Příloha č. 1 smlouvy o dílo Č.j. R- 04-1/11-2019

# TECHNICKÁ SPECIFIKACE

k veřejné zakázce s názvem „Elektronické služby pro Nemocnici Rudolfa a Stefanie Benešov, a.s. – zvýšení dostupnosti služeb Bezpečnost“

## 1 Část – Bezpečnost

### 1.1 Systém pro monitoring, vyhodnocování, analýzu toků v síti a monitorování výkonu aplikaci

Monitorovací systém musí umožňovat dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný.

Uložení a zpracování statistik musí být redundantní na k tomu určených specializovaných zařízeních – kolektorech. Ty musí být vybaveny SW či HW RAIDem. Kolektory musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat automatizované reporty i notifikace na nestandardní situace. Ukládání dat musí probíhat kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců. Samozřejmostí bude plná customizace způsobu prezentace dat a reportů na základě cílového prostředí.

Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow). Tato technologie představuje nejmodernějším prostředek pro monitorování sítě při zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní sítě.

Požadované řešení se musí skládat ze dvou na sobě nezávislých částí:

- Kolektor s automatickým vyhodnocováním NetFlow/NetStream dat;
- Fyzické sondy pro sběr dat z prvků nepodporující export flow záznamů

*Kolektor s detekcí anomálií*

Zadavatel požaduje minimálně následující parametry pro kolektor:

| Název požadavku | Popis požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|---|
| Ukládání flow statistik | Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce. | Ano | 150 000 toků/s |
| Granularita vizualizace | Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5-minutových nebo 30-sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků. | Ano | Konfigurovatelná hodnota |
| Podpora standardů datových toků | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. | Ano | NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. |
| Hlavní funkcionalita | Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení. | Ano | Přímo na dashboardu |
| Instalace | Snadná instalace do stávající síťové infrastruktury – racková montáž, maximálně 1U | Ano | 1U |
| Management rozhraní | Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. | Ano | 2x 10/100/1000 RJ 45 porty |
| Zabezpečená vzdálená správa | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. | Ano | SSH a HTTPS |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. | Ano | V menu administrátora |
| LDAP autentizace | Podpora autentizace vůči LDAP (Active Directory). | Ano | Autentizace proti LDAP |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+. | Ano | Autentizace proti RADIUS a TACACS+ |
| Podpora HOT SWAP a RAID | Hardwarové kolektory jsou vybavené HOT SWAP disky a podporují RAID včetně SMART detekce. | Ano | HW RAID5, 4x SATA hot swap |
| Dohled | Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. | Ano | Pomocí SNMP |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. | Ano | Pomocí NTP |
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. | Ano | Přístup přes SSH |

| | | | |
|---|---|---|---|
| Sériová linka pro konfiguraci zařízení | Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232). | Ano | Přístup přes RS-232 |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. | Ano | Kolektor podporuje DNS cache |
| Podpora Cisco AVC | Podpora standardu Cisco AVC vč. položek HTTP hostname a URL. | Ano | Podpora CISCO AVC |
| Podpora dalších flow standardů | Podpora pro Cisco NEL, Cisco NSEL, Cisco AVC, Cisco NBAR2. | Ano | Podpora CISCO NEL, NSEL AVC a NBAR2 |
| Podpora položek proměnlivé délky | Podpora IPFIX položek proměnlivé délky. | Ano | Popdora IPFIX |
| Monitoring výkonu sítě | Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety. | Ano | Podpora analýzy výkonu sítě |
| Monitoring informací z aplikační vrstvy | Podpora pro protokoly HTTP, VoIP SIP, DNS, Samba/CIFS, DHCP. | Ano | Podpora analýzy až na L7 |
| Monitorování rozšířených L3/L4 informací | Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů. | Ano | Podpora rozšířeních informací z L3/L4 |
| Přeposílání flow vč. možnosti samplingu | Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. | Ano | Možnost přeposílat data na jiný kolektor |
| Spolehlivý a šifrovaný přenos IPFIX dat | Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS). | Ano | Možnost přeposílat data na jiný kolektor |
| Automatická identifikace zdroje flow statistik | Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu. | Ano | Identifikace přímo z FLOW dat |
| Zálohování a obnova flow statistik | Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky. | Ano | Podpora zálohování a obnovení dat |
| Podpora pro uživatelské identity | Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele). | Ano | Podpora napojení na ISE nebo AD |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). | Ano | GUI v českém a anglickém jazyce |
| Vizualizace statistických dat | Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do | Ano | Plně definovatelné uživatelem |

| | | | |
|---|---|---|---|
| | 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. | | |
| Analýza dat a ad hoc výstupy | Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. | Ano | Podpora zobrazení a Exportu do PDF a CSV |
| Reporting | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště. | Ano | Podpora zobrazení a Exportu do PDF a CSV |
| Řízení uživatelského přístupu | Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem). | Ano | Plně konfigurovatelné hlavním administrátorem |
| Top N statistiky | Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků, nejvyšší hodnoty RTT, průmětné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu. | Ano | Plně definovatelné uživatelem |
| Filtrování a přizpůsobení výstupů | Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnovat do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace). | Ano | Podpora logických filtrů s parametry až na L7 |
| Uživatelsky definovatelné aletry | 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. | Ano | Alerty pomocí SNMP a emailu |
| Uživatelsky definované pohledy na datový provoz | Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, a pod.). | Ano | Plně definovatelné uživatelem |
| Drill-down | Možnost dohledat každý jednotlivý datový tok (flow záznam). | Ano | Skrze filtry definované uživatelem |
| Monitoring aktivních zařízení na sítí | Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, | Ano | Ano, po dobu uchování dat na kolektoru |

| | | | |
|---|---|---|---|
| | sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení. | | |
| Automatická podpora geolokace | Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). | Ano | Pravidelně aktualizovaná databáze geolokačních dat |
| Otevřené rozhraní | Kolektor poskytuje dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, a pod.). | Ano | Konfigurovatelné REST API |
| Aplikace pro mobilní zařízení | Aplikace pro mobilní zařízení platformy Android a iOS, pro zobrazování základních informací v podobě grafů a statistik per jednotlivý uživatel. | Ano | K dispozici od výrobce kolektoru |
| Monitorování dostupnosti zdroje flow dat | Monitorování dostupnosti zdroje flow dat pomocí SNMP. | Ano | Podpora SNMPv2 a v3 |
| Minimální velikost interního datového úložiště | 6 TB čisté kapacity na HW RAID5. | Ano | 6TB v HW RAID5 |
| Minimální velikost RAM paměti kolektoru | 32GB RAM. | Ano | 32GB RAM |
| Minimální počet toků/s který je kolektor schopen zpracovat | 150 000 toků/s. | Ano | 150 000 roků/s |

Systém pro automatické vyhodnocování IP toků musí umožnit automatickou detekci bezpečnostních nebo provozních a anomálií datové sítě a jejich hlášení formou událostí. Systém musí být založen na pokročilých metodách tzv. behaviorální analýzy a umožňovat tak odhalování hrozeb a incidentů, které překonají 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 doplní stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události bude 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 přispěje ke zjednodušení správy datové sítě, zvýšení její bezpečnosti a umožní proaktivní identifikaci příčin problémů.

Systém pro automatickou detekci musí být plně integrovatelný do prostředí kolektoru, tak aby mohl uživatel pracovat pouze s jedním GUI.

| Název požadavku | Popis požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|---|
| Podpora flow standardů | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. | Ano | NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. |
| Deduplikace | Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. | Ano | Podpora deduplikace přes zpracováním |
| Korelace před a za proxy | Systém umožňuje provést korelaci flow statistik před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli. | Ano | Podpora korelace |
| Vzorkování na úrovni toků | Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. | Ano | Možnost nastavit vzorkování – per zdroj flow |
| Identita uživatelů | Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. | Ano | Pomocí napojení na AD/LDAP |
| Persistence doménových jmen | Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. | Ano | Pomocí napojení na AD/LDAP |
| Detekční pravidla a algoritmy | Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. | Ano | Interní knihovna pravidelně aktualizovaných detekčních metod |
| Detekce síťových útoků | Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. | Ano | Interní knihovna pravidelně aktualizovaných detekčních metod |
| Detekce anomálií v síťovém provozu | Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. | Ano | Interní knihovna pravidelně aktualizovaných detekčních metod |
| Detekce nežádoucích aplikací | Detekce P2P sítí, a anonymizačních služeb (např. TOR). | Ano | Interní knihovna pravidelně aktualizovaných detekčních metod |
| Detekce událostí na základě „Threat intelligence“ dat | Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. | Ano | Interní knihovna pravidelně aktualizovaných detekčních metod |

| | | | |
|---|---|---|---|
| Detekce provozních problémů | Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti. | Ano | Interní knihovna pravidelně aktualizovaných detekčních metod |
| Detekce síťových anomálií | Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. | Ano | Automatické přizpůsobení vývoje monitorovaného prostředí |
| Konfigurační průvodce | Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. | Ano | Průvodce pro první zpuštění |
| Konfigurace detekčních schopností | Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ). | Ano | Plně konfigurovatelné detekčních metody |
| Detekce NATů | Detekce NATů v síti s využitím rozšířených informací z L3/L4. | Ano | Ve spoluprací s rozšířeními informaci z L3/L4 z kolektoru |
| Správa filtrů | Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu CSV nebo z tohoto formátu importovat. | Ano | Plně konfigurovatelné filtry a jejich export do CSV |
| Správa falešných poplachů | Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. | Ano | Plně konfigurovatelné detekční metody |
| Definice závažnosti událostí | Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit. | Ano | Interní knihovna pravidelně aktualizovaných detekčních metod včetně priorit |
| Agregace událostí | Detekované události je možné automaticky agregovat tak, aby související události byly prezentovány v rámci pojmenované hrozby (např. infikované zařízení v síti, chybně nakonfigurované zařízení, používání nevhodných aplikací nebo služeb apod.). | Ano | Podpora manuální i automatické agregace |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. | Ano | Plně konfigurovatelné hlavním administrátorem |

| | | | |
|---|---|---|---|
| CEF export | Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management. | Ano | Podpora systému integrace typu SIEM nebo log management |
| SNMP Trap | Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. | Ano | Podpora SNMPv2c, v3 a SNMP trap |
| E-mailové notifikace | Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k emailovému reportu. | Ano | Podpora zasílání mailových upozornění a reportů |
| Záchyt provozu v plném rozsahu | Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. | Ano | Možnost konfigurace záchytu per typ události |
| Spuštění skriptu | Na výskytu události je možné automaticky reagovat spuštěním uživatelsky definovaných skriptů. | Ano | Možnost konfigurace akce per událost |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí. | Ano | Plně konfigurovatelný dashboard pro každého uživatele v českém a anglickém jazyce |
| Integrace informací z jiných služeb | Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP. | Ano | Podpora synchronizace informací z externími subjekty pomocí protokolu HTTP |
| Kategorie a komentáře | Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře. | Ano | Možnost komentovat a přidávat příznaky |
| Vyhledávání událostí | Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.). | Ano | Podpora rychlého vyhledávání podle parametrů |
| Interaktivní vizualizace událostí | Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. | Ano | Jednoduché vykreslení informace o události |
| Reporting | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu | Ano | Podpora exportu do PDF |

| | | | |
|---|---|---|---|
| | PDF. Automatická distribuce reportů e-mailem. | | |
| CSV export | Události je možné exportovat do formátu CSV pro další zpracování. | Ano | Podpora exportu do CSV |
| Otevřené rozhraní | Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.). | Ano | Podpora REST API |
| Sledování změn konfigurace | Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management. | Ano | Veškeré změny dohledatelné v logu |
| Formát systémů | Systém musí běžet na HW zařízení kolektoru, musí být dostupný přes jednotné WEB GUI kolektoru. | Ano | Konfigurace přes GUI kolektoru |
| Výkon systému | Systém musí být schopen vyhodnotit minimálně 1 tisíc toků za vteřinu | Ano | 1000 toků za vteřinu |
| Počet zdrojů | Systém musí umět pracovat minimálně s jedním nezávislými zdroji dat (Flow instance). | Ano | Podpora 1 nezávislého zdroje dat |
| GUI systému | GUI musí být k dispozici v českém a anglickém jazyce. | Ano | České a anglické GUI |

Systém na monitorování výkonu aplikací musí být plně integrovatelný do prostředí kolektoru, tak aby mohl uživatel pracovat pouze s jedním GUI.

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

| **Název požadavku** | **Popis požadavku** | **Splňuje ANO/NE** | **Popis splnění požadavku/parametru** |
|---|---|---|---|
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Vizualizuje stav aplikace pomocí indexu výkonu aplikace, počtu transakcí a dalších informací ve formě grafů a tabulek. Umožnuje analyzovat stav | Ano | Podpora GUI v českém jazyce pro vyhodnocení výstupů z monitoringů |

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

| | | | |
|---|---|---|---|
| Skupiny | Systém umožňuje definovat skupiny pro sledování metrik pouze pro zvolenou podmnožinu transakcí (např. skupina pro PHP soubory, multimediální soubory, část klientů a uživatelů). | Ano | Možnost vytváření skupin |
| Reporting | Systém umožňuje vytvářet reporty dostupné prostřednictvím webového GUI, ve formátu PDF. Reporty je možné automaticky odesílat e-mailem. | Ano | Podpora reportů do PDF |
| Notifikace | Jako reakci na snížení indexu výkonu aplikace, případně další metriky umožňuje systém odeslat e-mail, syslog zprávu, SNMP trap, nebo spustit skript. | Ano | Podpora reakce na nedodržení SLA – email report/SNMP trap |
| Detaily HTTP transakcí | Pro každou transakci jsou dostupné detaily minimálně v rozsahu URL, parametry, user agenty, objem přenesených dat, návratová hodnota, cookie. | Ano | Detailní informace pro každé URL |
| Filtrace agregovaných transakcí | Systém umožňuje filtrovat nad seznamem agregovaných transakcí pomocí kritérií (např. APM, index, počet chyb, celkový objem přenesených dat a další). Díky tomu lze získat informace o tom, jaké části aplikace jsou nejpomalejší, vykazují nejvíce chyb, atd. | Ano | Plně konfigurovatelné filtry |
| Filtrace jednotlivých transakcí | Systém umožňuje filtrovat nad seznamem jednotlivých transakcí pomocí různých kritérií (např. IP adresa uživatele, doba odezvy, SLA, uživatelské jméno, začátek a konec transakce a další). Díky tomu lze získat informace o tom, jaká skupina uživatelů komunikovala s aplikací, jaká byla odezva aplikace, pro jaké uživatele a transakce byla aplikace nedostupná, atd. | Ano | konfigurovatelné filtry |
| CSV export | Systém umožňuje exportovat informace o transakcích ve formátu CSV. | Ano | Podpora reportů do CSV |
| Odvozené metriky | Systém sleduje další odvozené metriky jako je průměr, medián, 99-percentil a 95-percentil doby odezvy aplikace, zobrazuje přehled nejpomalejších transakcí, počet uživatelů souběžně pracujících s aplikací, počet transakcí dle splnění SLA, struktura chybových kódů. | Ano | Podpora předdefinovaných metrik |

| | | | |
|---|---|---|---|
| Výkonnost systému | Systém musí umět zpracovat minimálně 2000 transakcí za minutu. | Ano | 6000/s |
| Zdroje dat | Systém musí umět pracovat z daty z minimálně dvou nezávislých zdrojů (sond). | Ano | 2 |
| GUI systému | GUI musí být k dispozici v českém a anglickém jazyce. | Ano | České a anglické GUI |

### *Fyzické sondy pro sběr dat*

Zadavatel požaduje minimálně následující parametry pro fyzické sondy

Zdroje NetFlow/IPFIX dat (sondy) jsou výkonné autonomní zařízení, které monitorují síťový provoz, vytváří o něm statistiky v podobě IP toků (NetFlow/IPFIX data) a zasílají tyto statistiky na kolektor pro uložení a další zpracování. NetFlow/IPFIX data obsahují informace o tom, kdo komunikoval s kým, jak dlouho, jakým protokolem, kolik přenesl dat a další informace ze síťové (L3) a transportní (L4) vrstvy OSI modelu. Sondy rovněž umožňují analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP). Mimo objemových charakteristik provozu poskytují sondy rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti. Díky tomu přináší sonda komplexní přehled a detailní informace o dění v síti a usnadňuje tak řešení síťových problémů, správu a optimalizaci sítě a zvyšuje její bezpečnost.

Sondy jsou nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňují sledovanou síť. K síti jsou připojeny pasivně prostřednictvím SPAN/mirroring portu. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné.

**Obecné požadavky na sondy:**

| Název požadavku | Popis požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|---|
| Pasivní zapojení | Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty). | Ano | Sběr dat pomocí SPAN portů |
| Instalace | Snadná instalace do stávající síťové infrastruktury – hardwarové zařízení, maximální velikost 1U | Ano | 1U |
| Zabezpečená vzdálená správa | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. | Ano | SSH a HTTPS |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. | Ano | Podpora rolí – možnost definovat administrátorem |
| Dohled | Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. | Ano | Podpora SNMP |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. | Ano | Podpora NTP |

| | | | |
|---|---|---|---|
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím GUI. Základní správa prostřednictvím příkazové řádky a GUI. | Ano | Podpora SSH |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. | Ano | Podpora DNS cache |
| LDAP autentizace | Podpora autentizace vůči LDAP (Active Directory). | Ano | Podpora autentizace vůči LDAP a AD |
| Podpora protokolů pro výměnu dat | Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX. | Ano | Export pomocí IPFIX a NetFlow v5 a v9 |
| Zpracování datového provozu | Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor. | Ano | Podpora IPv4, IPv6, MPLS a VLAN parametrů |
| Analýza tunelovaného provozu | Monitorování provozu v tunelu GRE. | Ano | Podpora GRE |
| Uživatelsky definované šablony | Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX. | Ano | Export pomocí IPFIX a NetFlow v5 a v9 – uživatelsky definované |
| Monitorování MAC adres | Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu. | Ano | Podpora MAC parametrů |
| Detekce aplikací | Detekce aplikací dle standardu NBAR2. | Ano | Podpora NBAR2 |
| Analýza zpoždění na síti | Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Ano | Podpora analýzy výkonu sítě |
| Monitorování a analýza HTTP provozu | Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Ano | Podpora analýzy až na L7 |
| Profilování zařízení v síti | Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Ano | Párování informace o operačním systému s IP/MAC adresou pomocí informací z FLOW |
| Monitorování VoIP | Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto | Ano | Podpora práce s VoIP provozem |

| | | | |
|---|---|---|---|
| | rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | | |
| Monitorování DNS provozu | Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Ano | Podpora rozšířené analýzy DNS provozu z FLOW DAT |
| Monitorování Samba/CIFS provozu | Monitorování a analýza Samba/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Ano | Podpora rozšířené analýzy CISF/SAMBA provozu z FLOW DAT |
| Monitorování DHCP provozu | Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Ano | Podpora rozšířené analýzy DHCP provozu z FLOW DAT |
| Nastavení času pro expiraci toků | Podpora pro nastavení časů u aktivní a neaktivní expirace toků. | Ano | Možnost nastavení expirace pro jednotlivé toky |
| Vzorkování | Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků. | Ano | Možnost nastavení vzorkování pro jednotlivé toky |
| Simultánní export NetFlow statistik | Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX). | Ano | Podpora exportu flow dat na externí kolektory |
| Export na základě filtrování dat na sondě | Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky). | Ano | Podpora exportu flow dat na základě zadaných parametrů |
| Vyplňování identifikace AS | Podpora vyplňování AS na základě vestavěného či dodaného seznamu. | Ano | Podpora práce s polem pro AS a jeho doplňování |
| Vyplňování čísla interface | Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port. | Ano | Možnost doplnit číslo rozraní ze kterého data přišly |
| Záchyt provozu v plném rozsahu | Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu. Rozšíření je řešeno formou licence/instalace | Ano | Práce s daty v reálném čase |

| | | | |
|---|---|---|---|
| | SW bez nutnosti změny HW konfigurace. | | |
| Monitorování rozšířených L3/L4 informací | Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů. | Ano | Podpora rozšířených informací z L3/L4 |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+. | Ano | Podpora autentizace vůči TACACS+ a LDAP |
| GUI systému | GUI musí být k dispozici v českém a anglickém jazyce. | Ano | GUI v českém a anglickém jazyce |

**1G Sonda**

| Název požadavku | Popis požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|---|
| Kapacita paměti současných toků | Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port. | Ano | 500 000 |
| Monitorovací porty sond | Sonda obsahuje minimálně 4x 1GbE monitorovacích portů – rozhraní RJ45 | Ano | 4x 1GE RJ45 monitorovacích portů a 1x 1GE RJ45 pro management |
| Výkon sondy na 1GbE monitorovacími porty | Sondy jsou schopné zpracovávat více než 1,4Mp/s (pakety za sekundu) na každém portu | Ano | 1,48 Mp/s |

### 1.1.1 Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik

Požadovaný nástroj pro zajištění centrální správy IP adresního prostoru musí obsahovat integrované nástroje základních síťových služeb DNS a DHCP, L2 monitoring sítě a řízení přístupu do sítě (NAC - založený na standardu radius) – s jednotnou uživatelskou správou přes GUI.

Systém na vzdálených lokalitách (lokalitách krajských ředitelství) musí obsahovat systém pro generování Flow dat se stejným výstupem jako hardwarové sondy poptávané v části 1.1.

Požadavky na celý systém jsou rozděleny do několika částí, ale ve výsledku tvoří jeden funkční celek s unifikovaný a jednotným GUI.

*Obecné požadavky na systém*

| Definice požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|
| Řídící servery systému musí podporovat možnost provozu ve virtuálním prostředí (VMware) | Ano | Běh v prostředí VMware |
| Výkonné servery ve formě fyzických appliancí musí využívat zabezpečený operační systém, být schopné poskytovat požadované funkce i v případě nedostupnosti síťového připojení k centrálnímu serveru a komunikovat s centrálním serverem přes zabezpečený protokol (zabezpečení integrity přenášených dat a obsahu přenášených dat před odposloucháváním na síti) | Ano | Nezávislé servery s podporou OS Linux |
| Systém appliancí musí podporovat možnost nasazení v on-line clusteru a podporovat vícenásobnou redundanci i přes různé lokality | Ano | Možnost libovolného kaskádování |
| Možnost rozšíření funkčního rozsahu appliancí o sběr NetFlow/IPFIX dat o provozu ve vzdálených lokalitách a jejich odesílání do centrálního kolektoru monitorovacího systému | Ano | Licence na export dat do FLOW kolektoru |
| Systém musí obsahovat samostatný systém pro centrální správu a nastavení appliancí | Ano | Jednotné GUI pro správu |
| Systém musí být schopen integrace se systémy pokročilé síťové analýzy (NBA) nebo SIEM | Ano | Připojení na SIEM |
| Systém musí podporovat možnost napojení na SMS bránu pro odesílání autentizačních informací uživatelům | Ano | Možnost rozšířit o SMS bránu |
| GUI systému musí být k dispozici v českém a anglickém jazyce | Ano | Podpora českého a anglického jazyka |

*Systém pro adresní plánování*

| Definice požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|
| Nástroj pro návrh a definici IP adresního plánu s možností definice sítí, výběr konkrétní sítě a práce s ní | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat v sítích možnost definice bloků adres, výběry dle bloků adres | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat import MAC/IP adres z online monitoringu sítě, automatický výběr správné sítě pro importované adresy | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat import/export záznamů do/z adresního plánování v XML nebo CSV formátu | Ano | Systém podporuje export do CSV a XML |

| | | |
|---|---|---|
| Systém musí podporovat automatické generování pravidel pro DHCP servery z adresního plánování | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat automatické vytváření DNS záznamů z adresního | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat vytváření profilů dle sítí, po výběru profilu zobrazení a možnost práce pouze s IP adresami sítí daných profilem | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat nástroj pro hromadné práce s definovanými skupinami zařízení a podporu krizového řízení | | Plná podpora v IPAM modulu |

*Systém pro monitoring sítě*

| Definice požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|
| Systém musí podporovat monitoring na L2 vrstvě - MAC a IP adres v reálném čase, včetně toho, na kterém fyzickém portu switche se daná MAC adresa nachází, pokud switch tuto možnost poskytuje (na kterém portu kterého switche je připojené zařízení s danou MAC adresou), včetně podpory historie | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat dostupnost monitoringu i v lokalitách, kde je přístup přes třetí vrstvu (routované lokality), data musí být online k dispozici přes uživatelské rozhraní na centrální lokalitě | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat online sledování a vyhodnocení monitoringu ve formě: povolená dvojice MAC-IP, zakázaná dvojice MAC-IP, nekorektní DHCP MAC-IP, neznámá MAC-IP | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat vypsání „mrtvých“ MAC nebo IP adres (adresy, které se v síti nevyskytly např. půl roku), s možností přes uživatelské rozhraní provést vymazání z DHCP, DNS a Radius záznamů a vrácení příslušných IP adres do adresního plánování | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat export odmonitorovaných záznamů do XML nebo CSV | Ano | Systém podporuje export do CSV a XML |

### 1.1.2 Integrovaný DHCP server

| Definice požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|
| Musí se jednat o distribuovaný DHCP systém s možností existence více DHCP serverů na stejné síti (redundance) | Ano | Tvorba HA DCHP prostředí |
| Systém musí podporovat centrální řízení a zakládání pravidel | Ano | Jednotné GUI pro centrální správu |
| Systém musí podporovat podpora redundanci řídícího serveru, nezávislé na lokalitě | Ano | HA na úrovní virtuálního řídícího serveru |
| Systém musí podporovat uživatelsky definované DHCP volby | Ano | Plně konfigurovatelné DHCP volby |
| Systém musí podporovat definice adresních skupin, k nim vázané DHCP volby | Ano | Plně konfigurovatelné DHCP volby a skupiny |
| Systém musí podporovat vytvoření DHCP pravidla s vazbou více MAC na více IP adres | Ano | Plně konfigurovatelné DHCP návaznosti |
| Systém musí podporovat možnost definice i statického záznamu (pro danou MAC není přidělovaná adresa DHCP serverem, pouze existuje | Ano | V nastavení DHCP |

| | | |
|---|---|---|
| záznam pro Radius server a monitoring, že daná MAC a IP adresa je na síti platná) | | |
| Systém musí podporovat možnost existence DHCP záznamů jedné MAC adresy ve více různých sítích - v každé síti obdrží daná MAC adresa přesně svou IP adresu z rozsahu dané sítě - cestující uživatelé | Ano | V nastavení DHCP |
| Systém musí podporovat automatické vytvoření/změna/smazání DHCP záznamu při operacích v adresním plánování | Ano | Plná podpora v IPAM modulu |
| Systém musí podporovat automatickou propagaci MAC adres z DHCP záznamů v uživatelsky definovaném formátu do Radius serverů pro realizaci dalších bezpečnostních mechanizmů prostřednictvím aktivních prvků sítě (podpora heterogenních aktivních prvků pro 802.1x autentizaci) | Ano | Plná podpora v IPAM modulu |

*Integrovaný DNS server*

| Definice požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|
| Systém musí podporovat centrální řízení a zakládání pravidel | Ano | Jednotné GUI pro centrální správu |
| Systém musí podporovat automatické vytváření A a PTR záznamů z adresního plánování | Ano | Plná podpora v IPAM modulu |
| Centrální řídící server musí mít redundanci nezávislou na lokalitě | Ano | HA na úrovní virtuálního řídícího serveru |
| Systém musí podporovat možnost rozdělení zón na vnitřní a vnější pro stejnou zónu, definice vazby na vnitřní nebo vnější zónu dle IP adres (sítí) DNS klientů (klienti ve vnější sítí dostávají odpovědi pouze pro DNS záznamy z vnější zóny, klienti z vnitřní zóny dostávají DNS odpovědi pro vnitřní i vnější zónu) | Ano | Plná podpora v DNS modulu |
| Systém musí podporovat replikaci zvolených zónových souborů na podřízený DNS server | Ano | Plná podpora v DNS modulu |
| Systém musí podporovat automatického vytváření PTR reverzních záznamů při zakládání “A” záznamů | Ano | Plná podpora v DNS modulu |
| Systém musí podporovat porovnání DNS z Adresního plánování s DNS záznamy na DNS serveru, včetně automatizovaného nástroje pro řešení rozdílů | Ano | Plná podpora v DNS modulu |

*Bezpečnostní část/NAC*

| Definice požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|
| Systém musí podporovat řízení přístupu do sítě s využitím 802.1x / MAC autentizace a následné Autorizace (dynamické přidělení VLAN) | Ano | Plná podpora 802.1x |
| Systém musí podporovat krizové řízení – schopnost hromadné deaktivace síťové komunikace pro všechny zařízení mimo vyjmenovanou kritickou infrastrukturu organizace | Ano | Možnost nastavení krizového scénáře |
| Systém musí podporovat uživatelské rozhraní s možností přidělování různých stupňů oprávnění. Audit musí být schopen zaznamenat minimálně kdo, kdy a jaké typy operací v systému prováděl | Ano | Logování všech změn |
| Systém musí podporovat sledování incidentů na síti s možností generování bezpečnostních reportů | Ano | Logování všech incidentů |

*Spolupráce s aktivními prvky*

| Definice požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|
| Systém musí podporovat automatické zálohování konfigurací aktivních prvků | Ano | Pomocí FTP/SSH |
| Systém musí podporovat sledování výskytu MAC adres na portech s historií pro účely určení, kde se v daném čase vyskytuje nebo vyskytovala MAC adresa | Ano | Pomocí SSH |
| Systém musí podporovat automatické repository - informace o verzi firmare, typu zařízení, S/N apod. | Ano | Pomocí SSH |
| Systém musí podporovat sledování využití portů síťových prvků v čase - detekce nepoužívaných | Ano | Pomocí SSH/SNMP |

*BYOD část*

| Definice požadavku | Splňuje ANO/NE | Popis splnění požadavku/parametru |
|---|---|---|
| podporovaná veškerá funkcionalitu rovněž pro mobilní zařízení s přístupem přes WiFi | Ano | Plná správa WiFi zařízení |
| podpora samoobslužného rozhraní pro automatizovanou IP správu nových zařízení v síti | Ano | Plná správa v rámci IPAM modulu |
| možnost vytváření recepčních zón pro zajištění přístupů návštěv (Guest zóna) | Ano | Podpora tvorby GUEST zón |

### 1.1.3 Školení

Zadavatel požaduje dodání následujících školení:

- Administrátorské školení pro systém Monitoring a vyhodnocování toků v síti (rozsah 2MD),
- Administrátorské školení pro systém Monitoring sítě, správu adresního prostoru a systém řízení přístupových politik (rozsah 2MD)

### 1.1.4 Definice rozsahu nasazení

Zadavatel uvádí následující rozsah nasazení systému:

*Systém pro monitoring, vyhodnocování, analýzu toků v síti a monitorování výkonu aplikací*
Systém (kolektor a sondy) bude nasazen centrálně na úrovni centrálního datového centra a příslušných pavilonů.

*Systém pro monitoring sítě, správu adresního prostoru a systém řízení přístupových politik*
Systém podporující redundanci služeb L2 monitoringu a DHCP/DNS/NAC pro následující lokality, které budou vybaveny hardwarovým řešením:

- Jedna centrální lokalita – HA architektura

Celkové množství spravovaných zařízení bude cca do 5000 IP zařízení v síti.