TECHNICKÁ SPECIFIKACE / projekt - část - Konektivita

Střední škola André Citroëna Boskovice,
příspěvková organizace
náměstí 9. května 2153/2a,
680 11 Boskovice
IČO: 00056324
DIČ: CZ00056324 (plátce DPH)
bankovní spojení: 8232631/0100

TECHNICKÁ SPECIFIKACE

Základní požadavky na technické řešení

(1) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol [1] - uvedené v příloze č.1 (dále jen Standard konektivity). Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

Označení	Komodita	Počet
K1	Virtualizační platforma - serverová infrastruktura	1
K2	Zabezpečení LAN a Wifi – sítová infrastruktura	1
K3	Centrální logování	1

(2) Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil uživatelské a provozní potíže.

(3) Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

(4) Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu, přičemž nesmí překročit předpokládanou hodnotu zakázky.

(5) Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

1. TECHNICKÁ SPECIFIKACE – Konektivita

1.1. Specifické požadavky na technické řešení

(1) **K1 - Virtualizační platforma**

(a) Celé řešení je postaveno na třech fyzických serverech pro serverovou virtualizaci, které jsou napřímo připojeny ke sdílenému dvouřadičovému diskovému poli. Typ připojení diskového pole je SAS. Díky tomu je maximální počet k poli připojitelných serverů 4 (to odpovídá maximálnímu počtu portů na každém řadiči diskového pole). Networking vrstva je řešena dvěma ethernet CORE přepínači.

(b) Backup prostředí je řešen stávajícím vyhrazeným fyzickým serverem s VM a NAS diskovým polem připojeným do LAN včetně UPS. NAS a UPS budou součástí dodávky.

(c) Všechna propojení (jak k diskovému poli, tak do CORE switchů) jsou řešena redundantně.

(d) Vysoká dostupnost je zajištěna na úrovni serverů a CORE networkingu, ne na úrovni diskového pole a neCORE switchů.

(e) Součástí je i dodávka licencí operačních systémů a přístupových licencí s neomezeným počtem virtuálních serverů v licenčním programu pro EDU.

(f) výpadek jednoho fyzického serveru znamená nutnost využití HA funkcí Hyper-V, případně ruční zásah. VM, které běžely na porouchaném nebo z důvodu maintenance odstavovaném serveru, je třeba nastartovat na druhém fyzickém serveru. Servery mají dostatek procesorového výkonu a paměti na běh veškerých(případně vybraných) VM. Výpadek v poskytování služeb DC je pouze na dobu restartu VM

(g) výpadek jednoho ethernetového switche nezpůsobí výpadek v poskytování služeb DC

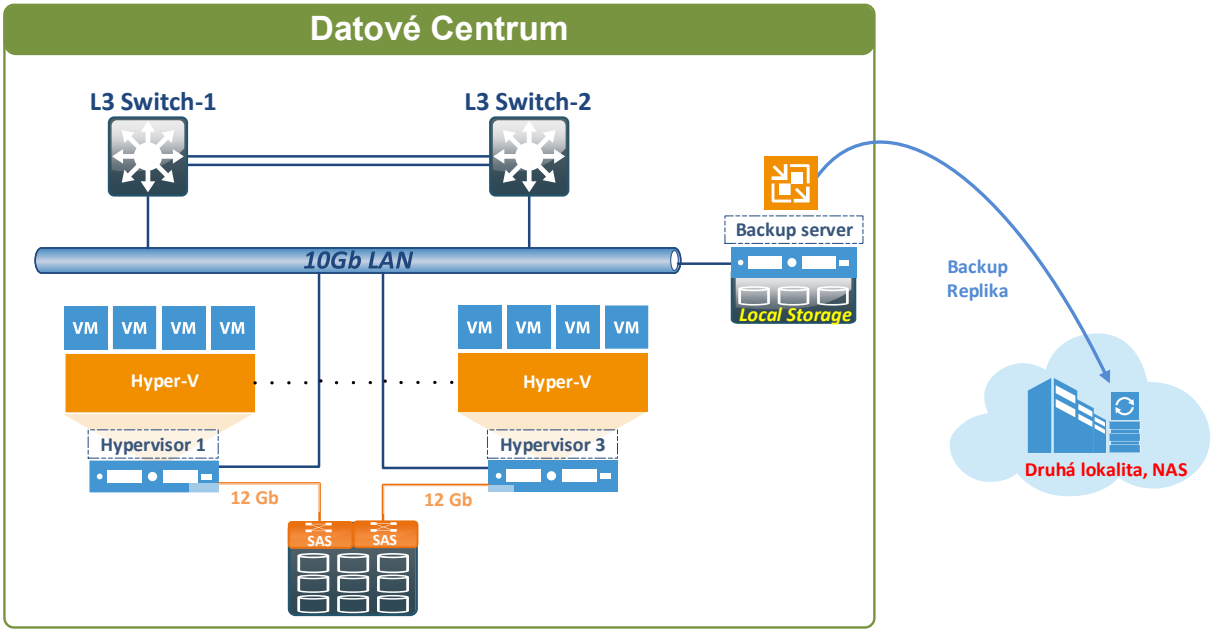
(h) výpadek jednoho řadiče diskového pole nezpůsobí výpadek v poskytování služeb DC

(i) výpadek celého diskového pole způsobí výpadek v poskytování služeb DC

(j) Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:

(i) Záložní zdroj napájení UPS zajistí chod serveru při výpadku napájení

(k) Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude vybudována centrální databáze identit na bázi adresářové služby. Adresářová služby umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic apod. Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agenta firewallu a dalších. Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, Internet atd.) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky atd.). Technické provedení bude založeno min. na 1 řadiči adresářové služby. Řadič bude provozován a bude pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP.


Datové Centrum
L3 Switch-1
L3 Switch-2
10Gb LAN
Backup server
Local Storage
Backup
Replika
VM
VM
VM
VM
Hyper-V
Hypervisor 1
12 Gb
SAS
SAS
VM
VM
VM
VM
Hyper-V
Hypervisor 3
12 Gb
Druhá lokalita, NAS

(2) **K2- Zabezpečení LAN a Wifi**

(a) Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.

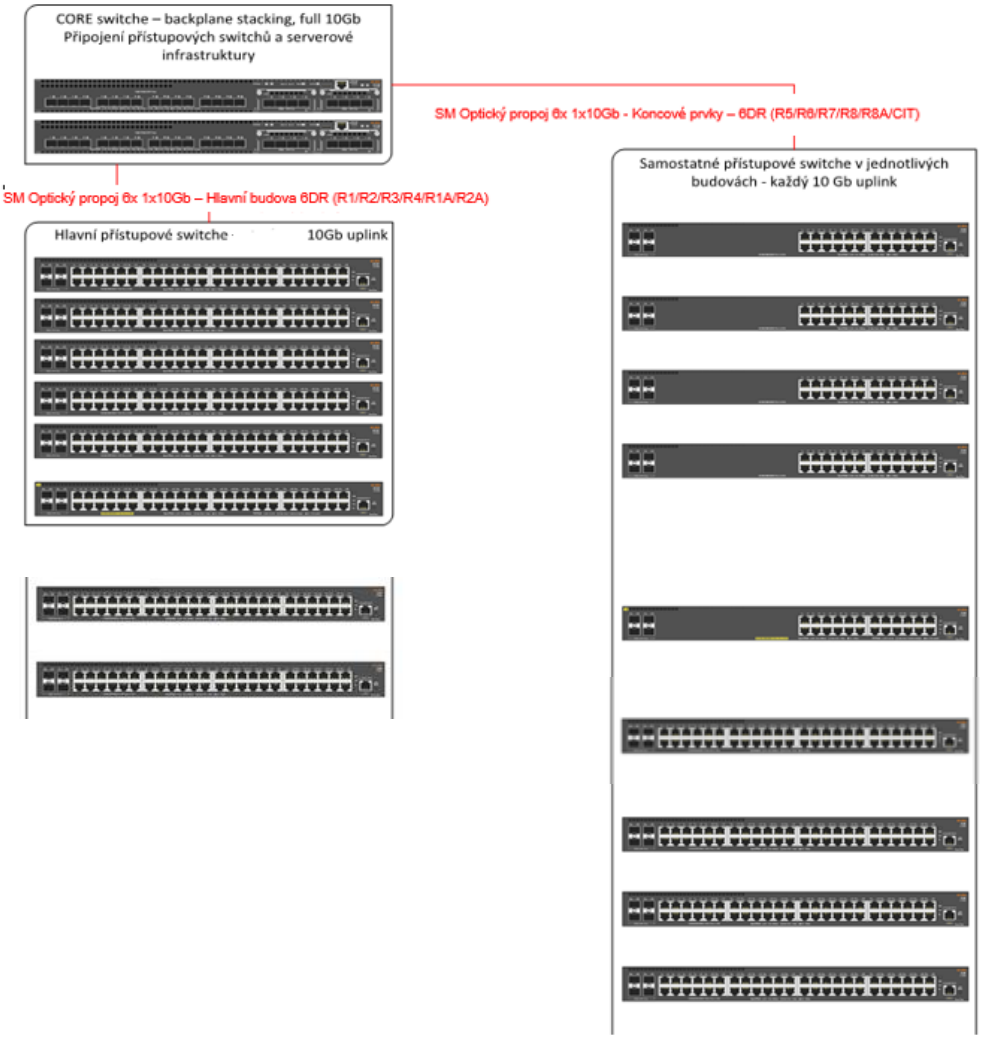
(b) Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (QualityofServices).

(c) Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem (řadičem), který bude součástí firmwarů přístupových bodů.

(d) Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN (tj. protokol 802.1X + radius). Wifi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na raduis servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové služby. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy - WPA2 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty (GuestWiFi).

(e) LAN Infrastruktura se skládá

- 2x CORE switche 24x 1000/10000 SFP+ portů (STACK)
- Hlavní přístupové switche – uplink 10Gb - Hlavní budova 6DR (R1/R2/R3/R4/R1A/R2A) – celkem 8KS aktivních prvků – rozložení dle přílohy: Rozvaděče
- Samostatné přístupové switche v jednotlivých budovách – uplink 10Gb - Koncové prvky – 6DR (R5/R6/R7/R8/R8A/CIT) – celkem 9KS aktivních prvků - rozložení dle přílohy: Rozvaděče
- LAN infrastruktura bude až ke koncovým aktivním prvkům v rychlostech 10Gb – koncové stanice budou připojeny rychlostí 1Gb



(3) **K3 - Centrální logování**

(a) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací - může jednat o jediné zařízení, softwarový nástroj či appliance. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Data bude 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).

(b) 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.

(c) Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze securityevent-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.

1.2. Implementační služby

(1) V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K3

(a) Dodávka a implementace předmětu plnění musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií. Musí být v souladu s nabídkou uchazeče a se Standardem konektivity.

(b) Zajištění projektového vedení realizace předmětu plnění.

(c) Provedení testů.

(d) Předání do plného provozu.

(2) Zadavatel dále požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

K1: Virtualizační platforma
a) Návrh a kompletní implementace serverové virtualizační platformy b) Implementace pořízených technologií c) Návrh vhodné struktury ActiveDirectory, její vybudování d) Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie e) Implementace zálohovacího SW včetně metodiky zálohování a obnovy dat f) Návrh a provedení akceptačních testů
K2: Zabezpečení LAN a Wifi
a) Implementace pořízených technologií b) Provedení segmentace LAN – VLAN, adresování, routování c) Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách d) Návrh a implementace 802.1X pro kabelovou LAN i WiFi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů - PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií e) Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu f) Vybudování VPN pro vzdálený přístup uživatelů LAN g) Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik h) Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity
K3: Centrální logování
a) Návrh a implementace systému pro centrální logování pro naplnění požadavků Standardu konektivity, především, ale nejen: • logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.) b) Provedení souvisejících konfigurací monitorovaných systémů

(3) Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti. Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity dle manuálu uveřejněného na http://www.strukturalni-fondy.cz/cs/Microsites/IROP/Novinky/Zverejneni-doporucujiciho-manualu-k-postupum-pri-prokazani-a-

kontrole včetně úspěšného provedení a doložení testu na https://www.standardkonektivity.cz/. Prokázání naplnění požadavků poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu.

1.3. Školení

(1) Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu:

(a) běžných administrátorských činností pro implementované systémy

(b) standardní údržby systémů pro administrátory zadavatele

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

(3) Minimální rozsah školení pro každou komoditu je 1MD, není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele.

1.4. Harmonogram projektu

(1) Zadavatel vyžaduje dodržení následujícího maximálního harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum podpisu smlouvy o dílo. Čísla značí počet kalendářních dnů.

Aktivita	Začátek	Termín
Podpis smlouvy	D	D
Zahájení projektu – úvodní projektová schůzka	D	D+7
Realizace předmětu plnění	D+7	D+47
Školení administrátorů	D+47	D+48
Akceptační testy	D+48	D+50
Zahájení ostrého provozu	D+60	-

(2) Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

(3) Dodavatel uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy.

1.5. Popis povinných parametrů dodávaného řešení

(1) V dále uvedených tabulkách jsou uvedeny povinné parametry prvků nabízeného řešení. Dodavatel musí všechny parametry splnit, v případě nesplnění požadavku zadavatele bude nabídka dodavatele vyřazena a dodavatel bude následně vyloučen z účasti v zadávacím řízení.

(2) Dodavatel ve své nabídce uvede značkové specifikace nabízených dodávek. Z popis způsobu naplnění bude možno určit, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.

Povinné parametry pro Komoditu K1 - Virtualizační platforma:

Parametr	
Formát serveru	Rackové provedení, min.. 1U, Pro přístup ke všem komponentám serveru není nutné nářadí. Barevně značené hot-plug vnitřní i vnější komponenty
CPU	Server musí být osazen 2x CPU, minimálně s osmi procesorovými jádry. Hodnocení výkonu nabídnutého serveru musí být publikované na webu: https://www.cpubenchmark.net s minimálními parametry: • Passmark CPU Mark, hodnota min: 22 000 /CPU
RAM	128GB v provedení min. DDR4, min. 2933 MHz
Diskový subsystém	Server musí být osazen min. dvěma pevnými disky s kapacitou alespoň 480GB SSD
Optická mechanika	Není požadována.
Síťové rozhraní + napájení	• 1x Broadcom 57412 2 Port 10Gb SFP+ + 5720 2 Port 1Gb Base-T, rNDC • 1x Broadcom 57412 Dual Port 10Gb, SFP+, PCIe Adapter, Low Profile • 1x SAS 12Gbps HBA External Controller, LP Adapter • Redundance napájení
Podpora a servis	Podpora na 60měsíců typu NBD, oprava v místě instalace serveru

Diskové pole	Diskové pole SAS (12Gb SAS 8 Port Dual Controller) musí být osazeno: 2x 960GB SSD SAS Read Intensive 12Gbps 512 2.5in Hot-plug 16x 1.8TB HDD 10K 512e SAS12 2.5
Podpora a servis	Podpora na 60měsíců typu NBD, oprava v místě instalace serveru do 4hodin od nahlášení

SW licence operačních systémů	Serverové operační systémy	3 ks licencí 64-bitového serverového operačního systému v aktuální verzi. Licence musí umožnit provoz neomezeného počtu virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace, dále provoz všech nabízených aplikací a management nástrojů.
	Klientské licence	klientské licence pro nabízené operační systémy umožňující využívat těchto systémů uživatelům je celkem 600 (user CAL).

SW licence zálohování	BACKUP SW	Zálohovací SW pro EDU pokrývající 3NODY (6CPU) – umožňující granulární obnovy
	Klientské licence	Záruka 60měsíců

UPS **1x**	Kapacita výstupního výkonu [W]: 4 500 Kapacita výstupního výkonu [VA]: 5 000 Jmenovité výstupní napětí [V]: 200/208/220/230/240V Topologie: Dvojitá on-line konverze se systémem PFC (korekce účiníku) Výstupní přípojky: -(8) IEC-320-C13 -(2) IEC-320-C19 -(1) Hardwired
	- KOMUNIKACE A SPRÁVA - Port rozhraní: 1 adaptér NMC, 1 USB port, 1 port RS232 (port USB a RS232 nemohou být použity současně), 4 bezpotenciálové kontakty (DB9), 1 miniaturní svorkovnice se svorkami pro dálkový start a odstavení, 1 svorkovnice pro dálkové vypnutí, 1 konektor DB15 pro paralelní chod - Ovládací panel: Vícejazyčný LCD displej
	Záruka: min. 60 měsíců

NAS **1x**	CPU min: 2400 bodu v CPU Benchmarks na https://www.cpubenchmark.net/ RAM 4GB, paměť rozšiřitelná až na: 64 GB (16 GB x 4 GB)
	- Šachta(y) pevného disku: 16 - Maximální počet šachet pevného disku s rozšiřující jednotkou: 28 - Kompatibilní typ disku: 3.5" SATA HDD, 2.5" SATA HDD, 2.5" SATA SSD - Maximální interní hrubá kapacita: 192 TB (12 TB drive x 16) - Maximální hrubá kapacita s rozšiřovacími jednotkami: 336 TB (192 TB + 12 TB drive x 12) - Maximální velikost jednoho svazku: 108 TB - Disky vyměnitelné za provozu: Ano - Min 2x 10Gb port - Ližiny do racku - Min. 4x 8T HDD (disk určený pro provoz v NAS)
	Záruka: min. 60 měsíců

Povinné parametry pro Komoditu K2 – Zabezpečení LAN a Wifi:

Firewall **1KS**
22 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 16 x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10G SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy. Max managed FortiAPs (Total / Tunnel) 128 / 64
Záruka min. 60 měsíců v režimu 24x7.

Centrální přepínač **2x**	- Management: Fully managed - Layer 3 Advanced: L2 switching / L3 Static routing / RIP routing / Multicast routing / OSPF - 24x 1000/10000 SFP+ port portů (možno 16portu + 8portu in slot)

	- podpora až 8x SFP+ portů nebo 2x 40GbE port s volitelným modulem - Redundantní zdroje - Možnost stohování - Montáž do 19“ racku. Úchytky jsou součástí balení. - Správa sítě a zabezpečení za pomoci nástorjů výrobce - Modulární 10GbE a 40GbE uplink pro bezdrátovou agregaci
	- 4-port module to allow stacking + kabel 1m
	Záruka: min. 60 měsíců, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady

Přístupové přepínače 17KS	**Společné parametry**	
	Základní parametry	L3 přepínač v rackovém provedení max. 1U – 6KS L2 přepínač v rackovém provedení max. 1U – 11KS
	Stohování	podpora stohování pro jednotný management (přepínače musí stohovatelné vzájemně bez ohledu na provedení - viz. Porty a propustnost)
	Propustnost	neblokovaná architektura
	Agregace portů	podpora LACP
	Dualstack	IPv4 a IPv6 dualstack včetně podpory ACL a QoS
	VLAN	VLAN 802.1Q, MAC i protocolbased, podpora zařazování do VLAN a přidělení QoS a přístupových filtrů na základě 802.1X ověření
	Ověřování uživatelů a zařízení	podpora 802.1X
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, sFlow, RMON, web rozhraní
	Záruka	min. 60 měsíců, odeslání náhradního zařízení max. následující pracovní den po nahlášení závady
	Specifické parametry	
	Porty a propustnost	**L3 switch 6 kus** – 48x 1 GB RJ-45 PoE + 4x SFP+ (nesdílené), min. 170 Gb/s **5 kusů** – 48x 1 GB RJ-45 + 4x SFP+ (nesdílené), min. 150 Gb/s **1 kusů** – 24x 1 GB RJ-45 + 4x SFP+ (nesdílené), min. 100 Gb/s **4 kusy** – 24x 1 GB RJ-45 PoE + 4x SFP+ (nesdílené), min. 100 Gb/s **1 kus** – 48x 1 GB RJ-45 PoE + 4x SFP+ (nesdílené), min. 170 Gb/s
WiFi přístupové body (AP) + montáž na strop 42KS – INDOOR	Základní funkce	Přístupový bod (AP) WiFi včetně montážního materiálu na stěnu nebo strop
	Frekvence	činnost v radiovém pásmu 2,4 a 5 GHz současně, 2 radiové moduly
	Anténní systém	interní systém min. MIMO 3x3 (5 GHz) a MIMO 2x2 (2,4 GHz), optimalizovaný pro montáž na strop
	Přenosové rychlosti	SU-MIMO (5GHz) až 1300Mbps, MU-MIMO až 867Mbps. 2,4GHz MIMO až 300Mbps.
	Standardy	podpora 802.3at, 802.11n, 802.11ac, 802.1x včetně přiřazování do VLAN
	Řízení klientů	automatické směrování komunikace klientů z 2.4 GHz na 5 GHz (pokud klienti podporují obě pásma)
	Rušení	průběžná detekce non-WiFi rušení a spektrální analýza
	Multi SSID	podpora vysílání min. 8 SSID (WiFi sítí) současně, podpora přiřazení každého SSID samostatné VLAN
	Zatížení	min. 250 přiřazených (asociovaných) klientů na radiový modul
	Porty	min. 1x 1Gb, PoE s podporou standardů 802.3at a 802.3af
	Úsporné napájení	podpora standardu 802.3az - Energy-EfficientEthernet (EEE)
	Řízení provozu	klasifikace a kontrola provozu, detekce obvyklých aplikací s možností určení priority nebo šířky pásma zvoleného provozu
	Řízení kvality služeb	automatické řízení kvality služeb (QoS) pro hlas a video
	Současná obsluha více klientů	Podpora MU-MIMO (Multi-User MIMO) - multi-user multiple input/multiple output
	Přenosové rychlosti	SU-MIMO (Single-User MIMO) min. 1300Mb, MU-MIMO min. 850 Mb
	Bezpečnost	Detekce cizích přístupových bodů zjištěných v LAN i v radiofrekvenčním pásmu
	Virtuální kontroler	Virtuální, vysoce dostupný kontroler obsažený ve firmware každého přístupového bodu. Umožňuje kompletní centrální správu WiFi infrastruktury a řízení jejího provozu včetně roamingu klientů.
	Monitoring a správa	plná podpora CLI, SSH, SNMP 1-3, syslog, web rozhraní

	Správa frekvenčního pásma	automatické dynamické přidělování kanálů a řízení výkonu přístupových bodů pro vyrovnané pokrytí a minimalizaci interference
	Záruka	min. 60 měsíců

Minigbic + DAC	Základní funkce	34x 10G SFP+ LC LR 10km 6x 10G SFP+ to SFP+ 3m DAC Cable

Povinné parametry pro Komoditu K3 – Centrální logování:

Monitorovací a logovací systém 1x	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, ActiveDirectory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and ServicesLogs", 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 - min. výsledky hledání
	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
	ActiveDirectory	integrace s ActiveDirectory 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 či filtrování bez tvorby dotazů - např. výběrem v kontextovém menu vybraného pole uloženého záznamu.
	Kompatibilita	Podpora provozu v prostředí nabízené serverové virtualizace
	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
	Záruka	min. 12 měsíců včetně poskytnutí opravných verzí

Příloha č.1

STANDARD KONEKTIVITY ŠKOL

1. Konektivita školy k veřejnému internetu (WAN)

Obecný popis: pro základní způsobilost projektu naplňujícího opatření „vnitřní konektivita škol" musí příslušná škola zajistit kvalitní připojení ke službám veřejného internetu a to i v případě, že vybavení pro připojení k internetu není předmětem projektové žádosti. Za toto připojení je považováno zajištění konektivity splňující následující minimální parametry v době ukončení realizace projektu:

- šíře pásma (bandwidth) odpovídající 128kbps/student[2] nebo 512kbps/počítač[3] nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů[4]
- vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy
- plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- validující DNSSEC resolver na straně školy
- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- síťové zařízení podporující ratelimiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
- u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.

Nad rámec těchto povinných parametrů je dále doporučeno v rámci projektu realizovat:

- symetrické připojení bez agregace a omezení (FUP)
- zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX[5] nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX

2. Vnitřní konektivita školy (LAN)

Obecný popis: vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojením je nutné pokrýt prostory dotčené hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být zdůvodněna ve studii proveditelnosti.

Povinné minimální bezpečnostní parametry projektu (bez ohledu typ síťového připojení):

- 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

[2] *Počet studentů je definovaný celkový počet studentů školy*

[3] *Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení*

[4] *Definováno jako saturace šířky pásma připojení k veřejnému internetu, která ani ve špičkách nedosáhne a to ani krátkodobě 100%*

[5] *V případě, kdy má ISP přidělené IP adresy od člena FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné adresy jsou v rámci FENIX propagovány.V případě, kdy má ISP vlastní ASn a není přímý člen FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné ASn propaguje do FENIX na základě smluvního vztahu některý ze členů FENIX.*

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 zařízeni s kapacitou pro uchování dat po dobu minimálně 2 měsíců

- Povinné řešení systému správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD, apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. síťovým službám.
- logování přístupu uživatelů do sítě umožňující dohledání vazeb *IP adresa – čas – uživatel*

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

- Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex
- Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex
- Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[6] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radiusbased MAC autentizace,…

V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:

- Podpora mechanismu izolace klientů
- Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů
- Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thinaccess pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …)
- Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

Nad rámec těchto povinných parametrů je dále doporučeno v rámci projektu realizovat:

- Minimálně pasivní zapojení[7] do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.

3. Další bezpečnostní prvky

Obecný popis: v rámci projektů je možné realizovat další aktivity naplňující principy bezpečného využívání IT prostředků. Zejména pak jde o:

- Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů
- Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)
- Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase)
- Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)

[6] *Požadavek se týká prvků, přes které je veden veškerý provoz, resp. jde o centrální prvky. Podružné přepínače (chodbové, očebnové) musí splňovat pouze požadavek na neblokující architekturou přepínacího subsystému*

[7] *Pasivním zapojením se rozumí poskytování služeb sítě eduroam na úrovni poskytovatele zdrojů – viz. http://www.eduroam.cz/_media/cs/cz_roam_policy_v2.0.pdf*

- Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))
- Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie
- Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)
- Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga)
- Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)
- Nástroje pro centrální správu a audit ICT prostředků
- Systémy zálohování a obnovy dat serverové infrastruktury
- Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů
- Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.
- Podpora vzdáleného přístupu (VPN)