Příloha č. 3.b Zadávací dokumentace (příloha č. 2 kupní smlouvy)

**Technická specifikace předmětu plnění**

**k Zadávací dokumentaci ve veřejné zakázce**

**„Kybernetická bezpečnost**

**Nemocnice Pelhřimov“**

**(dále jen „Technická specifikace“)**

Obsah

[**1.** **Zkratky a pojmy** 3](#_Toc158380832)

[**2.** **Místo plnění** 4](#_Toc158380834)

[**3.** **Doba plnění** 4](#_Toc158380835)

[**4.** **Způsob prokázání splnění požadavků minimálního plnění** 5](#_Toc158380836)

[**5.** **Požadavky na specifikaci jednotlivých bezpečnostních technologií** 6](#_Toc158380838)

[5.1 Technická specifikace Centrálních Firewallů 6](#_Toc158380839)

[5.2 Technická specifikace centrálního sběru a managementu logů 9](#_Toc158380840)

[**5.2.1 Technická specifikace řešení pro správu logů** 9](#_Toc158380841)

[**5.2.2. Požadavky na ucelené řešení pro monitorování sítí na bázi datových toků (NetFlow/IPFIX)** 14](#_Toc158380842)

[**5.2.3. Požadavky na řešení pro automatické vyhodnocování datových toků (NetFlow/IPFIX)** 19](#_Toc158380843)

[5.3 Technická specifikace zavedení segmentace sítě 22](#_Toc158380844)

[5.4 Technická specifikace DLP 25](#_Toc158380845)

[5.5 Technická specifikace úložiště pro PACS a NIS data formou NAS a S3 26](#_Toc158380846)

[5.6 Technická specifikace infrastruktury pro zálohování a rychlou obnovu 27](#_Toc158380847)

[5.7 Technická specifikace pro zvýšení dostupnosti záložního datového centra a lokální sítě 28](#_Toc158380848)

[5.8 Technická specifikace ochrany operačních systémů a mobilních platforem 36](#_Toc158380849)

[**5.8.1 Technická specifikace prostředí pro běh management a bezpečnostních prvků** 38](#_Toc158380850)

[5.9 Technická specifikace pro přihlašování k počítačům a aplikacím v rámci klinických a THP provozů 41](#_Toc158380851)

[**6.** **Fáze A - Instalace a implementace** 44](#_Toc158380852)

[**6.1 Zpracování a akceptace Detailního realizačního projektu** 48](#_Toc158380853)

[**6.2 Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)** 49](#_Toc158380854)

[**6.6.1 Předání a převzetí dokumentů** 49](#_Toc158380855)

[**6.2.2 Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)** 49](#_Toc158380856)

[**6.3 Školení** 51](#_Toc158380857)

[**6.4 Dokumentace** 51](#_Toc158380858)

[**7.** **Fáze B – provozní podpora dodaných technologií** 51](#_Toc158380859)

# **Zkratky a pojmy**

1. Zkratky a pojmy užité v Zadávací dokumentaci jsou uvedeny v Příloze 3.a. Zadávací dokumentace, specifické zkratky a pojmy poplatné zejména této části VZ jsou v následující tabulce.
2. Jedná se o podpůrnou informaci, kterou Zadavatel poskytuje pro zachování jednoznačného výkladu textu dokumentu.

|  |  |
| --- | --- |
| **Zkratka** | **Význam** |
| NGFW | Next-Generation Firewall |
| IPS | Intrusion Prevention System |
| CPU | Central Processing Unit |
| RAM | Random Access Memory |
| RAID | Redundant Array of Inexpensive Disks |
| HW | Hardware |
| SW | Software |
| VLAN | Virtual Local Area Network |
| LACP | Link Aggregation Control Protocol |
| LDAP | Lightweight Directory Access Protocol |
| AD | Active Directory |
| SNMP | Simple network management protocol |
| FTP | File Transfer Protocol |
| SMB | Server Message Block |
| SMTP | Simple Mail Transfer Protocol |
| DDoS | Distributed Denial of Service |
| VPN | Virtual private network |
| SSL | Secure Sockets Layer |
| SSH | Secure Shell |
| TCP | Transmission Control Protocol |
| SIEM | Security Information and Event Management |
| SOAR | Security orchestration, automation and response |
| NFS | Network File System |
| VM | Virtual Machine |
| VDI | Virtual Desktop Infrastructure |
| IPv4/v6 | Internet Protocol version 4 / version 6 |
| RIP | Routing Information Protocol |
| OSPF | Open Shortest Path First |
| BGP | Border Gateway Protocol |

# **Místo plnění**

Nemocnice Pelhřimov, příspěvková organizace, Slovanského bratrství 710, 393 01 Pelhřimov.

# **Doba plnění**

1. Dodávka bude zahájena po nabytí účinnosti smlouvy a bude řízena milníky uvedenými v tabulce Milníky.
2. Milníky Fáze A instalace a implementace dle Smlouvy.

| **Id** | **Činnosti** | **Termín** |
| --- | --- | --- |
| **01** | Podpis Smlouvy | Bude přesněno podle ukončení zadávacího řízení |
| **02** | Zahájení realizace projektu | Bezprostředně po podpisu smlouvy a nabytí její účinnosti |
| **Dodávka technologií, instalace, implementace** | | |
| **03** | **Zpracování a akceptace Detailního realizačního projektu**  Výstupem bude dokument Detailní realizační projekt  Předání dílčího plnění a Akceptace dílčího plnění | do 3 měsíců od ID 02 |
| **04** | **Dodávka a instalace technologií a implementace** | do 10 měsíců od ID 03 |
| **05** | **Zkušební a testovací provoz**  Akceptace Testovacího provozu | do 2 měsíců od ID 04 |
| **06** | **Produkční provoz**  Akceptace produkčního provozu, akceptace Fáze A  Dodávka a aktivace licencí  Ukončení Fáze A | Po ukončení  ID 05 |

1. Fáze B – HW a SW maintenance výrobce technologií a systémů dle Smlouvy bude zahájena ukončením Fáze A (ukončení projektu akceptací produktivního provozu).
2. Termín ukončení se může změnit z objektivních příčin, způsobených třetími stranami nebo jinými okolnostmi, nezávislými na vůli smluvních stran.
3. Dodavatel zpracuje jako součást Detailního realizačního projektu vyhotoveného dle odst. 6.1 této Technické specifikace vyhotoví detailní harmonogram realizace předmětu plnění v souladu s milníky, stanovenými zadavatelem výše.

# **Způsob prokázání splnění požadavků minimálního plnění**

1. Zadavatel požaduje, aby Dodavatelem nabízená dodávka splňovala veškeré dále uvedené požadavky (funkcionality a parametry) a tyto byly zahrnuty v nabídce Dodavatele a v celkové nabídkové ceně.
2. Dodavatel ve své nabídce jednoznačně deklaruje splnění, popřípadě absenci každého z níže uvedených požadavků v tabulkách označených jako „Minimální požadavky …“, a to vyplněním příslušného pole „Splněno“ jedno ze dvou nabízených možností:

„**ANO**“ v případě že dodávka Dodavatele (Nabídka) minimální požadavek **splňuje**

nebo **„NE“**  v případě že dodávka Dodavatele (Nabídka) minimální požadavek **nesplňuje**

1. Zadavatel požaduje, aby Dodavatel zpracoval a v nabídce předložil podrobný technický popis nabízeného plnění reflektující všechny dále uvedené požadavky (funkcionality a parametry) (dále také „**Technický popis nabízeného řešení**“); materiál bude v rámci nabídky předložen jako příloha č. 3 kupní smlouvy.

**Technický popis nabízeného řešení bude zadavateli sloužit ke kontrole splnění požadavků zadavatele na funkcionality a parametry nabízeného plnění – zejména ke kontrole splnění požadavků uvedených níže v tabulkách a označených jako „Minimální požadavky…“.** Zadavatel proto upozorňuje, že účastníci zadávacího řízení jsou v rámci nabídky povinni předložit Technický popis nabízeného řešení, jehož součástí musí být doklady, údaje a případně i informace, které budou jednoznačně prokazovat splnění deklarovaných parametrů a funkcionalit u požadavků uvedených níže v tabulkách označených jako „Minimální požadavky…“.

Technický popis nabízeného řešení:

1. **musí být zpracován přehledně a zejména strukturovaně ve vztahu k minimálním požadavkům uvedeným dále v odst. 5, v odst. 6 a v odst. 7** včetně jejich pododstavců, tj. bude zpracován tak, aby se svým obsahem vždy vztahoval k příslušnému odstavci (odst. 5; 5.1; 5.2.; 5.2.1; 5.2.3; 5.3, 5.4 atd. ….až odst. 7).
2. musí obsahovat grafické schéma a podrobný popis nabízených technologií a systémů, datové listy, snímky obrazovek atd.
3. u požadavků na funkcionality musí obsahovat informace o skutečné funkcionalitě nabízených řešení, které bude možné ověřit nejpozději v testovacím provozu, např. v rámci školení administrátorů;
4. u parametrových požadavků musí být jeho součástí přílohy - produktové materiály a ostatní doklady (např. datové listy, snímky obrazovek atd.), které bez nejmenších pochyb budou prokazovat splnění takových požadavků;
5. **u veškerého nabízeného plnění musí být uvedeny „part number“** včetně vysvětlujícího popisu a počtu kusů (tato podmínka se nevztahuje na spotřební materiál); zadavatel připouští předložení „part number“ k nabízenému plnění formou seznamu rozděleného dle jednotlivých odstavců definovaných výše u písm. a)

Zadavatel upozorňuje, že nepředložení Technického popisu nabízeného řešení obsahově plně odpovídajícího výše definovaným požadavkům zadavatele, může mít za následek vyloučení účastníka zadávacího řízení pro nesplnění podmínek účasti v zadávacím řízení.

1. V případě pochybností o splnění minimální technické specifikace může Zadavatel vyžádat prokázání splnění technické specifikace formou vzorku. Za poskytnutí vzorku nebude Uchazeči vznikat nárok na úhradu nákladů s tím spojených. Podrobnosti k poskytnutí vzorku viz textová část Zadávací dokumentace.
2. Nesplnění nebo neprokázání kteréhokoli ze stanovených minimálních požadavků, uvedených v této Technické specifikaci bude znamenat vyloučení účastníka ze zadávacího řízení.

# **Požadavky na specifikaci jednotlivých bezpečnostních technologií**

1. Předmětem VZ je dodávka bezpečnostních technologií, které jsou vyspecifikované v níže uvedených podkapitolách.

5.1 Technická specifikace Centrálních Firewallů

(1) Současný firewall nedokáže výkonem pokrýt datové požadavky uživatelů sítě, nelze ani dlouhodobě ukládat logy a celkově je technologicky nevyhovující, a to i z důvodu toho, že v případě výpadku není zajištěna vysoká dostupnost.

(2) Předmětem zadání je implementace 2ks NG segmentačních firewallů pro vytvoření clusteru s vysokou dostupností a dosavadního zajištění segmentace sítě (za použití standardů IEEE 802.1Q.a RFC 7348 pro řádově desítky segmentů). Dále pak 1ks SW licence pro analýzu logů firewallů a centrální správy celého systému firewallů. SW bude sloužit jako log proxy pro naplnění potřeby zjednodušení architektury toku logů. Log proxy bude nasazena mezi firewally a centrálním log management řešením. Funkce firewallu musí pokrýt okamžité potřeby správců firewallu a redukovat počet zdrojů logů na jeden. Řešení bude obsahovat firewall cluster v režimu vysoké dostupnosti active/activeactiveactive. Každý node clusteru pak bude umístěný v jednom DC.

(3) Kromě funkcionality síťového firewallu řešení bude také nabízet IPS, filtraci a kontrolu na úrovni aplikací a URL a dále pak ochranu před ransomware, malware a bude disponovat funkcí sandboxingu, antiviru a anti-bot. Musí být umožněna identifikace a definice politik na úrovni uživatelských identit a z toho plynoucí možnost integrace bezpečnostního řešení ke stávajícímu AD. Další rolí pak bude i funkce VPN koncentrátoru, licenčně by mělo být umožněno připojit nejméně 50 vpn uživatelů na každý firewall současně.

(4) Součástí řešení bude i nezávislý centrální management server ve formě virtuálního stroje ve stávající virtualizační platformě VMware. Firewall infrastruktura bude nasazena v distribuované architektuře, kdy je pomocí tohoto serveru centrálně spravována, management centrálních firewallů dále bude sloužit také pro tvorbu a správu bezpečnostních politik a správu administrátorů celého systému.

Současně pak centrální server zajistí sběr a interpretaci logů a událostí z firewallů a auditní log firewall infrastruktury, umožní korelaci a analýzu bezpečnostních incidentů. Z těchto dat bude možné následně generovat bezpečnostní reporty.

(5) **Minimální požadavky na technickou specifikaci** centrálních firewallů jsou uvedeny v následující tabulce. Parametry jsou uvedeny pro jeden firewall.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **01** | Požadované funkcionality NG Firewall, IPS, aplikační a URL filtering, malware a botnet ochrana, zero-day ochrana, inspekce ssl provozu, sandboxu emulace provozu. |  |
| **02** | HW akcelerovaný IP provoz. |  |
| **03** | Nejméně 16 GB operační paměti DDR5 s podporou ECC. |  |
| **04** | Redundantní HA konfigurace řešení složená min ze dvou fyzických prvků. |  |
| **05** | Podpora HA redundance active-active i active-standby, stavová synchronizace TCP, UDP a NAT. |  |
| **06** | Podpora L2 a L3 HA konfigurace. |  |
| **07** | Podpora IPv4 a IPv6. |  |
| **08** | Podpora VLAN a VXLAN (min. 1024 VLAN). |  |
| **09** | Podpora protokolů pro dynamické směrování OSPFv3 a BGPv4. |  |
| **10** | Podpora LACP bonding. |  |
| **11** | Podpora redundance Internetového připojení (active-standby, loadbalancing). |  |
| **12** | DHCP server. |  |
| **13** | Podpora NAT (včetně IPv6 NAT – NAT46/NAT64/NAT66). Požadavek dle potřeb paragrafu 27 Vyhlášky o dlouhodobém řízení informačních systémů veřejné správy. |  |
| **14** | Podpora 802.1X a integrace s řešením nástroje pro segmentaci sítě, viz technická specifikace Nástroje pro zavedení segmentace sítě. |  |
| **15** | Integrace s AD a LDAP, podpora RADIUS. |  |
| **16** | Možnost rozdělení řešení na jednotlivé nezávislé virtuální instance, včetně aplikace kompletní funkcionality nezávisle na konfiguraci ostatních instancí. Tento požadavek zjišťuje možné úplné oddělení interní a návštěvnické komunikace. |  |
| **17** | Propustnost firewall (SPI) min 25Gbps (Enterprise mix). |  |
| **18** | N+1 redundance – zachování propustnosti i při výpadku jednoho prvku. |  |
| **19** | Propustnost firewall+IPS+antivirus/antibot+aplikační kontrola+NAT+VPN min 5Gbps (Enterprise mix). |  |
| **20** | Plná kontrola každého paketu bez vlivu na propustnost FW+IPS+AV/AB+NAT+VPN min 5Gbps (ID 18). |  |
| **21** | Min 8mil současných spojení v jeden čas. |  |
| **22** | Min 100 000 nových spojení/s. |  |
| **23** | Všechny funkcionality konfigurovatelné pomocí bezpečnostních politik. |  |
| **24** | Plná integrace IPS a firewall. |  |
| **25** | Předdefinované a ihned použitelné IPS politiky. |  |
| **26** | Možnost definice IPS pravidel pomoci kombinace src, dst, služba, IPS signatura. |  |
| **27** | Možnost nastavit IPS v režimu monitoring nebo prevent globálně i pro jednotlivé pravidlo. |  |
| **28** | Automatické vypnutí IPS v případě přetížení (CPU nebo paměť) nad definovaný práh. |  |
| **29** | Nové signatury označeny a možnost nastavit je v režimu monitoring. |  |
| **30** | Podpora SSL/TLS inspekce, podpora TLS1.2 a TLS1.3. |  |
| **31** | Blokování spojení na úrovni DNS dotazu. Cílem tohoto požadavku je zabránit překladu adres s nežádoucím obsahem. |  |
| **32** | Min 5000 předdefinovaných služeb/protokolů/aplikací. |  |
| **33** | Možnost vytvářet vlastní IOC indikátory. |  |
| **34** | Sandbox emulace (zero-day ochrana) podporuje protokoly HTTP, HTTPS, FTP, SMTP a SMB. |  |
| **35** | Emulace souboru o velikosti min 100 MB. |  |
| **36** | Možnost odstranění potencionálně škodlivého aktivního obsahu ze souborů, podpora MS Office, PDF, obrazových formátů a archivů (.zip, .tar, .7z, .rar). |  |
| **37** | Odstranění aktivního obsahu nebo konverze souboru do bezpečného PDF. |  |
| **38** | Dynamická analýza souborů se sledováním změn v souborovém systému, registrech, procesech a síťové komunikaci. |  |
| **39** | Logování a reporting změn detekovaných analýzou. |  |
| **40** | Mitre ATTAACK reporting. |  |
| **41** | Ochrana proti botnet a Command & Control. |  |
| **42** | Detekce a filtrování malware URL. |  |
| **43** | Schopnost detekovat a zablokovat DDOS a bruteforce útoky. |  |
| **44** | Integrace řešení s AD bez nutnosti komponent třetích stran. |  |
| **45** | Definice bezpečnostních politik na základě AD skupin. |  |
| **46** | Možnost autentizace uživatele na základě portálu – podpora ověření za pomoci jméno/heslo a SSO Kerberos. |  |
| **47** | Podpora IPSec VPN. |  |
| **48** | Podpora SSL VPN v režimu tunel a v režimu web portal. |  |
| **49** | Podpora IP komprese S2S VPN. |  |
| **50** | VPN podporuje šifrování min AES-256. |  |
| **51** | VPN podporuje datovou integritu min SHA-256. |  |
| **52** | Min 50 SSL VPN konkurenčních spojení včetně licence, pokud je licenčně omezeno. |  |
| **53** | Podpora MFA pro SSL VPN jméno/heslo + 2FA (integrace s MS Authenticator, Email nebo SMS). |  |
| **54** | Management a konfigurace Firewall přes SSH. |  |
| **55** | Podpora 2FA administrátorského přístupu ozn. |  |
| **56** | Centrální management samostatný, fyzicky oddělený od firewall platformy. |  |
| **57** | Centrální management ve formě HW nebo virtuálního stroje. |  |
| **58** | Ukládání logů na oddělený centrální Log server. |  |
| **59** | Centrální správa politik a centrální konfigurace nastavení. |  |
| **60** | Centrální management podporuje režim HA. |  |
| **61** | Komunikace mezi firewallem a centrálním managementem je šifrovaná a autentizovaná. |  |
| **62** | Možnost vyhledat všechny logy na jednom místě pomoci definovaných filtrů (FW, IPS, malware logy). |  |
| **63** | Možnost exportu logů do souboru. |  |
| **64** | Možnost definice IPS politik přímo z logu. |  |
| **65** | Indexování logů umožňující rychlé prohledávaní. |  |
| **66** | Retence logů min 18měsíců. |  |
| **67** | Možnost přidat komentář ke každému pravidlu. |  |
| **68** | Možnost časově omezit platnost pravidel. |  |
| **69** | Možnost seskupování firewall pravidel do samostatných logických skupin a oddílů. |  |
| **70** | Možnost vyhledat využití objektů (výskyt v aktivních i neaktivních pravidlech, nebo v jiných objektech, např. ve skupinách). |  |
| **71** | Možnost práce a změn více administrátorů paralelně. |  |
| **72** | Detekce kolizí a duplicit v politikách. |  |
| **73** | Možnost definice skupin oprávnění ke změnám politik pro administrátory, možnost definovat práva na úrovní jednotlivých pravidel. |  |
| **74** | Konfigurace politik a nastavení prostřednictvím GUI. |  |
| **75** | Podpora autorizovaného a autentizovaného REST API. |  |
| **76** | Funkcionalita korelace logů, analýzy a správy bezpečnostních událostí s předefinovanými pohledy/dotazy a reporty. |  |
| **77** | Možnost vytváření uživatelsky definovatelných reportů (na základě log záznamů a bezpečnostních událostí), možnost periodických reportů. |  |
| **78** | Možnost integrace se SIEM, SOAR. |  |
| **79** | Dedikované mgmt rozhraní 1GbE. |  |
| **80** | Rozhraní pro lokální nezávislý management (out of band) - RJ45 + RS-232/USB. |  |
| **81** | Minimálně 8x síťové rozhraní 1/10GbE. |  |
| **82** | Minimálně 4x síťové rozhraní 10/25GbE. |  |
| **83** | Rozměry max 2U pro každý Firewall. |  |
| **84** | Rozměry standardní velikost 19“. |  |
| **85** | Redundantní napájení s podporou hot-swap. |  |
| **86** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

5.2 Technická specifikace centrálního sběru a managementu logů

1. V současné době není v Nemocnici Pelhřimov žádný centrální Log management.
2. Předmětem této části VZ je dodávka a instalace HW a SW. Bližší specifikace je uvedena v jednotlivých kapitolách níže (viz podkapitoly 5.2.1–5.2.3)
3. Obsluha si pro pokrytí všech požadovaných funkcí vystačí s grafickým rozhraním řešení ve webovém prohlížeči, bez nutnosti použití textového rozhraní (CLI/SSH) a bez instalace jakéhokoliv dodatečného nástroje v prostředí zadavatele.

**5.2.1 Technická specifikace řešení pro správu logů**

(1) Níže jsou uvedené minimální požadavky na systém pro centralizovanou správu logů, událostí a strojových dat. **Minimální požadavky** jsou uvedeny v následující tabulce.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat** | | |
| **01** | Systém pracuje jako Virtuální appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti, které je provozováno na stávající virtualizační platformě VMware vSphere 8.0 U1 nebo novější. |  |
| **02** | Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. 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. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. |  |
| **03** | Systém umožňuje uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní. Vytváření a testování parserů nesmí mít vliv na provoz systému. |  |
| **04** | Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat 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,PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. |  |
| **05** | 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, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech. |  |
| **06** | 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.). |  |
| **07** | 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. |  |
| **08** | Systém nesmí v žádném případě umožnit 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 musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci. |  |
| **09** | Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. |  |
| **10** | Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. |  |
| **11** | 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. |  |
| **12** | 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. |  |
| **13** | Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. |  |
| **14** | V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. |  |
| **15** | Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat. |  |
| **16** | Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. |  |
| **17** | Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace. |  |
| **18** | Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. |  |
| **19** | Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem. |  |
| **Výkonnostní a SW parametry systému** | | |
| **20** | Systém obsahuje všechny softwarové komponenty architektury řešení a nevyžaduje žádné externí zdroje (například externí databázi, aplikační server atd.). |  |
| **21** | Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. |  |
| **22** | Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 300 GB uložených událostí za den. |  |
| **23** | Systém musí podporovat 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 musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní. |  |
| **24** | 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, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd ... Na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem |  |
| **25** | Systém musí umožňovat 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. |  |
| **26** | Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Záloha musí být šifrovaná. |  |
| **27** | Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh. |  |
| **Alerty** | | |
| **28** | Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert. Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události. |  |
| **29** | Systém musí provádět konfigurace alertů a korelací. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. |  |
| **30** | Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. |  |
| **31** | 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). |  |
| **32** | Systém podporuje základní funkce SIEM – funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci. |  |
| **Sběr událostí z Microsoft prostředí** | | |
| **33** | Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. |  |
| **34** | 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. |  |
| **35** | 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. Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. |  |
| **36** | Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy. |  |
| **37** | Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem. |  |
| **38** | 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 musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. |  |
| **39** | 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. |  |
| **40** | Počet instalací Windows agenta nesmí být licenčně a časově omezen, pokud je licenčně nebo časově omezen, tak požadujeme dodání licencí na Windows agenty v množství 2500 na dobu předpokládané morální životnosti produktu – 7 let. |  |
| **41** | SW podpora výrobce na aktualizaci systému a parserů na **5** let**.** Podpora musí obsahovat aktualizaci SW minimálně 4x ročně, opravy chyb a telefonickou a emailovou podporu. |  |
| **Seznam podporovaných zdrojů logů** | | |
| **42** | Apache httpd, Tomcat |  |
| **43** | CEF (generický/standardizovaný formát) |  |
| **44** | Dell iDrac (Server OoB management) |  |
| **45** | Discard (speciální pravidlo na fitrování událostí) |  |
| **46** | Dropbear SSH (~součást Embedded Linux distribucí) |  |
| **47** | Epacs (http://www.epacs.cz/) |  |
| **48** | FlowMon |  |
| **49** | LEEF (generický/standardizovaný formát) |  |
| **50** | H3C networking |  |
| **51** | HAProxy (structured rfc5425 logformat) |  |
| **52** | HPE Aruba Instant AP (WLAN), Aruba Clearpass, Aruba Mobility Controller (WLAN), iLo (Server OoB management), IMC, routers, switches Aruba OS, switches Aruba-CX OS, switches Comware OS, Comware WLAN |  |
| **53** | ISC BIND, DHCP |  |
| **54** | Jivex |  |
| **55** | JSON (generický/standardizovaný formát) |  |
| **56** | Linux Bash commands log, Cron, Freeradius, Iptables, Postfix |  |
| **57** | Mikrotik |  |
| **58** | Microsoft365 (API), Azure (API), Exchange, Exchange tracking textový log (2010-2019), SharePoint, SQL, Defender, DHCP textový log, DNS debug textový log, Firewall (EVTx i textový log), IIS / FTP server textový log, IIS / Webserver textový log, logy z Event View, Sysmon |  |
| **59** | MySQL |  |
| **60** | Nginx |  |
| **61** | Office365 |  |
| **62** | OpenSSH server |  |
| **63** | PostgreSQL |  |
| **64** | Stapro FONS Enterprise, Akord, Openlims |  |
| **65** | Squid (Web Proxy) |  |
| **66** | RFC5425 (generický/standardizovaný formát) |  |
| **67** | Synology NAS DSM |  |
| **68** | VEEAM Backup and Restore |  |
| **69** | Vmware vCenter a ESXi (od verze 7.0.2 přes API) |  |
| **70** | Dodávané systémy požadované a popsané v této Technické specifikaci |  |

**5.2.2. Požadavky na ucelené řešení pro monitorování sítí na bázi datových toků (NetFlow/IPFIX)**

1. S ohledem na ucelené řešení pro monitorování sítí na bázi datových toků (NetFlow/IPFIX) je požadováno dodání 1 ks virtualizovaného kolektoru pro centralizaci sběru dat.
2. **Minimální požadavky** na technickou specifikaci 1 ks kolektoru jsou uvedeny v následující tabulce.
3. Zadavatel disponuje stávající technologií pro automatické vyhodnocování datových toků, reprezentovaných sondou a kolektorem Flowmon.

| **Id** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **01** | Minimální nastavení 4 CPU cores |  |
| **02** | Minimální nastavení 8 GB RAM |  |
| **03** | Minimální nastavení 1000 IOPS |  |
| **04** | Minimální kapacita provozní paměti 6 TB |  |
| **05** | Virtualizační prostředí VMware ESXi 5.5 a vyšší |  |
| **06** | Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce. |  |
| **07** | Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5 minutových, 1 minutových nebo 30 sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků |  |
| **08** | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. Podpora VPC flow logů z AWS, Azure a GCP. |  |
| **09** | 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. |  |
| **10** | Snadná instalace do stávající síťové infrastruktury – šablony pro nasazení virtuálního stroje. |  |
| **11** | Jednoduchá konfigurace pomocí dostupných konfiguračních šablon, které umožňují výběr z dostupných “Presets” a jejich aplikací vytvářet profily, kapitoly, reporty, alerty, widgety a dashboardy bez nutnosti manuální konfigurace. |  |
| **12** | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. |  |
| **13** | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. |  |
| **14** | Podpora autentizace vůči LDAP (Active Directory). |  |
| **15** | Podpora autentizace vůči TACACS+. |  |
| **16** | Virtuální kolektor bude dodán na výše zmíněné virtualizační platformě. HW požadavky jsou dány požadavky na virtualizační platformu. |  |
| **17** | Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. |  |
| **18** | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. |  |
| **19** | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. |  |
| **20** | Přístup na virtuální kontroler bude chráněn pomocí protokolu TLS 1.3 a vyšší. |  |
| **21** | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. |  |
| **22** | Podpora standardu Cisco AVC vč. položek HTTP hostname a URL. |  |
| **23** | Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2. |  |
| **24** | Podpora IPFIX položek proměnlivé délky. |  |
| **25** | Podpora rozšíření VMware NSX, Gigamon a Ixia IPFIX Extensions. |  |
| **26** | Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety. |  |
| **27** | Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS). |  |
| **28** | Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů. |  |
| **29** | Časové známky je možné přidat do flow záznamů, které tuto informaci nemají od zdroje flow záznamů. |  |
| **30** | Systém bude schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. Disková kapacita datového úložiště musí umožnit uložit záznamy statistik po dobu minimálně šesti měsíců. |  |
| **31** | Systém podporuje rozdílné samplovací (vzorkovací) poměry pro každé rozhraní u jednotlivých zdrojů flow dat. |  |
| **32** | 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. |  |
| **33** | Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011. |  |
| **34** | 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. |  |
| **35** | Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat. |  |
| **36** | 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. |  |
| **37** | 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). |  |
| **38** | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel). |  |
| **39** | Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu. Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů. |  |
| **40** | Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat). |  |
| **41** | 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. |  |
| **42** | Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami. |  |
| **43** | 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. |  |
| **44** | Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. |  |
| **45** | 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. |  |
| **46** | Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem). |  |
| **47** | Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu. |  |
| **48** | 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 zahrnout do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace). |  |
| **49** | 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. |  |
| **50** | 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.). |  |
| **51** | Možnost dohledat každý jednotlivý datový tok (flow záznam). |  |
| **52** | Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie. |  |
| **53** | 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. |  |
| **54** | Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). |  |
| **55** | Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.). |  |
| **56** | Monitorování dostupnosti zdroje flow dat pomocí SNMP. |  |
| **57** | Kolektory NetFlow dat jsou schopné zpracovat 40K toků za sekundu. Pro validaci tohoto požadavku jsou provedeny akceptační testy. |  |
| **58** | 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. |  |
| **59** | Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011. |  |
| **60** | 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. |  |
| **61** | Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat. |  |
| **62** | 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. |  |
| **63** | 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). |  |
| **64** | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel). |  |
| **65** | Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu. Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů. |  |
| **66** | Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat). |  |
| **67** | 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. |  |
| **68** | Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami. |  |
| **69** | 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. |  |
| **70** | Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. |  |
| **71** | 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. |  |
| **72** | Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem). |  |
| **73** | Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu. |  |
| **74** | 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. |  |
| **75** | 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.). |  |
| **76** | Možnost dohledat každý jednotlivý datový tok (flow záznam). |  |
| **77** | Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie. |  |
| **78** | 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. |  |
| **79** | Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). |  |
| **80** | Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.). |  |
| **81** | Monitorování dostupnosti zdroje flow dat pomocí SNMP. |  |
| **82** | Kolektory NetFlow dat jsou schopné 150K toků za sekundu. Pro validaci tohoto požadavku jsou provedeny akceptační testy. |  |
| **83** | Dostupnost historie plných flow dat po dobu 12 měsíců | |
| **84** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. | |

**5.2.3. Požadavky na řešení pro automatické vyhodnocování datových toků (NetFlow/IPFIX)**

1. Předmětem této části VZ je dodávka a instalace SW pro detekci anomálií v síti. Systém pro automatické vyhodnocování IP toků umožňuje automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém je založen na pokročilých metodách tzv. behaviorální analýzy a umožňuje tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplňuje stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události je možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů výrazně zjednodušuje správu datové sítě, zvyšuje její bezpečnost a umožňuje proaktivně identifikovat příčiny problémů.
2. **Minimální požadavky** na technickou specifikaci požadavků modulu na automatické vyhodnocování NetFlow dat.

| **Id** | **Požadované parametry** | **Splněno** | |
| --- | --- | --- | --- |
| **01** | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. Podpora VPC flow logů z AWS, Azure a GCP. |  | |
| **02** | Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií. |  | |
| **03** | Systém detekce anomálií poskytuje veřejně dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod apod.). |  | |
| **04** | 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. |  | |
| **05** | Systém pro automatické vyhodnocování NetFlow dat je schopné zpracovat 1K toků za sekundu. Pro validaci tohoto požadavku jsou provedeny akceptační testy. |  | |
| **06** | Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. |  | |
| **07** | Systém umožňuje korelovat toky před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli. |  | |
| **08** | Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. |  | |
| **09** | Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků. |  | |
| **10** | Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. |  | |
| **11** | Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. |  | |
| **12** | Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. |  | |
| **13** | Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. |  | |
| **14** | Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. |  | |
| **15** | Detekce NATů v síti s využitím rozšířených informací z L3/L4. |  | |
| **16** | Detekce P2P sítí a VPN komunikace. |  | |
| **17** | Systém umožňuje detekovat závadnou komunikací na základě rozlišení legitimních domén (druhé úrovně) od náhodně generovaných domén. |  | |
| **18** | Detekce použití TOR klientů v monitorované síti a detekce příchozí komunikace z TOR sítě na monitorované servery. |  | |
| **19** | Systém umožňuje detekovat závadné komunikace monitorování JA3 otisků v síťovém provozu a jejich porovnáváním se seznamem známých závadných JA3 otisků. |  | |
| **20** | 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. |  | |
| **21** | Systém lze napojit na MISP platformu a použít indikátory kompromitace (IoC) poskytované touto platformou k detekci závadných komunikací v monitorované síti. |  | |
| **22** | Detekce nadměrné zátěže sítě, výpadků služeb, nových a cizích zařízení připojených k síti. |  | |
| **23** | Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. |  | |
| **24** | 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.). |  | |
| **25** | Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí. |  | |
| **26** | 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.). |  | |
| **27** | 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. |  | |
| **28** | Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. |  | |
| **29** | Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP/HTTPS. |  | |
| **30** | Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP. |  | |
| **31** | Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře. |  | |
| **32** | Detekované události jsou mapovány na jednu nebo více MITRE ATT&CK taktik a technik pro poskytnutí širšího kontextu uživateli. Mapování je založeno na základě kontextové analýzy pro zajištění správného mapování taktiky a techniky na detekovanou událost. Stejný druh události tak může být mapován různě v závislosti na kontextu události nebo vývoji události v čase. |  | |
| **33** | Systém poskytuje dashboard pro vizualizaci MITRE ATT&CK matice, která zobrazuje počet událostí detekovaných v jednotlivých taktikách a technikách čímž umožňuje poskytnout přehled nad stávající bezpečností situací a zobrazit útoky v jejich různých fázích dle MITRE ATT&CK frameworku. |  | |
| **34** | Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. |  | |
| **35** | 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). |  | |
| **36** | 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. |  | |
| **37** | Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry. |  | |
| **38** | Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí. |  | |
| **39** | 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. |  | |
| **40** | Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. |  | |
| **41** | Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu. |  | |
| **42** | Pro definici falešných poplachů lze využít filtrů které mohou být upravovány nezávisle na dané definici pravidla falešného poplachu. |  | |
| **43** | Pravidla pro falešné poplachy je možné definovat pomocí čísel autonomních systémů (ASN) nebo pomocí plně kvalifikovaného doménového jména (FQDN), čímž lze označit provoz, který nebude zpracováván detekčními metodami. |  | |
| **44** | 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. |  | |
| **45** | 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 musí být event ID, které jednoznačně identifikuje danou událost. |  | |
| **46** | Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. |  | |
| **47** | Události je možné exportovat do formátu CSV pro další zpracování. |  | |
| **48** | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem. |  | |
| **49** | 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 e-mailovému reportu. |  | |
| **50** | Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. Tyto záchyty je možné uživatelsky spravovat. |  | |
| **51** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí NBD v místě instalace na 5 let. | |  |

5.3 Technická specifikace zavedení segmentace sítě

(1) Předmětem je implementace řešení, které ve spolupráci s LAN a WLAN infrastrukturou zajistí adaptivní řízení přístupu pro různé typy zařízení a různé uživatele. Bude možné rozlišit nastavení oprávnění a aplikování politik například pro zaměstnance, hosty nebo externí partnery, a to i z pohledu připojených zařízení.

(2) **Minimální požadavky** na technickou specifikaci pro zavedení segmentace sítě jsou uvedeny v následující tabulce.

(3) V Nemocnici Pelhřimov byly postupně nakoupeny a nasazeny tyto produkty technologie Aruba Networks:

JL558A Aruba 2930-48G 6 ks

Aruba 6200F 48G CL4 740W – JL728A 19 ks

Aruba AP-515 122 ks

Zbytek sítě je také postaven na prvcích Aruba Networks dříve nazývané HP Networking (Procurve s Provision OS, Colubris). V rámci Kraje Vysočina, jakožto zřizovatele nemocnice, byla  vysoutěžena, mimo další, i rámcová smlouva na prvky Aruba Networks. Zřizované organizace jsou metodicky vedeny k nákupu technologií právě z těchto rámcových smluv. Požadavek na kompatibilitu s technologiemi Aruba Networks (a to i v dalších kapitolách) se váže právě na tyto prvky.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **01** | Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení |  |
| **02** | Forma dodání: virtuální appliance pro VMware |  |
| **03** | Minimální celková kapacita řešení pro autentizaci unikátních koncových zařízení - 2500 v redundantním clusteru |  |
| **04** | Řešení musí poskytovat vysokou dostupnost tak, aby v případě výpadku primárního serveru převzal jeho roli sekundární server. |  |
| **05** | Možnost vytváření clusteru více virtuálních appliance. Minimální počet podporovaných appliance v clusteru - 2. |  |
| **06** | Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance. |  |
| **07** | Podpora předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě). |  |
| **08** | Požadované metody autentizace uživatelů a zařízení: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace. |  |
| **09** | Podpora RADIUS CoA. |  |
| **10** | Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD. |  |
| **11** | Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období. |  |
| **12** | Možnost TACACS+ autentizace správců síťových zařízení. |  |
| **13** | Další požadované autentizační a autorizační zdroje a metody: LDAP, MS AD, Token, MAC, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta). |  |
| **14** | Možnost integrace s MDM (Mobile Device Management) platformami třetích stran: minimálně AirWatch, Citrix, MobileIron, JAMF, InTune. |  |
| **15** | Podpora REST API pro většinu základních úkonů systému. |  |
| **16** | Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.) |  |
| **17** | Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení. |  |
| **18** | Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran. |  |
| **19** | Sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě. |  |
| **20** | LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter, Google+. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě s SMS, email ověřením nebo na elektronickou notifikaci a schválení pověřených pracovníků. |  |
| **21** | Možnost licenčního rozšíření o bezpečnou registraci soukromých zařízení do interní sítě na základě uživatelských údajů z AD či LDAP. Uživatel musí být schopen jednoduchým uživatelským wizardem instalovat osobní certifikát a síťový profil na své soukromé zařízení (BYOD systém). |  |
| **22** | Možnost licenčního rozšíření o certifikační autoritu pro vydávání certifikátů na soukromá zařízení musí být součástí systému. |  |
| **23** | Možnost licenčního rozšíření o samoobslužný portál pro hosty či interní uživatele s možností správy svých vlastních registrací. |  |
| **24** | Možnost licenčního rozšíření o systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení. |  |
| **25** | Možnost licenčního rozšíření o kontroly stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku. |  |
| **26** | Možnost licenčního rozšíření o podporu jednorázového i permanentního klienta pro kontroly na koncových zařízeních. Podpora klienta pro kontrolu koncových zařízení na OS Windows, MAC OS a Linux |  |
| **27** | Možnost licenčního rozšíření o integraci tohoto koncového klienta s VPN klientem |  |
| **28** | Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je systém. |  |
| **29** | Zadavatel požaduje předložení návrhu implementace segmentace sítě (VLAN) a rozložení HW zdrojů do objektu Active Directory. Po schválení návrhu provede uchazeč implementaci dle schváleného návrhu. |  |
| **30** | Řešení musí být kompatibilní se stávajícími prvky Aruba Networks. |  |
| **31** | Technické řešení segmentace sítě musí být integrováno s firewally za účelem sdílení identity a předávání stavových informací o bezpečnosti přistupujícího klienta. Nástroj segmentace musí být schopen komunikovat s firewallem oboustranně. Nejmenší množina atributů integrace je IP adresa, uživatelské jméno, uživatelská role, doména, typ zařízení (PC, chytrý telefon apod.), doménové jméno zařízení, operační systém zařízení a finálně postoj platformy ke stavu ověření. |  |
| **32** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

5.4 Technická specifikace DLP

(1) V současné době není implementována technologie DLP pro ochranu citlivých dat, a to jak na koncových stanicích, serverech nebo perimetru.

(2) Předmětem dodávky by měl být nástroj, který zajistí audit pohybu dat a detekci rizikových operací, pro klasifikaci citlivých a důvěrných dat a ochranu citlivých a důvěrných dat před únikem.

(3) **Minimální požadavky** na technickou specifikaci DLP pro 800 koncových stanic (PC, NB) jsou uvedeny v následující tabulce.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **01** | Klasifikace dat na základě obsahu minimálně v běžných textových souborech (čisté txt, office dokumenty, pdf apod.). |  |
| **02** | Vyhledávání vzorků pro obsahovou klasifikaci alespoň v nejběžnějších druzích obrázkových formátů (OCR) a to jak samostatně, tak i vnořených ve výše uvedených textových formátech (viz bod 01). |  |
| **03** | Možnost zadání vzorků pro obsahovou klasifikaci alespoň pomocí regulárních výrazů, výčtem vyhledávaných řetězců, importem (slovníky). |  |
| **04** | Existence předpřipravených vzorků pro obsahovou klasifikaci alespoň pro část informací obecně považovaných za citlivé. |  |
| **05** | Klasifikace dat na základě zdroje, ze kterého byly získány (konkrétní aplikace/skupina aplikací, konkrétní webová stránka/skupina webů, síťová cesta/lokální cesta). |  |
| **06** | Klasifikace dat na základě typů souborů (záchytná varianta pro typy nepodporované přímo obsahovou klasifikací). |  |
| **07** | DLP politiky definovatelné jak obecně, pro všechna přenášená data, tak i pro jednotlivé datové typy, které vzešly z některého typu datové klasifikace. |  |
| **08** | Možnost tvorby DLP politik i za využití metadat klasifikace třetích stran. |  |
| **09** | Možnost tvorby DLP politik s příslušnými atributy minimálně pro řízení e-mail komunikace (jak nativní aplikace, tak i webmaily), uploadu na síťová úložiště pomocí nativních aplikací, uploadu na web za použití browseru/webových aplikací obecně, uploadu souborů pomocí komunikačních aplikací (Teams, Zoom, instant messaging aplikace apod.). |  |
| **10** | Možnost řízení pohybu dat směrem na lokální výměnná datová úložiště (USB zařízení, Bluetooth přenosy apod.). |  |
| **11** | Možnost řízení tiskových operací (lokální/síťové tiskárny, tisk do souborů). |  |
| **12** | Možnost definovat reakci politiky alespoň ve variantách povolit, zaznamenat (případně navíc upozornit uživatele), blokovat. |  |
| **13** | Možnost definice výjimek z jednotlivých DLP politik. |  |
| **14** | Možnost uchování dokumentů zachycených politikou pro pozdější analýzu. |  |
| **15** | GUI pro správu DLP systému (nativní aplikace pro Win OS platformu, nebo aplikace běžící v standardních webových prohlížečích). |  |
| **16** | Integrace s AD (načítání a párování informací o klientských stanicích a uživatelích, možnost definice DLP politik na bázi AD objektů). |  |
| **17** | Centrální správa klientů (aktivace/deaktivace, upgrade). |  |
| **18** | Možnost deaktivace jednotlivých funkcionalit klienta pro případný troubleshooting. |  |
| **19** | Možnost zasílání upozornění o závažných provozních událostech a porušení DLP politik (e-mail, snmp trap apod.). |  |
| **20** | Uchování auditních záznamů o konfiguračních úpravách DLP. |  |
| **21** | Možnost exportu auditních informací do jiných systémů (např. centrální logování, SIEM) minimálně pomocí Syslog protokolu. |  |
| **22** | Generování reportů a grafů se záznamy o vyhodnocení/porušení DLP politik. |  |
| **23** | Komunikace mezi klientskými a serverovými komponentami, stejně jako mezi management rozhraním a serverem je zabezpečená kryptografickými prostředky aktuálně považovanými za bezpečné. |  |
| **24** | Administrátorům je možné přiřazovat role, které definují přístupová oprávnění k jednotlivým komponentám management rozhraní. |  |
| **25** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

5.5 Technická specifikace úložiště pro PACS a NIS data formou NAS a S3

(1) Pro nestrukturovaná data bude k dispozici úložiště postavené na technologii scale-out. Cílem fungování tohoto úložiště je zajištění bezpečného místa pro uložení objemných soborů jako jsou například PACS data, a tím zajistit dostupnost informací. Úložiště bude přímo integrováno s Microsoft Active Directory.

(2) Řešení bude obsahovat scale out architekturu s nejméně 4 identickými uzly postavenou na principu redundance médií pomocí technologie erasure coding. Řešení musí být odolné na výpadek jednoho hardware uzlu a nejméně 2 médií-disků z každého uzlu. Jednotlivé aplikace k úložišti mohou přistupovat pomocí protokolů S3, NFS a případně SMB.

(3) **Minimální požadavky** na technickou specifikaci úložiště pro PACS a NIS data formou NAS a S3 jsou uvedeny v následující tabulce.

|  |  |  |
| --- | --- | --- |
| **ID** | **Požadované parametry** | **Splněno** |
| **01** | Úložiště určené pro montáž do standardního racku 19“. |  |
| **02** | Nabízené úložiště je postavené na architektuře scale-out se škálovatelností min.na 30 nodů. |  |
| **03** | Požadujme minimálně 4 nody o celkové výšce max. 8 RU. |  |
| **04** | Úložiště má nativní podporu souborových protokolů SMB v3 a NFS v4.1 nebo vyšších verzí a objektového protokolu S3. |  |
| **05** | Data rozprostřená mezi nody jsou chráněna technologií erasure coding. |  |
| **06** | Úložiště pro získání identit či stromu přístupových oprávnění umí přistupovat do Microsoft Active Directory. |  |
| **07** | Podpora protokolu S3 pro přesouvání záloh z úložiště. |  |
| **08** | Požadujeme odolnost úložiště vůči výpadku jednoho nodu anebo nejméně dvou libovolných disků z libovolného nodu. |  |
| **09** | Datový prostor pro uživatele/aplikace musí být prezentován jako jeden prostor (name space). Požadujeme integrovaný load balancer pro rovnoměrné rozložení zátěže mezi nody. |  |
| **10** | Úložiště poskytuje funkce pro replikaci mezi dvěma úložišti na úrovni souborové vrstvy s kontinuálním průběhem (synchronní anebo asynchronní replikace). |  |
| **11** | Úložiště musí podporovat šifrování dat (data at rest encryption), minimálně na úrovni AES-256. Šifrování nesmí být závislé na hardware pro zajištění bezpečné přenositelnosti dat mezi různými hardwarovými platformami. Řešení musí zajistit ochranu dat proti krádeži médií i po vyřazení médií z provozu. Řešení podporuje externí PKI. |  |
| **12** | Požadujeme podporu vytváření uzamykatelných snapshotů, jako ochrana proti ransomware. Tato funkce ve spojení se zálohovacím softwarem by měla zaručit, že repositář záloh zůstane nezměnitelným úložištěm souborů. |  |
| **13** | Deduplikační a kompresní poměr nelze z důvodu ukládání již redukovaných dat započítat do celkové nabízené kapacity pole.  Požadovaná čistá kapacita úložiště dostupná aplikacím/uživatelům je nejméně 180 TB při zachování všech požadovaných vlastností. |  |
| **14** | Úložiště bude osazeno minimálně 8 x 25GbE porty tj. min. dva porty na každý nod. |  |
| **15** | Požadovaný výkon nabízeného pole musí být minimálně 46 000 IOPS (NFSv4.1). Celkový požadovaný výkon úložiště pro operace čtení je min. 6 GB/s a pro operace zápisu min. 4 GB/s. Jeden klient musí být schopen zapisovat kontinuální rychlostí minimálně 1 GB/s a číst rychlostí 2GB/s. Takový výkon musí být pole schopné poskytnout na 100% požadované kapacity. |  |
| **16** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

5.6 Technická specifikace infrastruktury pro zálohování a rychlou obnovu

(1) V současné chvíli zálohování nemocnice neodpovídá požadavkům zákona o kybernetické bezpečnosti (ochrana proti ransomware a off line zálohování). Nové řešení by mělo zajistit lepší dostupnost informací.

(2) Předmětem dodávky je zálohovací server a také pásková knihovna.

(3) **Minimální požadavky na** technickou specifikaci infrastruktury pro zálohování a rychlou obnovu jsou uvedeny v následující tabulce.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Zálohovací server** | | |
| **01** | Zálohovací server určený pro montáž do standardního racku 19“ o maximální výšce 2 RU. |  |
| **02** | Dvě CPU kompatibilní s virtualizační platformou VMware vSphere 8.0U2. Zadavatel předpokládá 2x8 jader. Pokud Uchazeč zvolí jinou kombinaci musí zajistit dostatečné licenční pokrytí počtu jader. CPU musí společně dosáhnout výkonu v testu SPEC CPU2017 nejméně 250 Floating point bodů pro metriku Base. Test by měl být vykonán nejméně na hardware stejného výrobce. |  |
| **03** | 8x 16 GB DDR4 DIMM o frekvenci min.2400MHz s rozšiřitelností na min. dvojnásobek DIMMů. |  |
| **04** | Min.6x 480 GB SSD pro rychlou obnovu a OS na nezávislém řadiči. |  |
| **05** | Min.24x 20TB 7,2k NL disků pro zálohy na nezávislém řadiči. |  |
| **06** | Min. 4x 10/25GbE SFP28 porty na dvou nezávislých NIC kartách. |  |
| **07** | FC HBA s dvěma porty, každý o rychlosti min. 16 Gb pro připojení páskové knihovny. |  |
| **08** | OOB management serveru s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, RedFish API s časově neomezenou licencí. |  |
| **09** | OOB management podporuje: MFA, integraci s MS AD, Silicon Root Of Trust, Secure Boot a Chain Of Trust (kontrola celého výrobního řetězce), TPM 2.0. |  |
| **10** | Min.2x 800 W hot-plug napájecí zdroj s platinovou účinností. |  |
| **11** | Součástí serveru je licence Microsoft Windows Standard 2022 na všechna CPU jádra serveru. |  |
| **12** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |
| **Pásková knihovna** | | |
| **13** | Pásková knihovna určená pro montáž do standardního racku 19“ o maximální výšce 2 RU. |  |
| **14** | Nabízená pásková knihovna musí interně uložit data o kapacitě min. 288TB (nekomprimovaně) respektive 720 TB (2.5:1 komprimovaně) pomocí technologie LTO-8. |  |
| **15** | Knihovna má minimálně 24 interních pozic pro pásky a má zabudovanou čtečku čárových kódů. |  |
| **16** | Knihovna je osazena LTO-8 páskovou mechanikou s FC 8Gb rozhraním s možností osazení další mechaniky. |  |
| **17** | Pásková mechanika musí umět přizpůsobovat svoji rychlost rychlosti přicházejících dat tak, aby nedocházelo k zbytečnému opotřebení mechanik i pásek. |  |
| **18** | Mechanika LTO-8 v knihovně musí podporovat zápis na WORM média a mít vestavěnou podporu šifrování min.na úrovni AES 256. |  |
| **19** | Součástí nabídky bude příslušenství 20 ks LTO-8 pásek včetně barcode štítků a jeden ks pásky na čištění mechanik. |  |
| **20** | Přímý propojovací kabel QSFP28 25GbE 3 metry, Originální kabel výrobce síťových prvků kompatibilní s dodávanými technologiemi, 40 ks |  |
| **21** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

5.7 Technická specifikace pro zvýšení dostupnosti záložního datového centra a lokální sítě

1. Žadatel v současné době nedisponuje žádným systémem, který by vhodně zajistil zabezpečení infrastruktury nemocnice, jak z pohledu spolehlivosti a vysoké dostupnosti, tak z pohledu kybernetické bezpečnosti.
2. Předmětem této části specifikace je popis technologie zajišťující přístup k informačním aktivům.
3. Technické řešení bude integrováno do stávajícího síťového prostředí, které je postaveno na prvcích společnosti Aruba Networks.
4. Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku.
5. Páteřní přepínače slouží k agregaci přístupových přepínačů a také k připojení ostatních technologií v rámci datového centra. Páteřní přepínače musí utvářet dva logické stohy, které budou nakonfigurovány, tak že bude mezi serverovnami možné sdílet stejné adresní rozsahy. Tento požadavek vyplývá z potřeby zajištění migrace jednotlivých VM mezi dvěma výše zmíněnými stohy bez nutnosti re-adresace VM (vMotion).
6. **Minimální požadavky** na technickou specifikaci zvýšení dostupnosti datového centra jsou uvedeny v následujících tabulkách této kapitoly.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Páteřní přepínače 4ks** | | |
| **1** | Rackmount 19“ |  |
| **2** | Plná podpora IPv4/IPv6 |  |
| **3** | Plnohodnotná licence bez nutnosti ověření na externích serverech, provoz po dobu 12-ti let s využitím všech požadovaných funkcí včetně aktivace všech portů |  |
| **4** | Provoz bez dostupnosti sítě internet |  |
| **5** | Jumbo frames větší než 9000 B |  |
| **6** | Management – serial konzole, SSH, https, SNMPv1,2,3, REST API |  |
| **7** | SNMPv3 trap, SYSLOG, RMON |  |
| **8** | NTP klient |  |
| **9** | IGMP, IGMP snooping |  |
| **10** | Plná implementace 802.1q – 4094 VLAN, určení nativní a management VLAN |  |
| **11** | Implementace LACP podle 802.3ad – minimálně 4 nezávislé skupiny po 4 fyzických portech |  |
| **12** | Implementace QoS – minimálně 8 HW fronty |  |
| **13** | RADIUS klient – přihlašování na MGMT s ověřením na RADIUS serveru s rozlišením minimálně dvou úrovní přístupu (dohled, administrator) |  |
| **14** | Definice rozdílných Radius serverů pro ověření MGMT přístupu a ověření uživatelů přes 802.1X |  |
| **15** | MSTP, RSTP, STP root guard, STP BPDU guard |  |
| **16** | Omezení počtu broadcastů na koncových portech – broadcast Storm control |  |
| **17** | Download/upload konfigurace v textovém tvaru |  |
| **18** | Archivování min. dvou verzí konfigurací a firmware přímo v zařízení |  |
| **19** | DHCP snooping, IPv6 MLD snooping |  |
| **20** | ARP inspection nebo obdobná funkcionalita dle výrobce |  |
| **21** | IP ACL na mgmt user interface |  |
| **22** | Možnost použití OEM SFP, SFP+, SFP28 a QSFP28 modulů |  |
| **23** | Nástroj pro vytváření uživatelských scriptů a jejich automatické spouštění |  |
| **24** | Přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků |  |
| **25** | 48 portů 10G/25G |  |
| **26** | 6 portů QSFP28 100G+ |  |
| **27** | Konfigurace jednotné rychlosti portů (1G/10G/25G) max. pro skupinu 4 portů |  |
| **28** | Dual stack IPv4 a IPv6 (včetně multicast komunikace pro obě rodiny protokolů) |  |
| **29** | Plná podpora L3 routingu IPv4, IPv6 (static, OSPFv3, BGPv4) |  |
| **30** | Stackování min. 2ks zařízení (jednotný management stacku jako jednoho zařízení včetně jednotné routovací tabulky), stohování přes QSFP28 moduly |  |
| **31** | MLAG – sdružení 8 linek přes 2 switche |  |
| **32** | LACP (802.3ad) při použití MLAG |  |
| **33** | Duální zdroje napájení hotswap |  |
| **34** | Data Center Bridging - DCBx Data Center Bridging Exchange Protocol, Priority Flow Control (PFC), Enhanced Transmission Selection (ETS) |  |
| **35** | Policy routing na základě ACL, IP prefix, as path |  |
| **36** | VRF s minimálně 16 instancemi při zapnutém dynamickém routingu |  |
| **37** | Směrování multicast provozu (včetně IPv6), IGMPv3 |  |
| **38** | Protokol VRRP, použití v rámci VRF instancí |  |
| **39** | Protokol ECMP |  |
| **40** | DoS prevention nebo obdobná funkcionalita dle výrobce |  |
| **41** | Packet Port Buffer nejméně 32MB |  |
| **42** | Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) a objem dat se vzorkováním min. 20:1 – analýza přímo na zařízení s historií 180dní nebo export informací na 2 cílové destinace. Sběr na min. na 8 portech současně. |  |
| **43** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Přístupové přepínače bez PoE 30ks** | | |
| **1** | Rackmount 19“ |  |
| **2** | Plná podpora IPv4/IPv6 |  |
| **3** | Plnohodnotná licence bez nutnosti ověření na externích serverech, provoz po dobu 12-ti let s využitím všech požadovaných funkcí včetně aktivace všech portů |  |
| **4** | Provoz bez dostupnosti sítě internet |  |
| **5** | Jumbo frames větší než 9000 B |  |
| **6** | Management – serial konzole, SSH, https, SNMPv1,2,3, REST API |  |
| **7** | SNMPv3 trap, SYSLOG, RMON |  |
| **8** | NTP klient |  |
| **9** | IGMP, IGMP snooping |  |
| **10** | Plná implementace 802.1q – 4094 VLAN, určení nativní a management VLAN |  |
| **11** | Implementace LACP podle 802.3ad – minimálně 4 nezávislé skupiny po 4 fyzických portech |  |
| **12** | Implementace QoS – minimálně 8 HW fronty |  |
| **13** | RADIUS klient – přihlašování na MGMT s ověřením na RADIUS serveru s rozlišením minimálně dvou úrovní přístupu (dohled, administrator) |  |
| **14** | Definice rozdílných Radius serverů pro ověření MGMT přístupu a ověření uživatelů přes 802.1X |  |
| **15** | MSTP, RSTP, STP root guard, STP BPDU guard |  |
| **16** | Omezení počtu broadcastů na koncových portech – broadcast Storm control |  |
| **17** | Download/upload konfigurace v textovém tvaru |  |
| **18** | Archivování min. dvou verzí konfigurací a firmware přímo v zařízení |  |
| **19** | DHCP snooping, IPv6 MLD snooping |  |
| **20** | ARP inspection nebo obdobná funkcionalita dle výrobce |  |
| **21** | IP ACL na mgmt user interface |  |
| **22** | Možnost použití OEM SFP, SFP+, SFP28 a QSFP28 modulů |  |
| **23** | Nástroj pro vytváření uživatelských scriptů a jejich automatické spouštění |  |
| **24** | Přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků |  |
| **25** | Min. 48 portů RJ45 10/100/1000 |  |
| **26** | Min. 4 porty 10G SFP/SFP+ |  |
| **27** | Stackování min. 4ks zařízení do kruhu (jednotný management stacku jako jednoho zařízení včetně konfigurace LACP z více členů stacku), stackování přes SFP+ moduly se zařízeními v rámci komodit 3 až 6 |  |
| **28** | Autentizace připojených zařízení dle 802.1x, MAC address - autorizace dvou zařízení (multi-user, multi-method authentication on each port), včetně splnění obou požadavků:  a. každé v jiné VLAN na portu (telefon, PC), ověřování MAC adress na port, omezení počtu MAC na port b. v budoucnu doplnění funkcionality formou licence nebo appliance - každé zařízení v jiné vlan, nastavení bezpečnostních přístupových politik formou ACL (realizováno na koncovém portu switche nebo provoz směrován přes centrální appliance s nastavením filtrace) |  |
| **29** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Přístupové přepínače s PoE 30ks** | | |
| **1** | Rackmount 19“ |  |
| **2** | Plná podpora IPv4/IPv6 |  |
| **3** | Plnohodnotná licence bez nutnosti ověření na externích serverech, provoz po dobu 12-ti let s využitím všech požadovaných funkcí včetně aktivace všech portů |  |
| **4** | Provoz bez dostupnosti sítě internet |  |
| **5** | Jumbo frames větší než 9000 B |  |
| **6** | Management – serial konzole, SSH, https, SNMPv1,2,3, REST API |  |
| **7** | SNMPv3 trap, SYSLOG, RMON |  |
| **8** | NTP klient |  |
| **9** | IGMP, IGMP snooping |  |
| **10** | Plná implementace 802.1q – 4094 VLAN, určení nativní a management VLAN |  |
| **11** | Implementace LACP podle 802.3ad – minimálně 4 nezávislé skupiny po 4 fyzických portech |  |
| **12** | Implementace QoS – minimálně 8 HW fronty |  |
| **13** | RADIUS klient – přihlašování na MGMT s ověřením na RADIUS serveru s rozlišením minimálně dvou úrovní přístupu (dohled, administrator) |  |
| **14** | Definice rozdílných Radius serverů pro ověření MGMT přístupu a ověření uživatelů přes 802.1X |  |
| **15** | MSTP, RSTP, STP root guard, STP BPDU guard |  |
| **16** | Omezení počtu broadcastů na koncových portech – broadcast Storm control |  |
| **17** | Download/upload konfigurace v textovém tvaru |  |
| **18** | Archivování min. dvou verzí konfigurací a firmware přímo v zařízení |  |
| **19** | DHCP snooping, IPv6 MLD snooping |  |
| **20** | ARP inspection nebo obdobná funkcionalita dle výrobce |  |
| **21** | IP ACL na mgmt user interface |  |
| **22** | Možnost použití OEM SFP, SFP+, SFP28 a QSFP28 modulů |  |
| **23** | Nástroj pro vytváření uživatelských scriptů a jejich automatické spouštění |  |
| **24** | Přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků |  |
| **25** | 48 portů RJ45 10/100/1000 |  |
| **26** | 4 porty 10G SFP/SFP+ |  |
| **27** | Stackování min. 4ks zařízení do kruhu (jednotný management stacku jako jednoho zařízení včetně konfigurace LACP z více členů stacku) stackování přes SFP+ moduly se zařízeními v rámci komodit 3 až 6 |  |
| **28** | PoE class 4 (PoE+ - 802.3at max. 30W/port) s možností využití na všech portech switche při současném příkonu 15,4 W/port. |  |
| **29** | Autentizace připojených zařízení dle 802.1x, MAC address - autorizace dvou zařízení (multi-user, multi-method authentication on each port), včetně splnění obou požadavků:  a. každé v jiné VLAN na portu (telefon, PC), ověřování MAC adress na port, omezení počtu MAC na port b. v budoucnu doplnění funkcionality formou licence nebo appliance - každé zařízení v jiné vlan, nastavení bezpečnostních přístupových politik formou ACL (realizováno na koncovém portu switche nebo provoz směrován přes centrální appliance s nastavením filtrace) |  |
| **30** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Přístupové přepínače bez PoE 24 portů 30ks** | | |
| **1** | Rackmount 19“ |  |
| **2** | Plná podpora IPv4/IPv6 |  |
| **3** | Plnohodnotná licence bez nutnosti ověření na externích serverech, provoz po dobu 12-ti let s využitím všech požadovaných funkcí včetně aktivace všech portů |  |
| **4** | Provoz bez dostupnosti sítě internet |  |
| **5** | Jumbo frames větší než 9000 B |  |
| **6** | Management – serial konzole, SSH, https, SNMPv1,2,3, REST API |  |
| **7** | SNMPv3 trap, SYSLOG, RMON |  |
| **8** | NTP klient |  |
| **9** | IGMP, IGMP snooping |  |
| **10** | Plná implementace 802.1q – 4094 VLAN, určení nativní a management VLAN |  |
| **11** | Implementace LACP podle 802.3ad – minimálně 4 nezávislé skupiny po 4 fyzických portech |  |
| **12** | Implementace QoS – minimálně 8 HW fronty |  |
| **13** | RADIUS klient – přihlašování na MGMT s ověřením na RADIUS serveru s rozlišením minimálně dvou úrovní přístupu (dohled, administrator) |  |
| **14** | Definice rozdílných Radius serverů pro ověření MGMT přístupu a ověření uživatelů přes 802.1X |  |
| **15** | MSTP, RSTP, STP root guard, STP BPDU guard |  |
| **16** | Omezení počtu broadcastů na koncových portech – broadcast Storm control |  |
| **17** | Download/upload konfigurace v textovém tvaru |  |
| **18** | Archivování min. dvou verzí konfigurací a firmware přímo v zařízení |  |
| **19** | DHCP snooping, IPv6 MLD snooping |  |
| **20** | ARP inspection nebo obdobná funkcionalita dle výrobce |  |
| **21** | IP ACL na mgmt user interface |  |
| **22** | Možnost použití OEM SFP, SFP+, SFP28 a QSFP28 modulů |  |
| **23** | Nástroj pro vytváření uživatelských scriptů a jejich automatické spouštění |  |
| **24** | Přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků |  |
| **25** | 24 portů RJ45 10/100/1000 |  |
| **26** | 4 porty 10G SFP/SFP+ |  |
| **27** | Stackování min. 4ks zařízení do kruhu (jednotný management stacku jako jednoho zařízení včetně konfigurace LACP z více členů stacku), stackování přes SFP+ moduly se zařízeními v rámci komodit 3 až 6 |  |
| **28** | Autentizace připojených zařízení dle 802.1x, MAC address - autorizace dvou zařízení (multi-user, multi-method authentication on each port), včetně splnění obou požadavků:  a. každé v jiné VLAN na portu (telefon, PC), ověřování MAC adress na port, omezení počtu MAC na port b. v budoucnu doplnění funkcionality formou licence nebo appliance - každé zařízení v jiné vlan, nastavení bezpečnostních přístupových politik formou ACL (realizováno na koncovém portu switche nebo provoz směrován přes centrální appliance s nastavením filtrace) |  |
| **29** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

1. Stávající přepínače využívají technologii Aruba Networks Virtual Switching Framework (VSF) pro stohování https://www.arubanetworks.com/techdocs/AOS-S/16.11/MCG/WC/content/wc/vir-swi-fra-vsf.htm . Zadavatel předpokládá využití technologie s nejméně stejnými vlastnostmi jako stávající VSF.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Transceiver 8ks 100GBASE-SR4** | | |
| **1** | Transceiver QSFP28 100GBASE-SR4, MM, 100m, DDM |  |
| **2** | Kompatibilní s dodávanými aktivními prvky |  |
| **3** | Propojovací optický patchcord o délce 5m, konektorové osazení dle požadavků zadavatele |  |
| **4** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Transceiver 4ks 100GBASE-LR4** | | |
| **1** | Transceiver QSFP28 100GBASE-SR4, MM, 100m, DDM |  |
| **2** | Kompatibilní s dodávanými aktivními prvky |  |
| **3** | Propojovací optický patchcord o délce 5m, konektorové osazení dle požadavků zadavatele |  |
| **4** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Bezdrátové přístupové body 70ks** | | |
| **1** | konfigurace minimálně via SSH, seriový console port |  |
| **2** | minimálně 1x RJ45 lan port 10/100/1000Mbit/s |  |
| **3** | napájení přes PoE |  |
| **4** | certifikace Wi-Fi Alliance |  |
| **5** | 802.11 g/n + 802.11a/n/ac/ax pracující v souběhu (dual radio) |  |
| **6** | WPA, WPA2, WPA3 |  |
| **7** | ruční i automatická volba kanálu (RF management) |  |
| **8** | AP v souladu s DFS a v souladu s podmínkami pro provoz systému v ČR |  |
| **9** | RF Management musí vybrat nové kanály na základě SNR (signal-to-noise ratio) a vytížení kanálu |  |
| **10** | virtuální SSID s podporou minimálně 10 vyzařovaných sítí/radio |  |
| **11** | 802.1q, mapování VLAN–BSSID i při nedostupnosti kontroleru |  |
| **12** | ochrana rychlejších klientů na stejném rádiu |  |
| **13** | L2 izolace bezdrátových klientů |  |
| **14** | CAPWAP tunelování provozu na kontroler a zapouzdření dat z vysílaných sítí do CAPWAP tunelu nebo obdobné tunelovací řešení |  |
| **15** | vyústění provozu ze SSID sítí lokálně na AP (do VLAN) nebo až na kontroleru |  |
| **16** | 802.11e protokol včetně WMM a U-APSD |  |
| **17** | “plug and play” instalace = (AP si vyhledá kontroler a nakonfiguruje se) |  |
| **18** | monitoring AP z kontroleru |  |
| **19** | při výpadku AP musí okolní AP zvýšit vlastní výkon - pokrytí. Optimální výběr kanálu musí být rekonfigurován dynamicky bez zásahu správce |  |
| **20** | 802.1X – rodinu EAP protokolů s možností volby alespoň dvou AAA serverů Radius per SSID/WPAx/802.1X |  |
| **21** | podpora IP Quality of Service na bezdrátové i drátové straně. Rozlišování paketů musí být podporováno na vstupu i výstupu na DiffServ, IP ToS a IP Precedence. |  |
| **22** | filtrování multicast provozu |  |
| **23** | SNMPv3, SNMPv3 trap, syslog ve standalone mode |  |
| **24** | LED diody informující o stavu zařízení s možností vypnutí |  |
| **25** | úchyt AP na zeď/strop (montážní kit) v dodávce |  |
| **26** | přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků |  |
| **27** | Wi-Fi standard a/b/g/n/ac/ax |  |
| **28** | minimálně 2x RJ45 lan porty 100/1000Mbps |  |
| **29** | LACP |  |
| **30** | PoE standard 802.3 at |  |
| **31** | 2x2 MIMO 2.4GHz pásmo |  |
| **32** | 04x4 MIMO 5 GHz pásmo |  |
| **33** | integrovaná anténou |  |
| **34** | Fyzická instalace AP a připojení ke kontroleru (instalace strukturované kabeláže není součástí) |  |
| **35** | Záruka bez omezení doby (tzv. doživotní záruka) nebo nejméně na 7 let |  |
| **36** | Záruka výrobce na hardware v režimu 9x5 s dodáním náhradního dílu do 10 pracovních dní |  |

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Bezdrátové kontroléry 2ks** | | |
| **1** | licenční pokrytí pro min. 330 zařízení |  |
| **2** | režim HA s automatickým failoverem AP na záložní kontroler |  |
| **3** | RF management přístupových bodů výše |  |
| **4** | možnost rozšíření počtu spravovaných přístupových bodů |  |
| **5** | počet připojených WiFi zařízení, klientů: minimálně 5000 per kontroler |  |
| **6** | CAPWAP tunel pro správu přístupových bodů nebo obdobné řešení |  |
| **7** | konfigurace via SSH, jednoduché a rychlé začlenění (AUTO DISCOVERY – L2 autodiscovery, DHCP option) nově přidaných nenakonfigurovaných přístupových bodů do centrálního managementu kontroleru |  |
| **8** | open/WEP/WPA/WPA2/ WPA3/AES(CCMP) 802.11i |  |
| **9** | Nastavení 4x SSID s určením radius server (SSID1 jiný radius server než SSID2 ...) |  |
| **10** | alertování, logování, monitoring přístupových bodů |  |
| **11** | zjišťování Rogue AP |  |
| **12** | automatické řízení zátěže přístupových bodů a jejich balancování |  |
| **13** | guest access přístup, rozhraní pro netechnickou osobu (např. recepce) pro vytvoření dočasného účtu pro hosty |  |
| **14** | rychlý WiFi roaming dle standardu 802.11r a 802.11k, včetně roamingu zařízení v režimu AAA |  |
| **15** | podpora IP Quality of Service na bezdrátové i drátové straně. Rozlišování paketů musí být podporováno na vstupu i výstupu na DiffServ, IP ToS a IP Precedence. |  |
| **16** | rate limiting per client a BSSID |  |
| **17** | L2-L4 access control listy |  |
| **18** | SNMPv3, lokální a vzdálený syslog, SNMPv3 trap |  |
| **19** | API pro získávání informací do monitorovacího systému |  |
| **20** | Ověřování MGMT na základě externích identit (např. RADIUS, Active directory,...) |  |
| **21** | centrální aktualizace firmware AP řízený kontrolerem |  |
| **22** | přístup k novým verzím firmware po dobu platnosti záručních a servisních požadavků |  |
| **24** | fyzický kontroler RACK mount provedení nebo jako součást AP |  |
| **25** | duální hotswap napájecí zdroje, redundantní úložiště dat a konfigurace (není požadováno při dodávce jako součást AP) |  |
| **26** | perpetual licence pro kontroler pro správu,mikrosegmentaci a dohled minimálně 330 přístupových bodů. |  |
| **27** | centralizování informací z jednotlivých AP |  |
| **28** | dohled stavu a výkonu AP, počtu klientů, bezdrátových sítí, aktuálně připojených uživatelů |  |
| **29** | statistiky, reporting o připojených klientech s retencí minimálně 180 dní, automatické odesílání definovaných reportů e-mailem |  |
| **30** | syslog, SNMP, REST API, alerting administrátora (zaslání informace o změně stavu systému) |  |
| **31** | architektura klient – server, šifrované připojení klienta |  |
| **32** | perpetual licence pro dohled 330 AP |  |
| **33** | server musí být dodán jako virtuální appliance pro VMWare ESX a Microsoft HyperV |  |
| **34** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

5.8 Technická specifikace ochrany operačních systémů a mobilních platforem

1. Řešení bude sloužit jako kompletní antivirová, antiransomware, antibot nebo antiphishing ochrana koncových stanic. Za přispění funkcí sandboxingu a extrakce potencionálně škodlivého obsahu musí zajistit aktivní prevenci na úrovni koncových klientů.
2. Plánované nasazení na servery, stanice a mobilní zařízení musí být kompatibilní s OS Windows, MacOS, Linux a také nejnovějším Android a iOS. S ohledem na celkový počet koncových stanic je vyžadována možnost centrální správy klientů, logování bezpečnostních incidentů a jejich reportingu.
3. **Minimální požadavky** na technickou specifikaci bezpečnosti koncových zařízení jsou uvedeny v následující tabulce.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **01** | Modulární architektura, která umožní zapnutí/vypnutí jednotlivých komponent. |  |
| **02** | Řešení ve formě SW na servery, uživatelské počítače a klientské mobilní zařízení (telefony, tablety). |  |
| **03** | Management formou virtuální appliance do prostředí VMware vSphere 7.0 a vyšší. Centrální správa koncových SW klientů, logování a reporting bezpečnostních incidentů. |  |
| **04** | Integrovaná funkce IPSec VPN klienta kompatibilní s VPN koncentrátorem. |  |
| **05** | SW na koncových stanicích nevyžaduje instalaci programů nebo nástrojů s administrativními funkcemi. |  |
| **06** | SW na koncových stanicích nevyžaduje lokální administrátorská práva ke spuštění. |  |
| **07** | Řešení využívá jiný AV engine než systém pro ochranu síťové bezpečnosti (NGFW). |  |
| **08** | Ochrana zabraňující koncovým uživatelům provádět změny (odinstalace, zastavit/spustit služby, změna zásad zabezpečení…). |  |
| **09** | Schopnost detekovat a zablokovat pokus o infekci známým malwarem. |  |
| **10** | Schopnost detekovat a odstranit malware na základě kombinace signatur, blokátorů chování a heuristické analýzy. Vyhledávání na základě IoC minimálně s těmito atributy (doména, IP adresa, URL záznam, MD5, SHA1). |  |
| **11** | Schopnost detekovat a identifikovat přítomnost virů v paměti systému, bootovacích sektorech, tabulkách oddílů a na všech formách dat uložených na pevném disku systému a jiných vyměnitelných médiích. |  |
| **12** | Schopnost detekovat, blokovat a odstranit škodlivé aplikace v reálném čase. |  |
| **13** | Skenování virů s minimálním dopadem na výkon koncové stanice. |  |
| **14** | Schopnost provést nápravná opatření k odstranění virového kódu z infikovaných souborů, zaváděcích sektorů nebo tabulek oddílů. |  |
| **15** | Přesun souboru infikovaného virem do karantény na místním pevném disku pro další kontrolu nebo akci. |  |
| **16** | Možnost karantény souborů nebo procesů. |  |
| **17** | Schopnost skenovat dokumenty Microsoft Office, komprimované soubory a grafické soubory. |  |
| **18** | Automatická identifikace vstupního bodu malware. |  |
| **19** | Extrakce potencionálně škodlivého obsahu, min podpora grafických souborů, MS Office a PDF. |  |
| **20** | Schopnost blokovat útoky bez ohledu na to, zda jsou webové, e-mailové, nebo z vyměnitelného média. |  |
| **21** | Řešení odolné proti "evasion" technikám moderního malwaru. |  |
| **22** | Schopnost detekovat zero-day útoky, detekcí a odesláním podezřelých souborů do prostředí sandboxu. |  |
| **23** | Podpora emulace spustitelných souborů, archivů, dokumentů, a Java souborů. |  |
| **24** | Detekce a ochrana proti „Command & Control“ komunikaci. |  |
| **25** | Detekce a ochrana proti ransomware. |  |
| **26** | Schopnost obnovit soubory při pokusu o zašifrování včetně automatické remediace systému. |  |
| **27** | Využití strojového učení pro detekci nových variant malwaru. |  |
| **28** | Uživatel má možnost provést AV kontrolu určitých jednotek, adresářů nebo souborů. |  |
| **29** | Schopnost ověřit integritu update virových signatur před aplikací. |  |
| **30** | Inkrementální update virových signatur. |  |
| **31** | SW klient schopen získat update signatur z centrálního management serveru i z internetu. |  |
| **32** | Nové signatury pravidelně vydávány a zpřístupněny alespoň jednou denně. |  |
| **33** | Shromážděné forenzní údaje jsou uloženy lokálně a data jsou chráněna před neoprávněným přístupem nebo narušením struktury. |  |
| **34** | Kolekce informací z OS, min. informace o procesech, síťové komunikaci, změny v registrech, přístupu k souborovým systémům. |  |
| **35** | SW informuje uživatele o pokusu infekce malwarem. |  |
| **36** | Možnost automaticky vygenerovat forenzní zprávu o provedení útoku. |  |
| **37** | Detekce mobilního malwaru. |  |
| **38** | Schopnost chránit před útoky na integritu mobilních operačních systémů. |  |
| **39** | Možnost white a black listing mobilních aplikací. |  |
| **40** | Detekce „rooting“ a „jailbraking“ zařízení. |  |
| **41** | Analýza rizika používaných mobilních aplikací. |  |
| **42** | Možnost blokovat přístup (URL filtering) podle kategorizace stránek. |  |
| **43** | Schopnost detekovat phishing nejen na základě reputace IP/URL, ale také na základě analýzy obsahu stránky. |  |
| **44** | Možnost pozdržet download ve webovém prohlížeči. |  |
| **45** | Centrální správa bezpečnostních politik a nastavení koncových klientů. |  |
| **46** | Centrální ukládání logů. |  |
| **47** | Komunikace mezi management serverem a koncovým klientem musí být autentizovaná a šifrovaná. |  |
| **48** | Integrace s AD. |  |
| **49** | Možnost vytvořit a spravovat logické skupiny napříč několika funkčními (AD) skupinami. |  |
| **50** | Schopnost vytvořit politiku na úrovni uživatele a skupiny. |  |
| **51** | Kontrola stavu koncové stanice (bezpečnostní politiky, verze OS, instalovaný SW, verze AV…). |  |
| **52** | Možnost vyhledat infikované stanice podle zvoleného IOC. |  |
| **53** | Možnost spuštění automatické analýzy incidentu. |  |
|  | Schopnost karantény nebo izolování koncové stanice. |  |
| **54** | Řešení nesbírá a nevyužívá žádná privátní uživatelská data. |  |
| **55** | Schopnost automaticky generovat podrobný forenzní report z detekovaných incidentů. |  |
| **56** | Schopnost generovat agregovaný report, obsahující data o koncových stanicích a síťová data. |  |
| **57** | Možnost zobrazení všech souvisejících událostí a incidentů. |  |
| **58** | Automatický report rozsahu vniknutí škodlivého softwaru. |  |
| **59** | Reporty obsahují seznam zasažených souborů a dat. |  |
| **60** | Úplný stromový přehled událostí a útoků. |  |
|  | Možnost automatizovat analýzu událostí. |  |
| **61** | Automatická analýza incidentů produktů třetích stran. |  |
| **62** | Zobrazení reputace souboru ve forenzní zprávě. |  |
| **63** | Možnost generování a stažení reportů uživatelem i administrátorem. |  |
| **64** | Možnost integrace se SIEM, SOAR. |  |
| **65** | Možnost integrace s MDM / EMM systémy. |  |
| **66** | Podpora zařízení typu BYOD a firemních zařízení |  |
| **67** | Podpora Internetových prohlížečů MS Edge, Google Chrome, Firefox. |  |
| **68** | Podpora "Split tunnelling". |  |
| **69** | Podpora připojení VPN v prostředí za NAT zařízeními a bránami firewall, které neumožňují IPSec provoz (možnost tuneloval VPN přes HTTPS). |  |
| **70** | Podpora ověřování VPN pomocí uživatelského jména/hesla, klientského certifikátu, LDAP/AD. |  |
| **71** | Podpora multi-faktorové autentizace VPN. |  |
| **72** | Podpora OS serverů a koncových stanic nejméně pro tyto systémy (Windows 7 SP1 (32-bit a 64-bit), Windows 10 (32-bit a 64-bit), Windows 11, Windows 2016, Windows 2019, MAC OS 11/12, Debian 10/11, Ubuntu 20/21/22, RHEL verze 7.8 – 8.7 a novější. ). |  |
| **73** | Podpora OS Android a iOS. |  |
| **74** | Licence musí pokrýt nejméně 800 koncových stanic (PC, NB) a 100 mobilních stanic (chytrý telefon, tablet apod). |  |

**5.8.1 Technická specifikace prostředí pro běh management a bezpečnostních prvků**

1. S ohledem na požadovaný výkon a funkce bezpečnostních platforem je nezbytné vytvořit nezávislé prostředí pro běh management nástrojů. Je požadováno dodání 2ks virtualizačních serverů a blokové diskové úložiště pro zajištění jejich vysoké dostupnosti.
2. Požadované licence pro technologii VMware a Veeam se vztahují výhradně k novým prvkům a musí zapadnout do stávajícího prostředí, které je postaveno na těchto produktech:

VMware vSphere, vSAN, vCenter server na několika platformách ve verzích Standard příp. Enterprise edition

Veeam Data Platform Foundation Standard Edition

1. **Minimální požadavky** na technickou specifikaci 2 ks serverů jsou uvedeny v následující tabulce. (platí pro jeden server)

| **Id** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **1** | montáž do standardního 19“ racku o maximální výšce 1 RU, chassis pro min. 8x 2,5“ disků |  |
| **2** | minimálně jeden 16-jádrový procesor s hodnotou dle SPECrate®2017\_int\_base min. 160 a SPECrate®2017\_fp\_base min. 220 pro 1 CPU konfiguraci (údaje musí být k dispozici na www.spec.org) |  |
| **3** | min. 512 GB RAM (min. 64GB moduly 4800MT/s s podporou ECC), server s celkem 32 DIMM pozicemi, každý paměťový kanál musí být osazen nejméně jedním modulem, všechny paměťové moduly musí být identické. Podpora rozšiřitelnosti až na min. 8TB RAM per server. |  |
| **4** | min. 2x 480GB NVMe RAID1 úložiště nevyužívající 2,5“ diskovou pozici |  |
| **5** | min. 4x 1GbE RJ-45 porty |  |
| **6** | min. 6x 10/25GbE SFP28 porty na třech nezávislých síťových kartách |  |
| **7** | management serveru nezávislý na operačním systému s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, časově neomezená licence |  |
| **8** | management musí podporovat dvoufaktorovou autentikaci, filtrování přístupu na základě IP adres (IP blocking) a AD/LDAP, podpora Silicon Root Of Trust, Secure Boot a TPM 2.0 |  |
| **9** | pro management požadujeme vestavěné GUI s podporou HTML5 a možnost komunikace pomocí: HTTPS, CLI, IPMI, REDFISH |  |
| **10** | nejméně 2 redundantní, za chodu vyměnitelné napájecí zdroje s platinovou účinností min. 800W každý |  |
| **11** | rackové ližiny a rameno na kabeláž na zadní straně serveru |  |
| **12** | dodání včetně 4x SFP28 25Gb twinaxial kabelů o délce 3m pro každý server |  |
| **13** | certifikace pro VMware 6.7u3 a vyšší, Windows Server 2016 a vyšší, Red Hat Enterprise Linux a SUSE Linux Enterprise Server |  |
| **14** | pro oba servery dohromady dodání 1x licence VMware vSphere Essentials Plus na všechna CPU jádra s podporou na 5 let |  |
| **15** | Zálohovací SW Veeam Data Platform Foundation na všechna CPU socket s podporou na 5 let |  |
| **16** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

1. **Minimální požadavky** na technickou specifikaci 1 ks blokového diskového úložiště jsou uvedeny v následující tabulce.

| **Id** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **1** | montáž do standardního 19“ racku o maximální výšce 4 RU |  |
| **2** | diskové pole musí být typu All Flash - NVMe pole s disky podporujícími PCI Gen4 technologii. |  |
| **3** | podpora aktuální verze nejpoužívanějších OS min. VMware vSphere 8.0, Windows 2022, RedHat Linux 9, Ubuntu 22.04. |  |
| **4** | diskové pole musí poskytovat min.hrubou (RAW) kapacitu 45TB. Tato kapacita bude očištěna o systémovou a spare kapacitu a s využitím technik datové redukce bude dostupná kapacita pro ukládání dat alespoň 60TB. Tato kapacita diskového pole musí být v budoucnu rozšiřitelná alespoň na dvojnásobek. (v rámci základního šasi nebo přidáním diskových polic) |  |
| **5** | diskové pole musí být flexibilně škálovatelné tj.podporovat škálování scale-up přidáváním NVMe diskových polic i scale-out pomocí zabudovaného klastrování. |  |
| **6** | Nabízené pole musí být škálovatelné alespoň na 24 NVMe disků v rámci základního šasi a musí být v budoucnu rozšiřitelné min. na dvojnásobek počtu disků v přídavných NVMe diskových policích (celkem tedy min. 48 NVMe disků). |  |
| **7** | V případě scale-out rozšiřování musí být možné rozprostřít LUNy přes všechy řadiče škálovatelného úložiště. |  |
| **8** | diskové pole musí být dodáváno s nejméně 64GB cache na jeden řadič pro operace čtení a zápisu. |  |
| **9** | operace zápisu musí být zcela chráněny a v případě výpadku napájení nesmí dojít ke ztrátě dat. Tento mechanismus se nesmí spoléhat na baterie. |  |
| **10** | diskové pole nesmí obsahovat Single Point Of Failure tj.musí být odolné min.proti výpadku jedné komponenty typu řadiče, zdroje, cache, ventilátoru, HBA apod. |  |
| **11** | výpadek žádné komponenty včetně řadiče diskového pole nesmí způsobit pokles požadovaného výkonu pole. |  |
| **12** | během kritických podpůrných činností, jako je aktualizace Firmwaru, aplikaci patche atd., musí být pole dostupné a nesmí dojít k degradaci výkonu. |  |
| **13** | diskové pole poskytuje na front-end portech diskového pole min. takovýto ustálený výkon:  55 tis.IOPS pro 100% random zátěž, velikost bloku 8kB a poměr čtení zápis 50/50.  2GB/s sekvenční čtení a 700MB/s sekvenční zápis při velikosti bloku 256kB. |  |
| **14** | diskové pole musí být odolné proti výpadku až tří disků současně. V případě, že to výrobce nepodporuje, pak RAID pole musí mít velikost maximálně 6D+2P |  |
| **15** | diskové pole musí být možné povýšit na novější generaci výměnou řadičů, aniž by bylo nutné měnit disky a případné diskové police. |  |
| **16** | Povýšení na novější generaci musí být možné provést bez odstávky diskového pole |  |
| **17** | diskové pole musí být dodáno min. s dvěma řadiči a 4x 25Gb IP porty. (každý front-end PCI slot musí mít nejméně 8 linek PCI Gen4) |  |
| **18** | diskové pole musí mít také podporu pro 100Gb ETH porty (pro případné rozšíření) |  |
| **19** | diskové pole musí podporovat nastavení Quality of Services (QoS) na úrovni LUN nebo VMware vVol s granularitou nastavení min. na úrovni IOPS a MB/sec. |  |
| **20** | diskové pole musí podporovat tyto funkce - inline de-duplikace, komprese a thin provisioning |  |
| **21** | diskové pole musí podporovat ne-deduplikované a duplikované LUNy současně |  |
| **22** | diskové pole musí podporovat synchronní i asynchronní replikaci dat mezi diskovými poli. |  |
| **23** | disková pole musí umět vytvořit jedno logické pole pro vytvoření storage geo-klastru s automatickým transparentním failoverem mezi lokalitami a funkcionalitou svědka na třetí lokalitě pro zabránění split-brain syndromu |  |
| **24** | diskové pole musí mít schopnost replikovat data z All Flash do Hybridního diskového pole, nebo naopak v rámci dané rodiny polí. |  |
| **25** | Prodejce poskytne licence pro všechny požadované funkce, jako je Snapshot, Clone, Replikace, QoS, management apod., pro celkovou kapacitu pole. Pro budoucí zvýšení kapacity nebude vyžadována žádná dodatečná softwarová licence. Jakákoli dodatečná licence vyžadovaná pro splnění technické specifikace musí být nabídnuta předem. |  |
| **26** | dodání včetně 4x SFP28 25Gb twinaxial kabelů o délce 3m |  |
| **27** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |

5.9 Technická specifikace pro přihlašování k počítačům a aplikacím v rámci klinických a THP provozů

1. Řešení nabídne univerzálně funkční SSO technologie pro jakékoli webové/desktopové/cloudové/virtualizované aplikace, která by pomohla výrazně snížit čas uživatelů potřebný k přihlašování do IT systémů a aplikací.
2. **Minimální požadavk**y na technickou specifikaci pro přihlašování k počítačům a aplikacím v rámci klinických a THP provozů jsou uvedeny v následující tabulce.

| **ID** | **Požadované parametry** | **Splněno** |
| --- | --- | --- |
| **Obecné požadavky** | | |
| **01** | Klientská část řešení musí podporovat Windows Desktop OS (Windows 10 a novější), Linuxové OS tenkých klientů a v případě mobilních klientských zařízení minimálně operační systémy Windows a Android. Řešení musí licenčně pokrýt min. 1000 jmenovitých uživatelů. |  |
| **02** | Řešení bude ve výchozím stavu navrženo a dodáno jako vysoce dostupné, s odolností vůči výpadku jednoho serverového prvku, s minimálně dvěma vzájemně zastupitelnými prvky. Při výpadku jednoho prvku zůstává řešení plně funkční, zbylý funkční prvek/prvky nadále poskytují plnou funkčnost. K překlopení na funkční prvek/prvky musí dojít automaticky, bez nutnosti ručního zásahu, maximálně v jednotkách sekund. Všechny prvky si vzájemně replikují nastavení a data, v případě výpadku prvku tedy nedojde ke ztrátě nastavení či dat. Všechny prvky řešení musí být spravovány jako jeden celek, jednotnou správou z webové konzoly, napříč datovými centry případně cloudy. |  |
| **03** | Serverová část řešení bude nasazena ve formě virtuálních strojů (podpora minimálně VMware vSphere, Microsoft Hyper-V). Virtuální stroje musí být možné, a ze strany výrobce podporované, provozovat v cloudu (podpora minimálně Microsoft Azure). Řešení musí být možné nasadit také v hybridním režimu, kdy jeden nebo více virtuálních strojů je provozováno v datovém centru on premises a další virtuální stroj nebo stroje v cloudu, formou SaaS. |  |
| **04** | Řešení musí umožnovat definovat práva na činnosti ve správcovských nástrojích na základě členství v Active Directory skupinách. Řešení musí být schopno definovat různé úrovně administrátorských přístupů – delegování administrativních oprávnění – vytvořením kombinací (sad) oprávnění. |  |
| **05** | Řešení musí být integrováno na adresářovou službu Microsoft Active Directory Directory Services (AD DS), identita – uživatelský účet – uživatele dodaného řešení musí odpovídat identitě v AD DS. Změny v AD DS (změny stavu účtu, atributů, členství ve skupinách) musí být automaticky synchronizovány s dodaným řešením. Řešení nesmí modifikovat schéma Active Directory. Dodané řešení musí být možné integrovat na další adresářové (LDAP) služby. Řešení musí podporovat Security Assertion Markup Language 2.0 (SAML 2.0) a federaci s krajským řešením Vysočina ID. |  |
| **06** | Komunikace mezi jednotlivými komponentami řešení v rámci HTTPS komunikace musí být šifrována TLS protokolem minimálně verze 1.2, uložená citlivá data – zejména přihlašovací údaje uživatelů – musí být chráněna šifrováním AES 256. |  |
| **Více-faktorová autentizace** | | |
| **07** | Řešení musí umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci, minimálně: kontaktní čipové karty (smart karty), bezkontaktní karty včetně karet Mifare DesFire a FIDO, USB tokeny, bezkontaktní RFID předměty, biometrické prvky (otisk prstu), login/heslo (s vazbou i bez vazby na adresářovou službu), a jejich vzájemné kombinace. Vyžádání druhého faktoru musí být možné definovat dynamicky, na základě splnění podmínky (např. uplynutí časového intervalu). |  |
| **08** | Řešení musí pro vybrané uživatele poskytnout funkci tzv. „Push“ autentizace a/nebo autentizace pomocí OTP (One-Time Password) pro přihlášení ke koncovým zařízením s Windows OS a do VPN prostřednictvím mobilní aplikace (podporované mobilní OS: minimálně Android a iOS). |  |
| **09** | Řešení musí umožnit volbu parametrů autentizačního PIN kódu pro více-faktorové ověřování (podobně, jako u hesla např. v Active Directory). Délku PINu v rozmezí alespoň od 4 do alespoň 16 znaků, musí umožnit exspiraci PIN kódu po definovaném časovém intervalu, musí umožnit použití jak čistě numerického PINu, tak PINu obsahujícího čísla a písmena a speciální znaky. Řešení dále musí umožnit vynucení historie PINu a zamezit uživateli, aby si při obnově PINu zvolil dříve jím použitý PIN kód (je požadováno, aby si systém pamatoval alespoň 8 posledních PINů). Řešení musí umožnit vynutit nastavení, které uživateli zamezí nastavit si snadno uhodnutelný PIN (minimálně nedovolit opakování stejných po sobě jdoucích znaků, jako např. „1111“ a jednoduchou číselnou řadu, jako např. „1234“). |  |
| **10** | Řešení musí obsahovat technologii pro automatizaci přihlašovacího procesu, která uživateli umožní přihlášení do vzdálené plochy s využitím již zadaných přihlašovacích pověření, bez nutnosti opakovaně zadávat přihlašovací údaje, potvrzovat připojovací dialogy, znovu použít autentizační předmět, znovu zadávat PIN kód. Tato technologie musí podporovat nejběžnější produkty pro virtualizaci aplikací a desktopů (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, VMware Horizon). |  |
| **11** | Řešení musí umožňovat režim redukovaného uživatelského rozhraní, tzv. "appliance mode", na tenkých klientech. V tomto režimu je běžné uživatelské rozhraní tenkého klienta nahrazeno přihlašovací obrazovkou pro více-faktorovou autentizaci. |  |
| **12** | Řešení musí umožnit nastavení různých kombinací přihlašovacích faktorů pomocí politik, a tyto politiky aplikovat na skupiny uživatelů, skupiny koncových zařízení, typy koncových zařízení s rozlišením alespoň fyzická stanice/virtuální desktop/server vzdálené plochy. |  |
| **13** | Řešení musí zajistit funkčnost více-faktorové autentizace pomocí bezkontaktních karet i v případě, kdy klientské zařízení není připojeno k síti (je offline) nebo není dostupná serverová strana řešení. |  |
| **14** | Řešení musí poskytnout funkce více-faktorové autentizace na koncových (klientských) zařízeních používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce více-faktorové autentizace na koncovém (klientském) zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být více-faktorové ověření provedeno jménem konkrétního uživatele, tedy přihlašování musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény. |  |
| **15** | Podpora a záruka výrobce 9x5 NBD v pracovních dnech s dvouhodinovou reakční dobou vzdáleně a s reakcí následující pracovní den v místě instalace na 5 let. |  |
| **Autentizační předměty** | | |
| **16** | Je požadováno dodání 1900 ks autentizačních předmětů v provedení:  1800 ks klíčenka  100 ks karta (velikost ID-1 dle ČSN ISO/IEC 7810) |  |
| **17** | Dodaná klíčenka a karta bude obsahovat minimálně následující bezkontaktní čipy: nízkofrekvenční 125 kHz EM4200 a vysokofrekvenční 13,56 MHz NXP MIFARE S50, 1kb). |  |
| **18** | Dodaná karta musí být ve velikosti bankovní karty, formát: ID-1, v provedení umožňující potisk karty. |  |
| **19** | Dodaná klíčenka musí být v provedení přívěsku, z materiálu, který zaručuje odolnost vůči mechanickému poškození a voděodolnost. |  |
| **20** | Je požadováno dodání 100 ks autentizačních prostředků pro čisté operační sály nebo pro izolované zóny. |  |
| **21** | Autentizační prostředek pro čisté operační sály nebo pro izolované zóny (např. náramek pod ochranný oděv) bude obsahovat bezkontaktní vysokofrekvenční čip 13.56 MHz, minimálně NXP MIFARE S50, 1kb pro dvou-faktorové přihlašování ke koncovým (klientským) zařízením. Je požadováno voděodolné provedení, potisk náramku: Logo organizace a pořadové číslo prostředku. |  |
| **Čtečky karet** | | |
| **22** | Je požadováno dodání 800 ks stolních čteček s USB rozhraním pro připojení k PC |  |
| **23** | Požadované parametry stacionárních čteček bezkontaktní části karty, které v současnosti nemocnice používá:   * Pracovní frekvence: 13,56 MHz * Podpora bezkontaktních karet/předmětů: rodina NXP Mifare® * Rozhraní: připojitelná přes USB * Typ: externí * Napájení: přes USB rozhraní * Formát: stolní * Přenos dat: zabezpečený, přes API (nesmí simulovat stisky kláves)   Kompatibilita OS: Windows 10 a vyšší |  |
| **Single Sign-On (SSO)** | | |
| **24** | Řešení musí poskytovat funkci automatického přihlášení SSO (Single Sign-On) alespoň do následujících aplikací:  FONS Enterprise, FONS Openlims, FONS Akord Diet, FONS Medix, Anete Kredit, LEKIS. V případě webových aplikací musí být pro funkci SSO podporovány minimálně tyto prohlížeče: Microsoft Edge Chromium verze 110 a vyšší, Google Chrome verze 110 a vyšší. Dále musí být pro webové aplikace podporována autentizace pomocí protokolu SAML a pomocí OpenID Connect. |  |
| **25** | Řešení musí poskytovat funkci Single Sign-On do aplikací FONS Enterprise, FONS Openlims, FONS Akord Diet, FONS Medix, Anete Kredit, LEKIS) z koncových (klientských) zařízení používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce SSO do aplikací (popsaných v předchozím bodu) na koncovém zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být funkce SSO poskytovány jménem konkrétního uživatele, tedy přihlašování do aplikací musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné také na koncových stanicích, které nejsou členy Active Directory domény. |  |
| **26** | Řešení musí zajišťovat funkčnost SSO pro aplikace, jejichž klientská strana běží jak na fyzických stanicích, tak ve virtuální ploše – VDI, virtualizované aplikace, server vzdálené plochy. Řešení musí poskytnout plnou funkčnost SSO pro nejběžnější technologie virtualizace aplikací a desktopů na trhu (Microsoft Remote Desktop Services, Citrix Virtual Apps and Desktops, VMware Horizon). |  |
| **27** | Přihlašovací údaje do jednotlivých aplikací musí být dostupné jen příslušnému uživateli Přihlašovací údaje do jednotlivých aplikací a systémů jsou šifrovány, a musí být ukládány na serverovou stranu řešení, aby byly dostupné na každé koncové stanici, ke které se uživatel přihlašuje. Systém musí umožnit, aby pro kritické aplikace bylo přihlášení pomocí SSO vynucováno. |  |
| **28** | Řešení musí umožnit funkci SSO přihlašování do aplikací jak identitou (účtem) z Active Directory, tak účtem spravovaným danou aplikací. Řešení musí dále poskytovat funkcionalitu Identity Provider (IdP), kdy neuchovává přihlašovací údaje uživatelů. |  |
| **29** | Řešení bude obsahovat integrovaný správce hesel (Password Manager) pro všechny uživatele, s možností uživatelské správy. IT správce musí mít možnost nastavit, zda uživatel může přihlašovací údaje editovat nebo jen zobrazit, a dále, zda může zobrazit heslo v čitelné podobě. Funkce zobrazení hesla v čitelné podobě musí být možné dodatečně zabezpečit (např. vyžádáním hesla, PINu apod.). |  |
| **30** | Řešení musí obsahovat grafické uživatelské rozhraní pro vytváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní a uživatelsky přívětivé, bez nutnosti psát kód, programovat, používat řádkové příkazy a umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace uživatelsky, vlastními silami, bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu těchto aplikací. |  |
| **31** | Podpora celého řešení na 5 let. Záruka na dodaný HW /čtečky, autentizační předměty 2 roky. |  |
| **Samoobslužný reset hesla** | | |
| **32** | Řešení musí poskytnout integraci na funkci samoobslužný reset hesla Active Directory účtu a musí umožnit vyvolání této funkce z přihlašovací obrazovky klientské stanice, bez nutnosti se předem přihlásit. |  |

# **Fáze A - Instalace a implementace**

1. Instalace a implementace technologií popsaných v kapitolách 5.1 až 5.9 bude provedena v jednotlivých požadovaných krocích a termínech uvedených v kapitole 3.
2. Požadavky na Instalaci a implementaci technologií jsou uvedeny v následující tabulce.

| **Id** | **Rozsah plnění členěný podle kapitol 5.1 až 5.9** |
| --- | --- |
| **5.1 Centrální Firewally** | |
| **01** | Technický návrh |
| **02** | Fyzická instalace FW, instalace centrálního mmgmt serveru do virtuálního prostředí, úvodní síťová konfigurace. |
| **03** | Segmentace interní LAN |
| **04** | Tvorba bezpečnostních politik a migrace stávajících pravidel. Počet bezpečnostních politik dosahuje řádově desítek. Každá bezpečnostní politika má řádově desítky pravidel. |
| **05** | Integrace se zdrojem identit (AD, LDAP, Radius…) |
| **06** | Rekonfigurace routingu a změna default GW na testovací skupině sítí |
| **07** | Kompletní rekonfigurace routingu a migrace klientů do nových subnetů |
| **08** | Implementace Threat prevention funkcionalit a politik |
| **09** | Fáze ladění |
| **10** | Dokumentace skutečného provedení. |
| **5.2.1 Centrální správa logů** | |
| **01** | Instalace systému jako virtuálního stroje do VMW infrastruktury zadavatele a nastavení management komunikace. |
| **02** | Konfigurace síťových rozhraní LM. |
| **03** | Vytvoření záznamů v DNS. |
| **04** | Napojení LM na AD a vytvoření skupin pro přístup. |
| **05** | Dle dokumentu „Detailní realizační projekt“. |
| **06** | Nastavení email komunikace. |
| **07** | Úprava nastavení Windows auditu na doménových serverech a řadičích. |
| **08** | Instalace agenta log manageru na Windows servery pomocí GPO či manuálně. |
| **09** | Individuální nastavení serverů s extra logováním typu DHCP, IIS, Exchange. |
| **10** | Napojení LM na Vmware. Součinnost poskytuje zadavatel. |
| **11** | Napojení LM na O365. Technické řešení musí být realizováno pomocí API bez instalace dalších komponent. API musí umožnit třídění logů podle jednotlivých aplikací v rámci O365. |
| **12** | Nastavení Syslog na síťových zařízeních typu Switch, firewall, AP. Úpravy úrovně logování jsou v kompetenci zadavatele. |
| **13** | Nastavení klasifikace logů dle zařízení a zařazení do prefixlistů. |
| **14** | Doplnění LM do další dashboardy pro snažíš správu Windows serverů. |
| **15** | Nastavení základních alertů. |
| **5.2.2 Monitorování sítí na bázi datových toků (NetFlow/IPFIX)** | |
| **01** | Technický návrh zapojení. |
| **02** | Konfigurace a nastavení síťových rozhraní. |
| **03** | Instalace a konfigurace virtuálního kolektoru. |
| **04** | Nastavení uživatelských účtů. |
| **05** | Konfigurace kvót datových uložišť pro jednotlivé moduly. |
| **06** | Nastavení monitoring centra a profilů, vestavěného kolektoru a pole databáze toků. |
| **07** | Konfigurace dashbordů a reportů. |
| **5.2.3 Automatické vyhodnocování datových toků (NetFlow/IPFIX)** | |
| **08** | Nastavení modulu ADS, konfigurace zdrojů dat, základní filtry IP rozsahů a nastaví implicitní parametry detekčních metod, IP rozsahy a veřejné adresy |
| **09** | Dokumentace skutečného provedení |
| **5.3 Zavedení segmentace sítě** | |
| **01** | Instalace a konfigurace dvou VM boxů do clusteru. |
| **02** | Instalace posledního stabilního firmware. |
| **03** | LDAP připojení do domény. |
| **04** | Instalace/konfigurace certifikační autority. |
| **05** | Vytvoření templates na certifikační autoritě pro klienty a nastavení automatické instalace pro zařízení v doméně. |
| **06** | Vydání certifikátu pro RADIUS. |
| **07** | Revize zapojených zařízení v síti LAN a WLAN. |
| **08** | Vytvoření ověřovací matice – definice ověřování uživatelů, zařízení, jejich kombinace, druh autentikační metody a přiřazení definovaných rolí na základě splnění autorizačního procesu. |
| **09** | Konfigurace podmínek ověřovacích služeb. |
| **10** | Konfigurace a ověřování přístupu hostů do izolované sítě. |
| **11** | Distribuce nastavení suplikanta pro zařízení ověřovaná metodou 802.1x. |
| **12** | Ruční nastavení suplikanta a nahrání certifikátu pro zařízení, u kterých nelze toto zajistit pomocí hromadné distribuce. |
| **13** | Konfigurace přístupových switchů a AP – definice ověřovacích serverů a služeb, konfigurace DHCP relay a konfigurace portů či ESSID. |
| **14** | Ověření funkčnosti na vybraném vzorku zařízení a uživatelů. |
| **15** | Po ověření funkčnosti kompletní nasazení pro celou síť. |
| **16** | Dokumentace skutečného provedení. |
| **5.4 DLP** | |
| **01** | Příprava MS SQL |
| **02** | Instalace Management Serveru na dedikovaný virtuál |
| **03** | Základní konfigurace, zalicencování |
| **04** | Nasazení Clienta na vybranou testovací skupinu |
| **05** | Sběr logů, analýza provozu |
| **06** | Vytvoření DLP politik, klasifikace dat a datových zón |
| **07** | Ověření politik na testovací skupině |
| **08** | Postupné rozšiřování Clienta a politik na zbytek uživatelů |
| **09** | Dokumentace skutečného provedení. |
| **5.5 Úložiště pro PACS a NIS data formou NAS a S3** | |
| **01** | Technický návrh řešení, design nasazení |
| **02** | HW instalace 4ks storage nodů |
| **03** | Fyzické zapojení úložiště do síťového prostředí |
| **04** | Konfigurace OOB managementu |
| **05** | Instalace OS/SW/firmware v dohodnuté verzi |
| **06** | Konfigurace storage clusteru, IP adresace |
| **07** | Konfigurace vzdáleného dohledu |
| **08** | Připojení k LDAP |
| **09** | Konfigurace práv uživatelských/administrátorských účtů |
| **10** | Konfigurace sdílených adresářů/namespace a práv k nim |
| **11** | Připojení úložiště k systémům, které budou toto úložiště využívat |
| **12** | Testovací nasazení |
| **13** | Výkonnostní testy (zálohy, souborové servery atp.) |
| **14** | Produkční nasazení |
| **15** | Dokumentace skutečného provedení. |
| **5.6 Infrastruktura pro zálohování a rychlou obnovu** | |
| **01** | Technický návrh řešení, design nasazení |
| **02** | HW instalace 1ks zálohovacího serveru a 1ks páskové knihovny |
| **03** | Fyzické zapojení zálohovacího serveru a páskové knihovny do síťového/SAN prostředí |
| **04** | Instalace OS/SW/firmware v dohodnuté verzi |
| **05** | Konfigurace operačního systému, systémová nastavení |
| **06** | Konfigurace OOB managementu |
| **07** | Instalace zálohovacího software |
| **08** | Konfigurace práv uživatelských/administrátorských účtů |
| **09** | Konfigurace komponent zálohovacího software (backup server, proxy, dohled) |
| **10** | Integrace s úložišti záloh |
| **11** | Integrace zálohovacího software s primárním prostředím (virtualizace, úložiště) |
| **12** | Definice zálohovacích / archivačních úloh |
| **13** | Testovací nasazení |
| **14** | Výkonnostní a funkční testy (zálohy, archivace, obnovy) |
| **15** | Produkční nasazení |
| **16** | Dokumentace skutečného provedení. |
| **5.7 Zvýšení dostupnosti záložního datového centra a lokální sítě** | |
| **01** | Fyzická instalace a konfigurace dvou HW controllerů do clusteru v režimu active-active, který zajistí předávání session a patřičných licencí |
| **02** | Instalace posledního stabilního firmware |
| **03** | Návrh a konfigurace mikrosegmentace mezi gateway a koncovým prvkem (switch/AP). Integrace s RADIUS serverem |
| **04** | Ověření funkčnosti na vybraném vzorku zařízení a uživatelů |
| **05** | Po ověření funkčnosti kompletní nasazení pro celou síť |
| **06** | Dokumentace skutečného provedení |
| **5.8 Ochrana operačních systémů a mobilních platforem** | |
| **01** | Tvorba bezpečnostních politik v centrálním mgmt |
| **02** | Integrace se zdrojem identit (AD) |
| **03** | Distribuce a instalace SW klientů na testovací skupinu stanic a testování |
| **04** | Kompletní nasazení systému EDR a SW klientů |
| **05** | Ladění politik a nastavení |
| **06** | Dokumentace skutečného provedení. |
| **5.9 Přihlašování k počítačům a aplikacím v rámci klinických a THP provozů** | |
| **01** | Technický návrh |
| **02** | Instalace a konfigurace infrastrukturních části |
| **03** | Integrace požadovaných aplikací |
| **04** | Napojení adresářových služeb, synchronizace uživatelů |
| **05** | Vytvoření profilů uživatelů, koncových stanic, aplikací |
| **06** | Konfigurace pro mobilní zařízení |
| **07** | Migrace koncových stanic do Active Directory |
| **08** | Ladění, ověřování |
| **09** | Deployment, rollout |
| **10** | Dokumentace skutečného provedení |

## **6.1 Zpracování a akceptace Detailního realizačního projektu**

1. Dokument Detailní realizační projekt bude obsahovat minimálně:
2. definici cílového stavu, která bude vycházet z požadavků na budoucí stav, viz tento dokument,
3. akceptační kritéria cílového stavu;

pro ověření plnění Dodavatele v rámci Smlouvy jsou uvedena v tomto dokumentu, a to v tabulkách označených „Minimální požadavky …“, kde Dodavatel bude deklarovat svoji připravenost poskytovat bezvadné plnění již v rámci Zkušebního (testovacího) provozu.

1. detailní harmonogram realizace zakázky, který vychází z milníků uvedených v kapitole3
2. **Předání a převzetí Detailního realizačního plánu bude provedeno** vzájemně odsouhlaseným Předávacím protokolem realizačního plánu (Dodavatel předává dokument Detailní realizační projekt) a Akceptačním protokolem realizačního plánu, kterým Zadavatel akceptuje splnění podmínek.

## **6.2 Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)**

**6.6.1 Předání a převzetí dokumentů**

1. Dokumenty, které mají být vypracovány Dodavatelem a které se poskytují Zadavateli jako součást poskytování díla (zejména Detailní realizační koncept), budou nejdříve předloženy Zadavateli ve formě návrhu k posouzení.
2. Dodavatel se zavazuje předat první verzi dokumentu Zadavateli k akceptaci ve lhůtě domluvené mezi Dodavatelem a Zadavatelem na základě Smlouvy, nebo jinak stanovené v souladu se Smlouvou.
3. Zadavatel je oprávněn ve lhůtě deseti (10) pracovních dnů od doručení příslušného dokumentu písemně předložit Dodavateli své připomínky k návrhu.
4. Po diskusi o těchto připomínkách upraví Dodavatel příslušný návrh v souladu s dohodnutými změnami a se zapracováním těchto dohodnutých změn jej předá ve stejné lhůtě deseti (10) pracovních dnů Zadavateli.
5. V případě, že Zadavatel nemá k předaným dokumentům výhrady, považují se za převzaté   
   k okamžiku doručení jejich konečné verze Zadavateli.
6. V případě, že Zadavatel připomínky ve lhůtě deseti (10) dnů nepředloží, má se za to, že s předloženým dokumentem souhlasí a dokument se považuje za řádně převzatý.

**6.2.2 Předání a převzetí ostatních plnění dle Smlouvy (vyjma služeb)**

1. V případě, že součástí poskytování plnění Dodavatelem dle Smlouvy je plnění, které podléhá akceptaci Zadavatelem, musí dojít k podpisu Předávacích protokolů ohledně tohoto plnění   
   v termínech uvedených v harmonogramu, není-li výslovně uvedeno jinak.

Zadavatel vybere klíčové funkce z výše popsaných technických parametrů a ty stanoví jako akceptační kritéria. Akceptace je možná pouze za předpokladu, že akceptační kritéria budou splněna bez dalších výhrad.

Jestliže plnění nebo jeho jednotlivé části splní kritéria akceptačního řízení, považují se za řádně ukončené a Zadavatel je povinen jej převzít.

1. Akceptační procedury zahrnují porovnání skutečných vlastností plnění se závaznou specifikací předmětu plnění dle Smlouvy.
2. Akceptační procedura bude zahrnovat akceptační testy, které budou probíhat na základě specifikace akceptačních testů obsahující popis testů, testovací data, příslušné prostředí, pořadí provádění testů a akceptační kritéria.

Nedohodnou-li se smluvní strany jinak, vypracuje specifikaci akceptačních testů Dodavatel a předá Zadavateli k odsouhlasení v termínu deseti (10) pracovních dnů před zahájením akceptační procedury dle harmonogramu.

Odsouhlasení bude provedeno písemnou formou v termínu deseti (10) pracovních dnů před zahájením akceptační procedury. Jestliže se Zadavatel v této lhůtě ke specifikaci akceptačních testů písemně nevyjádří, má se za to, že specifikaci akceptačních testů odsouhlasil.

Jestliže Zadavatel specifikaci akceptačních testů v uvedené lhůtě neodsouhlasil, je povinen Zadavatel v této lhůtě sdělit připomínky k Dodavatelem předložené specifikaci akceptačních testů a poskytnout Dodavateli veškerou potřebnou součinnost k dokončení a odsouhlasení specifikace akceptačních testů.

Lhůta pro provedení akceptačních testů a lhůta pro předání plnění nebo jeho části se prodlužuje o dobu, o kterou se prodloužilo písemné odsouhlasení specifikace akceptačních testů z důvodu připomínek na straně Zadavatele oproti lhůtě stanovené.

1. Dodavatel bude písemně informovat Zadavatele, resp. jeho oprávněné osoby nejméně deseti (10) dní předem o termínu zahájení akceptačních testů.

Zadavatel je oprávněn se těchto testů zúčastnit a osvědčit jejich konání, a to formou předávacího protokolu (nebo dílčích předávacích protokolů), podepsaného (podepsaných) oprávněnými osobami obou smluvních stran. Pokud se Zadavatel nedostaví v termínu určeném pro provedení akceptačních testů, ačkoli byl s tímto termínem řádně seznámen, je Dodavatel oprávněn provést příslušné akceptační testy bez jeho přítomnosti.

Takto provedené akceptační testy se považují za provedené v přítomnosti Zadavatele. Kopie veškerých dokumentů vypracovaných v souvislosti s provedením těchto akceptačních testů budou Zadavateli poskytnuty do deseti (10) dnů.

1. Základním předpokladem pro řádné předání plnění (nebo jeho části) Dodavatelem a převzetí tohoto plnění (nebo jeho části) Zadavatelem, a to formou předávacího protokolu podepsaného oprávněnými osobami obou smluvních stran je skutečnost, že plnění splní kritéria akceptačních testů uvedená v dohodnutých kontrolních specifikacích a bude provedeno v souladu se závaznou specifikací předmětu plnění dle Smlouvy.
2. Jestliže plnění nebo jeho část splní akceptační kritéria akceptačních testů, Dodavatel se zavazuje v den následující po ukončení akceptačních testů umožnit Zadavateli plnění nebo jeho část převzít a Zadavatel se zavazuje v tomto termínu plnění nebo jeho část převzít.

Pokud Zadavatel plnění nebo jeho část v tomto termínu nepřevezme, ačkoli převzetí plnění nebo jeho části bylo Dodavatelem řádně umožněno, má se za to, že plnění nebo jeho část bylo řádně předáno a Zadavatelem převzato právě v den následující po ukončení akceptačních testů.

1. Jestliže plnění nesplňuje stanovená akceptační kritéria kteréhokoliv akceptačního testu, budou výsledky akceptačního testu (splněno/nesplněno/s výhradami) spolu s uvedením termínů pro nápravu uvedeny ve vyhodnocení Akceptačního protokolu.

Dodavatel napraví tyto nedostatky a příslušné akceptační testy budou provedeny znovu.

Tento proces testování a následných oprav se bude opakovat, přičemž výše uvedená ustanovení se použijí obdobně.

Proces testování a následných oprav lze opakovat, dokud Dodavatel nesplní veškerá akceptační kritéria pro příslušný akceptační test, nejvýše však natřikrát (3x).

V situaci, kdy by bylo nutné opakovat akceptační testy více jak třikrát (3x) pro konkrétní fázi projektu, je v takovém případě nutný souhlas nadřízeného orgánu projektu – tzn. řídícího výboru nebo ředitelů projektu dle použité metodiky řízení projektu.

1. Žádný akceptační test se však nebude považovat za nesplněný, jestliže daný nedostatek nebyl způsoben Dodavatelem, nebo byl zjištěn nebo měl být zjištěn Zadavatelem před nebo při předcházejícím akceptačním testu, ale nebyl v té době oznámen Dodavateli, nebo byl nepodstatný, tzn., neměl vliv na řádné poskytování funkčnost díla nebo jeho části tak, jak jsou vymezeny ve Smlouvě.
2. Při převzetí plnění nebo kterékoliv jeho části v souladu s tímto článkem je Zadavatel povinen podepsat potvrzení o přijetí plnění nebo dané části a Zadavatel i Dodavatel se zavazují podepsat příslušný předávací případně akceptační protokol (dílčí předávací případně akceptační protokoly), tj. potvrzení o předání a přijetí (převzetí) plnění nebo jeho určité části.

## **6.3 Školení**

1. Dodavatel poskytne školení pro administrátory IS tak, aby byli schopni řádně užívat, respektive administrovat, instalované technologické části specifikované v kapitole 5. Rozsah školení bude 5 pracovních dnů pro nejvýše 5 technických specialistů Zadavatele. Zadavatel počet školených technických specialistů upřesní před provedením samotného školení. Zadavatel může rozhodnout o dělení školení na 5 nespojitých setkání. Součástí školení bude vždy ukázka na dodávané technologii a teoretická část vysvětlující principy fungování technologie.

## **6.4 Dokumentace**

1. Dodaná dokumentace slouží k zachycení a vyhodnocování plánovaných činností a též k dokumentaci skutečného stavu.

# **Fáze B – servisní a provozní podpora dodaných technologií**

1. Požadavky, které musí dodavatel minimálně naplnit na servisní a provozní podporu dodaných technologií, jsou v níže uvedené tabulce.

| **Id** | **Plnění požadavku** | **Splněno** |
| --- | --- | --- |
| **01** | Dodavatel zajistí Helpdesk v režimu 24x7 bez přerušení. HelpDesk musí být možné kontaktovat pomocí telefonu, e-mailem a webového rozhraní s přehledem řešených požadavků. Helpdesk musí hovořit českým jazykem. Lhůty pro plnění ze strany Uchazeče jsou pozastaveny za předpokladu:  a) Čekání na součinnost zákazníka  b) Čekání na součinnost třetí strany (například výrobce HW nebo SW, či bug výrobce) |  |
| **02** | Veškeré požadavky budou evidovány v systému servisní podpory Dodavatele nebo výrobce zařízení (HelpDesk). |  |
| **03** | Kontaktní místo umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím služby HelpDesk, popř. služby Hot-line. |  |
| **04** | Služba HelpDesk umožní Zadavateli upřesnit nebo doplnit požadavek. |  |
| **05** | Služba HelpDesk bude Zadavateli poskytovat přehled o aktuálně nahlášených požadavcích, jejich stavu a aktuálním způsobu jejich řešení.  Služba HelpDesk bude Zadavateli zasílat notifikace o změně stavu jeho požadavku (např. zadaný, v řešení, uzavřený atd.) a musí Zadavateli umožnit schvalování uzavření nahlášeného požadavku. |  |
| **06** | Služba HelpDesk bude poskytovat Zadavateli přístup i k uzavřeným požadavkům  a způsobu jejich řešení, bude poskytovat podrobné údaje o historii požadavků od jejich nahlášení, po jejich vyřešení. |  |
| **07** | Dodavatel zajistí podporu certifikovaných expertů v režimu 24x7. Technické specialisty musí být možné kontaktovat pomocí oddělení Helpdesk. Podpora bude obsahovat tyto technologické pohotovosti:  a) Kybernetická bezpečnost  b) Síťové prvky  c) Technologie Datových center  každá pohotovost v každé oblasti musí být držena nejméně čtyřmi certifikovanými technickými specialisty na dodávané technologie. Jeden technický specialista může být členem nejvýše dvou pohotovostí. Technická certifikace musí odpovídat požadavkům na technickou kvalifikaci dle Zadávací Dokumentace. |  |
| **08** | Technická podpora je poskytována s rozpočtem čtyři člověkodny měsíčně. V případě nevyužití služby jsou nevyužité dny převáděny do dalších měsíců v rámci kalendářního roku. |  |
| **09** | Bude prováděna průběžná aktualizace dokumentace k programovému vybavení tak, aby u Zadavatele byla vždy aktuální dokumentace k provozované technologii. |  |
| **10** | Bude poskytována součinnost při zásadním upgrade softwarových částí instalované infrastruktury na vyšší verze. |  |
| **11** | Bude zajištěna udržitelnost SW třetích stran, dodaných Dodavatelem v rámci veřejné zakázky. |  |
| **12** | HW a SW maintenance výrobce budou poskytovány po celou dobu smluvního vztahu. |  |
| **13** | Technická podpora a servis zařízení HW a SW budou zabezpečeny Dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce. |  |
| **14** | Technická podpora a servis budou realizovány v místě Zadavatele.  Výjimku tvoří činnosti realizované vzdáleným připojením Dodavatele, výrobce zařízení do prostředí Zadavatele. Uchazeč musí disponovat vlastní provozní dokumentací, kolaborativním správcem hesel v souladu s Vyhláškou Zákona o Kybernetické Bezpečnosti. Provozní dokumentace Uchazeče musí být na vyžádání k dispozici Zadavateli online. |  |
| **15** | Dodavatel zajistí provozní monitoring všech dodávaných komponent po dobu poskytování služby. Monitorována budou následující:   * U každé technologie alespoň jedna služba (nebo typ služby), která nejvíce odpovídá charakteru zařízení. (například u diskového pole pro nestrukturovaná data dostupnost single namespace apod.) * Alespoň jeden fyzický interface prokazující dostupnost zařízení.   Monitorovací intervaly by měly být nastaveny podle charakteru služby v intervalu 5 vteřin a 5 minut. Monitorovací metoda nesmí zbytečně přetěžovat monitorovanou komponentu. |  |

1. V rámci zajištění podpory a servisu po dobu udržitelnosti projektu platí následující parametry SLA.

Definice stupňů závažnosti incidentů:

|  |  |  |
| --- | --- | --- |
| **Závažnost Závady nebo Chyby** | | **Definice závažnosti Závad a Chyb** |
| **A** | **Kritická chyba** | Chyba způsobí, že poskytované řešení nelze zcela provozovat nebo má kritický vliv na provozované aplikace či stav podporovaného systému – vyžaduje okamžité řešení. Typická situace je výpadek všech i redundantních prvků poskytujících řešení. Za kritickou chybu se dále považuje situace, kdy poskytované řešení obsahuje ***bezpečnostní zranitelnost*** s **kritickou** mírou závažnosti. |
| **B** | **Provozní chyba** | Chyba, která ovlivňuje provozní vlastnosti, ale nebrání v užití poskytovaného řešení. Provozní chybou se rozumí výpadek pouze dílčí části poskytovaného řešení. Typická situace je výpadek jednoho z redundantních prvků, kdy jiný prvek je stále dostupný. Za provozní chybu se dále považuje situace, kdy poskytované řešení obsahuje ***bezpečnostní zranitelnost*** se **střední** mírou závažnosti. |
| **C** | **Změnový požadavek nebo incident s nízkou mírou bezpečností zranitelnosti** | Požadavek na změnu konfigurace řešení, či konzultace. Za změnový požadavek se dále považuje situace, kdy poskytované řešení obsahuje ***bezpečnostní zranitelnost*** s **nízkou** mírou závažnosti. |

Kategorie bezpečnostních zranitelností:

| **Kategorie** | **Popis** |
| --- | --- |
| **Kritická** | Zranitelnost dosáhne základního skóre 7.0 – 10.0 bodů dle obecného systému hodnocení zranitelností (otevřený standard CVSSv3.1 base score). |
| **Střední** | Zranitelnost dosáhne základního skóre 4.0-6.9 bodů dle obecného systému hodnocení zranitelností (CVSSv3.1 base score). |
| **Nízká** | Zranitelnost dosáhne základního skóre 0.0-3.9 bodů dle obecného systému hodnocení zranitelností (CVSSv3.1 base score) . |

Definice maximální doby nástupů k řešení incidentů podle závažnosti:

|  |  |  |  |
| --- | --- | --- | --- |
| **Závažnost Chyby** | **Doba zahájení činnosti**  **(od nahlášení)** | **Doba odstranění chyby** | **Řešení** |
| **A** | 4 pracovní hodiny | Nejpozději do 24 hodin | **a)** |
| **B** | 8 pracovní hodiny | Nejpozději do tří pracovních dní (7:00-17:00) | **a), b)** |
| **C** | 1 pracovní den | Nejpozději do šesti pracovních dní (7:00-17:00) | **b)** |

Struktura dohody o úrovni poskytování služeb (dále jen SLA).

1. Řešením se rozumí:
2. Odstranění chyby řešení. Opravy Chyb bude provádět Dodavatel do Aktualizované verze (kritické chyby ihned). Na odstranění chyby pracuje Dodavatel neodkladně,
3. Poskytnutí přijatelného náhradního řešení problému ze strany Dodavatele.
4. Technické požadavky se závažností chyby A a B lze čerpat na následující technologické oblasti dle kapitol:

5.1 Centrální firewall (kybernetická bezpečnost)

5.3 Segmentace sítě

5.5 Úložiště pro PACS a NIS data formou NAS a S3 (datová centra)

5.6 Infrastruktura pro zálohování a rychlou obnovu (datová centra)

5.7 Zvýšení dostupnosti záložního datového centra a lokální sítě (síťové prvky)

5.8 Ochrana operačních systémů a mobilních platforem (kybernetická bezpečnost)

5.9 Přihlašování k počítačům a aplikací v rámci klinických a THP provozů

1. Na ostatní části lze čerpat pouze podporu se závažností chyby C. Tyto části jsou:

5.2 Řešení pro správu logů

5.4 DLP