Příloha č. 3

TECHNICKÁ SPECIFIKACE

veřejná zakázka

„Rozvoj síťové infrastruktury“

1. Popis výchozího stavu

Organizace Krajská knihovna Karlovy Vary sídlí ve 3 budovách, kde pracuje většina zaměstnanců a je zde umístěná převážná část IT technologií.

Serverová infrastruktura

Do SAN infrastruktury je zapojena disková virtualizace Datacore tvořenými servery 2x DELL R740XD vSAN Ready Node a 1x DELL server Dell EMC R640 pro nasazení VDI. Účelem diskové virtualizace je zajištění pokročilých služeb – zejména zrcadlení úložišť, zajištění vysoké dostupnosti úložišť a abstrakce úložišť vůči fyzickým i virtuálním serverům. KKKV využívá virtualizační platformu vmWare. Servery jsou provozovány na platformě Windows 2016/2019 Server nebo GNU/Linux.

Zadavatel má implementovánu adresářovou službu Active Directory a související základní síťové služby DHCP a DNS. Dodavatel může využít tyto služby jako pomocné (nadřazené), ale jím nabízené řešení musí být plně funkční nezávisle na těchto službách.

Antivirus

Symantec Endpoint Protection

LAN infrastruktura

Hlavní budova

- Firewall: 1x FortiGate 100E
- Centrální Core Switch: 2x DELL EMC N3024ET-ON (zapojené redundantně)
- Uživatelské přístupové switche: 4x HP (HPE) 1810 a 4x Aruba řad 2530
- Síťová infrastruktura LAN (hlavní budova) je osazena převážně aktivními prvky
- Stávají firewall na hlavní budově nemá již dostatečný výkon pro zajištění plné bezpečností kontroly aktuálního provozu a bude v rámci projektu nahrazen a vyřazen.

Archiv

- propojeno optikou s hlavní budovou
- Síťová infrastruktura LAN (budova archivu) je osazena aktivními prvky DELL řad EMC N3xxx.
- 2x DELL EMC N3024ET-ON
- 2x DELL EMC N3048P

Příloha č. 3

Pobočka Lidická

- Firewall: 1x FortiGate 60F
- Uživatelské přístupové switche: 3x HP (HPE) řad 1920

Wi-Fi

- Softwarový Controler - Windows 2019 - Ubiquiti - UniFi 7.x
- 12x Ubiquiti - Unifi - UAP-AC-LR
- je nakonfigurováno 6 SSID z možných 8 SSID

Rozdělení sítí – VLAN

Hlavní budova:

- Zaměstnanci
- Vzdělávací centrum
- Veřejnost
- Servisní síť (fyzické servery a switche)
- WiFi - 6 sítí pro SSID
- DMZ

Pobočka:

- Zaměstnanci,
- Veřejnost
- Servisní síť

2. Technická specifikace předmětu plnění

Předmětem plnění veřejné zakázky této položky Rozvoj sítové infrastruktury je dodávka zařízení včetně služeb pořízení aktivních prvků dodání a konfiguraci firewallů, switchů, AP - Wi-Fi, rozčlenění sítí, nastavení serverů, PC, tiskáren, dalších specifických zařízení dodání licencí systému včetně zaškolení obsluhy a technické dokumentace. Řešení musí být navrženo tak, aby náklady na provoz systému byly co nejmenší.

2.1. Switche

Dodání a konfigurace 2ks switchů dle následující specifikace:

Popis:	***Název a parametry nabízeného výrobku***
Počet: 2x	***2x CBS350-48P-4X-EU***
Základní vlastnosti	***Základní vlastnosti:***
RJ-45 - 48xGigabit Ethernet	**Ano**
SFP+ - 4x	**Ano**
POE - 48x (min 370W)	**Ano**
Rack-mountable – ano	**Ano**
Switching Capacity (Gbps) - min 176	**Ano – 176 Gbps**
Kapacita (mpps) - min 130	**Ano - 130.94 Mpps**
HW stacking - Ano- stackovací kabel součástí - 1ks(min 1m)	**Ano**
Podpora 802.1x – ano	Ano
Záruka min. 60 měsíců, NBD	60 měsíců NBD

- **Instalace a konfigurace dle požadavků KKKV**
  - Namontování switchů do rozvaděče určeného KKKV - Ano
  - Instalace switche do stávající topologie sítě - Ano
  - Nastavení VLAN – dle požadavků KKKV - Ano
  - LACP do páteřní sítě – dle požadavků - Ano
  - Přístup na MGMT pouze SSHv2, HTTPS - Ano
  - DHCP snooping - Ano
  - MAC address flooding - Ano
  - Dynamic ARP inspection - DAI - Ano
- Konfigurace 802.1x pro přístup správy aktivních prvků - Ano
- Konfigurace NPS na stávajícím AD - Ano
  - Vytvoření AD skupiny LAN_Admin s právy pouze pro přístup na aktivní prvky LAN, WAN a WIFI sítě. - Ano
- Rekonfigurace stávajících 2x ARUBA 2530-48G - (J9775A) - Ano
- Přepojení zařízení připojených do stávajících prvku se stejnou konfigurací sítí- Ano
- Zaškolení pracovníků IT - ovládání, administrace a nastavování sítí zařízení v minimálním rozsahu 8 hodin a maximálně dvou zaměstnanců KKKV. - Ano
- Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu. - Ano

2.2. Firewally

Je požadováno dodání 2ks fyzických firewallů, kteří splňují vlastnosti dle následující specifikace:

Nabízené řešení bude tvořit kombinace dvou nově pořízených firewallů sestavená a zkonfigurovaná do vysoce dostupného firewallu-clusteru, tím bude zajištěna dostatečná ochrana směrem dovnitř KKKV a jeho organizací a stejně tak bude možné zamezit nežádoucí aktivitě směrem ven. Firewally budou shodně typu NGFW (Next Generation Firewall). Takové firewally umožňují při konfiguraci pravidel intuitivně využívat logické objekty srozumitelné i bez speciálních znalostí (např. názvy aplikací místo portů, jména uživatelů/počítačů místo IP adres apod.). Významným způsobem se tak zjednodušuje správa těchto sofistikovaných zařízení a současně snižuje riziko možného omylu obsluhy.

Technická specifikace

Popis:	***Název a parametry nabízeného výrobku***
Počet: 2x	***Počet: 2***
Základní vlastnosti	***Základní vlastnosti: FortiGate 100F, HW s licencí, HW + 24x7 Unified Threat Protection 1YR***
Montáž do 19“ racku	Ano
2 napájecí zdroj AC	Ano
Kapacitní požadavky a počty portů	***Kapacitní požadavky a počty portů:***
Počet WAN rozhraní copper, RJ45 10/100/1000 – min 2x	Ano
Počet interních síťových rozhraní copper, RJ45 10/100/1000 - min 22x.	Ano
Počet SFP: 4 x GbE SFP.	Ano
1x console port	Ano
Výkonnostní parametry HW	***Výkonnostní parametry HW***
RIP, BGP, OSPF, IS-IS	Ano
Policy routing.	Ano
Traffic Shaping, QoS s podporou DSCP markování a ToS.	Ano
Bezdrátový kontrolér, podpora vytváření inteligentní bezdrátové sítě, funkce ARRP (Automatic Radio Resource Provisioning), možnost detekce a reportování tzv. Rogue AP), bezdrátová sítě je založená na principu tenkých AP s inteligentní správou kontrolérem.	Ano
Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu.	Ano
WAN optimalizace (optimalizace vybraných protokolů, byte chaching), Web Cache, Explicitní Proxy, Reverzní proxy, WCCP.	Ano
Podpora silné autentizace uživatelů - integrovaná podpora generátor jednorázových hesel (OTP) - dvoufaktorová autentizace, podpora certifikátů pro ověření uživatelů.	Ano
Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 20 Gbps, 18 Gbps, 10 Gbps.	Ano
Latence firewallu (64 B UDP paket) - max 5 mikro sec.	Ano
Propustnost - Packet per Second: min 15 (Mpps)	Ano
Souběžné relace (TCP) - min 1.5 M.	Ano
Počet nových spojení za sekundu - min. 50 000.	Ano
Propustnost IPSEC VPN (512 B paket) - min. 10 Gbps.	Ano

Propustnost SSL VPN min 1 Gbps.	Ano
Propustnost IPS – min 1 Gbps.	Ano
Podpora virtualizace (min. 10 virtuálních kontextů).	Ano
Podpora funkce bezdrátový kontrolér	Ano
Integrovaná podpora	Ano
Funkce L2/L3	***Funkce L2/L3***
Podpora pro režim vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky mezi nódy v clusteru.	Ano
Režim fungování L2 - transparentní režim, L3 - NAT/Router.	Ano
Podpora multicast, vytváření politiky pro multicast routování.	Ano
Podpora High availability	Ano
Podpora VPN	***Podpora VPN***
(portálový režim, tunelový režim), podpora protokolu	Ano
Funkce firewallu	***Funkce firewallu***
Možnost nastavovat firewall politiku na základě geografických údajů.	Ano
Podpora Identity based policy - nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru.	Ano
Funkce Load Balancing - možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora healt check funkcí, podpora SSL offload.	Ano
Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace.	Ano
UTM funkce, možnost výběru mezi file based režimem (buffer) nebo flow based (inspekce on-the-fly).	Ano
Antivirus pro vybrané protokoly, možnost volby různých databází, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd).	Ano
E-mail filter - jednoduchá antispamová a antivirová inspekce elektronické pošty.	Ano
Intrusion Protection System - detekce útoků založena na signaturové části a na anomálním filtru, možnost vytvářet vlastní signatury.	Ano
Web Filter - založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty - uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne.	Ano
Data Leak Prevention s funkcí document fingerprinting.	Ano
Application Control - detekce, monitoring, povolení či zakázání síťových aplikací na základě signatury dané aplikace, nikoliv dle portu.	Ano
Deep scanning - možnost kontroly komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…).	Ano
DoS Policy prevence proti základním útokům typu DoS, syn proxy.	Ano

Endpoint Control a monitoring - kontrola připojené pracovní stanice na patch level, instalovaný vhodný service pack, antivirový software, personální firewall či jiný soft	Ano
Vulnerability Scan - možnost naplánování aktvního testu vnitřní sítě na známé zranitelnosti, test je založen na signaturové databázi. Možnost vygenerování report.	Ano
Ověřování uživatelů LDAP, Active Directory, ověřování na základě certifikátu	Ano
Dynamické profily - možnost přiřadit konkrétní profil uživateli na základě jeho ověření.	Ano
Management	***Management***
Cluster boxů s full UTM supportem celkem na 1 rok.	Ano
Podpora	***Podpora***
Záruka 1 rok, v režimu 24hod x 7dnů.	Ano
Podpora včetně AV/AS, IPS, App. Control a Webfiltering.	Ano

Konfigurační požadavky

- Dodávané Firewally budou zapojeny v režimu vysoké dostupnosti (High availability) Ano
- Přenos a revize pravidel ze stávajícího FW Ano
- Aktualizace firmwaru na požadovaný firmware KKKV Ano
- Nastavení tzv. Trafic Shaping policy pro jednotlivé vlany (počet pravidel může být po návrhu a konzultaci s KKKV upraven)
    - standartní protokoly Ano
    - přenášená videa, streamy Ano
    - velké soubory Ano
    - další dle Best-practice Ano
- Ukládání logů dodávaných firewallů do FortiAnalazeru Ano
- Zajištění funkčnosti stávající VPN-ky mezi hlavní budovou a pobočkou Lidická. Ano
- Řešení problému - nastavení - u pravidel - jestli má být Flow-Based nebo Proxy-Based. (u Antiviru a Web Filter nastavení) - The flow-mod policy is using proxy feature set profiles. Proxy features will not work in a flow policy. Ano
- Zaškolení pracovníků IT - ovládání, administrace a nastavování firewallů zařízení v minimálním rozsahu 8 hodin a maximálně dvou zaměstnanců KKKV. Ano
- Zaškolení pracovníků IT - Fortigate a FortiAnalyzer na současné infrastruktuře v minimálním rozsahu 4 hodin a maximálně dvou zaměstnanců KKKV. Ano
- Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu. Ano

2.3. Wi-Fi zařízení

Je požadováno dodání 18 ks Wi-Fi zařízení

Popis:	***Název a parametry nabízeného výrobku***
Počet: 18x	18x
Základní vlastnosti:	***Základní vlastnosti:***
UniFi - UAP-AC-LR + 10 m UTP kabel cat. min 5e	UniFi - UAP-AC-LR + 10 m UTP kabel cat. 5e
Záruka - min. 24 měsíců	Záruka - 24 měsíců

Příloha č. 3

Zadavatel v současné době disponuje 12 ks Wi-Fi zařízení UniFi - UAP-AC-LR, připojených na softwarový controller.

Z důvodu zachování kompatibility požaduje zadavatel dodání 18 ks stejných zařízení (PN: UAP-AC-LR)

Instalace a konfigurace dle požadavků KKKV:

- Montáž zařízení do umístění dle specifikace KKKV (bude zajištěno LAN kabeláž zadavatelem) Ano
- Vytvoření a upravení stávajícího systému UniFi dle požadavků KKKV Ano
- Začlenění nových zařízení do stávajícího systému UniFi. Ano
- Vytvoření dvou nových SSID dle specifikace KKKV Ano
- Konfigurace 802.1x pro přístup správy Ano
- Konfigurace NPS na stávajícím AD Ano
- Vytvoření AD skupiny LAN Admin s právy pouze pro přístup na Controler Ano
- Vytvoření pravidel NPS Ano
- Vytvoření pravidel pro dynamické přidělování WLAN, ale skupiny v AD Ano
- Sjednocení SSID, která budou ověřována přes 802.1x a dynamické přidělování vlan dle požadavků KKKV Ano
- Návrh, vytvoření a nastavení pravidel na firewallech mezi jednotlivými WiFi sítěmi (SSID) a stávajícími VLany sítí. Ano
- Nastavení logování přístupů k jednotlivým AP - WiFi a logování přístupu na internet klientů WiFi. Uchování logů za určité časové období. Ano
- Rekonfigurace jednotného řídícího software pro jednotné ovládání WiFi zařízení Ano
- Instalace a konfigurace automatického vydávání jednorázového přístupu pro veřejnost Ano
- Zaškolení pracovníků IT – ovládání, administrace a nastavování WiFi zařízení v minimálním rozsahu 8 hodin a maximálně dvou zaměstnanců KKKV. Ano
- Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu. Ano

Jako součást dodávky požaduje KKKV dodání syslog serveru pro ukládání logů ze softwarového kontroleru Unifi s následujícími minimálními požadavky:

- Podpora protokolů
  - Syslog Ano
- Možnost ukládání
  - Textový soubor Ano
  - Databáze Ano
- Podpora pro parsování logů (může být řešeno další aplikaci) Ano
- Možnost použití pro další zařízení podporující protokol syslog Ano
- Webové rozehranní nebo aplikace pro vyhledávání v parsovaných logách Ano
- Automatické mazaní historických logů (na základě času nebo kapacity úložiště logů) Ano
- Jsou možné pozměňující úpravy po dohodě s KKKV. Ano
- Pokud bude použito licencí v tomto řešení je nutné je zahrnout do tohoto projektu. Ano

2.4. Zaškolení pracovníků ovládání, administrace a konfigurace SysLogu v rámci řešení WiFi. Rozdělení a rekonfigurace sítí VLAN

Navrhněte a realizujte rozložení sítí VLAN, tak aby došlo k oddělení dle funkčního zařazení. A to všech fyzických, virtualizovaných serverů, počítačů, síťových prvků, dalších prvků a zařízení do logických celků dle jejich povahy, aby se zvýšila stávající bezpečnost. (Počet sítí VLAN může být po návrhu a konzultaci s KKKV upraven).

Požadované činnosti dodavatele:

- Analýza stávajícího stavu formou konzultací s KKKV Ano
- Analýza klíčových zařízení, serverů a aplikací. Určení možností přesunu do nových segmentů a nezbytných závislostí a součinností dalších stran, tak aby byla zachována stávající funkčnost Ano
- Analýza komunikačních požadavků jednotlivých zařízení Ano
- Návrh nové segmentace sítě dle aktuálních bezpečnostních doporučení dle předchozí analýzy Ano
- Návrh zabezpečení komunikace mezi jednotlivými segmenty sítě Ano
- Návrh plánu zavádění nových VLAN zahrnující Ano
- Konfigurace síťové infrastruktury, firewallu a dalších nezbytných služeb, tedy
    - upgrade firmware na všech zařízení typů switch v KKKV Ano
    - distribuce stávajících a nově navrhovaných VLAN na všechny switche v KKKV Ano
    - konfigurace firewallu pro zajištění komunikace nových VLAN a její zabezpečení dle předchozí analýzy Ano
    - konfigurace nových VLAN na síťové prvky Ano
    - konfigurace virtualizační platformy pro zajištění komunikace nových VLAN Ano
    - konfigurace dalších služeb nutných pro provoz nových VLAN (např. DHCP, DNS, atd.) Ano
    - Přesunutí zařízení do cílových VLAN Ano
- konfigurace aplikací a stanic pro zajištění funkčnosti korektní komunikaci s readresovanými zařízením Ano
- Zaškolení pracovníků IT – ovládání, administrace a nastavování sítí zařízení v minimálním rozsahu 8 hodin a maximálně dvou zaměstnanců KKKV. Ano
- Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu. Ano

2.5. Doplnění HW

Doplnění stávajícího serveru HPE MicroServer Gen10 o kartu HPE Smart Array E208i-p Gen10 (PN: 804394-B21), rekonfigurace stávajícího serveru. Nastavení Raid-1. Zachování stávajících dat a nastavení. Ano

3. Požadavky na školení

Účastník zajistí školení pracovníků zadavatele – administrátorů – na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu předávané provozní dokumentace.

Školení zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.

Minimální rozsah školení je:

- Switche - 8 hodin Ano
- Firewally - 8 hodin Ano
- Školení Fortigate a FortiAnalyzer na současné infrastruktuře - 4h Ano
- WiFi - školení administrace UniFi a Syslog - 8 hodin Ano
- VLAN - 8 hodin Ano

Školení bude probíhat v sídle zadavatele. V případě dohody vzdáleně. Ano

Předpokládá se účast max. 2 administrátorů. Ano

Náklady na školení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují. Ano

4. Požadavky na provedení akceptačních testů, zkušební provoz a přechod do ostrého provozu

Účastník navrhne způsob a provedení akceptačních testů.

Součástí akceptačních testů musí být pro každou komoditu minimálně:

- Prokázání kompletnosti dodávky a splnění povinných i hodnocených požadavků. Ano
- Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována. Ano
- Prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná. Ano
- Pro každou komoditu navrhne účastník vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení Ano

O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol. Ano

5. Dokumentace

Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení a popisu činností běžné údržby a administrace systémů a činností pro spolehlivé zajištění provozu. Ano

6. Ostatní

Dodavatel řeší všechny vzniklé problémy ve spolupráci s KKKV dle požadavků KKKV. Musí být zachována funkčnost před migrací. Ano

Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje maximální možné 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.

Dodavatel bude při implementaci respektovat provozní řád Krajské knihovny Karlovy Vary, vybraný dodavatel bude s provozním řádem seznámen před podpisem smlouvy o dílo.

Požadavky na architekturu technického řešení

- Architektura komodit musí být navržena tak, aby vhodně využívala a doplňovala stávající infrastrukturu. Ano

Požadavky na rozhraní

- Veškeré nabízené aktivní hardwarové produkty musí disponovat rozhraním SNMP min v2 pro management a vzdálenou správu. Ano

Požadavky na bezpečnost informací

- Veškeré nástroje pro správu musí umožňovat správu interních účtů (min. jméno a heslo) a/nebo napojení na Active Directory. Ano
- Veškeré nástroje pro správu musí umožňovat definici s minimálně 2 úrovněmi oprávnění – monitoring (pouze čtení), administrátor (plná správa) Ano
- Veškeré nástroje pro správu musí komunikovat se zařízeními šifrovanými protokoly (SSH apod.). Také v případě vestavěných nástrojů (např. www rozhraní) musí být použita šifrovaná komunikace (např. HTTPS). Ano

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

- jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce, Ano
- mají plnou záruku od výrobce, Ano
- mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce, Ano
- obsahují všechny nezbytné licence na používání příslušného softwaru, Ano
- jsou určeny pro provoz v České republic Ano e,
- z databází výrobce, distributora či prodejce bude možné výše uvedené skutečnosti doložit. Ano
- Tyto skutečnosti dodavatel doloží nejpozději při dodání čestným prohlášením výrobce/distributora, popř. dodavatelem samotným, nelze-li prohlášení distributora získat. Ano

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.

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