linux.

(2) K ukládání sdílených souborů je využíváno prostředků Windows serveru a diskového úložiště.

(3) Data informačních systémů a ostatních aplikací jsou ukládána převážně do databází Microsoft SQL Server.

(4) Groupwarové služby zajišťuje systém IceWarp. Systém zajišťuje i obsluhu mobilních zařízení.

(5) Pro správu požadavků koncových uživatelů je využíván systém Service Desk.

(6) Hlavními informačními systémy Zadavatele jsou:

(a) Nemocniční informační systém je Fons Enterprise (výrobce Stapro)

(b) Laboratorní informační systém OpenLIMS (výrobce Stapro) a Lims (výrobce Dssoft)

(c) Ekonomický informační systém Helios Green (výrobce Asseco)

(d) Zobrazovací systém PACS MARIE-PACS (výrobce OR-CZ)

(e) Mzdový a personální systém Avensio (výrobce Alfa Software)

(f) Docházkový systém (výrobce IVAR a.s.)

(g) Nemocniční lékárna (výrobce Apatyka servis s.r.o.)

(h) Dále systémy menších agend potřebných pro provoz nemocnice – systém pro objednávání stravy a další

1.4. Popis dokumentace

(1) K provozování a řízení rozvoje ICT je využívána a udržována Provozní dokumentace ICT.

(2) Provozní dokumentace ICT popisuje základní nastavení technologií, hardwarových a softwarových systémů.

(3) Citlivé údaje (přístupové účty apod.) jsou uloženy odděleně od Provozní dokumentace ICT.

(4) Relevantní části dokumentace budou Uchazeči zpřístupněny až po podpisu Smlouvy o dílo k této zakázce.

1.5. Popis způsobu řešení incidentů

(1) Zadavatel zajišťuje podporu 1. úrovně včetně požadavků koncových uživatelů.

(2) Incidenty a požadavky, které nevyřeší interní specialisté, jsou zadávány do helpdeskových systémů dodavatele systému, který vykazuje incident nebo na který směřuje požadavek uživatele. Hlášení incidentů a požadavků je prováděno telefonicky, emailem nebo přímo zadáním ticketu/požadavku do helpdeskového systému dodavatele.

1.6. Aktualizace a update existujícího prostředí

Aplikace aktualizací a oprav virtuálních serverů provádějí specialisté Zadavatele dle potřeby a s přihlédnutím k minimalizaci omezení uživatelů. Zadavatel nemá v současné době pevně definovaná pravidelná servisní okna. Jejich nastavení je součástí požadavků specifikovaných níže.

2. Popis cílového stavu předmětu plnění

2.1. Plnění obecnéých požadavků

(1) Cílem projektu je modernizace počítačové sítě náhradou zastaralých prvků (přepínače, firewally, přístupové body) a zvýšení její kapacity doplněním nových prvků. Současně bude pro zvýšení úrovně zabezpečení počítačové sítě implementován systém řízení přístupu k síti NAC na bázi protokolu IEEE 802.1X s napojením na centrální databázi identit Active Directory a systém řízení identit Identity management. NAC bude implementován jako jednotný pro drátovou i bezdrátovou část sítě a dynamické zařazování koncových zařízení do VLAN na základě ověření, typu zařízení apod. Nedílnou součástí projektu je systém na bezpečnostně provozní monitoring implementovaných technologií s dále specifikovanými parametry.

(2) Navrhované řešení v maximální míře využije stávající prostředky a neomezí chod klíčových aplikací Zadavatele.

(3) Řešení je funkční a spravovatelné i v tzv. ostrovním režimu, tj. bez přístupu k síti Internet.

(4) Z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů bude využito stávajících prostředků a používaných technologií.
Uchazeč zajistí v případě potřeby rozšíření konektivity stávajících serverů v rámci nabídkové ceny.

(5) Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, splňují následující podmínky:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,

(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,

(d) obsahují všechny nezbytné licence na používání příslušného softwaru,

(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu,

(f) jsou určeny pro provoz v České republice.

(6) Veškerá dokumentace vytvořená v rámci veřejné zakázky, bude zhotovena v českém jazyce, bude dodána v elektronické formě ve standardních editovatelných formátech (např. MS Office) používaných Zadavatelem na datovém nosiči a 1x v papírové formě. Papírová forma bude logicky a věcně strukturovaná, bude připravena pro použití (např. provozní dokumentace ICT ve formě vhodné pro použití administrátory v serverovně). Struktura i forma dokumentace bude před předáním předána ke kontrole a výslovně schválena Zadavatelem.

2.2. Plnění Specifických požadavků – Část prvky na segmentaci a ochranu komunikace

(1) Dodané prvky budou konfigurovány jako dva vysoce dostupné clustery v režimu active-active – v každé lokalitě bude umístěn jeden cluster.

(2) Pro nastavení těchto prvků a jejich politik bude převzatá konfigurace stávajících firewallů. V rámci implementace dojde k aktualizaci této konfigurace ve vztahu k optimálnímu využití nabízených prvků a jejich funkcí, s ohledem na doporučení výrobců a autorit v oblasti kybernetické betpečnosti (NÚKIB apod.), s uplatněním osvědčených praktik (best practices).

2.3. Plnění Specifických požadavků – Část Distribuční přepínače a Centrální přepínače

(1) Dodavatel provede analýzu současné síťové topologie (vícenásobná hvězda) v obou lokalitách. V rámci detailního implementačního plánu předloží návrh její optimalizace s využitím nabízených prvků a po schválení Objednatelem zajistí v součinnosti a dozorem zadavatele její realizaci.

(2) Centrální přepínače budou konfigurovány jako vysoce dostupný stoh, který nahradí současný stoh tvořený přepínači HPE 5700 a vytvoří tak novou „core“ vrstu LAN. Pro stávající stoh bude v rámci implementačního plánunavrženo nové umístění v síti pro zvýšení kapacity a dostupnosti sítě.

(3) Přístupové přepínače nahradí stávající zastaralé přepínače v obou lokalitách a doplní topologii tak, aby všechny (bude-li to technicky možné) přístupové porty pro koncová zařízení byly plně řiditelné protokolem IEEE 802.1X a poskytovali rychlost min. 1 Gb.

(4) Topologie sítě bude v maximální míře využívat pokročilé stohovací a agregační technologie pro zjednodušení síťového designu (zejména v oblasti redundance/vysoké dostupnosti) a správy a vyloučení provozně potenciálně náročnějších technologií (spannig tree apod.).

(5) Všechny dodané přepínače budou zařazeny do systému centrální správy, nebo budou s tímto systémem integrovány tak, aby byl zachován plnohodnotný centrální monitoring a správa sítě včetně akualizací firmware prvků, řízení VLAN atd. jedním nástrojem.

(6) Dodavatel provede v KV vybudování 10 optických tras (každá 12 vláken). Trasy budou zakončeny optickou 19“ vanou v racku, kde budou navařena všechna optická vlákna. Trasy povedou teplovodními šachtami. Součástí dodávky je jejich proměření a zadokumentování skutečného stavu. Nově vybudované trasy budou využity k propojení páteřních prvků s distribučními stohy.

(a) 3x Trasa z budovy B do budovy C (1PP RDG, 2NP neurologie, 3NP kardiologie)

- Délka cca 1x 200m, 1x 250m, 1x 300m

(b) 3x Trasa z budovy B do budovy D (-1PP patologie, 1PP mikrobiologie, 2NP OKBH)

- Délka cca 1x 350m, 1x 400m, 1x 450m

(c) 1x Trasa z budovy B do budovy J (energocentrum)

- Délka cca 1x 200m

(d) 1x Trasa z budovy B do budovy H (LSPP zubni, kožní ambulance)

- Délka cca 1x 150m

(e) 1x Trasa z budovy B do budovy E (1NP ambulnace bolesti)

- Délka cca 1x 300m

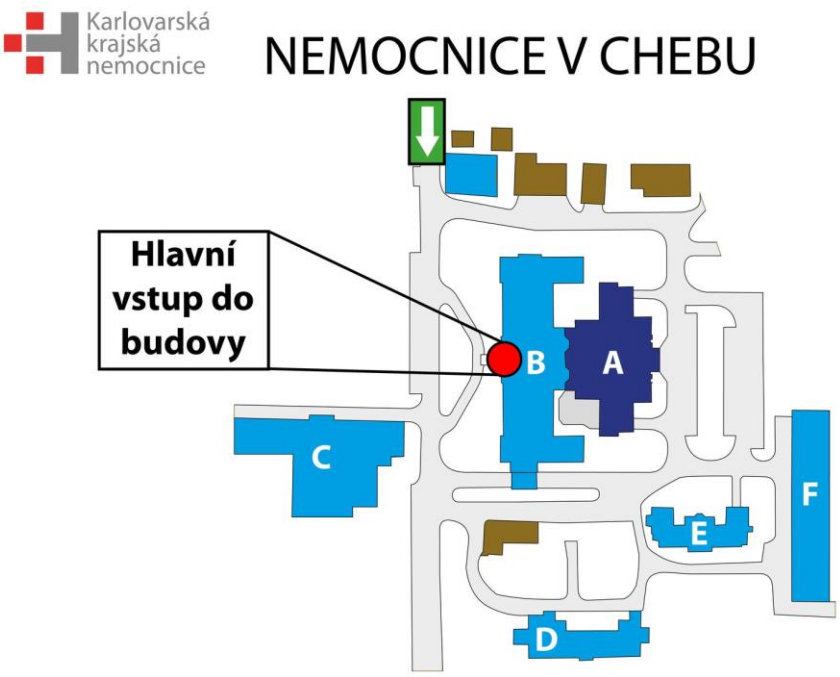
(f) 1x Trasa z budovy B do budovy N (2NP administrativa)

- Dělka cca 1x 150m

(7) Dodavatel provede v CH vybudování 1 optické trasy (12 vláken). Trasa bude zakončena optickou 19“ vanou v racku, kde budou navařena všechna optická vlákna. Trasa povede existujícím kolektorem. Součástí dodávky je jejich proměření a zadokumentování skutečného stavu. Nově vybudovaná trasa bude využita k propojení páteřních prvků s distribučními stohy.

(a) 1x Trasa z budovy A do budovy C

- Dělka cca 1x 150m



2.4. Plnění Specifických požadavků – Fyzické zabezpečení komunikace

(1) Pro zabezpečení nově dodané infrastruktury budou dodány následující zdroje UPS:

Lokalita	Výstupní výkon	Počet
KV	3000 VA	3x
KV	1000 VA	8x
CH	3000 VA	2x
CH	1000 VA	4x

2.5. Specifické požadavky – Část WiFi přístupové body (AP)

(1) Dodavatel provede analýzu současné WiFi sítě v lokalitě Karlovy Vary, návrh její modernizace s využitím nabízených prvků a po schválení Objednatelem její realizaci. Stávající prvky budou nahrazeny nabízenými a využity jinde v organizaci.

(2) Bezdrátová síť bude sloužit pro posílení odolnosti sítě a bude především určena pro provoz a připojení specifických přístrojů – Dodavatel navrhne a implementuje vhodné politiky pro jednotlivé účely použití včetně autentizačních mechanismů.

(3) Bezdrátová síť bude využívat moderní technologie pro maximalizaci „uživatelské zkušenosti“ (rychlost odezvy apod.) – roaming, pásma 2,4 i 5 GHz.

(4) Bezdrátová síť bude centrálně spravovaná a její provoz a správa bude řízen virtuálním kontrolerem, který je nedílnou součástí nabídky.

2.6. Plnění Specifických požadavků – Část Systém řízení přístupu do sítě podle standardu IEEE 802.1X

(1) Součástí implemntačního plánu bude návrh nasazení systému řízení přístupu do sítě podle standardu IEEE 802.1X (NAC) a po schválení objednatelem dojde k jeho implementaci.

(2) Systém bude implementován jako jednotný pro drátovou i bezdrátovou část sítě.

(3) Systém bude využívat stávající centrální identitní systém Active Directory pro autentizaci uživatelů a zařízení.

(4) Systém bude ukládat historii přístupů a bude exportovat ukládané údaje do nadřazeného systému pro správu logů.

2.7. Plnění Specifických požadavků – Část provozně bezpečnostního monitoringu

(1) V rámci projektu bude implementován systém pro provozně bezpečnostní monitoring celého prostředí sítě v obou lokalitách (tj. KV a Ch), tak aby všechny aktivní prvky infrastruktury a serverů byly schopny s tímto systémem komunikovat a ukládat do něj požadované provozní a bezpečnostní logy.

(2) Centrální úložiště pro sběr a analýzu logů s možností následné analýzy a řešení bezpečnostních událostí/incidentů z kritických systémů a aplikací. Systém bude zachovávat originál logů za účelem bezpečnostního auditu a umožňovat splnění legislativních norem a požadavků, zejména pak doložením souladu nabízeného systému s požadavky ISO/ČSN 27001:2013 pro pořizování auditních záznamů. Systém bude shromažďovat provozní data ze všech důležitých systémů na jednom místě a dlouhodobě je uchovávat. Tímto operátor IT/Bezpečnosti dostane možnost zjistit informace o bezpečnostních incidentech, provozních stavech a případných závadách v IT v reálném čase i v pohledu do minulosti nejméně jeden rok zpět. Toto úložiště bude schopné generovat reporty o aktivitách systémů i uživatelů, včetně auditních reportů na vyžádání, nebo se stanovenou periodicitou s definovatelným obsahem, a to bez nutnosti používat SQL syntaxi.

(3) Systém umožňuje procházení těchto logů integrovaným grafickým rozhraním s předdefinovanými pravidly pro rychlé vyhledávání (např. jako jsou změny v systémech provedené administrátory; seznam nově vytvořených účtů v MS AD a Office365 za zvolenou periodu; změny v přístupových právech pro zadaného uživatele nebo k zadané složce; monitoring privilegovaných účtů, sdílených účtů a změn konfigurací; sledování souborových systémů apod.) Dále umožňuje sledovat chování uživatelů a systémů s možností upozorňování na překročení pravidel, a to na základě limitů nebo korelací událostí stanovených administrátorem systému.

(4) Vznikne jednotné úložiště logů s pokročilými nástroji analýzy a upozorňování, ke kterému budou mít přístup pouze autorizovaní pracovníci zadavatele. Systém vylučuje možnost modifikace logů ze strany administrátorů nebo uživatelů. Systém dále umožňuje snadnou klasifikaci dat, tvorbu uživatelsky definovaných parserů, filtrů, upozornění a korelací bez účasti výrobce nebo dodavatele v intuitivním grafickém rozhraní bez nutnosti používat znalostí programátora. Součástí dokumentace bude návod, jak takovéto činnosti provádět, a to včetně vzorových příkladů.

(5) Zálohování konfigurace i dat a jejich obnova je nezbytnou nutností, kterou musí dodaný systém podporovat. Protože není předem známo přesné množství logů vznikajících v naší organizaci, požadujeme, aby dodaný systém podporoval plánované
i ad-hoc zálohování vzniklých dat na externí zálohovací systém, optimálně za využití SMB protokolu. Zálohováním dat na externí systém musí umožnit dosáhnout požadavku na délku uložení logovaných událostí po dobu minimálně 18 měsíců. Platí však, že je nutné, aby systém umožňoval on-line zobrazit hodnoty nad všemi interně uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat.

(6) Pokud jsou v nabízeném řešení zahrnuty jakékoliv licence, jejich legální používání nesmí být časově omezeno. Nabízené řešení tedy musí být plně funkční i po uplynutí doby placené podpory. V případě pochybností o vlastnostech nabízeného systému si Zadavatel vyhrazuje právo vyžádat funkční vzorek nabízeného řešení pro ověření funkčních vlastností a provést ověřovací testy ještě před ukončením výběrového řízení. V tomto případě je dodavatel povinen dodat funkční vzorek do 1 týdne od výzvy zadavatele a poskytnout součinnost s testováním.

(7) Zadavatel vyžaduje, aby nabízené řešení mělo níže požadované funkce již v době podání nabídky, nikoliv aby se jednalo o budoucí funkce plánovaných verzí software pro nabízené řešení.

(8) Systém bude implementován v obou lokalitách, přičemž bude využit a integrován do tohoto řešení existují prvek Zadavatele, což je LogManager ve verzi M, který je v současné době umístěn v datovém centru v lokalitě KV.

(9) Navržený systém splňuje všechny požadavky NÚKIB a vyhlášky č. 82/2018 pro část sběru logů.

(10) Nedílnou součástí tohoto systému bude monitoring síťových toků s možností jejich vyhodnocování a dodatečnými bezpečnostními funkcemi.

2.8. Popis povinných parametrů a funkčních vlastností dodávaného řešení

(1) V dále uvedených tabulkách jsou uvedeny parametry prvků nabízeného řešení.

(2) **Tabulka parametrů a funkčních vlastností řešení**

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Firewall (KV) 2x	Porty	min. 16x 1GbE, 8x 1 Gb SFP (mohou být sdílené) a 2x 10 Gb SFP+	**FortiGate 200F (FG-200F)** 2 x GE RJ45 HA/ MGMT,16 x GE RJ45 Ports, 2 x 10 GE SFP+ Slots, 2 x 10 GE SFP+ FortiLink Slots, 8 x GE SFP Slots	fortigate-200f-series.pdf
	NGFW	min. základní funkce Next-generation firewall - viz https://en.wikipedia.org/wiki/Next-generation_firewall - firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.	funkce Next-generation firewall - s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.	fortigate-200f-series.pdf
	Počet současných spojení	min. 3 miliony	3 miliony	fortigate-200f-series.pdf
	Propustnost SSL VPN	min. 2 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 200 klientů	2 Gbps	fortigate-200f-series.pdf
	Propustnost SSL inspekce	min. 4 Gbps	4 Gbps	fortigate-200f-series.pdf
	Propustnost firewallu	min. 25 Gbps pro pakety 512 bytů a větší	27 Gbps pro pakety 512 bytů a větší	fortigate-200f-series.pdf
	Propustnost NGFW	min. 3 Gbps	3,5 Gbps	fortigate-200f-series.pdf
	Propustnost IPS	min. 5 Gbps	5 Gbps	fortigate-200f-series.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Propustnost detekce škodlivého kódu	min. 3 Gbps	3,5 Gbps	fortigate-200f-series.pdf
	Vysoká dostupnost	režim Active/Active se společnou konfigurací	režim Active/Active se společnou konfigurací	fortigate-200f-series.pdf
	Dualstack	podpora současného běhu IPv4 a IPv6	podpora současného běhu IPv4 a IPv6	fortigate-200f-series.pdf
	Aplikační kontrola	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…)	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…)	fortigate-200f-series.pdf
	Antivir	integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)	integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)	fortigate-200f-series.pdf
	Kategorizace a blokace provozu	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne	fortigate-200f-series.pdf
	Antispam	antispamová a antivirová inspekce elektronické pošty	antispamová a antivirová inspekce elektronické pošty	fortigate-200f-series.pdf
	Sandbox	integrovaný sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro	integrovaný sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované	fortigate-200f-series.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		napojení na externí službu výrobce zařízení (služba součástí dodávky)	rozhraní pro napojení na externí službu výrobce zařízení (služba součástí dodávky)	
	Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení	fortigate-200f-series.pdf
	Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu, podpora SAML pro integraci s autentizačními systémy	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu, podpora SAML pro integraci s autentizačními systémy	fortigate-200f-series.pdf
	Management a monitoring	HTTP/S, SSH, SNMP, syslog	HTTP/S, SSH, SNMP, syslog	fortigate-200f-series.pdf
	SD-WAN	integrovaná podpora SD WAN - min. rozkládání zátěže a vysoká dostupnost více internetových přípojek a VPN	integrovaná podpora SD WAN - rozkládání zátěže a vysoká dostupnost více internetových přípojek a VPN	fortigate-200f-series.pdf
	Sledování toků	přímý export síťových toků (Netflow nebo ekvivalent)	přímý export síťových toků (Netflow nebo ekvivalent)	fortigate-200f-series.pdf
	Standardní funkce	NAT, statické a dynamické routování, publikace interních serverů	NAT, statické a dynamické routování, publikace interních serverů	fortigate-200f-series.pdf
	Virtuální kontext	podpora minimálně 5 virtuálních kontextů	podpora 10 virtuálních kontextů	fortigate-200f-series.pdf
	Kompatibilita	kompatibilita konfiguračních skriptů se stávajícími firewally nebo nástroj na opakovanou konverzi konfiguračních skriptů stávajících firewallů součástí dodávky	kompatibilita konfiguračních skriptů se stávajícími firewally	fortigate-200f-series.pdf
	Záruka	min. 36 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Odesláním náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware	24x7 **Unified Threat Protection** 60 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Odesláním náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní	fortigate-200f-series.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		a bezpečnostních funkcí - URL filtrace, IPS, antimalware, antispam, aplikační kontrola, sandbox)	aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalware, antispam, aplikační kontrola, sandbox)	
Firewall (CH) 2x	Porty	min 12x 1GbE, 4x 1 Gb SFP (mohou být sdílené) a 2x 10 Gb SFP+	**FortiGate 100F (FG-100F)** 2 x GE RJ45 MGMT/DMZ Ports 2 x GE RJ45 WAN Ports 2 x GE RJ45 HA Ports 12 x GE RJ45 Ports 1GbE 2 x 10 GE SFP+ 4 x GE SFP Slots 4 x GE RJ45/ SFP sdílené	fortigate-100f-series.pdf
	NGFW	min. základní funkce Next-generation firewall - viz https://en.wikipedia.org/wiki/Next-generation_firewall - firewall, aplikační firewall s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.	Next-generation firewall - s DPI, IPS. Administrace na bázi "objektů" (aplikace, uživatelů, lokality apod.) namísto IP adres, portů apod.	fortigate-100f-series.pdf
	Počet současných spojení	min. 1,5 miliony	1,5 miliony	fortigate-100f-series.pdf
	Propustnost SSL VPN	min. 1 Gbps, při licenčním nebo technickém omezení počtu klientů požadujeme min. 200 klientů	1 Gbps	fortigate-100f-series.pdf
	Propustnost SSL inspekce	min. 1 Gbps	1 Gbps	fortigate-100f-series.pdf
	Propustnost firewallu	min. 10 Gbps pro pakety 512 bytů a větší	18 Gbps pro pakety 512 bytů a větší	fortigate-100f-series.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Propustnost NGFW	min. 1,5 Gbps	1,6 Gbps	fortigate-100f-series.pdf
	Propustnost IPS	min. 2,5 Gbps	2,6 Gbps	fortigate-100f-series.pdf
	Propustnost detekce škodlivého kódu	min. 1 Gbps	1 Gbps	fortigate-100f-series.pdf
	Vysoká dostupnost	režim Active/Active se společnou konfigurací	režim Active/Active se společnou konfigurací	fortigate-100f-series.pdf
	Dualstack	podpora současného běhu IPv4 a IPv6	podpora současného běhu IPv4 a IPv6	fortigate-100f-series.pdf
	Aplikační kontrola	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…)	detekce, monitoring, povolení či zakázání obvyklých síťových aplikací na základě signatury dané aplikace, nikoliv dle portu Kontrola komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…)	fortigate-100f-series.pdf
	Antivir	integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)	integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd)	fortigate-100f-series.pdf
	Kategorizace a blokace provozu	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne	založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne	fortigate-100f-series.pdf
	Antispam	antispamová a antivirová inspekce elektronické pošty	antispamová a antivirová inspekce elektronické pošty	fortigate-100f-series.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Sandbox	integrovaný sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba součástí dodávky)	integrovaný sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba součástí dodávky)	fortigate-100f-series.pdf
	Aktualizace	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení	automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení	fortigate-100f-series.pdf
	Ověřování uživatelů	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu, podpora SAML pro integraci s autentizačními systémy	LDAP, Active Directory, Single Sign On vůči Active Directory, Radius, Ověřování na základě certifikátu, podpora SAML pro integraci s autentizačními systémy	fortigate-100f-series.pdf
	Management a monitoring	HTTP/S, SSH, SNMP, syslog	HTTP/S, SSH, SNMP, syslog	fortigate-100f-series.pdf
	SD-WAN	integrovaná podpora SD WAN - min. rozkládání zátěže a vysoká dostupnost více internetových přípojek a VPN	integrovaná podpora SD WAN - min. rozkládání zátěže a vysoká dostupnost více internetových přípojek a VPN	fortigate-100f-series.pdf
	Sledování toků	přímý export síťových toků (Netflow nebo ekvivalent)	přímý export síťových toků (Netflow nebo ekvivalent)	fortigate-100f-series.pdf
	Standardní funkce	NAT, statické a dynamické routování, publikace interních serverů	NAT, statické a dynamické routování, publikace interních serverů	fortigate-100f-series.pdf
	Virtuální kontext	podpora minimálně 5 virtuálních kontextů	podpora 10 virtuálních kontextů	fortigate-100f-series.pdf
	Kompatibilita	kompatibilita konfiguračních skriptů se stávajícími firewally nebo nástroj na opakovanou konverzi konfiguračních skriptů stávajících firewallů součástí dodávky	kompatibilita konfiguračních skriptů se stávajícími firewally	fortigate-100f-series.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Záruka	min. 36 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Odesláním náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalware, antispam, aplikační kontrola, sandbox)	24x7 **Unified Threat Protection** 60 měsíců v režimu 24x7 poskytovaná výrobcem zařízení. Odesláním náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a bezpečnostních funkcí - URL filtrace, IPS, antimalware, antispam, aplikační kontrola, sandbox)	fortigate-100f-series.pdf
Distribuční přepínače 24x	Základní parametry	L2/L3 přepínač v rackovém provedení, neblokovaná architektura	Aruba 6200M 48G Class4 PoE 4SFP+ Switch R8Q70A + zdroj 680W JL086A	CX 6200.pdf
	Porty a propustnost	min. 48x 1 GbE a 4x 1/10 Gb SFP+, minimální neblokovaná přepínací propustnost switche 176 Gb	48 portů 1GbE PoE+ a 4 porty 1/10 b SFP+, neblokovaná přepínací propustnost 176 Gbps	CX 6200.pdf
	PoE	podpora IEEE 802.3at a IEEE 802.3af na všech metalických portech, celkový PoE výkon min. 370 W	podpora IEEE 802.3at a IEEE 802.3af na všech metalických portech, celkový PoE více než 400W (max. 1440W se 2 napájecími zdroji)	CX 6200.pdf
	Agregace portů	podpora minimálně LACP	Podpora EEE 802.3ad LACP	CX 6200.pdf
	Směrování	hardwarové statické routování včetně VLAN, dynamické směrování min. RIP a OSPF	hardwarové statické routování včetně VLAN, dynamické směrování RIPv2 a OSPFv2	CX 6200.pdf
	Řízení provozu	víceúrovňový QoS, klasifikace provozu na L2-L4, podpora min. standardu 802.1p, limitace na úrovni portu a VLAN	víceúrovňový QoS, klasifikace provozu na L2-L4, podpora standardu 802.1p, limitace na úrovni portu a VLAN	CX 6200.pdf qos_6200.pdf
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN a přidělení QoS	CX 6200.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
			a přístupových filtrů na základě 802.1X ověření	
	Ověřování uživatelů a zařízení	podpora 802.1x	podpora IEEE 802.1X	CX 6200.pdf
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování, QoS a správy	plný IPv4 a IPv6 dualstack včetně směrování, QoS a správy	CX 6200.pdf
	Monitoring a správa	plná podpora CLI, SSHv2, SNMPv3, syslog, sFlow, web HTTP/S rozhraní, správa prostřednictvím cloudového nebo on-premise managementu výrobce	plná podpora CLI, SSHv2, SNMPv3, syslog, sFlow, web HTTP/S rozhraní, správa prostřednictvím cloudového nebo on-premise managementu výrobce	CX 6200.pdf
	MAC	podpora min. 10 000 MAC adres	Podpora 16 000 MAC adres	CX 6200.pdf
	Centrální správa	podpora monitorování a centrální správy včetně sledování vytížení, zobrazení a ovládání portů, upgrade a verzování firmware, konfigurace VLAN, vizualizace topologie v reálném čase	podpora monitorování a centrální správy včetně sledování vytížení, zobrazení a ovládání portů, upgrade a verzování firmware, konfigurace VLAN, vizualizace topologie v reálném čase - součást **Systém pro správu a monitorování**	CX 6200.pdf
	Stohování	pokročilé stohování po standardních SFP+ portech - 2 a více přepínačů ve stohu, které se chovají jako jeden z pohledu správy i připojených zařízení.	pokročilé stohování VSF po standardních SFP+ portech - 2 a více přepínačů ve stohu, které se chovají jako jeden z pohledu správy i připojených zařízení.	CX 6200.pdf
	Zrcadlení provozu	zrcadlení síťového provozu portu(ů) a VLAN na lokální nebo vzdálený port, možnost výběru provozu např. ACL	zrcadlení síťového provozu portu(ů) a VLAN na lokální nebo vzdálený port, možnost výběru provozu např. ACL	CX 6200.pdf
	Podporované standardy	Podpora minimálně těchto standardů: IEEE 802.3ad, 802.1x, 802.1ax, 802.1AE	Podpora standardů IEEE 802.3ad, 802.1x, 802.1ax, 802.1AE	CX 6200.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Záruka	min. 36 měsíců poskytovaná výrobcem zařízením, včetně nároku na opravné verze firmware. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	Doživotní záruka poskytovaná výrobcem zařízením, včetně nároku na opravné verze firmware. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	CX 6200.pdf
Centrální přepínače 2 ks	Základní parametry	L2/L3 přepínač v rackovém provedení	**Aruba 8360- 48Y6C v2** MACsec, Front-to-Back 5 Fans, 2 AC Power Supplies, JL704C	CX 8360_v2.pdf
	Porty	min. 48x 1/10 Gb SFP+, 6x 40/100Gb QSFP28 a vyhrazený 1 Gb port pro správu (out-of-band management)	48 portů 1Gb/10Gb/25Gb 6 portů 40GbE/100GbE (QSFP+/QSFP28) 1x vyhrazený 1Gb RJ-45 port pro out-of-band management	CX 8360_v2.pdf
	Propustnost	neblokovaná architektura, přepínání/směrování min. 1 Tbps	neblokovaná architektura, přepínání/směrování 4.8 Tbps	CX 8360_v2.pdf
	Agregace portů	podpora LACP	Podpora IEEE 802.3ad LACP	CX 8360_v2.pdf
	Směrování	statické a dynamické routování včetně VLAN, min. RIPv2, podpora IPv4 a IPv6, min. 8000 statických routovacích záznamů pro každou verzi IP	Statické i dynamické (BGP, OSPF) routování, podpora IPv4 a IPv6, 145 780 routovacích záznamů pro každou verzi IP	CX 8360_v2.pdf
	Řízení provozu	víceúrovňový QoS, klasifikace provozu min na L2 a L3 včetně DSCP hodnot, podpora standardu 802.1p, prioritizace a limitace na úrovni portu a VLAN	Víceúrovňový QoS s klasifikací provozu na L2 i L3 včetně DSCP (Differentiated Service Code Point) hodnot, prioritizace a limitace na úrovni portu i VLAN. Podpora standardu IEEE 802.1p	qos_8360.pdf
	VLAN	VLAN 802.1Q, MAC i protocol based, podpora zařazování do VLAN na základě 802.1X ověření, podpora Q-In-Q a VXLAN	VLAN IEEE 802.1Q, MAC i protocol based, podpora zařazování do VLAN na základě 802.1X ověření, podpora Q-In-Q a VXLAN	l2_bridging_83xx.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Ověřování uživatelů a zařízení	podpora 802.1X	Plná podpora IEEE 802.1X	CX 8360_v2.pdf
	Dualstack	plný IPv4 a IPv6 dualstack včetně směrování a QoS	plný IPv4 a IPv6 dualstack včetně směrování a QoS	CX 8360_v2.pdf
	MAC, ARP	podpora min. 64 000 MAC adres a min. 64 000 ARP záznamů	Podpora 212 992 MAC adres a 140 000 ARP záznamů	CX 8360_v2.pdf
	Centrální správa	podpora monitorování a centrální správy včetně sledování vytížení, zobrazení a ovládání portů, upgrade a verzování firmware, konfigurace VLAN, vizualizace topologie v reálném čase	Podpora monitorování a centrální správy včetně sledování vytížení, zobrazení a ovládání portů, upgrade a verzování firmware, konfigurace VLAN, vizualizace topologie v reálném čase – součást **Systém pro správu a monitorování**	CX 8360_v2.pdf
	Stohování	pokročilé stohování po standardních portech 40 Gb – 2 přepínače ve stohu se chovají jako jeden z pohledu správy i připojených zařízení, přepínač musí umožňovat redundantní stohovací spoje s celkovou propustností min. 80 Gbps	pokročilé stohování po standardních portech 40 Gb – 2 přepínače ve stohu se chovají jako jeden z pohledu správy i připojených zařízení, přepínač musí umožňuje redundantní stohovací spoje s celkovou propustností min. 80 Gbps	CX 8360_v2.pdf
	Zrcadlení provozu	zrcadlení síťového L2 a L3 provozu portu(ů)na lokální nebo vzdálený port, řízení obsahu zrcadleného provozu na základě definovaných kritérií	zrcadlení síťového L2 a L3 provozu portu(ů)na lokální nebo vzdálený port, řízení obsahu zrcadleného provozu na základě definovaných kritérií	CX 8360_v2.pdf
	Podporované standardy	Podpora minimálně těchto standardů: IEEE 802.3ad, 802.1x, 802.1ax, 802.1AE	Podpora standardů IEEE 802.3ad, 802.1x, 802.1ax, 802.1AE	CX 8360_v2.pdf
	Napájení	interní redundantní zdroje (min 2) vyměnitelné za provozu a ventilátory	interní redundantní zdroje (min 2) vyměnitelné za provozu a ventilátory	CX 8360_v2.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Monitoring a správa	plná podpora CLI, SSHv2, SNMPv3, syslog, sFlow, RMON, web rozhraní HTTP/S	plná podpora CLI, SSHv2, SNMPv3, syslog, sFlow, RMON, web rozhraní HTTP/S	CX 8360_v2.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem zařízením, včetně nároku na opravné verze firmware. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	Doživotní záruka poskytovaná výrobcem zařízením, včetně nároku na opravné verze firmware. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	CX 8360_v2.pdf
WiFi přístupové body (AP) 60 ks	Základní funkce	přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na stěnu nebo strop	R2H22A **Aruba AP-504** JW009A AP-ANT-1W 2.4/5G 4/6dBi Omni Q9G71A AP-MNT-MP10-D Campus AP mount bracket kit přístupový bod (AP) standardu Wi-Fi 6 včetně montážního materiálu na stěnu nebo strop	ARUBA AP500.pdf
	Frekvence	činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly s podporou standardu OFDMA	činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly s podporou standardu OFDMA	ARUBA AP500.pdf
	Anténní systém	externí systém pro min. 2x 2 MIMO, optimalizovaný pro montáž na stěnu, dvě antény (2.4 a 5 GHz) součástí dodávky	externí systém pro 2x 2 MIMO, optimalizovaný pro montáž na stěnu, dvě antény (2.4 a 5 GHz) součástí dodávky	ARUBA AP500.pdf
	Přenosové rychlosti	SU-MIMO 5GHz min 1200Mbps, SU-MIMO 2.4 GHz min. 550Mbps	SU-MIMO 5GHz 200Mbps, SU-MIMO 2.4 GHz 574Mbps	ARUBA AP500.pdf
	Standardy	podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN	podpora 802.3at, 802.11n, 802.11ax, 802.1x včetně přiřazování do VLAN	ARUBA AP500.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Řízení klientů	automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)	automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)	ARUBA AP500.pdf
	Rušení	detekce non-WiFi/WiFi rušení/interference a spektrální analýza	detekce non-WiFi/WiFi rušení/interference a spektrální analýza	ARUBA AP500.pdf
	Multi SSID	podpora vysílání min. 16 SSID (WiFi sítí) současně v obou pásmech, podpora přiřazení každého SSID samostatné VLAN	podpora vysílání min. 16 SSID (WiFi sítí) současně v obou pásmech, podpora přiřazení každého SSID samostatné VLAN	ARUBA AP500.pdf
	Zatížení	min. 250 přiřazených (asociovaných) klientů na radiový modul	256 přiřazených (asociovaných) klientů na radiový modul	ARUBA AP500.pdf
	Porty	min. 1x 1Gb, PoE s podporou standardů 802.3at a 802.3af	1x 1Gb, PoE s podporou standardů 802.3at a 802.3af	ARUBA AP500.pdf
	Řízení provozu	klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu	klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu	ARUBA AP500.pdf
	Řízení kvality služeb	automatické řízení kvality služeb (QoS) pro hlas a video	automatické řízení kvality služeb (QoS) pro hlas a video	ARUBA AP500.pdf
	Současná obsluha více klientů	podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output	podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output	ARUBA AP500.pdf
	Bezpečnost	Integrovaný bezpečnostní modul TPM pro uložení citlivých údajů (přihlašovací údaje, šifrovací klíče apod.). Detekce škodlivých přístupových bodů.	Integrovaný bezpečnostní modul TPM pro uložení citlivých údajů (přihlašovací údaje, šifrovací klíče apod.). Detekce škodlivých přístupových bodů.	ARUBA AP500.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Virtuální kontroler	virtuální, vysoce dostupný kontroler. Musí umožnit kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů. Zadavatelem akceptované možnosti jsou: cloud (nicméně při zachování ostatních požadavků v zadávací dokumentaci, tj. schopnost fungování při nedostupnosti sítě Internet), management aplikace, HW appliance či bez potřeby externích systémů (například sdílením v rámci jednotlivých AP).	virtuální, vysoce dostupný kontroler. Umožňuje kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů. Zadavatelem akceptované možnosti jsou: cloud (nicméně při zachování ostatních požadavků v zadávací dokumentaci, tj. schopnost fungování při nedostupnosti sítě Internet), management aplikace, HW appliance či bez potřeby externích systémů (například sdílením v rámci jednotlivých AP).	ARUBA AP500.pdf
	WPA, OE	podpora standardu WPA3 (Wi-Fi Protected Access III) a Enhanced Open	podpora standardu WPA3 (Wi-Fi Protected Access III) a Enhanced Open	ARUBA AP500.pdf
	Monitoring a správa	podpora monitorování a centrální správy včetně sledování vytížení, upgrade a verzování firmware, konfigurace VLAN, plná podpora SSH, SNMP 1-3, syslog	podpora monitorování a centrální správy včetně sledování vytížení, upgrade a verzování firmware, konfigurace VLAN, plná podpora SSH, SNMP 1-3, syslog	ARUBA AP500.pdf
	Správa frekvenčního pásma	automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference	automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference	ARUBA AP500.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem zařízením, včetně nároku na opravné verze firmware. Odeslání náhradního zařízení max.	Doživotní záruka poskytovaná výrobcem zařízením, včetně nároku na opravné verze firmware. Odeslání náhradního zařízení max. následující pracovní den po	ARUBA AP500.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	nahlášení závady, nahlašování závad v režimu 24x7	
Systém řízení přístupu do sítě podle standardu IEEE 802.1X	Provedení	softwarová appliance pokročilého NAC (network access control) na bázi standardu IEEE 802.1X. Integrovaná podpora autentizace, autorizace a účtování (přístupů) uživatelů i koncových zařízení, integrovaný RADIUS server a databáze uživatelů a zařízení	**Aruba ClearPass Policy Manager + licence pro 3000 zařízení (trvalé licence)**	Aruba ClearPass.pdf
	Nastavení přístupů	nastavení síťového přístupu uživatelů a zařízení podle politik min. pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém	Umožňuje nastavení síťového přístupu uživatelů a zařízení podle politik pomocí přiřazení VLAN, ACL. Atributy pro definici politik min. IP, MAC, port, VLAN, QinQ VLAN, hostname (PC name), uživatelské jméno (z Active Directory), operační systém	Aruba ClearPass.pdf
	Autentizace	zajištění IEEE 802.1X autentizace a autorizace pro bezdrátové sítě, Ethernet LAN sítě a VPN	Poskytuje IEEE 802.1X autentizaci a autorizaci pro bezdrátové sítě, Ethernet LAN sítě a VPN	Aruba ClearPass.pdf
	Základní autentizační metody	min. PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace, certifikáty	Obsahuje autentizační mechanismy PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC, certifikáty	Aruba ClearPass.pdf
	Identity	vestavěná databáze identit pro autentizaci, podpora standardních identitních databází - Active Directory, LDAP, ODBC	Integrovaná databáze identit pro autentizaci, podpora standardních identitních databází - Active Directory, LDAP, ODBC	Aruba ClearPass.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Nezávislá autentizace a autorizace	úplné oddělení autentizace a autorizace, např. autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi.	Umožňuje úplné oddělení autentizace a autorizace, včetně autentizace proti službě Active Directory, ale autorizace proti externí SQL databázi.	Aruba ClearPass.pdf
	Rozšířená autentizace a autorizace	podpora autentizace a autorizace min. LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta).	Vestavěná podpora autentizace a autorizace LDAP, Microsoft Active Directory, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On SAML 2+ IdP a SP, OAuth, Shibboleth a Okta.	Aruba ClearPass.pdf
	Kontexová autorizace	autorizace zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory	Umožňuje autorizaci zařízení a uživatelů na základě kontextových informací jako čas, typ připojení, osobní profil či členství ve skupině v Active Directory	Aruba ClearPass.pdf
	Externí identity	podpora autentizace externími identitami - min. Microsoft, Google	Podporuje autentizaci externími identitami Microsoft, Google	Aruba ClearPass.pdf
	Komplexní autorizace	autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. pro omezení celkového času online či objemu přenesených dat za delší časové období	Umožňuje autorizaci uživatelů na základě jejich vlastních accounting informací z předchozích připojení včetně omezení celkového času online či objemu přenesených dat za delší časové období	Aruba ClearPass.pdf
	Dynamická autorizace	podpora RADIUS CoA podle RFC3576. Možnost změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení.	Plně podporuje RADIUS CoA podle RFC3576. Umožňuje změnit autorizační stav zařízení bez nutnosti změny definice autorizační politiky, včetně odpojení nebo karantény koncových zařízení.	Aruba ClearPass.pdf
	Izolace klientů	zpracovávání syslog zpráv z externích zdrojů, vyhledávání definovaných událostí a	Umožnuje zpracovávání syslog zpráv z externích zdrojů, vyhledávání	Aruba ClearPass.pdf CPPM TechNote.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		automatizovaná reakce na ně. Minimálně v rozsahu příjmu zpráva ze stávajícího firewallu a izolace konkrétního klienta na základě těchto zpráv	definovaných událostí a provádění automatizovaných reakcí na ně. Podporuje příjem zpráv ze stávajícího firewallu Fortinet a izolaci konkrétního klienta na základě těchto zpráv	
	Bezpečnost	podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky (např. překročení objemu dat, časového intervalu, stavu zařízení apod.)	Integrovaná podpora okamžitého odpojení zařízení při vypršení libovolné autorizační podmínky, včetně překročení objemu dat, časového intervalu, stavu zařízení a dalších podmínek.	Aruba ClearPass.pdf
	Správa	vestavěné nástroje pro testování politik, diagnostiku chování systému i spravovaných zařízení	Součástí produktu jsou integrované nástroje pro testování a ladění politik, diagnostiku systému i spravovaných zařízení.	Aruba ClearPass.pdf
	Ochrana identit	veškeré identitní údaje v systému budou uložena ve výrobcem dodané a podporované šifrované databázi, které bude nativní součástí dodaného produktu, s minimální enkrypcí uložených dat ve standardu AES min. 128-bit.	Všechny identitní údaje jsou uloženy v nativní integrované databázi dodané a podporované výrobcem. Data jsou šifrována standardem AES-256	ClearPass_release_note. pdf
	Speciální zařízení	podpora autentizace a řízení přístupů speciálních ("nepočítačových") zařízení např. tiskárny, modality, technologické prvky, IoT	Systém podporuje autentizaci i řízení přístupů speciálních ("nepočítačových") zařízení včetně tiskáren, modalit, technologických prvků, IoT zařízení.	Aruba ClearPass.pdf
	Vysoká dostupnost	integrovaná podpora vysoké dostupnosti v režimu active-active, tj. vytvoření clusteru min. 2 appliance. Druhá appliance není součástí dodávky	Systém obsahuje podporu vysoké dostupnosti v režimu active-active. Lze jej doplnit o druhou appliance a vytvořit cluster. Licence druhů appliance není součástí nabídky.	Aruba ClearPass.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Licence	Licence (tzn. licence/právo používat na dobu min 10 let) pro min. 3000 současně připojených koncových zařízení ověřovaných pomocí 802.1X	Trvalé licence Aruba ClearPass Policy Manager + 3000 zařízení	Aruba ClearPass.pdf
	Automatizace a integrace	REST-API rozhraní min. pro základní funkce AAA, příjem syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Tvorba/modifikace vlastních parserů syslog	Integrované REST-API pro základní i rozšířené funkce,	Aruba ClearPass.pdf
	Kompatibilita	appliance určena pro provoz v prostředí stávající serverové virtualizace	Appliance systému je určena pro provoz v prostředí stávající serverové virtualizace Hyper-V	Aruba ClearPass.pdf
	Záruka	záruka min. 36 měsíců v místě instalace, včetně podpory výrobce a nároku na nové verze software včetně aktualizací	Záruka 36 měsíců v místě instalace, včetně podpory výrobce a nároku na nové verze software včetně aktualizací	Zahrnuto v nabídce
Systém pro správu a monitorování	Licence	licence (tzn. licence/právo používat na dobu min 10 let) pro kompletní stávající i nově pořízené prvky řešení stávajícího systému pro provozní monitorování a správu síťových prvků, Wi-Fi a NAC	**Trvalé licence HPE/Aruba IMC, Airwave, Clearpass a dodavatelských úprav/rozšíření/skriptů** pro kompletní stávající i nově pořízené prvky řešení stávajícího systému pro provozní monitorování a správu síťových prvků, Wi-Fi a NAC licence. Trvalá licence je licence/právo používat na dobu min 10 let	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
	Podporovaná zařízení	centrální management (cloudový, on-premise nebo kombinovaný) navrhované infrastruktury včetně bezdrátové sítě a prvků třetích stran (tj. i existujících prvků v prostředí KKN)	Centrální management on-premise navrhované infrastruktury včetně bezdrátové sítě a prvků třetích stran (tj. i existujících prvků v prostředí KKN)	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Základní vlastnosti management nástroje	klient – Server architektura	klient – Server architektura	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		požadovaný formát zařízení VA (virtual appliance) pro server na platformě vmware nebo hyper-v nebo kvm	Formát zařízení VA (virtual appliance) pro server na platformě vmware nebo hyper-v nebo kvm – součásti řešení v rámci nabízených licencí budou dodány ve formátu jednotné (zintegrované) virtuální appliance pro stávající platformu Hyper-V	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		plnohodnotná klientská část podporovaná na operačních systémech Linux, Windows i OS X	Plnohodnotná klientská část podporovaná na operačních systémech Linux, Windows i OS X – plnohodnotným a nativním klientem nabízeného řešení je webová aplikace podporovaná v prohlížečích v operačních systémech Linux, Windows i OS X	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		plnohodnotný přístup přes HTML pomocí webového prohlížeče (minimálně Edge, Firefox, Chrome)	Plnohodnotný přístup přes HTML pomocí běžných webových prohlížečů, včetně Edge, Firefox, Chrome	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		víceúrovňová práva přístupu, podpora paralelní práce více uživatelů	Víceúrovňová práva přístupu, podpora paralelní práce více uživatelů je standardně podporována	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		podpora autentizace operátorů pomocí LDAP, Radius	Podpora autentizace operátorů pomocí LDAP i Radius	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		RBAC = rozdílní uživatelé mají práva k rozdílným prvkům a rozdílným funkcionalitám	Podpora RBAC = rozdílní uživatelé mají práva k rozdílným prvkům a rozdílným funkcionalitám	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Požadované funkcionality	podpora IPv4 i IPv6	podpora IPv4 i IPv6	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		podpora SNMPv1, SNMPv2, SNMPv3, AES pro SNMPv3 (netSNMP)	podpora SNMPv1, SNMPv2, SNMPv3, AES pro SNMPv3 (netSNMP)	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		periodická záloha vlastní konfigurace	Automatická periodická záloha vlastní konfigurace	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		import MIB třetích stran	import MIB třetích stran	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		pro všechna dodávaná síťová zařízení podpora minimálně v následujícím rozsahu: - záloha a obnovení konfigurace - aktualizace firmware - nastavení syslog a trap cílů - zobrazení a nastavení data a času, zobrazení uptime - detekce a zobrazení L2 topologie sítě formou mapy - vyhledávání koncových zařízení na síti přes IP, Subnet, MAC, uživatelské jméno - načítání informací z MIB – spanning tree info, spanning tree port statistics, resources utilization, Inventory, VLAN, LACP, MSTP, interface utilization, možnost definice vlastních tabulek/pohledů	Podpora všech dodávaná síťová zařízení v následujícím rozsahu: - záloha a obnovení konfigurace - aktualizace firmware - nastavení syslog a trap cílů - zobrazení a nastavení data a času, zobrazení, uptime - detekce a zobrazení L2 topologie sítě formou mapy - vyhledávání koncových zařízení na síti přes IP, Subnet, MAC, uživatelské jméno - načítání informací z MIB – spanning tree info, spanning tree port statistics, resources utilization, Inventory, VLAN, LACP, MSTP, interface utilization, možnost definice vlastních tabulek/pohledů	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		- export a periodický export zobrazovaných hodnot minimálně do html a csv - vizualizace zařízení (porty, sloty)	- export a periodický export zobrazovaných hodnot minimálně do html a csv - vizualizace zařízení (porty, sloty)	
	Správa bezpečnostních profilů	bezpečnostní přístupový profil je kombinace minimálně VLAN, L2-L4 ACL, L2-L4 QoS pravidel	bezpečnostní přístupový profil je kombinace VLAN, L2-L4 ACL, L2-L4 QoS pravidel	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		vytváření, správa, rušení bezpečnostních přístupových profilů centrálně s automatickou distribucí do aktivních prvků i WiFi sítě	Vytváření, správa, rušení bezpečnostních přístupových profilů centrálně s automatickou distribucí do aktivních prvků i WiFi sítě	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		aplikování bezpečnostního přístupového profilu na port aktivního prvku	Aplikování bezpečnostního přístupového profilu na port aktivního prvku	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		SNMP trap server, Syslog server, BootP server	SNMP trap server, Syslog server, BootP server	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		podpora vyčítání a zobrazování RMON	podpora vyčítání a zobrazování RMON	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		možnost reakce na přijatý trap a syslog, výpadek konektivity pomocí technik email, trap, syslog, spuštění skriptu	Možnost reakce na přijatý trap a syslog, výpadek konektivity pomocí technik email, trap, syslog, spuštění skriptu	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		network discovery na základě IP rozsahu, rekurzivního dotazování sousedů	Network discovery na základě IP rozsahu, rekurzivního dotazování sousedů	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Správa konfigurací	hromadná záloha konfigurace ze spravovaných zařízení pomocí TFTP, SCP, FTP	hromadná záloha konfigurace ze spravovaných zařízení pomocí TFTP, SCP, FTP	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		automatická záloha konfigurace spravovaných zařízení minimálně jednou, denně, týdně, při startu	automatická záloha konfigurace spravovaných zařízení jednou, denně, týdně, při startu nebo volitelně dle požadavků správce	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		inventarizace sériových čísel jednotlivých komponent (zdroje, moduly)	inventarizace sériových čísel jednotlivých komponent (zdroje, moduly)	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		obnovení konfigurace	Podpora obnovení konfigurace	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		klonování konfigurace z jednoho prvku na druhý	Podpora klonování konfigurace z jednoho prvku na druhý	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		vytváření, správa a aplikování konfiguračních šablon na aktivní prvky	Vytváření, správa a aplikování konfiguračních šablon na aktivní prvky	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
	Minimální požadavky na reporting	generování reportu na vyžádání	generování reportu na vyžádání	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		naplánování odeslání reportu do emailu (hodinově, denně, týdně, měsíčně)	naplánování odeslání reportu do emailu (hodinově, denně, týdně, měsíčně)	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		porty s nejvyšším vytížením, chybovostí, nejnižší dostupností	porty s nejvyšším vytížením, chybovostí, nejnižší dostupností	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		nejdéle nevyužívané porty	nejdéle nevyužívané porty	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		prvky s nejvyšším vytížením byte/packet, vytížení CPU, vytížením paměti	prvky s nejvyšším vytížením byte/packet, vytížení CPU, vytížením paměti	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		systém musí být schopen zobrazit o všech zařízeních v síti minimálně následující informace: MAC, IP, hostname, typ zařízení, uživatelské jméno, port / SSID+AP, aktivní prvek, stav připojen/odpojen, health check, první a poslední výskyt zařízení	systém bude schopen zobrazit o všech zařízeních v síti minimálně následující informace: MAC, IP, hostname, typ zařízení, uživatelské jméno, port / SSID+AP, aktivní prvek, stav připojen/odpojen, health check, první a poslední výskyt zařízení	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		systém musí být schopen vyhledat zařízení minimálně na základě následujících kritérií: MAC, IP, hostname, typ zařízení, username, port / SSID+AP, aktivní prvek, stav připojení připojen/odpojen, risk status, čas prvního a posledního výskytu	systém bude schopen vyhledat zařízení minimálně na základě následujících kritérií: MAC, IP, hostname, typ zařízení, username, port / SSID+AP, aktivní prvek, stav připojení připojen/odpojen, risk status, čas prvního a posledního výskytu	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		systém musí být schopen udržovat minimálně 30-ti denní historii o kterémkoliv zvoleném zařízení v síti, a to v minimálně v následujícím rozsahu: IP, hostname, typ zařízení, uživatelské jméno, port /SSID+AP, aktivní prvek, stav připojen/odpojen, health check.	systém bude schopen udržovat minimálně 30-ti denní historii o kterémkoliv zvoleném zařízení v síti, a to v minimálně v následujícím rozsahu: IP, hostname, typ zařízení, uživatelské jméno, port /SSID+AP, aktivní prvek, stav připojen/odpojen, health check.	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		systém musí být schopen zobrazit informace o aktuálním i historickém stavu, statistikách,	systém bude schopen zobrazit informace o aktuálním i historickém stavu,	Central management.pdf Aruba ClearPass.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		vytížení aktivního prvku/AP kde je hledané zařízení připojeno	statistikách, vytížení aktivního prvku/AP kde je hledané zařízení připojeno	HPE IMC.pdf
		systém musí umožňovat export informací do externího úložiště (Log management, SIEM) v uživatelsky definovaném formátu	systém umožní export informací do externího úložiště (Log management, SIEM) v uživatelsky definovaném formátu	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		systém musí být schopen vygenerovat email při změně stavu zařízení	systém bude schopen vygenerovat email při změně stavu zařízení	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
	Podpora automatizace	na nově přidaný aktivní prvek do sítě je automaticky (bez zásahu obsluhy) nainstalován referenční firmware	na nově přidaný aktivní prvek do sítě lze automaticky (bez zásahu obsluhy) nainstalovat referenční firmware	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		na nově přidaný aktivní prvek do sítě jsou automaticky (bez zásahu obsluhy) distribuovány konfigurace VLAN, SYSLOG a SNMP trap cílů	na nově přidaný aktivní prvek do sítě lze automaticky (bez zásahu obsluhy) distribuovat konfigurace VLAN, SYSLOG a SNMP trap cílů	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		na nově přidaný aktivní prvek do sítě jsou automaticky (bez zásahu obsluhy) distribuovány konfigurace bezpečnostních profilů	na nově přidaný aktivní prvek do sítě lze automaticky (bez zásahu obsluhy) distribuovat konfigurace bezpečnostních profilů	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		na nově přidaný aktivní prvek do sítě jsou automaticky (bez zásahu obsluhy) distribuovány konfigurace Radius serverů	na nově přidaný aktivní prvek do sítě lze automaticky (bez zásahu obsluhy) distribuovat konfigurace Radius serverů	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		definice akcí, které je možné spustit v určeném pořadí (akcí může být minimálně CLI skript, SNMP komunikace, volání API či spuštění skriptu na management stanici)	Podpora definice akcí, které je možné spustit v určeném pořadí - akcí může být CLI skript, SNMP komunikace, volání API či spuštění skriptu na management stanici	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		mezi akcemi je možno používat podmínečné větvení na základě výsledku předchozí akce	mezi akcemi lze používat podmínečné větvení na základě výsledku předchozí akce	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		mezi akcemi je možno používat podmínečné větvení na základě hodnoty proměnné	mezi akcemi lze používat podmínečné větvení na základě hodnoty proměnné	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
	Správa uživatelů	podpora autentizace pomocí LDAP, Radius	podpora autentizace pomocí LDAP, Radius	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		RBAC (rozdílní uživatelé mají práva k rozdílným prvkům a rozdílným funkcionalitám)	Podpora RBAC - rozdílní uživatelé mají práva k rozdílným prvkům a rozdílným funkcionalitám	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		konfigurace, monitoring i reporting systému přes HTTPs rozhraní ve standardním webovém prohlížeči (minimálně Edge, Firefox, Chrome)	konfigurace, monitoring i reporting systému přes HTTPs rozhraní ve standardním webovém prohlížeči včetně Edge, Firefox, Chrome	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		možnost systém rozšířit o služby agentového skenování (assessmentu) pouze aplikací licenčního klíče	možnost systém rozšířit o služby agentového skenování (assessmentu) i bez aplikací licenčního klíče (v rámci nabízených licencí)	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		systém musí být schopen výměny informací s dalšími systémy (otevřené a dokumentované API). API musí poskytnout minimálně následující funkce: při dotazu na MAC či IP či hostname poskytnout informace: MAC, IP, hostname, typ zařízení, uživatelské jméno, port / SSID+AP, aktivní prvek, stav	systém bude schopen výměny informací s dalšími systémy (otevřené a dokumentované API). API musí poskytnout minimálně následující funkce: při dotazu na MAC či IP či hostname poskytnout informace: MAC, IP, hostname, typ zařízení, uživatelské jméno, port / SSID+AP, aktivní prvek, stav	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		připojen/odpojen, health check, první a poslední výskyt zařízení	připojen/odpojen, health check, první a poslední výskyt zařízení	
		na základě MAC vynutit reautentizaci uživatele	na základě MAC lze vynutit reautentizaci uživatele	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		změnit koncovému zařízení přístupový profil (přesun do karantény, z karantény, do jakéhokoliv jiného bezpečnostního přístupového profilu)	Lze změnit koncovému zařízení přístupový profil – např. přesun do karantény, z karantény, do jakéhokoliv jiného bezpečnostního přístupového profilu apod.	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		změnit uživateli přístupový profil (přesun do karantény, z karantény, do jakéhokoliv jiného bezpečnostního přístupového profilu)	Lze změnit uživateli přístupový profil – např. přesun do karantény, z karantény, do jakéhokoliv jiného bezpečnostního přístupového profilu)	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		odpojit koncové zařízení ze sítě	Lze odpojit koncové zařízení ze sítě	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		vytvořit, aktivovat a deaktivovat uživatelský účet (jméno a heslo do lokální databáze)	Lze vytvořit, aktivovat a deaktivovat uživatelský účet (jméno a heslo do lokální databáze)	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		integrace se stávající adresářovou službou pomocí LDAPs a Radius protokolů	Podpora integrace se stávající adresářovou službou Active direktory pomocí LDAPs a Radius protokolů	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
		autentizace - možnost autentizovat zařízení minimálně pomocí 802.1X, MAC a webovým portálem	autentizace - možnost autentizovat zařízení minimálně pomocí 802.1X, MAC a webovým portálem	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		- možnost autentizovat a autorizovat vice identit na jednom portu (telefon, PC, virtuální stroje) - IEEE 802.1X minimálně EAP-TLS, EAP-TTLS, EAP-MD5, EAP-PEAP, EAP-LEAP, EAP-RSA a – EAP-SIM - MAC autentizace minimálně PAP, CHAP a EAP- MD5 - vnitřní databáze MAC včetně podpory bitového maskování MAC adres - autentizace vůči nadřazenému Radius serveru - autentizace vůči nadřazenému LDAP serveru - autentizace vůči vnitřní databázi - použití různých autentizačních autorit, minimálně dle lokality kde se uživatel nachází, dle uživatelského jména a dle domény	- možnost autentizovat a autorizovat vice identit na jednom portu (telefon, PC, virtuální stroje) - IEEE 802.1X minimálně EAP-TLS, EAP-TTLS, EAP-MD5, EAP-PEAP, EAP-LEAP, EAP-RSA a EAP-SIM - MAC autentizace minimálně PAP, CHAP a EAP-MD5 - vnitřní databáze MAC včetně podpory bitového maskování MAC adres - autentizace vůči nadřazenému Radius serveru - autentizace vůči nadřazenému LDAP serveru - autentizace vůči vnitřní databázi - použití různých autentizačních autorit, minimálně dle lokality kde se uživatel nachází, dle uživatelského jména a dle domény	
		autorizace - systém musí být schopen aplikovat rozdílné bezpečnostní přístupové profily minimálně na základě kombinace všech těchto podmínek: MAC, OUI, port/přepínač, den v týdnu, čas, příslušnost uživatele i počítače v LDAPu a Radiusu, typu autentizace, typu koncového zařízení a typu	autorizace - systém bude schopen aplikovat rozdílné bezpečnostní přístupové profily minimálně na základě kombinace všech těchto podmínek: MAC, OUI, port/přepínač, den v týdnu, čas, příslušnost uživatele i počítače v LDAPu a Radiusu, typu autentizace, typu koncového zařízení a typu operačního systému koncového zařízení	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		operačního systému koncového zařízení - systém musíbýt schopen dynamicky přidělit VLANu a ACL pro jednotlivá koncová zařízení - systém musí být schopen dynamicky přidělit QoS pro jednotlivá koncová zařízení (802.1p a DSCP/ToS hodnoty rozdílné pro rozdílná zařízení) - systém musí podporovat využití CoA (RFC 3576) - systém musí umožnit uživatelům registraci vlastních zařízení bez zásahu administrátora (onboarding)	- systém bude schopen dynamicky přidělit VLANu a ACL pro jednotlivá koncová zařízení - systém bude schopen dynamicky přidělit QoS pro jednotlivá koncová zařízení (802.1p a DSCP/ToS hodnoty rozdílné pro rozdílná zařízení) - systém bude podporovat využití CoA (RFC 3576) - systém umožní uživatelům registraci vlastních zařízení bez zásahu administrátora (onboarding)	
		centrální správa	centrální správa	Central management.pdf Aruba ClearPass.pdf HPE IMC.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem, včetně nároku na opravné verze softwaru, nové verze (funkcionality), nahlašování závad v režimu 24x7	min. 36 měsíců poskytovaná výrobcem, včetně nároku na opravné verze softwaru, nové verze (funkcionality), nahlašování závad v režimu 24x7	Zahrnuto v nabídce
Optické moduly a kabely - sada	SFP moduly	*320 ks modulů SFP+ 10 Gb, SM min. 10 km včetně DMI diagnostiky pro nabízené přepínače* *12 ks modulů QSFP+ 40 Gb, MM min. 100 m pro nabízené přepínače*	*320 ks modulů SFP+ 10 Gb, SM 10 km včetně DMI diagnostiky pro nabízené přepínače* *12 ks modulů QSFP+ 40 Gb, MM 100 m pro nabízené přepínače*	Zahrnuto v nabídce
	Patch kabely	*300 ks optický kabel SM s konektory LC-SC, délka 2 m*	*300 ks optický kabel SM s konektory LC-SC, délka 2 m*	Zahrnuto v nabídce

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		6 ks optický kabel MM s konektory LC-LC, délka 1 m *90 ks optický kabel SM s konektory LC-LC, délka 1 m*	*6 ks optický kabel MM s konektory LC-LC, délka 1 m* *90 ks optický kabel SM s konektory LC-LC, délka 1 m*	
	Záruka	*min. 36 měsíců poskytovaná výrobcem zařízením. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7*	*36 měsíců poskytovaná výrobcem zařízením. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7*	Zahrnuto v nabídce
Vybudování 11 optických tras	Optický kabel	2900 m optický kabel 9/125 12vl pancéř včetně jeho instalace	2900 m optický kabel 9/125 12vl pancéř včetně jeho instalace	Zahrnuto v nabídce
	Optické vany	22 ks optická vana 12xSC komplet včetně instalace	22 ks optická vana 12xSC komplet včetně instalace	Zahrnuto v nabídce
	Optický svár	528 x optický svár	528 x optický svár	Zahrnuto v nabídce
	Dokumentace	měřící protokol včetně zadokumentování skutečného stavu	měřící protokol včetně zadokumentování skutečného stavu	Zahrnuto v nabídce
	Záruka	min. 36 měsíců poskytovaná výrobcem zařízením. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	36 měsíců poskytovaná výrobcem zařízením. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	Zahrnuto v nabídce

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
Ostatní kabeláž		dodavatel v rámci svého řešení zahrne veškerou nezbytnou kabeláž, propojovací prvky, patch panely a další bižuterii, která bude nezbytná pro zapojení všech nových a případného přepojení stávajících prvků v infrastruktuře Zadavatele	veškerá nezbytná kabeláž, propojovací prvky, patch panely a další bižuterie, která bude nezbytná pro zapojení všech nových a případné přepojení stávajících prvků v infrastruktuře Zadavatele	Zahrnuto v nabídce
Zdroje napájení UPS	Specifikace	rackové provedení max. 4U, do rozvaděče s max. hloubkou 800 mm	**Kehua KR1000-RM Li, Kehua KR3000-RM Li,** rackové provedení 2U, do rozvaděče s max. hloubkou 800 mm	UPS KR1-3K RM Li.pdf
		online technologie	online technologie	UPS KR1-3K RM Li.pdf
		životnost baterie minimálně 36 měsíců	životnost baterie minimálně 36 měsíců	UPS KR1-3K RM Li.pdf
		doba zálohování min. 10 min při plném výkonu	doba zálohování 11 min při plném výkonu	UPS KR1-3K RM Li.pdf
		min. 6 výstupních zásuvek IEC C13	6 výstupních zásuvek IEC C13	UPS KR1-3K RM Li.pdf
		management rozhraní WEB + SNMP, management porty USB a LAN min. 100 Mb	management rozhraní WEB + SNMP, management porty USB a LAN . 100 Mb	UPS KR1-3K RM Li.pdf
		kompletní management software pro správu a všechny nabízené zdroje napájení musí být možné vzdáleně spravovat, poskytnutá licence musí být trvalá	kompletní management software pro správu a všechny nabízené zdroje napájení je možné vzdáleně spravovat, poskytnutá licence je být trvalá	UPS KR1-3K RM Li.pdf
		možnost integrace do monitorovacích a logovacích systémů KKN	možnost integrace do monitorovacích a logovacích systémů KKN	UPS KR1-3K RM Li.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		podpora všech obvyklých OS pro infrastrukturu KKN (viz popis prostředí a požadovaných prvků)	podpora všech obvyklých OS pro infrastrukturu KKN (viz popis prostředí a požadovaných prvků)	UPS KR1-3K RM Li.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem zařízením. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	36 měsíců poskytovaná výrobcem zařízením. Odeslání náhradního zařízení max. následující pracovní den po nahlášení závady, nahlašování závad v režimu 24x7	UPS KR1-3K RM Li.pdf
Systém pro provozní a bezpečnostní monitoring	Záznam provozních a bezpečnostních událostí z provozu	požadován jeden prvek pro lokalitu KV s databází o velikosti 80TB a jeden prvek pro lokalitu Ch o velikosti databáze 40TB. Systém musí umožnit sledovat provozní i bezpečnostní události na celé infrastruktuře Zadavatele. Pro lokalitu Ch je možno využít stávajícího prvku umístěného v lokalitě KV, pokud se Uchazeč rozhodne tuto platformu využít.	LOGM-L-5Y **LOGmanager-L** - samostatný box LOGM-L-ADD40TB Rozšíření diskové kapacity LOGmanager-L jeden prvek pro lokalitu KV s databází o velikosti 80TB a využitá stávajícího prvku v lokaitě Ch o velikosti databáze 40TB. Systém umožňuje sledovat provozní i bezpečnostní události na celé infrastruktuře Zadavatele.	Logmanager.pdf
	Záruka	min. 36 měsíců poskytovaná výrobcem, včetně nároku na opravné verze softwaru, nahlašování závad v režimu 24x7	60 měsíců poskytovaná výrobcem, včetně nároku na opravné verze softwaru, nahlašování závad v režimu 24x7	Logmanager.pdf
Vyhodnocování síťového provozu	Vyhodnocování síťového provozu s ohledem na budovanou infrastrukturu	monitorovací systém musí umožňovat dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny	IFP-10000-SFP+ **Progress Flowmon Probe 10000 SFP+** IFC-6000-VA **Progress Flowmon Collector 6000 VA**	flowmon_probe.pdf flowmon_collector.pdf Flowmon ADS.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný	FPC-ADS-B **Progress Flowmon ADS Business** monitorovací systém umožňuje dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě umožní v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nebude monitorovací systém detekovatelný	
		uložení a zpracování statistik musí být redundantní na k tomu určených specializovaných zařízeních – kolektorech. Ty musí být vybaveny SW či HW RAIDem, případně provozovány na virtualizované infrastruktuře. Kolektory musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat	Uložení a zpracování statistik bude redundantní na k tomu určených specializovaných zařízeních – kolektorech. Ty budou provozovány na virtualizované infrastruktuře. Kolektory budou poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat automatizované	flowmon_probe.pdf flowmon_collector.pdf Flowmon ADS.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
		automatizované reporty i notifikace na nestandardní situace. Ukládání dat probíhá kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců. Samozřejmostí je plná customizace způsobu prezentace dat a reportů na základě cílového prostředí. Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow). Tato technologie představuje nejmodernějším prostředek pro monitorování sítě a oproti konkurenčním technologiím nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní sítě nebo specializovaná prostředí průmyslových sítí	reporty i notifikace na nestandardní situace. Ukládání dat bude probíhat kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců. Plná customizace způsobu prezentace dat a reportů na základě cílového prostředí. Systém bude pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow). Tato technologie představuje nejmodernějším prostředek pro monitorování sítě a oproti konkurenčním technologiím nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní sítě nebo specializovaná prostředí průmyslových sítí	
		požadujeme jeden kolektor pro každou lokalitu a jeden centrální prvek na vyhodnocování síťových toků s dalšími funkcemi popsanými níže v detailní specifikaci	jeden kolektor pro každou lokalitu a jeden centrální prvek na vyhodnocování síťových toků s dalšími funkcemi popsanými níže v detailní specifikaci	flowmon_probe.pdf flowmon_collector.pdf Flowmon ADS.pdf

Část	Parametr	Popis povinného parametru	Uchazeč popíše způsob naplnění tohoto povinného parametru včetně značkové specifikace nabízených dodávek	Uchazeč uvede odkaz na přiloženou část nabídky, kde je možné ověřit naplnění parametru
	Záruka	min. 36 měsíců poskytovaná výrobcem, včetně nároku na opravné verze softwaru, nahlašování závad v režimu 24x7	60 měsíců poskytovaná výrobcem, včetně nároku na opravné verze softwaru, nahlašování závad v režimu 24x7	

Dále jsou specifické požadavky na systém pro provozní a bezpečnostní monitoring. Uchazeč ve své nabídce navrhne řešení pro obě lokality, jak je specifikováno v detailních parametrech.

(1)	**Obecné požadavky pro provozní a bezpečnostní monitoring**
(2)	Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Přiložen katalogový list Logmanager.pdf
(3)	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
(4)	Veškerá konfigurace systému se bude provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.
(5)	Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace bude obsahovat přehledný návod na vytváření zákaznických parserů a systém obsahuje možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nemá vliv na provoz systému. Pro psaní parserů nebude použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(6)	Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#

(7)	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém umožňuje příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(8)	Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimální rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace je možné přidávat i v uživatelsky definovaných parserech.
(9)	Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).
(10)	Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.
(11)	Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
(12)	Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
(13)	Systém neumožňuje mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log je dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
(14)	Systém umožňuje konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nebude použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(15)	Systém provádí konsolidaci logů na interním storage logovacího systému.

(16)	Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj je integrální součástí navrhovaného systému a je obsažen v jednotném rozhraní nabízeného produktu. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(17)	Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace je dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
(18)	Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.
(19)	Systém provádí automatické doplňování reverzních DNS záznamů a GeoIP informací k událostem a u GeoIP jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace, manuální aktualizace a umožňuje používat tuto funkci jen pro vybrané IP adresné prostory. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(20)	Systém podporuje nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/web/sources/o365.html
(21)	V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nedochází ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události jsou ukládány do vyrovnávací paměti.
(22)	Systém umožňuje unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno,zdrojová IP, značka/tag apod.).
(23)	Potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Dokumet: Potvrzení o zavedení systému ISO 27001-2013.pdf

(24)	Systém má možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nejdou administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.
(25)	Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data se nepoužívá povinně SQL jazyk.
(26)	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
(27)	Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.
(28)	Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním je identické v anglickém i v českém jazyce. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(29)	Systém nabízí kapacitní i výkonovou škálovatelnost.
(30)	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně **12TB (Ch) / 80TB (KV)** dat.
(31)	Ze systému je možné za běhu vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků neovlivňuje požadovanou kapacitu úložiště.
(32)	Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.
(33)	Systém obsahuje REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňuje autorizovaný přístup ke strukturované databázi logů. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(34)	Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. Dokumet: Prohlaseni_o_shode-zakon o kybernetické bezpečnosti_MK_2019.pdf

(35)	Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(36)	Systém umožňuje jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/index.html#
(37)	Dodaný systém obsahuje ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.
(38)	Systém podporuje ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému podporuje ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
(39)	**Minimální HW parametry požadovaného systému**
(40)	Jedna hardwarová appliance o velikosti 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.
(41)	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.
(42)	2 procesory, 16 jader každý, s podporou HyperThreadingu nebo Multi-Threadingu.
(43)	128GB DDR-4 a možnost rozšíření o NVMe paměťové pole pro zpracování dat v čase blízkém reálnému (Near Real-Time).
(44)	12TB (Ch) /80TB (KV) pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache 8GB. Řadič diskového pole obsahuje zálohovací baterii nebo být vybaven flash pamětí. Server DELL.

(45)	systému obsahuje 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti 7200 otáček/m.
(46)	4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému a doložte příslušný odkaz na dokumentaci.
(47)	Větráky v systému jsou vyměnitelné za provozu a redundantní.
(48)	2x napájecí zdroje s redundancí napájení 1+1.
(49)	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.
(50)	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).
(51)	**Výkonnostní a SW parametry systému**
(52)	Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).
(53)	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace jsou prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Odkaz: https://doc.logmanager.cz/manual/3.9.11/cs/release-notes.html
(54)	Systém podporuje downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. https://doc.logmanager.cz/manual/master/cs/downgrade.html
(55)	Průměrný trvalý příjem min. 5000 událostí/s. Výkon je dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém prokazatelně kompletně zpracuje přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), bude zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.

(56)	Špičkový příjem minimálně 10000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém prokazatelně kompletně zpracuje přijaté události, bude zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nedovoluje ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí. https://logmanager.com/cs/podpora/c7efb546-479e-48db-9ea2-c5dfdb7ab12a?do=downloadDocument
(57)	Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Logmanager je licenčně neomezený na počet zařízení a pro příjem zasílaných událostí. Integrovaná databáze s čistou velikostí 40TB s podporou komprese ukládaných dat.
(58)	Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk umožňuje uživateli psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. https://doc.logmanager.cz/manual/3.9.11/cs/language_reference.html
(59)	Konfigurace uživatelských parserů umožňuje automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy. https://doc.logmanager.cz/manual/3.9.11/cs/blocks/types/ip/ip.html https://doc.logmanager.cz/manual/3.9.11/cs/blocks/types/mac/mac_subscript.html
(60)	Systém podporuje doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací jsou tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní. https://forum.logmanager.cz/viewtopic.php?p=340
(61)	Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů je možnost vložení minimálně 20 testovacích zpráv současně. https://doc.logmanager.cz/manual/3.9.11/cs/whitepapers/parser-manual.html https://doc.logmanager.cz/manual/3.9.11/cs/web/parser/parsers.html#parsers

(62)	V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd...
(63)	Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.
(64)	Pro budoucí nasazení ve vysoké dostupnosti je vyžadována podpora sestavení v clusteru – podpora 2 nodů. Nastavení clusteru se kompletně realizuje v grafickém rozhraní správcovské konzole v jednom kroku. Systém ve vysoké dostupnosti přehledně informuje o stavu clusteru a procesu synchronizace databází. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/web/system/cluster.html#cluster
(65)	V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech.
(66)	V případě rozšíření systému na cluster je navrhovaný systém schopen zajistit bezvýpadkovost sběru logů.
(67)	Řešení umožňuje rozšíření mezipaměti diskového subsystému o SSD nebo NVRAM typu o kapacitě minimálně 3TB.
(68)	Systém umožňuje export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.
(69)	Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/web/system/backup.html
(70)	Podpora důvěryhodného zálohování dat na externí systém. Plánované i ad-hoc zálohování. Zálohy dat jsou vhodně kompresovány. https://doc.logmanager.cz/manual/3.9.11/cs/web/system/backup.html
(71)	**Alerty**
(72)	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.

(73)	Text emailu vygenerovaného alertem je uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.
(74)	Systém obsahuje výrobcem předpřipravené sety/vzory alertů a korelací.
(75)	Systém bude provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů umožňuje okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/web/parser/filter_contexts.html
(76)	Jako výstupní pravidlo Alertu systém umí odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu je možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/web/logs/syslogOutput.html
(77)	V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/web/parser/filter_contexts.html
(78)	Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a podporuje možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci.
(79)	**Sběr událostí z Microsoft prostředí**
(80)	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent současně podporuje jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se instaluje prostřednictvím MS AD Group Policy a nevyžaduje žádnou konfiguraci na cílovém systému.
(81)	Agent provádí instalaci a podporuje centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon a výběr z několika přednastavených konfigurací Sysmon v grafickém rozhraní centrální správcovské konzole systému. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/web/beats/sysmon.html

(82)	Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahoď logy s EventId 7036.
(83)	Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Dokumentace: https://doc.logmanager.cz/manual/3.9.11/cs/web/sources/windowsfilters.html?highlight=windows
(84)	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace je kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace je automaticky distribuována přímo z centrální konzole systému. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.
(85)	Komunikace Windows agenta a centrálního systému je zabezpečena TLS 1.2 a výše a odporuje ověřování certifikátem.
(86)	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířit Sysmonem. Dále Windows agent podporuje centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. https://doc.logmanager.cz/manual/3.9.11/cs/devices/logmanager-orchestrator.html https://doc.logmanager.cz/manual/3.9.11/cs/web/beats/global-config.html https://doc.logmanager.cz/manual/3.9.11/cs/web/beats/orchestrators.html
(87)	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K bezpečnostním událostem hodným pozornosti doplňuje značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytváří SHA256 hash.
(88)	**Podpora pro sběr událostí z poboček**
(89)	Systém obsahuje centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. https://doc.logmanager.cz/manual/3.9.11/cs/forwarder.html

(90)	Systém podporuje centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.
(91)	Řešení je schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou umí spojení automaticky obnovit.
(92)	Řešení komunikuje po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.
(93)	Řešení poskytuje kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.
(94)	Řešení pro sběr dat z poboček má výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.
(95)	Řešení poskytuje podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.
(96)	Řešení bude k dispozici jako fyzický systém
(97)	Řešení je schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).
(98)	Řešení je schopno vyhodnocovat lokální provoz a zároveň odesílat data do nadřazeného systému.
(99)	**Vysoká dostupnost, SW Podpora a záruka na hardware**
(100)	Volitelná podpora pro nasazení ve vysoké dostupnosti.
(101)	HW - 5letá servisní podpora na hardware appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady.
(102)	Systém podporuje vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.
(103)	SW - Podpora výrobce na aktualizaci systému a parserů na **5** let**.** Podpora obsahuje aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.

Vyhodnocování síťového provozu. Dále jsou uvedeny detailní parametry pro systém na vyhodnocování síťového provozu, rozložení jednotlivých prvků je popsáno výše ve specifikaci.

Obecné požadavky:

Požadavek	**Popis**
Ucelený, škálovatelný NetFlow/IPFIX monitorovací systém	Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, jFlow, cflowd, NetStream).
Podpora infrastruktury	Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s.
Decentralizovaný monitoring lokalit s centrální správou	Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému.
Distribuovaná architektura	Distribuce flow záznamů mezi vícero jednotek pro rozložení zátěže při zpracování dat. Jednotky mohou být přidávány pro zvýšení výkonu nebo kapacity. Řešení je centrálně spravováno a konfigurováno z centrální jednotky a poskytuje centrální pohled na flow analýzu, alerting a reporting.
Nezávislost na stávající infrastruktuře	Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce).
Zdroje NetFlow statistik (sondy)	Specializovaná dedikovaná zařízení (sondy) pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5,v9, IPFIX)
Bezeztrátový sběr flow statistik z více zdrojů	Bezeztrátový sběr dat na kolektorech z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlowv v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream).
Ukládání statistik a vyhodnocování bezpečnostních hrozeb	Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů.
Zákaznická podpora	Plná zákaznická podpora v českém jazyce.
Reference	Systém ověřený instalacemi v rozsáhlé síťové infrastruktuře (datové linky 10 Gbps a výše). Referenční zakázky uvádí výrobce na https://www.flowmon.com/cs/our-customers

Rozhraní pro integraci nástrojů třetích stran	Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran.

Požadavky na zdroje (Netflow/IPFIX) dat:

Požadavek	**Popis požadavku**
Pasivní zapojení	Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty).
Instalace	Snadná instalace do stávající síťové infrastruktury – racková montáž
Management rozhraní	Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat.
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.
Nastavitelná rychlost monitorovací linky	Možnost nastavení rychlosti monitorované linky
Dohled	Sondu je možné integrovat do dohledového systému 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.
Minimální výkon	Výkon 1 milion paketů za sekundu na každém portu, možnost upgradu na verzi s wire-speed garancí zpracování všech paketů.
Podpora příkazové řádky	Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.
DNS cache	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.
LDAP autentizace	Podpora autentizace vůči LDAP (Active Directory).

TACACS+ autentizace	Podpora autentizace vůči TACACS+
Podpora protokolů pro výměnu dat	Programové vybavení sondy umožňuje vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX.
Podpora spolehlivého a šifrovaného exportu toků dle standardu	Zařízení umožňuje exportovat statistiky o síťovém provoze (toky) pomocí spolehlivého a zabezpečeného komunikačního kanálu dle standardu RFC 5153.
Zpracování datového provozu	Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor.
Analýza tunelovaného provozu	Monitorování provozu v tunelu (deenkapsulace) GRE, ESP a OTV.
Uživatelsky definované šablony	Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX.
Monitorování MAC adres	Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu.
Detekce aplikací	Detekce aplikací dle standardu NBAR2, nebo ekvivalentních.
Analýza zpoždění na síti	Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
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 (šablony NetFlow v9 nebo IPFIX).
Profilování zařízení v síti	Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování VoIP	Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování DNS provozu	Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování SMB/CIFS provozu	Monitorování a analýza SMB/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování DHCP provozu	Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).

Monitorování e-mailového provozu	Monitorování e-mailového provozu – protokolů SMTP, POP3, IMAP a položek jako uživatelské jméno, jméno odesílatele, selhání autentizace a další. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování MS SQL (TDS protokolu) provozu	Monitorování Microsoft SQL provozu (TDS protokolu) – položky jako typ dotazu, verze klienta a serveru, uživatelské jméno a další. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitoring (SSL) šifrovaného provozu	Schopnost monitorování a reportování různých charakteristik provozu šifrovaného pomocí SSL/TLS. To zahrnuje verzi protokolu, šifrovací algoritmus, cipher suite, detaily certifikátu a další.
Monitorování IOT/ICS sítí	Podpora monitoringu nativních IoT a ICS/SCADA prostředí včetně protokolů IEC 61850 (Goose, MMS), DLMS, CoAP a IEC 104. Tyto statistiky jsou monitorovány pomocí standardní IPFIX technologie.
Monitorování rozšířených L3/L4 informací	Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů.
Kapacita paměti současných toků	Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port.
Nastavení času pro expiraci toků	Podpora pro nastavení časů u aktivní a neaktivní expirace toků.
Vzorkování	Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků.
Simultánní export NetFlow statistik	Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX).
Export na základě filtrování dat na sondě	Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky).
Vyplňování identifikace AS	Podpora vyplňování AS na základě vestavěného či dodaného seznamu.
Vyplňování čísla interface	Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port.
Záchyt provozu v plném rozsahu	Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace.
Podpora vysokorychlostních sítí	Řešení podporuje sítě s rychlostmi 1/10/40/100GbE (Gigabit Ethernet).
Monitorovací porty sond	Sondy obsahují 1x 10Gb SFP+ na zařízení

Detailní požadavky na kolektor dat:

Požadavek	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 nebo 30-sekundových intervalech.
Podpora standardů datových toků	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite.
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.
Instalace	Snadná instalace do stávající síťové infrastruktury –šablony pro nasazení virtuálního stroje.
Management rozhraní	Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat.
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. Separace dat s omezením přístupu pro jednotlivé role/uživatele.
LDAP autentizace	Podpora autentizace vůči LDAP (Active Directory).
TACACS+ autentizace	Podpora autentizace vůči TACACS+.
Podpora HOT SWAP a RAID	Hardwarové kolektory jsou vybavené HOT SWAP disky a podporují RAID včetně SMART detekce.
Dohled	Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP.
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.
DNS cache	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.
Podpora Cisco AVC	Podpora standardu Cisco AVC vč. položek HTTP hostname a URL.
Podpora dalších flow standardů	Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2.
Podpora položek proměnlivé délky	Podpora IPFIX položek proměnlivé délky.

Podpora IPFIX rozšíření jiných výrobců	Podpora rozšíření VMware NSX, Gigamon a Ixia IPFIX Extensions.
Monitoring výkonu sítě	Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety.
Monitoring informací z aplikační vrstvy	Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS).
Monitorování rozšířených L3/L4 informací	Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů.
Kapacita datového úložiště	Systém je schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. Disková kapacita datového úložiště umožňuje záznamy statistik bez jakékoliv redukce v horizontu minimálně 1 měsíce. Tato odstraněná data budou archivována po dobu min 2let.
Rozlišování rozdílných samplovacích poměrů pro každé rozhraní zdroje flow dat	Systém podporuje rozdílné samplovací (vzorkovací) poměry pro každé rozhraní u jednotlivých zdrojů flow dat.
Přeposílání flow vč. možnosti samplingu a převodu formátu	Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik.
Spolehlivý a šifrovaný přenos IPFIX dat	Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 5153
Automatická identifikace zdroje flow statistik	Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu.
Zálohování a obnova flow statistik	Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky.
Podpora pro uživatelské identity	Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele).
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).

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.
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, 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 bytů, paketů, toků, nejvyšší hodnoty RTT, průměné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.
Filtrování a přizpůsobení výstupů	Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnovat do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace).
Uživatelsky definovatelné alerty	Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu.
Uživatelsky definované pohledy na datový provoz	Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.).

Drill-down	Možnost dohledat každý jednotlivý datový tok (flow záznam).
Monitoring aktivních zařízení na sítí	Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení.
Automatická podpora geolokace	Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země).
Otevřené rozhraní	Kolektor poskytuje dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.).
Monitorování dostupnosti zdroje flow dat	Monitorování dostupnosti zdroje flow dat pomocí SNMP.
Podpora flow standardů	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream.
Streamové zpracovávání flow dat	Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií.
Deduplikace	Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou.
Vzorkování na úrovni toků	Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním.
Správa zdrojů síťových toků	Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků.
Identita uživatelů	Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události.
Persistence doménových jmen	Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události.
Detekční pravidla a algoritmy	Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií.
Detekce síťových útoků	Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby.
Detekce anomálií v síťovém provozu	Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace.
Detekce nežádoucích aplikací	Detekce P2P sítí, a VPN komunikace
Detekce událostí na základě „Threat intelligence“ dat	Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a

	aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci.
Detekce provozních problémů	Detekce nadměrné zátěže sítě, výpadků služeb,, nových a cizích zařízení připojených k síti.
Detekce síťových anomálií	Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace.
Vytváření událostí	Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí
Přímý přístup k události přes unikátní URL s využitím ID události	Systém je schopen poskytnout přímý přístup k evidované události za pomoci ID události z externích systémů za pomoci unikátního URL, které je možné sestavit v externím systému při znalosti ID události.
Konfigurační průvodce	Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen.
Konfigurace detekčních schopností	Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ).
Správa detekčních metod	Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry.
Definice vlastních detekčních metod	Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování, atd.).
Detekce NATů	Detekce NATů v síti s využitím rozšířených informací z L3/L4.
Správa filtrů	Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. K jednotlivým záznamům a filtrům lze připojit uživatelský popis účelu.
Správa falešných poplachů	Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní.
Pozastavení platnosti pravidla falešných poplachů	Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu
Smazání falešných poplachů	Systém umožňuje při vytváření pravidel pro falešné poplachy smazat již detekované falešné události.

Dynamické definice falešných poplachů	Pro definici falešných poplachů lze využít filtrů které mohou být upravovány nezávisle na dané definici pravidla falešného poplachu
Definice závažnosti událostí	Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit.
Různé pohledy na události podle uživatelských rolí	Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí.
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele.
CEF export	Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management. Součástí exportu jsou event ID, které jednoznačně identifikuje danou událost.
SNMP Trap	Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap.
E-mailové notifikace	Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k emailovému reportu.
Záchyt provozu v plném rozsahu	Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. Tyto záchyty je možné uživatelsky spravovat.
Spuštění skriptu	Na výskyt události je možné automaticky reagovat spuštěním uživatelsky definovaných skriptů.
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí.
Integrace informací z jiných služeb	Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP.
Získávání doplňujících informací z adresářových služeb	Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP.
Kategorie a komentáře	Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře.

Vyhledávání událostí	Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.).
Interaktivní vizualizace událostí	Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána.
Reporting	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem.
CSV export	Události je možné exportovat do formátu CSV pro další zpracování.
Otevřené rozhraní	Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.).
Sledování změn konfigurace	Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management.
Škálovatelnost řešení	Systém umožňuje postupné rozšiřování řešení pro automatické vyhodnocení přidáním dalších instancí systému při zachování jednoho uživatelského rozhraní pro dané řešení bez ohledu na počet zapojených instancí.
Minimální množství flow/sec	Systém na detekci síťových anomálií umožní zpracovat minimálně 4000 flow/sec.

3. Implementační služby

3.1. Plnění obecných požadavků

(1) V rámci implementace předmětu plnění budou provedeny následující služby:

(a) Zajištění projektového vedení realizace předmětu plnění, včetně pravidelných kontrolních dnů 1x za 14 dní v prostorách Zadavatele a reportingu 1x za týden eletronickou formou.

(b) Provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu ve formě detailního implementačního projektu. Výstupem bude prováděcí projekt a první verze dokumentace skutečného provedení, která bude představovat projektovou dokumentaci, podle které se projekt v součinnosti se zadavatelem bude realizovat. Implementační projekt a prováděcí dokumentace bude připravena před zahájením vlastní realizace dodávek, tzn. Po provedení předimplementační analýzy a zpracování finálního návrhu cílového stavu a bude výslovně schválena Zadavatelem, včetně detilního časového plánu jednotlivých kroků, potřebných součinností, plánovaných výpadků / odstávek jednotlivých služeb, návrh akceptačních kritérií a akceptačních testů, časový harmonogram testovacích a akceptačních milníků.

(c) Předvedení nabízených technologií v případě vyžádání funkčního vzorku v prostředí zadavatele.

(d) Dodávka a implementace nabízeného předmětu plnění splňující povinné parametry technického řešení a zajištění technické podpory.

(e) Zpracování provozní dokumentace (dokumentace skutečného provedení v udržovatelném stavu) implementovaného systému v rozsahu popisu implementovaných funkcionalit a popisu činností běžné údržby a administrace systémů. Zpracování měřících protokolů a dkumentace skutečného provedení optických tras. Dokumentace bude poskytnuta i formou lokalizované (české) vestavěné nebo online nápověda či příručky.

(f) Provedení školení,

(g) Zajištění zkušebního provozu,

(h) Provedení akceptačních testů / akceptace,

(i) Předání detailní dokumentace skutečného provedení,

(j) Formální ukončení etapy I.,

(k) Předání do ostrého / rutinního provozu,

(l) zahájení podpory provozu dle servisní smlouvy.

(2) Veškeré náklady na provedení implementačních služeb jsou zahrnuty v nabídkové ceně k položce, ke které se vztahují (je vyčíslena samostatně).

(3) Činnost omezující práci uživatelů budou prováděny mimo běžnou pracovní KKN, tj. mimo pracovní dny 7:00 – 19:00 hod.

3.2. Zpracování implementačního projektu / prováděcí dokumentace

(1) Před zahájením implementačních prací bude zpracována prováděcí dokumentace, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

(2) Jako podklad pro zpracování prováděcí dokumentace bude provedena předimplementační analýza, která bude zohledňovat stávající prostředí zadavatele ve vztahu ke konkrétnímu nabízenému plnění uchazeče, zejména pak s ohledem na uchazečem použité technické řešení, pro následující oblasti:

   (a) Stávající stav (vstupy) relevantní pro návrh implementace komodity.

   (b) Způsob začlenění nabízených komodit do stávajícího prostředí.

   (c) Konfigurační změny nabízeného systému potřebné pro naplnění povinných požadavků.

   (d) Virtualizační infrastruktura (serverová, síťová, disková i aplikační) ve vztahu k plánovanému využití.

   (e) Integrace nabízených softwarových systémů.

   (f) Požadované součinnosti Zadavatele a jejich rozsah.

   (g) Návrh opatření k odstranění neshod zjištěných v průběhu analýzy.

(3) Prováděcí dokumentace zohlení podmínky stávajícího stavu, požadavky cílového stavu dle zadávací dokumentace a konkrétního technického řešení nabízeného uchazečem a bude obsahovta tyto části:

   (a) Popis cílového stavu / konfigurace nabízeného systému (viz. první verze dokumentace skutečného provedení),

   (b) Detailní časový harmonogram realizace včetně uvedení kritických milníků, součinností, odstávek a postupných testů jednotlivých funkčních celků, postupně začleňovaných do stávající infrastruktury,

   (c) Návrh akceptačních kritérií a akceptačních testů.

(4) Prováděcí dokumentace musí být před zahájením realizace dalších etap plnění výslovně a písemně schválena zadavatelem.

(5) Veškerá dokumentace bude provedena v souladu s doporučeními NÚKIB a OHA na zpracování dokumentace. Veškerá schémata budou ve formátech obecně k tomuto účelu používaných (tj. Archimate a podobné).

3.3. Harmonogram realizace

(1) Bude zajištěno projektové vedení po celou dobu realizace zakázky projektovým manažerem. Popis metodiky je v příloze Popis postupu implementace předmětu plnění – projektová metodika

(2) Harmonogram plnění – zde jsou lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy o dílo. Čísla značí počet kalendářních dnů.

	Etapa projektu – činnost	Zahájení etapy	Ukončení etapy
1	Předimplementační analýza a zhotovení Prováděcí dokumentace včetně vypořádání připomínek a akceptace Zadavatelem	D	D+40
2	Dodávky a implementace	D+80	
3	Školení administrátorů	D+100	zahájení zkušebního provozu, nejpozději do 16.10.2023
4	Zkušební provoz	D+120	nejpozději do 15.11.2023
5	Akceptační testy	D+140	nejpozději do 11.12.2023
6	Zahájení plného provozu	nejpozději do 11.12.2023	-

(3) Součinnosti jsou posány v příloze Popis postupu implementace předmětu plnění – projektová metodika

3.4. Školení

(1) Bude zajištěno školení pracovníků Zadavatele – administrátorů– na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace ICT a uživatelských příruček k jednotlivým komoditám.

(2) Školení zajistí seznámení administrátorů Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin. Rozsah školení pro administrátory je 12 hodin.

(3) Školení bude probíhat v sídle Zadavatele.

(4) Předpokládá se účast max. 5 administrátorů.

(5) Náklady na školení administrátorů jsou zahrnuty v nabídkové ceně

3.5. Testovací prostředí

(1) Pro implementaci není vyžadováno testovací prostředí

3.6. Provedení akceptačních testů, zkušební provoz a přechod do ostrého provozu

(1) V rámci zpracování implemetačního projektu navrhneme způsob a provedení akceptačních testů.

(2) Součástí akceptačních testů budou pro každou komoditu:

(a) Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků.

(b) Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.

(c) Prokázání přiměřených odezev systému při náročnějších operacích

(d) Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná.

(3) Pro každou komoditu budou navrženy vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení.

(4) O provedení akceptace a jejím výsledku bude vyhotoven písemný protokol.

(5) Uchazeč zajistí zkušební provoz v délce 10 dnů včetně technické podpory 1 specialisty na dodané řešení s dojezdem do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h v případě kritických závad, omezující .

(6) Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace díla včetně vypořádání všech vad a nedodělků.

4. Záruky a servisní podmínky

(1) **Provedení záruční opravy – tj. reakční doba na nahlášený incident a doba vyřešení, dle typu incidentu, dle níže uvedené tabulky.**

(2) Veškeré opravy po dobu záruky budou bez dalších nákladů pro zadavatele.

(3) Bezplatný (zahrnutý v ceně zakázky) přístup k aktualizacím SW firmware dodaných komodit po dobu záruky.

(4) Veškeré komponenty, náhradní díly a práce, poskytnuté v rámci záruky budou poskytnuty bezplatně.

(5) **Hlášení incidentů bude probíhat telefonicky, nebo emailem na Servicedesk Poskytovatele, odpovědnými osobami určenými Objednatelem. V případě telefonického hlášení Objednatele Oba způsoby hlášení požadavku jsou rovnocenné a čas reakce Poskytovatele se počítá od doby zadání požadavku Objednatelem.**

(6) **Odstraňování závad – viz. tabulka:**

Typ incidentu	Reakční doba na nahlášený incident	Doba vyřešení
Kategorie III Nefunkčnost komunikační infrastruktury jako celku nebo nefunkčnost klíčové součásti dodaného předmětu plnění, eventuálně kybernetický bezpečnostní incident nebo událost. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky obnovena funkčnost systému a zabráněno dalšímu šíření	**30 minut**	**následující pracovní den**

kybernetického bezpečnostního incidentu nebo události včetně minimalizace vzniklých i potenciálních škod.		
Kategorie II Výrazně ztěžuje nebo komplikuje činnost uživatelů využívajících komunikační infrastrukturu z důvodu selhání nebo omezení některé ze systémových funkcí podporujících důležité procesy. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky obnovena funkčnost systému včetně minimalizace vzniklých škod.	**30 minut**	**následující pracovní den**
Kategorie I Vyskytuje v izolované části díla nebo dílčího plnění. Využívání díla je částečně ztíženo a nemá vliv na ostatní funkce. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky obnovena funkčnost systému včetně minimalizace vzniklých škod.	**30 minut**	**do 2 pracovních dnů**