Příloha č. 1 smlouvy – Technická specifikace zadavatele (kupujícího)

Technická specifikace (dokumentace) veřejné zakázky
**„Implementace opatření v oblasti kybernetické bezpečnosti MěÚ Stod“**
v rámci projektu „Kybernetická bezpečnost MěÚ Stod“

# 1 Popis předmětu plnění této technické specifikace

Objednatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci. Předmětem plnění je zejména:

- dodávka HW komponent (server, diskové úložiště, aktivní prvky, tenký klient, diesel generátor),
- dodávka SW řešení (monitorovací a logovací systém SIEM, centrální správa tenkých klientů, provozní monitoring),

a jejich příslušenství.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

**Uvedení konkrétních označení a názvů**

Pokud tyto zadávací podmínky obsahují požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, pak je to z důvodů, že se jedná o stávající zařízení v majetku zadavatele a systémy, se kterými musí být nabízené vybavení kompatibilní. V ostatních případech, pokud by se v některé části ZP takové požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu vyskytly, pak je to z důvodů, že stanovení technických podmínek jiným způsobem nemůže být dostatečně přesné a srozumitelné. V každém takovém případě je v souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, možné nabídnout i jiné, rovnocenné řešení.

## 1.1 Popis současného stavu

### 1.1.1 Komunikační systém LAN MěÚ

LAN je realizována nejprve CORE částí složenou z páteřních přepínačů HP A5800 vždy v redundantním zapojení na lokalitě – označené jako CORE 1 nebo 2. Mezi lokalitami jsou CORE spojeny optickým vedením 10 Gb. Do CORE jsou zapojeny hlavně servery, disková pole, FW a NAS úložiště přes separátní VLAN, v které je provozováno ISCSI. Připojení tohoto HW je vždy minimálně jedním 10 Gb do jednoho switche a jedním 1Gb záložně do druhého. SW CORE1 a SW CORE 2 jsou spojeni do jednoho logického celku. Do CORE jsou dále zapojeni podružné switche SW 1 – 3 a SW VOIP 1 – 3. Do SW 1 – 3 (HP 2510) jsou zapojeni již klientská zařízení jako PC, tencí klienty, tiskárny, všechny porty disponují rychlostí 1Gb. Do SW VOIP 1 – 3 (HP 2530) jsou zapojeny VoIP telefonní přístroje CISCO, Access pointy UNIFI a z těchto switchů je realizováno i POE napájení těchto přístrojů – opět všechny porty disponují rychlostí 1 Gb. Pasivní částí LAN je rozvod strukturované kabeláže CAT 5e v obou lokalitách MěÚ. CORE switche dále obsahují na každé lokalitě rozšiřují optický modul, do kterého jsou optickým spojem 1 Gb napojeny lokality a kamerové body MAN optické sítě. V současné době MěÚ nepoužívá žádný monitoring infrastruktury ani systém pro centrální správu. LAN ve své podstatě zprostředkovává připojení na služby IS města a služby poskytované např. ISZR – přes různé systémy jako elektronická spisová služba, CzechPoint, CzechPoint@Office, Registr vozidel a řidičů atd.

**Firewall** – V současné době je komunikační systém osazen dvěma FW Fortinet Fortigate 200B, které jsou zapojeny v HA módu. I když nyní FW poskytuje ochranu na úrovni Full UTM (AntiVirus, App. Control, Email Filter, Intrusion Protection, Web Filter, SSL Inspection), po nasazení SSL inspekce začalo docházet k výkonostním problémům, FW již po stránce HW nedokáže splňovat požadované funkce. Díky tomu musela být přenastavena hicarchie z původního nastavení active/pasive, kdy mohlo dojít k výpadku jednoho firewallu, na active/active. To znamená, že se nyní na výkonu podílí oba FW a v případě poruchy jednoho ze zařízení již dojde k bezpečnostní hrozbě, jelikož kvůli zachování základní funkce musí dojít k vypnutí ostatních bezpečnostních služeb a FW spadne do tkzv. conserve módu. Pokud by došlo k úplnému výpadku služeb, dojde k úplnému kolapsu IS, přes FW prochází veškerá komunikace LAN, MAN a VOIP, jelikož na FW probíhá routing celé sítě.

**Přepínače** – Hierarchie sítě je od core přepínačů HP A5800 po HP 2510 a HP 2530.

### 1.1.2 Komunikační systém LAN METRO

LAN METRO je připojena z CORE switchů, z jednoho v každé lokalitě. V současné době obsahuje pouze jeden ze SW CORE na každé lokalitě optický modul, do kterého jsou optickým spojem 1 Gb napojeny lokality a kamerové body MAN optické sítě. MAN je realizována v drtivé většině jako kruh, v případě výpadku (překopu optiky) umožňuje po pasivním zásahu obnovit komunikaci po druhé straně kruhu. MAN však v tuto chvíli není odolná proti výpadku optického modulu nebo CORE switche, kde je modul osazen. MAN nyní využívají již všechny organizace zřizované městem (ZŠ a MŠ, ZUŠ, Kult. dům, domy s pečovatelskou službou atd.) a krajem (SOUDOM Domažlice – škola Stod v počtu 4 budov, chráněná dílna s pekárnou a průjezdový radar), kterým

poskytujeme služby firewallu, připojení k internetu, hlasové služby a hosting virt. serverů, případně přímé napojení na CamelNet – krajskou optickou síť pokrývající celé západní Čechy. Přes MAN je dále realizován již velmi rozsáhlý kamerový systém, který je provozován v oddělené VLAN spolu s kamerovým serverem a dohledovým centrem místního odd. PČR. Síť MAN je realizována na aktivních prvcích MikroTik RB2011, kde je i na úrovní vnitřního switche oddělena LAN pro kamery a LAN pro ostatní provoz (VOIP, Internet, Wi-Fi apod.). Pasivní část sítě je v rámci etap budována uložením chrániček do výkopů a následným zafoukáním a navařením optických vláken. Vlákna jsou zakončována v připojených lokalitách nebo optických komorách v případě potřeby připojení např. kamerového bodu. Převod optika/metalika je vždy integrován v routeru MikroTik.

**Firewall** – Celá MAN je opět routována výše zmíněným firewalem, kde je dle pravidel striktně nastavena komunikace. Celá MAN je dle lokalit dělena na VLAN, která je vždy připojena vlastním interfacem a dle toho jsou na ní aplikována potřebná pravidla ohledně komunikace.

**Přepínače** – Hiearchie sítě je od core přepínačů HP A5800 po routery MikroTik RB2011.

# 2 Technická specifikace

## 2.1 Základní požadavky na technické řešení

Hlavním cílem je zvýšení kybernetické bezpečnosti a naplnění požadavků daných zákonem číslo 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), tj. v souhrnu zajištění a zvýšení bezpečnosti informačních a komunikačních systémů Města Stod.

Zadavatel z důvodů jednotné správy IT infrastruktury a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.

Veškeré komponenty, které dodavatel dodává v rámci předmětu plnění, musí splňovat následující podmínky:

| |
|---|
| Jedná se o nové a nerepasované komponenty. |
| Byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce. |
| Mají plnou záruku od výrobce. |
| Mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce. |
| Obsahují všechny nezbytné licence na používání příslušného softwaru. |
| Jsou v databázi výrobce uvedeny jako prodaná kupujícímu - zadavateli. |

Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

## 2.2 Obecné požadavky na řešení

| |
|---|
| Oblast sběru a vyhodnocení kybernetických bezpečnostních událostí |
| Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací – může se jednat o jediné zařízení, softwarový nástroj či appliance. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze HTTPS bez nutnosti instalace klienta. Data budou ukládána do jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů (např. přepínače/ netflow a firewall/syslog). |
| Veškeré dále požadované informace si bude systém automaticky získávat, vyčítat z monitorovaných systémů a současně bude umožňovat příjem protokolů určených pro přenos logovacích, provozních informací, alertů a událostí. Systém bude přijímat informace standardními protokoly ze síťových a dalších aktivních zařízení a Windows server systémů. |
| Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze security event-logu adresářové služby, dále z informací o probíhajících komunikacích prostřednictvím firewallu a dalších přístupových a autentifikačních systémů (např. radius logy). Dále budou získávány informace o překladu zdrojových, vnitřních IP adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím musí být po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení. Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky a to i zpětně. |
| Vzhledem k možnému časovému prodlení mezi vznikem incidentu a jeho vyšetřováním, je požadováno, aby monitorovací a logovací systém umožňoval retenci dat min. 180 dnů. Na tento rozsah retence musí být dostatečně dimenzován, především z hlediska diskové kapacity, RAM i CPU, tak aby nedocházelo k výkonovým ani kapacitním problémům a systém měl dostatečnou rezervu pro očekávatelný budoucí nárůst informací a jejich zdrojů. |

| Oblast zajišťování úrovně dostupnosti informací |
| --- |
| Pro provoz veškerých pořízených systémů a aplikací bude pořízen jeden server. Hardware serveru bude virtualizován pomocí SW VMWare vSphere, díky čemuž bude na serveru možno provozovat několik virtuálních serverů. Server bude připojen do sítě duální optickou linkou 2× 10 Gb. Pořízený server musí být výrobcem určen pro provoz v běžném, neklimatizovaném prostředí do teploty 40°C (krátkodobě až 45 stupňů Celsia), např. dle ASHRAE Class A4. |
| Pro uložení dat budou pořízeny 2 ks midrange diskových polí, vybavených pokročilými systémy diskové virtualizace, automatického tieringu a budou rovněž připojeny pomocí 10 Gb ethernet síťových rozhraní. |
| Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí zvýšení dostupnosti infrastruktury v lokalitě Sokolská. Tato lokalita bude vybavena motor generátorem. |
| Pro zajištění úrovně dostupnosti informací na koncových zařízeních úřadu bude dodán nový HW v podobě tenkých klientů kompatibilních se SW řešením pro centrální správu stávajících tenkých klientů. |

| Oblast zajištění ochrany integrity komunikačních sítí |
| --- |
| V rámci této komodity bude dodána dvojice next-generation firewallů vybavených funkcionalitou anti-X (antivir, antispam, antimalware, kategorizace URL a SSL inspekce). Na nové firewally budou migrovány veškeré funkcionality stávajících firewallů (Fortinet FG-200B) a budou zprovozněny příslušné next-generation služby. |
| Součástí dodávky bude také rozšíření stávajících přepínačů HPE 5800-24G o modul 16× 1Gb SFP a doplnění stávajících IRF clusterů o celkem 4 ks přepínačů. |
| Na všech koncových zařízeních úřadu a všech relevantních aktivních prvcích bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X. |
| Pro hosty a externí uživatele bude zřízena samostatná VLAN (Guest VLAN), která bude komunikačně (min. L3 pravidla, ACL) oddělena od vnitřních sítí organizace. Tato VLAN bude mít své L3 rozhraní až na úrovni firewallu, tak aby bylo možné komunikaci podrobit kontrole za pomoci UTM nástrojů (min. AV, IPS, kategorizace obsahu) a mohl jí být přiřazen samostatný profil odlišný od profilů pro interní zaměstnance úřadu. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu - webové autorizace. Captive portál bude zajištěn firewallem s důrazem na bezpečné oddělení uživatelského provozu od zbytku vnitřních sítí. |
| Ověřování přístupu do LAN bude realizováno protokolem 802.1X vůči adresářové službě prostřednictvím protokolů radius a PEAP. Nabízená zařízení v rámci komodity K4 musí být vybavena tzv. suplikantem - softwarovou komponentou, která dokáže předávat ověřovací požadavky síťovým prvkům, které tyto požadavky ověří vůči adresářové služby. Pro ověření zařízení bez suplikantů (např. starší tiskárny, zařízení na bázi jednoduchých operačních systémů či firmware apod.) bude použit jiný - dodavatelem navržený - vhodný způsob ověření. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Intranet). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN. Součástí dodávky je konfigurace 802.1x na všech koncových zařízeních úřadu. |

| Oblast zaznamenávání činnosti |
| --- |
| Jako doplňující součást řešení bude dodán a nasazen nástroj pro provozní monitoring infrastruktury zadavatele. Je však požadována integrace s nástrojem na vyhodnocování bezpečnostních incidentů. |

## 2.3 Funkční požadavky na řešení – povinné parametry dodávaného řešení

V této části jsou uvedeny povinné parametry prvků nabízeného řešení.

Uchazeč v nabídce detailně popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek a uvede konkrétní technické parametry nabízeného zboží, včetně uvedení výrobce a obchodního / typového označení jednotlivých komponentů.

Ke každé nabízené komponentně (s výjimkou příslušenství) budou uvedeny údaje o výrobci a obchodním (nebo typovém) označení.

Konkrétní parametry jednotlivých komponent uchazeč buď vypíše nebo je doloží např. formou katalogových listů v takovém případě ale musí být uveden jasný odkaz na část nabídky, ve které je možné splnění parametrů ověřit.

Popis způsobu naplnění každého povinného parametru musí být konkrétní, úplný a musí jasně prokazovat, že nabízené řešení jednoznačně splňuje požadované parametry.

### 2.3.1 Oblast sběru a vyhodnocení kybernetických bezpečnostních událostí

Monitorovací a logovací systém (SIEM)

| Parametr | Požadavek |
|---|---|
| Základní funkce | Systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů |
| Protokoly sběru logů | syslog, TCP, UDP, HTTP, AMQP, JSON |
| Sběr síťových toků | netflow či kompatibilní dle nabízeného firewallu a centrálního přepínače |
| Zdroje logů | Min. REST API, textové soubory, Radius, Active Directory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and Services Logs", síťové prvky - syslog a netflow, ostatní aktivní prvky - syslog, SNMP trap |
| Parsování logů | Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod. |
| Retence | Uchovávání logů min. 6 měsíců, automatická retence logů a indexů |
| Geolokace | Podpora automatické doplňování logů o informaci o lokalitě podle IP adresy |
| Normalizace logů | Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji |
| Rozšíření logů | Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem. |
| Rozšiřitelnost | Podpora snadného rozšíření funkčnosti pomocí plug-inů nebo modulů |
| Bezpečnost | Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.) |
| Výkon | Min. 500 EPS (event per second), 5000 FPM (flows per minute) |
| Dashboardy | Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek) |
| Export dat | Export dat do CSV a/nebo XLS formátu (min. výsledky vyhledávání) |
| Kanály | Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod. |
| Alerty, notifikace | Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílání upozornění |
| Active Directory | integrace s Active Directory pro ověřování uživatelů, nastavení oprávnění min. administrátor a operátor |
| Vyhledávání | Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání nebo filtrování bez tvorby dotazů, např. výběrem v kontextovém menu vybraného pole uloženého záznamu. |
| Ovládání | Intuitivní grafické rozhraní. |
| Kompatibilita | Podpora provozu v prostředí nabízené serverové virtualizace. |
| Ukládání dat | Ukládání dat do databáze, případná databázová licence musí být součástí dodávky. |

| | |
|---|---|
| Výstupy | Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem. |
| Podpora ze strany výrobce | Podpora ze strany výrobce po dobu 48 měsíců – nárok poskytnutí opravných verzí (podpora bude uhrazena současně s dodávkou). |
| Podpora a dohled ze strany dodavatele | Podpora a dohled ze strany dodavatele je podrobně specifikována v kapitole 5. |

Monitorovací a logovací systém bude nasazen / konfigurován na HW prvky (konkrétně na server, disková úložiště, firewally a páteřní přepínače) dodávané v rámci tohoto předmětu plnění a dále na současné, tj. již stávající vybrané a níže uvedené prvky v ICT architektuře MěÚ Stod:

| Typ zařízení | Počet a označení |
|---|---|
| Servery | 2× HP ProLiant DL360p Gen8 |
| | 1× Cisco BE6000 UCS C220 M3 MD |
| Disková úložiště, NAS | 2× HP Lefthand P4500 G2 |
| | 1× Synology RS3614xs |
| | 1× Synology DS1815+ |
| LAN, SAN přepínače | 3× HP e2510 |
| | 3× HP e2530 |
| | 4× HP v1920 |
| | 4× HP A5800 |

## 2.3.2 Oblast zajišťování úrovně dostupnosti informací

1× server

| Parametr | Požadavek |
|---|---|
| Form Factor a vnitřní uspořádání | šasi pro montáž do standardního racku o velikosti 1U, požadujeme dodání serveru s rackmount příslušenstvím včetně pohyblivého ramene pro zachycení kabeláže |
| CPU | dvousocketový systém osazený dvěma 14 jadrovými CPU s minimálním výkonem podle benchmarku SPEC CPU 2006 (viz. www.spec.org):<br>• CINT2006 Rates, hodnota base-line – 1500 bodů<br>• CFP2006 Rates, hodnota base-line – 1170 bodů |
| RAM | Osaditelnost až 24 ks DIMM paměťových modulů o kapacitě až 128GB (maximální kapacita 3TB při použití DDR4 LRDIMM nebo až 768GB při použití DD4 RDIMM s taktem 2600 MHz). Ochrana paměti: Advanced ECC s multi-bit error protection, Online spare, mirrored memory a fast fault tolerance.<br>Požadavek: 512GB RAM osazených rovnoměrně ve všech šesti kanálech na každý procesor |
| Diskový subsystém | server musí podporovat min. 8× 2,5" diskové sloty typu hotplug. Server musí akceptovat disky s rozhraním SATA\|NLSAS\|SAS typu HDD (rotační ) \| SSD nebo jejich libovolné kombinace. |
| Flash/USB Drive | server musí bát vybaven minimálně: jedním seriovým portem, Micro-SD slotem a minimálně 5ks USB 3.0 portů (jeden zepředu, dva zadní a dva uvnitř) |
| | možnost osazení PCIe karty s M.2 SSD, podpora RAID1 na úrovni hardware. Požadujeme osadit 2× duální MicroSD Flash USB 8GB |
| Interface | min. 3× externí USB, z toho min. 2×USB 3.0<br>min. 1× interní USB 3.0 port |

| | |
|---|---|
| | min. 2× VGA port |
| Napájecí zdroje | server musí být osazen redundantními hot-plug větráky a musí být osaditelný až dvěma hot-plug napájecími zdroji s účinností až 94% a výkonem min. 700W |
| Rozšiřující sloty | Server musí disponovat celkem 3ks PCI-Express 3.0 slotů, z nichž minimálně dva musí být x16 PCIe |
| Síťové porty | Požadavek na celkem:<br>min. 2 porty 1Gbit RJ-45<br>min. 2 porty 10Gbit SFP+<br>z toho min. 2× 10Gbit SFP+ onboard (karta nezabírá externí PCIe slot) |
| Podpora operačních systémů a virtualizace | Microsoft Windows Server<br>Red Hat Enterprise Linux (RHEL)<br>SUSE Linux Enterprise Server (SLES)<br>Vmware<br>ClearOS |
| Server management | Musí být umožněn rychlý pohled na spravované serverové zdroje. Minimální zobrazované položky Dashboardu jsou Server Profiles, Server Hardware a Appliance Alerts. Přístup do managementu musí být řízen pomocí rolí. Management sw musí být integrovatelný minimálně do Vmware vCenter a Microsoft SCVMM. Systém musí umožňovat proaktivní notifikaci o aktuálních nebo hrozících selháních kritických komponent jako jsou procesory, paměť a disky. Systém musí být dostupný přes vlastní portál odkudkoliv. Systém musí být schopen upozornit na out-of-date BIOS, ovladače a agenty server managementu a umožnit vzdálený update těchto komponent. Server management sw musí být od stejného výrobce, jako je výrobce serveru. |
| Management a vzdálená správa | Server musí disponovat vyhrazeným Gb portem pro vzdálený management, port musí mít k dispozici úložiště pro firmware, ovladače a další sw komponenty. Úložiště musí být konfigurovatelné pro vytváření instalačních sad s možností rollback/patch při pádu aktualizace. Server musí podporovat bez agentový vzdálený management. Vzdálený management musí podporovat standardní webové prohlížeče pro grafickou vzdálenou konzoli spolu s tlačítkem pro Virtual Power a podporovat vzdálený boot z DVD/CD/USB zařízení a být schopen uchovávat historická data o sw upgradech a patchích. Musí být podporována vícefaktorová autentikace. Musí být monitorovány změny v hw a systémové konfiguraci, musí být podporována rychlá diagnostika vzniklých problémů. Pro vzdálenou správu musí být podporována mobilní zařízení Android a Apple iOS. Vzdálená konzola musí umožnit současný přístup až 6 uživatelům během pre-OS a OS runtime operací, musí existovat schopnost uchovat video z poslední zásadní poruchy a posledního bootovacího procesu, musí být podporována MS TS integrace včetně 128 bitové SSL enkrypce a Secure Shell Version 2, musí být podporovány AES a 3DES na prohlížeči a vzdálený firmware update a JAVA free pro vzdálenou konzoli. Musí být podporována současná podpora většího množství serverů a to v následujících komponentách: Power Control, Power Caping, Firmware Update, konfigurace, Virtual Media, Licence Activation. Musí být podporována RESTFullAPI integrace a předávání hw událostí přímo na výrobce serveru. |
| Ladění výkonu | Server musí umožňovat práci s profily pro výkonovou optimalizaci. |
| Secure Encryption | Server musí podporovat šifrování dat (Data at Rest) jak na interních discích, tak na cache diskových řadičů použitím šifrovacích klíčů. Musí být podporován lokální management klíčů pro jeden server, ale také management pro vzdálenou správu klíčů více serverů. |
| Systém Security | UEFI Secure Boot and Secure Start support |
| | Security feature to ensure servers do not execute compromised firmware code |
| | FIPS 140-2 validation |
| | Common Criteria certification |
| | Configurable for PCI DSS compliance |
| | Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser |
| | Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms |
| | Tamper-free updates – components digitally signed and verified |
| | Secure Recovery – recover critical firmware to known good state on detection of compromised firmware |

| | |
|---|---|
| | Ability to rollback firmware |
| | Secure erase of NAND/User data |
| | TPM (Trusted Platform Module) 1.2 option |
| | TPM (Trusted Platform Module) 2.0 option |
| | Bezel Locking Kit option |
| | Chassis Intrusion detection option |
| Záruční servis | Záruční servis 5 let, odstranění závady nejpozději následující pracovní den (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace. |
| | Bezplatné aktualizace firmware po dobu záručního servisu. |
| | Možnost stažení ovladačů a management software na webových stránkách výrobce. |
| | Možnost automatického generování servisního incidentu přímo u výrobce hardware. |

2× diskové úložiště

| Parametr | Požadavek |
|---|---|
| | 2 ks síťového úložiště, každé o min. kapacitě RAW 25TB s možností růstu na min 50TB. |
| Form Factor | Nabízené úložiště musí mít šasi pro montáž do standardního racku o velikosti max. 2U. |
| Požadavky na konektivitu | Nabízené úložiště bude využívat SAN infrastrukturu na protokolu iSCSI 10Gb. |
| | Požadujeme, aby nabízené úložitě obsahovalo min. 2 porty 10Gbit SFP+, včetně 10G BASE-SR modulů a min. 4 porty 1 Gbit Base-T. |
| Požadavky na úložná zařízení | Nabízené řešení musí umět virtualizovat kapacitu z vnitřních i externě připojených úložišť a tuto kapacitu poskytovat pomocí standardního protokolu. |
| | Řešení musí podporovat SSD, SAS i NL-SAS disky v jednom úložišti současně. |
| | Požadujeme využití 2 vrstev pro tiering na úložišti – vrstvu SSD min. 20 % kapacity a vrstvu HDD 10tis otáček/minutu zbylá kapacita úložiště. |
| Funkční požadavky | Nabízené řešení musí podporovat No Single Point of Failure řešení tak, aby při havárii libovolného storage nodu/řadiče provoz plynule pokračoval bez odstávky. Rovněž upgrade systému storage clusteru (HW, firmware …) musí být možné provést bez přerušení provozu. |
| | Řadiče nabízeného řešení musí podporovat režim active/active a automaticky rozkládat zátěž každého LUNu na všechny disky v dané vrstvě. |
| | Nabízené řešení umožní synchronní replikaci dat mezi uzly clusteru pro zvolené datové oblasti na úrovni nodů clusteru a synchronní replikaci LUNů mezi dvěma lokalitami. |
| | Nabízené řešení umožní asynchronní kopírování dat. Tyto asynchronní repliky, využívané zejména pro efektivní a rychlé zálohování, musí být možno synchronizovat/integrovat se službou Microsoft VSS pro zajištění konzistence dat, případně výrobce musí dodat integrační agenty pro provozované aplikace (MS Exchange, MS SQL). |
| Požadavky na licence a další podpůrný SW | Požadujeme licence pro následující funkce: |
| | kompletní management/GUI a command line. Grafické rozhraní pro správu musí být intuitivní a jednoduše ovladatelné. Preferované je řešení založené na Java kódu, vzhledem k jeho větší nezávislosti na provozované platformě/operačním systému |
| | snapshot - až 64 snapshotů z jednoho logického disku |
| | clone |
| | thin provisioning |
| | automatický tiering |
| | synchronní replikace |
| | asynchronní replikace/remote snap |
| | podpora multipathing a Microsoft MPIO DSM |
| | Podpora Vmware VAAI |
| | Veškeré licence budou dodány pro požadovanou kapacitu. |

| | |
|---|---|
| Kompatibilita | Nabízené řešení musí podporovat min. OS Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Linux, Vmware 5.0 a vyšší, Hyper-V, HP-UX 11i v3 |
| Záruční servis | Záruční servis 5 let, odstranění závady nejpozději následující pracovní den (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace. |
| | Bezplatné aktualizace firmware po dobu záručního servisu. |
| | Možnost stažení ovladačů a management software na webových stránkách výrobce. |
| | Možnost automatického generování servisního incidentu přímo u výrobce hardware. |

1× diesel generátor

| Požadavek |
|---|
| třífázový motor generátor |
| výkon min. 40kW |
| dlouhodobý odběr min. 37kW |
| hlučnost max. 55dB(A) |
| ohřev motoru, upraveni pro aut.start |
| ekologická vana pod DA |
| doprava stroje do místa instalace |
| nastěhování stroje v místě (nutnost rozložení stroje, |
| nastěhování po částech, složení stroje v místě) |
| stykačová kombinace 63A/400V v TNC |
| rozvaděč pro AUT start |
| karta pro dálkový dohled |
| instalace rozvaděče + ožívení stroje |
| výdechové potrubí (tvarové potrubí 2m, žaluzie, pružný člen) |
| nasávací potrubí (tvarové potrubí, žaluzie) |
| el.klapky s pohonem |
| instalace: mechanická část |
| výfukové potrubí (certifikované dílce třísložkové provedení až nad střechu, včetně revize komínu, napojení na stroj) |
| drobný a kotvící materiál: mechanika |
| kabelová příprava: silový kabel |
| kabelová příprava: ovládací kabel |
| nosné žlaby – kabely |
| instalace: kabelová příprava |
| stavební příprava |
| projektová dokumentace |
| výchozí revize zapojení |
| Záruční servis 24 měsíců, servisní zásah do 5 pracovních dnů ode dne nahlášení závady v místě instalace. |

41× tenký klient

| Parametr | Požadavek |
|---|---|
| Procesor | Dvoujádrový |
| Systémová paměť | 4 GB DDR3 SDRAM |
| Flash memory | 32 GB |
| Podporované protokoly | Citrix® Ica; Citrix® Hdx; Microsoft Rdp; Microsoft Remotefx (Rfx); Vmware® Horizon View™ prostřednictvím PcoIP; Vmware® Horizon View™prostřednictvím RDP |
| Podporované OS | MS Windows Embeded, Windows 10 Iot Enterprise pro tenké klienty |
| Podpora Smart Card | ANO |

| | |
|---|---|
| Komunikační rozhraní | 1× Ethernet (Rj-45),Wake On Lan (Wol), Pxe, Tcp/Ip S Podporou Dns A Dhcp, UDP, volitelný adaptér Wi-Fi s Bluetooth®, |
| Porty a konektory | 2× USB prot, 1× konektor pro náhlavní soupravu, 1× RJ-45, 1× displej port, 1× VGA, |
| Napájecí konektor | ANO |
| Vstupní zařízení | standardní CZ klávesnice, dvoutlačítková optická myš s rolovacím kolečkem (USB) – standardní velikost, ne mini. |
| Napájecí zdroj AC 230 V | ANO |
| Kompatibilita | Plně kompatibilní s uvažovaným systémem správy HP Device Manager 4.6 |
| Záruka | Záruční servis 5 let, odstranění závady nejpozději následující pracovní den (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace. |

SW pro centrální správu tenkých klientů

| Parametr | Požadavek |
|---|---|
| Funkcionalita centrální správy tenkých klientů | • jednoduché grafické uživatelské rozhraní<br>• automatické rozpoznání a registrace zařízení<br>• seskupování zařízení pro snadné rozpoznání<br>• přiřazení bezpečnostních certifikátů<br>• nástroje auditu a reportingu zpráv, podpora formátů: CSV, Excel, PDF, RTF, HTML<br>• identifikace stavu online / offline<br>• nástroj pro zálohování a obnovu<br>• upgradování operačního systému<br>• ukládání do mezipaměti - pro bezdrátové připojení a zobrazování v bezpečném prostředí 802.1x<br>• konfigurace zařízení, klonování, nasazení<br>• komplexní vzdálený přístup ke všem položkám registru, stejně jako možnost vzdálené správy souborů tenkých klientů.<br>• nativní skriptování a příkazy<br>• řízení spotřeby<br>• Vzdálený restart počítače<br>• Vzdálené vypnutí<br>• Konfigurace Wake-on-LAN<br>• řízení uživatelů a skupin včetně omezení spustitelných funkcí<br>• integrace služby Active Directory<br>• podporované platformy: minimálně MS Windows Server 2008, 2012, 2016 |
| Komunikační rozhraní | Grafické komunikační rozhraní v podobě HTTPS aplikace a jednotlivými GUI pro management terminálových služeb a tenkých klientů. |
| Záruka | Záruka 2 roky. |

### 2.3.3 Oblast zajištění ochrany integrity komunikačních sítí

2× Firewall

| Parametr | Požadavek |
|---|---|
| Základní specifikace | |
| Typ zařízení | Statefull firewall |
| Formát zařízení | HW do RACKu 1U |

| | |
|---|---|
| Počet fyzických portů | Min. 12× GE RJ45 (min. 2× WAN), 2× GE SFP, USB |
| Interní úložiště (pro uložení logovacích záznamů a cache) | min. 400 GB |
| Výkonová specifikace | |
| Propustnost FW – stavový filtr | 8 Gbps |
| Propustnost IPSec VPN | 8,5 Gbps |
| Propustnost SSL VPN | 800 Mbps |
| Latence firewallu | < 5 mikro sec. |
| Propustnost IPS (HTTP / Enterprise Traffic Mix) | 5 500 / 2 000 Mbps |
| Propustnost Threat Protection = aktivní min. IPS, Aplikační kontrola a Anti-Malware (Enterprise Traffic Mix) | 1000 Mbps |
| Funkční specifikace | podporuje |
| HA zapojení, L2, Active-Active nebo Active-Passive | podporuje |
| Režim nasazení – L2 transparentní, nebo L3 NAT/Router | podporuje |
| Linková agregace 802.3ad | podporuje |
| Možnost vytvořit IPv4 a IPv6 vlan interface | podporuje |
| Podpora IPv4, IPv6 | podporuje |
| NAT, PAT | podporuje |
| IPSec VPN v režimu GW to GW a GW to Client | podporuje |
| Podpora SSL VPN, tunelový a portálový režim | podporuje |
| Podpora NTP, SNMPv3, Syslog | podporuje |
| Logování v lokálním režimu a na centrální logovací systém | podporuje |
| Dynamické směrování pro IPv4 and IPv6 (RIP, OSPF, BGP a Multicast IPv4) | podporuje |
| Policy based routing a source based routing | podporuje |
| WAN optimalizace, linkový balancer | podporuje |
| Traffic shaping | podporuje |
| Explicitní Proxy, Reverzní proxy | podporuje |
| Více správcovských účtů s různým oprávněním | podporuje |
| Virtuální kontexty s oddělenou konfigurací a správou | 10 |
| Správa přes min. HTTPS, SSH | podporuje |
| Dedikovaný port pro management | podporuje |
| Integrovaná podpora pro dvoufaktorovou autentikaci | podporuje |
| Integrace s Active Directory pro SSO | podporuje |
| Licencování na neomezený počet uživatelů | podporuje |
| Intrusion Protection Systém (IPS) | podporuje |
| Aplikační kontrola na L7 (>3000 signatur síťových aplikací) | podporuje |
| Antivir (Proxy nebo Flow), Antispyware a Antimalware | podporuje |
| Antispam | podporuje |
| Web filtering, kategorizace obsahu | podporuje |
| Reputační databáze obsahující známe IP adresy a domény C&C Botnet sítí | podporuje |
| Pravidelné automatické aktualizace signatur od výrobce | podporuje |
| Data Leak Prevention | podporuje |
| Záruční servis | Záruční servis 5 let, odstranění závady nejpozději následující pracovní den (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace. |
| | Bezplatný nárok na nejnovější firmware. |
| | Pravidelná aktualizace signatur popř. přístup na on-line služby výrobce. |
| | UTM technický support výrobce 5 let v režimu 8×5. |

## 2 ks Rozšiřující karty do přepínačů

Zadavatel požaduje dodání 2× rozšiřující modul do stávajících přepínačů HPE 5800-24G (1 ks do každého DC).

Je požadován modul s 16× SFP porty pro zapojení lokalit MAN v režimu vysoké dostupnosti. Označení modulu výrobce JC095A. Záruční servis 5 let, odstranění závady nejpozději následující pracovní den (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace.

## 4 ks Páteřní přepínače

Zadavatel požaduje dodání 4× přepínač (každý 24× 1Gb portů, 8x 10Gb SFP+ portů) (2 ks do každého DC) – nutná 100 % kompatibilita pro tvorbu clusteru IRF se stávajícími přepínači HPE 5800-24G. Ve výsledném stavu musí cluster tvořit 8 ks přepínačů (4 stávající, 4 nové). Technické parametry každého jednoho přepínače:

| Parametr | Požadavek |
|---|---|
| Základní specifikace | |
| Třída zařízení | L2/L3 switch |
| Formát zařízení | fixní konfigurace 1RU |
| Stohovatelný | ano |
| Počet portů 1 Gbit/s | 24× |
| Počet portů 10 Gbit/s SFP+ | 8× SFP+ |
| Možnost volby 1Gbit/s nebo 10Gbit/s rychlosti portu vhodným transceiverem | ano |
| Redundantní napájecí zdroj | volitelně |
| Možnost interního AC napájecího zdroje | ano |
| Výkonostní parametry | |
| Minimální propustnost L2/L3 přepínacího systému | 200 Gb/s |
| Minimální paketový výkon přepínače | 150 milionu paketů/vteřinu |
| Wirespeed (neblokující) na všech portech | ano |
| Vlastnosti stohování | |
| Minimální počet přepínačů ve stohu | 9 |
| Stohování zařízení přes standardizované síťové rozhraní | ano |
| Virtuální zařízení podporuje distribuované přepínání paketů | ano |
| Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | ano |
| Virtuální zařízení podporuje funkce: single-IP management, spanning tree | ano |
| Virtuální chassis se musí chovat jako jedno L3 zařízení (router, gateway, peer) | ano |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | ano |
| Podpora stohování mezi geograficky odlišnými lokalitami, vzdálenost mezi lokalitami 40km | ano |
| Podpora funkce In-service software upgrade (ISSU) v rámci virtuálního zařízení | ano |
| Protokoly fyzické vrstvy | |
| IEEE 802.3-2005 | ano |
| Podpora "jumbo rámců" do velikosti 10k | ano |
| Protokoly II. vrstvy | |
| IEEE 802.3ad | ano |
| Počet záznamů v MAC adres tabulce | 32000 |
| IEEE 802.1Q | ano |
| Počet aktivních VLAN | 4000 |
| Protokol-based VLAN | ano |
| MAC-based VLAN | ano |
| IP subnet-based VLAN | ano |

| | |
|---|---|
| Podpora GVRP | ano |
| Podpora Multiple VLAN Registration Protocol (MVRP) | ano |
| IEEE 802.1s - Multiple spanning tree | ano |
| IEEE 802.1w - Rapid spanning Tree | ano |
| Podpora STP instance per VLAN s 802.1Q tagováním BPDU (například PVST+) | ano |
| IEEE 802.1p - Minimální počet front | 8 |
| Podpora IEEE 802.1ad - QinQ | ano |
| Podpora MPLS a VPLS | ano |
| Podpora Layer3 MPLS VPN | ano |
| Podpora Layer2 MPLS VPN (VPLS,VLL) | ano |
| Protokoly III. vrstvy | |
| IPv4 a IPv6 směrování | ano |
| Podpora IPv4 a IPv6 QoS | ano |
| Hardware podpora IPv4 a IPv6 ACL | ano |
| Podpora IPv4 a IPv6 VRRP | ano |
| DHCP Server pro IPv4 a IPv6 | ano |
| DHCP Relay pro IPv4 a IPv6 | ano |
| Podpora zapouzdření provozu GRE | ano |
| Směrovací protokoly | |
| OSPFv2, OSPFv3 | ano |
| BGP4, BGP4+ | ano |
| Statické směrování | ano |
| Policy based routing | ano |
| Podpora virtualizace směrovacích systemů (Virtual Routing and Forwarding) pro IPv4 a IPv6 | ano |
| Multicast | |
| IGMP Snooping v2/v3 | ano |
| MLD snooping v1/v2 | ano |
| Směrování multicast IPv4, PIM-DM, PIM-SM, PIM-SSM, BIDIR-PIM, Multicast BGP | ano |
| Směrování multicast IPv6, PIM-DM, PIM-SM, PIM-SSM | ano |
| Bezpečnost | |
| DHCP snooping | ano |
| IPv6 DHCP snooping | ano |
| Podpora ověřování 802.1X | minimálně 1024 ověřených uživatelů na systém |
| Podpora ověřování MAC adres | minimálně 1024 ověřených MAC addres na systém |
| Podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření | ano |
| Ověřování přístupu do sítě s podporou odlišných Guest VLAN (nedojde k pokusu o přihlášení), Fail VLAN (přihlášení selže) a Critical VLAN (nedostupnost RADIUS serveru) | ano |
| Podpora IP source Guard pro IPv4 | ano |
| Management | |
| CLI rozhraní | ano |
| SSHv2 | ano |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |
| Hierarchický management | ano |
| SNMPv3 | ano |
| Sériová nebo USB konzolová linka | ano |

| | |
|---|---|
| AAA ověřování uživatelů (autentizace, autorizace, accounting) | ano |
| Podpora zrcadlení portů (SPAN) a vzdáleného zrcadlení portů (RSPAN) | ano |
| Podpora zrcadlení provozu provozu na základě ACL (traffic mirroring) | ano |
| Vzdálený mirroring (RSPAN) | ano |
| Podpora více monitorujících portů současně, minimálně tří - pro připojení rozdílných analyzačních nástrojů | ano |
| Podpora IP-SLA nebo alternativního způsobu monitorování provozu a dostupnosti služeb s možnou návazností na automatické konfigurační změny systému pro zajištění zachování dostupnosti služeb, zařízení funguje jak IP-SLA iniciátor. | ano |
| Podpora IEEE 802.1ag | ano |
| Podpora Ethernet OAM (IEEE 802.3ah) | ano |
| Podpora technologie monitoringu provozu sFlow podle RFC 3176, včetně podpory exportu ve VRF | ano |
| Podpora odchytávání datového provozu včetně možnosti exportu do formátu PCAP | ano |
| Ostatní | |
| Součástí dodávky pro každý přepínač: | 1× SFP+ twinax kabel, min. délka 50cm<br>7× SFP+ 10G-BASE-SR<br>odpovídající počet patch kabelů |
| Záruční servis 5 let, odstranění závady nejpozději následující pracovní den (servis je poskytován výrobcem nebo autorizovaným zastoupením), oprava v místě instalace. | |

Systém pro ověřování uživatelů 802.1x *(jako součást dodávky páteřních přepínačů)*

| Parametr | Požadavek |
|---|---|
| Obecná charakteristika ověřovacího řešení | Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti a guest přístup definující pravidla přístupu k síti v závislosti na kontextu připojení (uživatel, typ zařízení, stav zařízení, místo připojení, čas připojení apod.) |
| | Ve spolupráci s aktivními prvky (LAN přepínači, bezdrátovými AP nebo řídícími moduly, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné LAN síti, bezdrátové wifi síti (metodou 802.1x) a pro VPN přístup |
| | Poskytuje AAA funkce (viz níže) |
| | Podporuje centralizované nebo distribuované nasazení pro vysokou odolnost a rozšiřování capacity |
| | Umožňuje snadné zálohování , rychlou a úplnou obnovu konfigurace |
| | Forma virtuálního stroje na platformách ESX nebo ESXi |
| | AAA funkce (ověřování, autorizace a záznamy o průběhu připojování uživatelů a zařízení k síti) |
| | RADIUS pro autentizaci, autorizaci, zaznamenávání |
| | proxy funkce pro externí RADIUS |
| | PAP, MS-CHAP, MS-CHAPv2, EAP - MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST |
| | podpora TACACS+ pro administraci zařízení |
| Podporované databáze uživatelů | Active Directory |
| Ověřování uživatelů a zařízení | Ověření uživatelů heslem nebo certifikátem |
| | Ověření MAC adresou připojovaného zařízení |

| | |
|---|---|
| Accounting | Zaznamenávání aktivity uživatelů a zařízení připojených k síti |
| | Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA) |
| Funkce pro správu ověřovacího systému | Centralizovaná správa |
| | Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému |
| | Zjednodušení správy vytvářeními skupin uživatelů, koncových a síťových zařízení |
| | Grafické rozhraní pro definici pravidel přístupu k síti |
| | Grafické rozhraní pro monitorování, řešení problémů |
| | Zaznamenávání událostí na externí syslog server |
| | Podpora SNMPv3 |
| | NTP pro synchronizaci času |
| | Propojení s DHCP a RADIUS |
| | Přiřazení zařízení a uživatelů do místností a sítí (budovy, WiFi, LAN apod.) |
| | Řízení přístupu k síti na základě umístění, možnost řízení přístupu pomocí jednoduchého GUI |
| | Požadovaný počet licencí (endpointů) 250 |
| Záruka | Záruka 2 roky. |

### 2.3.4 Oblast zaznamenávání činnosti

Provozní monitoring

| Parametr | Požadavek |
|---|---|
| Základní požadavky | monitoring bude poskytovaný prostřednictvím virtuální appliance |
| | data budou ukládaná a zpracovávaná v místě služby bez nutné návaznosti na stávající SQL systémy |
| | monitoring bude prováděn 24x7, bude možno vidět procentuální vyhodnocení dostupnosti každého zařízení a také i konkrétní měřené hodnoty u každého zařízení, licence bude pro monitorování min. 1000 senzorů |
| | výstup formou webového interface funkčního i na mobilních platformách (Android, iOS) |
| | GUI (Windows, iOS, Android) se stejnou mírou obsahu jako prim. www rozhraní |
| | integrovaná uživatelská tvorba mapových podkladů pro sledování stavů sítí (tzv. NOC (network operations center) s použitím dynamických hodnot a tabulek z monitoringu |
| | nativní podpora min. těchto management protokolů.: SNMP (v1-3), WMI, NetFlow (v5, v9), Jflow(v5, v9), Sflow(v5, v9), WBEM, Soap, ICMP |
| | nativní podpora min. těchto komunikačních protokolů: http (transaction, content), FTP, POP, IMAP, SMTP, CIFS (SMB), NTP, LDAP, RADIUS, RDP, SSH, LDAP, AD |
| | nativní podpora monitorování min. těchto db systémů: MySQL, MS SQL (2000-2008), Oracle a obecně ADO select |
| | integrovaný reportér pro pravidelné zasílání zvolených výstupních dat monitoringu ve formátu (html, PDF) |
| | notifikace min. těmito notifikačními kanály: Email (vestavený MTA), SMS, Event log, Syslog, http Action, Execute program, SNMP Trap |
| | vestavený Syslog a SNMP Trap server včetně filtrování a uchování zpráv příchozích zpráv v centrálním místě služby |

| | |
|---|---|
| | podpora pro vzájemné porovnání (základní matematické operace) různých snímaných hodnot do jednoho výstupu |
| | kontrola kvality služby VoIP např. dle informací z Cisco SLA agentu a nativními prostředky mezi sledovanými lokalitami |
| | granulární systém uživatelských práv, dědičnost oprávnění směrem dolu v monitoring stromu |
| | dědičnost nastavených notifikačních akcí směrem dolů v monitoring stromu vč. Případného potlačení zpráv ve zvoleném období |
| | zvlášť konfigurovatelné notifikační a eskalační skupiny pro každé zařízení nebo danou část monitoring stromu |
| | podpora pro tvorbu šablon zařízení a import libovolných SNMP MiB souboru |
| | automatické účtování (billing) na základě výstupu z monitoringu |
| | Automatická detekce neobvyklých stavů (unusal) |
| Záruka | Záruka 2 roky. |

# 3 Instalace a zprovoznění

V rámci předmětu plnění zadavatel požaduje provedení min. následujících služeb:

- dopravu jednotlivých komponent do místa plnění do technologické místnosti budovy na adrese MěÚ Stod, nám. ČSA 294, případně na pracoviště na adrese Sokolská 566, Stod,
- zpracování a předání dokumentace,
- integrace definovaných stávajících a nově dodávaných zařízení,
- vytvoření centrálních politik pro ověřování uživatelů (802.1x a na next-generation firewallu),
- migrace uživatelských informací a uživatelských dat do nové infrastruktury,
- migrace centrálních systémů do nové infrastruktury (na nový server a nová disková pole),
- migrace a konfigurace nově dodaných koncových zařízení úřadu (41 PC) do prostředí s tenkými klienty,
- dodávka požadovaných SW licencí,
- zaškolení IT administrátorů na dodané technologie v rozsahu min. 16 hodin.

## 3.1 Popis instalačních služeb

Zadavatel požaduje provést následující práce na dodaných komponentách a dalších zařízeních:

| |
|---|
| Oblast sběru a vyhodnocení kybernetických bezpečnostních událostí |
| Instalace systému pro centrální logování minimálně v rozsahu (další události budou definovány v prováděcí dokumentaci):<br>• monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)<br>• logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)<br>• 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) - RFC3954 nebo ekvivalent (např. netflow) – systém pro monitorování a sběr provozně – lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízení<br>Provedení souvisejících konfigurací monitorovaných systémů.<br>Nasazení, napojení a konfigurace Monitorovacího a logovacího systém (SIEM) na HW prvky (konkrétně na server, disková úložiště, firewally a páteřní přepínače) dodávané v rámci předmětu plnění a dále na současné, tj. již existující vybrané a prvky v ICT architektuře MěÚ Stod viz. jejich výčet v bodě 2.3.1.<br>Na nové firewally budou migrovány veškeré funkcionality stávajících firewallů (Fortinet FG-200B) a budou zprovozněny příslušné next-generation služby. |
| Oblast zajišťování úrovně dostupnosti informací |
| Návrh a kompletní integrace serverové virtualizační platformy s nově dodaným serverem.<br>Implementace pořízených technologií.<br>Analýza dat a systémů na stávajících serverech a jejich migrace na novou serverovou platformu a nové diskové úložiště.<br>Návrh rozložení dat na novém diskovém úložišti – tiering apod.<br>Začlenění nové serverové infrastruktury do stávajícího prostředí, konfigurace prvků vysoké dostupnosti.<br>Konfigurace synchronní replikace nově dodaných diskových polí mezi obě datová centra zadavatele.<br>Úpravy v zálohovacích plánech stávajícího zálohovacího řešení Veeam Backup and Replication.<br>Instalace a zprovoznění motorgenerátoru, včetně potřebných stavebních úprav, dokumentace skutečného provedení a revizní zprávy.<br>Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie.<br>Návrh a provedení akceptačních testů, musí zahrnovat výkonové testy. |

| |
|---|
| Instalace nově dodaných tenkých klientů u uživatelů. |
| Nastavení stávajícího MS RDS prostředí pro všechny dotčené uživatele. |
| Migrace uživatelských nastavení a dat do nového prostředí. |
| Zprovoznění pracovního prostředí všech dotčených uživatelů. |
| Oblast zajištění ochrany integrity komunikačních sítí |
| Analýza stávajícího síťového prostředí a návrh nové architektury LAN. |
| Implementace pořízených technologií. |
| Provedení segmentace LAN – VLAN, adresování, routování v rámci nasazení 802.1x. |
| Návrh a implementace 802.1X pro kabelovou LAN včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů – PC, notebooky síťové tiskárny. Systém 802.1x musí být integrován s adresářovou službou úřadu - MS ActiveDirectory. |
| Integrace se systémem centrálního dohledu a bezpečnostní správy dodávané infrastruktury. |
| Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií), a dále přenos konfigurace ze současných dvou firewallů. |
| Vybudování VPN pro vzdálený přístup uživatelů LAN na bázi webového portálu. |
| Implementace portálu pro registraci a řízení přístupů hostů, tzv. captive portál. |
| Revize, redefinice a redesign struktury MS Active Directory dle nových bezpečnostních požadavků. Revize potřebnosti všech stávajících oprávnění uživatelů/skupin/kontejnerů a nastavení pouze minimálního nezbytného množství oprávnění |
| Revize nastavení group-policy. |
| Provedení všech potřených nastavení na dotčených komponentech pro zajištění ověřování pomocí protokolu 802.1x. |

## 3.2 Dokumentace

Zadavatel požaduje zpracování a předání níže uvedené dokumentace. Dokumentace musí být zhotovena v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. PDF, ODT atd.) na datovém nosiči a 1× v papírové formě.

### 3.2.1 Prováděcí dokumentace

Prováděcí dokumentace bude sloužit jako podklad pro vlastní implementaci řešení do prostředí objednatele, musí zahrnovat detailní popis cílového stavu a postupu implementace, včetně plánovaných změn v konfiguraci současné infrastruktury.

### 3.2.2 Provozní dokumentace

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat minimálně následující oblasti:

- Monitorovací a logovací systém – vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce,
- LAN 802.1x – připojení zařízení včetně podrobných uživatelských postupů pro připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 7 a 10, Android, iOS a MacOS,
- Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele a skupinu.

## 3.3 Zaškolení IT administrátorů

Zhotovitel zrealizuje v sídle objednatele prezenční zaškolení pro IT administrátory objednatele. Školení bude pokrývat všechny komponenty dodávané v rámci předmětu plnění, a to minimálně v rozsahu (1) běžných administrátorských činností pro implementované systémy, (2) standardní údržby systémů pro administrátory zadavatele a (3) základní identifikace nestandardních stavů systému a jejich příčin.

Minimální požadovaný rozsah zaškolení pro administrátory je 16 hodin. Součástí zaškolení je zpracování a předání školících materiálů ze strany dodavatele.

Objednatel pro účely zaškolení zajistí a zpřístupní učebnu vybavenou notebookem nebo PC, prezentační technikou (ve smyslu projektor, tabule pro psaní / kreslení) a dále zajistí konektivitu do vnitřní sítě objednatele.

## 4 Záruky

Veškeré opravy po dobu záruky a záručního servisu budou provedeny bez dalších nákladů ze strany Zadavatele.

# 5 Podpora a dohled ze strany dodavatele pro Monitorovací a logovací systém (SIEM)

| **Specifikace rozsahu poskytování technické podpory a dohledu** | |
|---|---|
| Rozsah podpory a dohledu v rámci paušální ceny za služby | Technická podpora – Monitorovací a logovací systém (SIEM):<br><br>Základní rozsah technické podpory v rámci čtvrtletního paušálu:<br><br>• profylaxe – minimálně každých 6 měsíců,<br>• pravidelná aktualizace verzí systému dle doporučení výrobce,<br>• patch management,<br>• provádění monitoringu systému a zpracovávaných dat v rozsahu potřebném pro provádění následujících služeb v režimu 9×5<br>  ○ informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomocí základních komunikačních nástrojů (mail / SMS / telefon),<br>  ○ zahájení řešení bezpečnostního incidentu do 4 hodin od vzniku (v SIEM nástroji), řízení souvisejících činností správců a případných dalších dotčených osob,<br>  ○ zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBU, NCKB, CSIRT atd.,<br>  ○ rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření 1× měsíčně. Vzdálená prezentace reportu např. formou videokonference,<br>  ○ pravidelné skenování aktiv a zranitelností min. 1× týdně.<br><br>Dodavatel zpracuje a poskytne objednateli každý měsíc report, ve kterém bude popsán průběh realizace Plnění za uplynulé období, provedené služby a návrh doporučených opatření pro další období pro zvýšení bezpečnosti a dostupnosti IT infrastruktury objednatele a prevenci incidentů.<br><br>Pro možnost předávání incidentů a vedení komunikace je povinen dodavatel zpřístupnit vlastní nástroj (např. servis desk), který bude sloužit jako hlavní přístupový komunikační bod s těmito funkcionalitami:<br><br>• příjem Požadavků – webovou aplikací, telefonicky, e-mailem,<br>• zakládání Požadavků – při vzniku požadavku z monitoringu či jiné aktivity Prodávajícího,<br>• předání na řešitelské týmy (pracovníky Prodávajícího) a Třetí strany (např. výrobce),<br>• řízení životního cyklu Požadavků,<br>• administrativní uzavírání Požadavků po akceptovaném vyřešení Prodávajícím. |
| Dostupnost služby | Časové pokrytí služby technické podpory: pracovní dny v čase 8.00 až 17.00 hodin.<br><br>Garance doby identifikace zdroje problému nebo závady k možnosti jeho odstranění nebo řešení na straně objednatele: max. 4 hodiny od nahlášení nebo detekce problému. |