Úvod

Předmětem jsou dodávky zařízení a služeb (dále také jen „řešení“) vybudování technologie zajišťující – servery s operačními systémy, diskové úložiště, systém pro centrální logování, vyhodnocování a správu událostí a bezpečnostních incidentů, identity management, aplikační firewall, aktivní prvky LAN a zálohovací systém. Součástí plnění je dále podpora provozu na dobu minimálně 60 měsíců po předání řešení do plného provozu. Řešení musí být navrženo tak, aby náklady na provoz systému byly co nejmenší.

Stávající řešení:

Připojení k internetu je řešeno DSL technologií doplněnou o firewall/router Zyxel.

Serverová infrastruktura je postavena na trojici jednoprocesorových serverů HP ML110 gen7, gen9, gen 10. Zálohování je manuální.

Aktivní prvky jsou vzhledem k postupnému rozšiřování sítě v historii rozmístěny v jednotlivých kabinetech (4 až 12 portové bez managementu), učebnách (24 a 48 portové bez managementu) a v hlavním racku v prostorách skladu (48 portové s managementem) v 1.NP. Realizovaná přístavba má hlavní rack v technické místnosti (48 portové s managementem).

Do těchto místnosti je také směřována veškerá strukturovaná kabeláž CAT5e ve staré budově i přístavbě. Propojení staré budovy a přístavby je řešeno metalicky CAT 5e.

V budově se nachází dvě oddělené WLAN struktury – původní Mikrotik 802.1g a nová Unifi 802.1ax, která však pokrývá budovu pouze omezeně.

Škola využívá školní informační systém Bakaláři, který je propojen se systémem Otvírač a Stravou.

Každá učebna je vybavena počítačem s připojením na internet a projektorem s projekčním plátnem nebo interaktivní tabulí.

Škola využívá tři specializované učebny pro výuku Informatiky – dvě vybavené 17 počítači a jednu vybavenou 30 notebooky.

Školní mobilní zařízení představuje 96 Chromebooků a 16 Android tabletů.

Obecné požadavky:

Podmínkou realizace je detailní popis vazby na stávající systémy, přenos funkcionality a dat bez omezení provozu, harmonogram všech činností.

Při výstavbě, správě a provozu ICT technologií bude striktně dodrženo hledisko technologické neutrálnosti, tj. využití technologií takovým způsobem, který neomezuje implementaci technologií různých výrobců.

Z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů preferujeme využití stávajících prostředků a používaných technologií.

Položky obsahují na pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu.

Pokud účastníkem navržené řešení (HW i SW) vyžaduje využití konkrétních produktů, neobsažených v popisu předmětu plnění, a jím zvolený přístup k řešení zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

Pro každý softwarový produkt budou výslovně uvedeny všechny licenční nebo výkonové požadavky spojené s instalací a provozem řešení, včetně uvedení konkrétní infrastruktury, na které bude řešení provozováno.

Všechny položky, pokud není uvedeno jinak, jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce a mají zajištěný servis v ČR.

Po realizaci jednotlivých částí a před předáním do plného provozu musí dojít k provedení školení zaměstnanců, kteří budou dodaná zařízení používat, zajištění zkušebního provozu po dobu minimálně 3 týdnů .

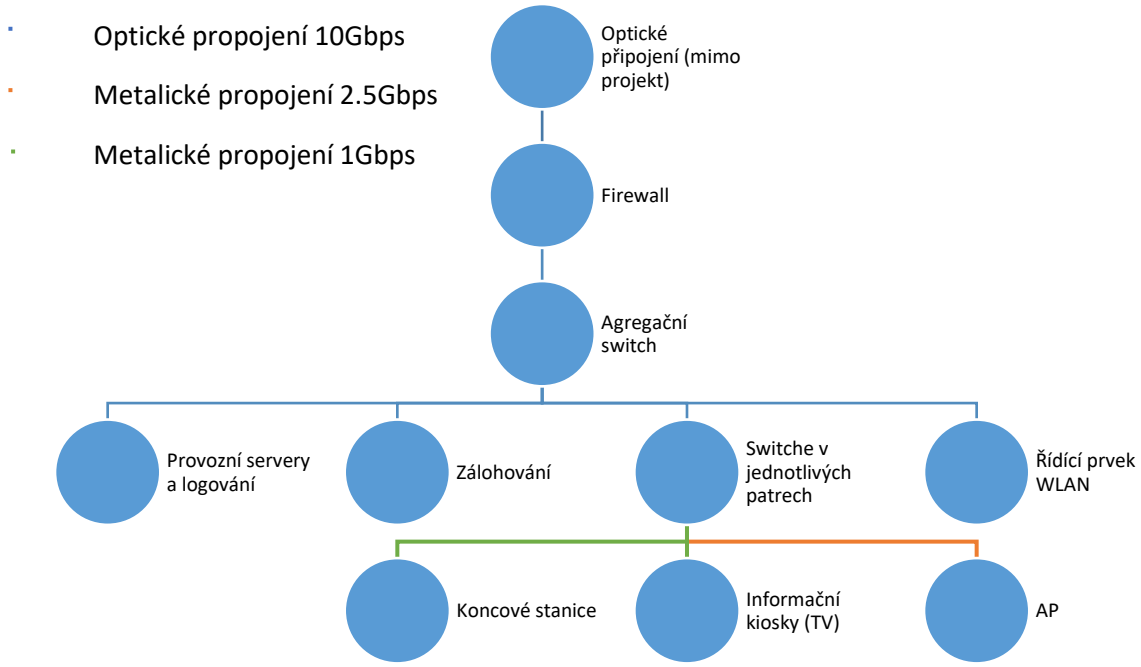
Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, PDF) na datovém nosiči a 1x v papírové formě. Papírová forma bude logicky a věcně strukturovaná, bude připravena pro použití (např. provozní dokumentace ve formě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

V rámci projektu je třeba zajistit naplnění Standardu konektivity škol a toto naplnění prokázat dle dokumentu PROKÁZÁNÍ A KONTROLA NAPLNĚNÍ STANDARDU KONEKTIVITY ŠKOL z března 2024 Č.j. MSMT-27467/2023-1 (viz https://www.edu.cz/digitalizujeme/standard-konektivity-skol/#prokazani).

Technické řešení:

Technické řešení bude založeno na omezeném využití již existujících technologií zadavatele. Technické parametry dodávaných zařízení jsou specifikovány v Příloze 2. Technické parametry jsou vždy minimální.

Síťová infrastruktura bude ve staré budově vybudována nově viz. následující schéma:



Strukturová kabeláž:

Požadovaná je minimálně CAT 6/Class E s dosaženou přenosovou rychlostí 2.5Gbps pro propojení switch/AP a 1Gbps pro ostatní metalická propojení. Propojení switchů, serverů, zálohování, FW bude realizováno opticky pomocí minimálně 8 single modových vláken a v případě propojení do přístavby

12 single modových vláken vždy přímo s agregačním switchem s dosaženou přenosovou rychlostí 10Gbps.

Popis a provedení pasivní části systémů je řešeno v samostatném dokumentu.

Serverové řešení:

Budou pořízeny technologie zajišťující centrální služby – servery s operačními systémy, diskové úložiště, systém pro centrální logování, vyhodnocování a správu událostí a bezpečnostních incidentů, identity management, aplikační firewall, aktivní prvky LAN a zálohovací systém.

Bude pořízena dvojice nových serverů s virtualizační platformou pro základní role, nový server pro logování a server/HW prvek pro správu a řízení WLAN a to včetně licencí OS.

Součástí virtualizační platformy bude vybudování aplikačního firewallu pro publikaci webových aplikací a systémů vzdáleného přístupu a správy.

Pro zálohování bude v rámci projektu pořízeno síťové uložiště NAS s dostatečnou kapacitou pro ukládání provozních záloh a archivů logů systému centrálního logování. Zálohování bude řízeno pokročilým zálohovacím software, který bude prostřednictvím virtualizačního hypervizoru zálohovat všechny virtuální servery. Zálohovací systém umožní zálohovat i fyzické servery a osobní počítače. Bude nastaveno automatické zálohování serverů (fyzické/virtuální) a klíčových stanic s intervalem maximálně 14 dní pro úplné zálohy a každodenním inkrementálním zálohováním. Systém umožní archivaci dat na externí zařízení.

Nutností je zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu.

Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agenta firewallu a dalších.

Technické provedení adresářové služby bude založeno min. na 2 řadičích adresářové služby, které budou provozovány ve virtuálním prostředí a budou pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP, obě v konfiguraci pro vysokou dostupnost. Ověřování identit musí být dostupné i systémům, které přímo nepodporují LDAP nebo jiný protokol adresářové služby. Součástí projektu bude proto i vybudování tzv. zprostředkovatelů identit, které umožní ověřování i jinými protokoly.

LAN, WLAN a zabezpečení:

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 sítí bude zřízena samostatná VLAN (Guest VLAN), které bude komunikačně (min. L3 pravidla, ACL) oddělena od vnitřních sítí organizace. Tato VLAN bude mít své L3 rozhraní až na úrovní 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 učitele a žáky. Ověřování přístupu do této VLAN bude zajištěno pomocí tzv. captive portálu – webové autorizace. Captive portál bude zajištěn firewallem případně jiným samostatným řešením nebo prvkem, ale vždy s důrazem na bezpečné oddělení uživatelského provozu od zbytku vnitřních sítí.

Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (Quality of Services).

Architektura WiFi bude založena na řešení s centrální správou prováděnou HW kontrolerem (řadičem). Bude konfigurován v režimu vysoké dostupnosti a zajistí automatické rozložení zátěže klientů, roaming mezi spravovanými přístupovými body a automatické ladění kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení. Navrhované řešení musí umožnit samostatnou a nezávislou funkci WIFI sítě při postupné realizaci částí projektu.

Ověřování přístupu do LAN/WLAN bude realizováno protokolem 802.1X vůči adresářové službě. Neověřená zařízení nezískají přístup do sítě vůbec nebo jim bude zpřístupněna pouze VLAN s omezeným přístupem (např. Guest). Spolu s ověřováním (autentizací) bude implementována i autorizace, tedy dynamické zařazení klientského zařízení nebo uživatele do určené VLAN. Systém musí být plně použitelný pro stávající zařízení s operačním systémem ChromeOS. Pro síť určenou výhradně pro neověřená zařízení, kde bude realizován tzv. captive portál zajišťující webovou autentizaci hostů pomocí přidělených účtů nebo za pomoci před-generovaných číselných kupónů.

Publikované interní služby (školské informační systém Bakaláři, Moodle apod.) budou publikovány na přidělených IPv4 a IPv6 adresách a bezpečnost přenášených informací bude zajištěna šifrováním pomocí SSL – webové rozhraní bude přístupné protokolem https.

Firewall zajistí oddělení vnitřního a vnějšího provozu na základě tzv. zón a mezi nimi postavených komunikačních pravidel (ACL/xACL), tzv. politik. Firewall bude schopen blokovat nejčastější útoky typu odepření služby (DoS) a bude účinně blokovat podvržení adresy (spoofing).

Firewall zajistí zosobnění žáků a zaměstnanců s jejich internetovými aktivitami napojením na účty v doméně adresářové služby tak, aby byla na firewallu neustále k dispozici aktuální vazba uživatel-IP adresa, případně i zdrojový rozsah portů. Konfigurace politik firewallu a jeho jednotlivých rolí umožní pohodlnou práci s účty i skupinami adresářové služby namísto IP adres, a to ve všech úrovních, tedy vč. kategorizace a filtrace provozu. Role politiky budou schopny pracovat minimálně s těmito objekty – IP/subnet, uživatel/skupina, typ zařízení/operační systém.

Kontrola webového provozu nešifrovaného i šifrovaného (protokoly http a https), logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben je mandatorním požadavkem Standardu konektivity škol a firewall ji bude umožňovat spolu s další UTM funkcionalitou.

Antivirová kontrola prováděná firewallem bude umožňovat konfiguraci minimálně dvou úrovní hloubky kontroly/rychlosti a vytvoření tzv. profilů, které bude možno dle potřeby uplatnit v jednotlivých komunikačních pravidlech (politikách) firewallu, dle druhu a povahy konkrétního pravidla. Antivirová kontrola bude aplikována i na šifrovaná spojení (https, SSL). Infikované soubory musí být možno odstranit či zablokovat.

Ochrana proti průniku (IPS) pracuje podobně jako antivirus na základě definic připravených výrobcem. Definice mají výrobcem nastavenu zároveň i výchozí akci, jak s identifikovanou komunikací naložit (min. blokace, monitorování, reset). Ve většině případů jsou výchozí akce plně vyhovující a lze důvěřovat výrobci firewallu, že v definicích použité výchozí akce jsou pravidelně revidovány a rozšiřovány o nově identifikované hrozby vč. jejich případně blokace. Zařazením profilů IPS do vybraných v komunikačních pravidlech firewallu bude zajištěna automatická blokace identifikovaného útoku bez nutnosti zásahu správce.

DNSSEC kontroly budou probíhat výhradně na DNS resolveru, tak aby nebyla nutná jakákoliv úprava konfigurace vnitřních klientů. Validující DNSSEC resolver bude konfigurován tak, aby se sám dotazoval

výhradně tzv. ROOT serverů nebo jiných důvěryhodných DNSSEC serverů, které bude zároveň používat jako tzv. Trust Anchors.

Centrální logování:

Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware a sledování síťových toků a detekce anomálií. Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 6 měsíců).

Uživatelsky přívětivý přístup ke všem komponentám systému z jednotného grafického uživatelského rozhraní (GUI). Konfigurace, definice zdrojů logů, definice korelačních pravidel, tvorba reportů, řešení událostí a další běžné operace musí probíhat z jediné řídící konzole s jednotným GUI.

Automatické jednorázové i plánovatelné vyhledávání i ruční přidávání Prvků a detekce jejich typů a vlastností. Prvkem se rozumí hw i sw (např. OS) s IP adresou. Prvky jsou typicky zdroji dat – logů a událostí.

Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Spolu s tím bude po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení.

Podpora detekce zranitelností s i bez přihlášení (autentizací) ke kontrolovanému prvku.

Automatická kontrola výskytu škodlivého kódu (malware, rootkity, neobvyklé chování) v monitorovaných operačních systémech Windows, Linux a macOS.

Automatické kontrola konfigurací a nastavení monitorovaných operačních systémů Windows, Linux a macOS a aplikací, hodnocení úrovně zabezpečení monitorovaného systému.

Monitoring a analýza uživatelských aktivit, logů, integrity souborů a registrů atd.

Monitorování síťových toků technologií netflow (min. verze 5,9) či kompatibilní (ipfix, netstream) dle nabízených přepínačů.

Viditelnost síťového provozu – zobrazení, prohledávání, filtrování síťových toků včetně historie.

Podporované protokoly min. syslog, windows events collection (pomocí agenta I bezagentově (např. WMI), snmp, s/ftp, nfs, cifs, netflow.

Pokročilé prohledávání a filtrování raw logů, podpora indexování pro zrychlení hledání.

Podpora automatické rotace raw logů s nastavením doby expirace.

Podpora zálohování logů na externí síťové úložiště.

Konsolidace logů na jednom centrálním místě a standardizace přijatých logů do jednotného formátu.

Automatické doplňování reverzních DNS a hostname záznamů k IP adresám, geolokace.

Výkon min. 1000 EPS (event per second), 5000 FPM (flows per minute).

Systém musí zajistit bezpečné, úplné a nezpochybnitelné ukládání, vyhodnocování a archivaci logů ICT prostředí zadavatele a naplnění požadavků dle zákona č. 181/2014 Sb. (ZKB) a vyhlášky č. 82/2018 Sb. (VKB), o kybernetické bezpečnosti.

IDM:

Bude udržovat a spravovat identity a organizační strukturu organizace: třídy, učitelský sbor, administrativa atd.

Poskytnutá licence umožní nasazení a provoz IDM bez omezení na počet uživatelů, spravovaných identit a napojených systémů.

Integrovaná správa uživatelských rolí, včetně zařazení uživatele do odpovídající role v příslušných IS.

Podpora intuitivní tvorby pravidel v grafickém prostředí pro automatické vytváření uživatelských účtů, začleňování uživatelů do skupin a přiřazování aplikačních rolí uživatelům na základě libovolných atributů identity a přidružených referenčních objektů.

Systém bude poskytovat auditní logy pro pořizovaný logovací a monitorovací systém. Systém obsahuje logování min. následujících typů událostí: události systému (aplikační log), změny entit evidovaných systémem a změny konfigurace systému (auditní log), synchronizace s napojenými systémy (synchronizační log), odeslané notifikace a upozornění (notifikační log),

Systém umožní nastavení samostatných nezávislých administrátorských oprávnění pro správu jednotlivých referenčních objektů.

Systém bude obsahovat mechanismus zabránění hromadným změnám z důvodu případných chybných vstupních dat (např. z personálního systému), aby nedošlo k hromadným nežádoucím změnám (například smazání objektů v Active Directory apod).

Vestavěný export přehledů a seznamů zobrazených do souborů CSV nebo obdobného strojově zpracovatelného a současně běžně čitelného formátu.

IDM umožní spravovat licence pro jednotlivé evidované aplikace a přiřazovat je jednotlivým uživatelům (identitám).

Po vypršení platnosti přiřazení IDM roli přiřazenému objektu automaticky odebere.

IDM bude obsahovat samoobslužné uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).

Veškeré změny vyvolané požadavky uživatele a administrátorů/správců IDM budou provedeny transakčně. Budou logovány tak, aby bylo možné zpětně prokázat co, kdo a kdy měnil v identitách a referenčních objektech i v administraci a konfiguraci IDM. Záznam v logu bude obsahovat původní i novou hodnotu.

Umožní ruční i automatické spuštění synchronizací s propojenými systémy.

Zobrazení jednotlivých stavů průběhu synchronizace bude k dispozici v uživatelsky přístupné podobě.

Rozhraní bude poskytovat minimálně následující synchronizační služby: organizační struktury, seznam identit, seznamu aplikační rolí, seznamu uživatelů dané aplikace a jejich zápis a změna.

IDM bude napojeno na školský informační systémy Bakaláři (www.bakalari.cz). Z těchto systémů budou načítány údaje o organizační struktuře, osobách a tyto údaje budou pro IDM sloužit jako zdrojové. Systém musí umožňovat změnu zdrojového systému na běžné alternativy ŠkolaOnLine (www.skolaonline.cz), iškola (www.iskola.cz) a EduPage (www.edupage.org).

IDM bude spravovat identity a řídit oprávnění v dále vyjmenovaných systémech. V těchto systémech bude IDM vytvářet, aktualizovat, vytvářet uživatele a nastavovat jim oprávnění k rolím.

- Microsoft Active Directory

- Microsoft Office 365

- Google Suite

- Moodle

Školení

Dodavatel provede pro každou část odborné školení na obsluhu a práci s dodanými zařízeními a systémy v celkové rozsahu min. 16 hodin. Školení bude provedeno minimálně v rozsahu:

- běžných administrátorských činností pro implementované systémy
- standardní údržby systémů pro administrátory zadavatele

Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz a běžnou údržbu.

Školení bude probíhat v sídle zadavatele. Předpokládá se účast max. 3 osob.

Akceptační testy

Akceptační testy musí pro všechny části zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti, dále prokázání aktivací software i hardware aktivačními klíči či jinými prostředky, je-li aktivace potřebná. Dále pro každou část navrhne účastník vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost a odpovídající výkon a stabilita dodaného řešení. Návrh vhodných akceptačních kritérií bude součástí Prováděcí dokumentace.

Implementační služby

V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené části následující služby, které jsou zahrnuté v ceně dodávky:

- Zpracování popisu cílového stavu a postupu implementace (včetně plánovaných změn v konfiguraci současné infrastruktury) a provedení související nezbytné analýzy současného stavu. Výstupem bude prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena zadavatelem. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best practices) a doporučení výrobců nabízených technologií.
- Dodávka a implementace předmětu plnění dle schválené prováděcí dokumentace včetně technické podpory.
- Zajištění projektového vedení realizace předmětu plnění.
- Zpracování provozní dokumentace v rozsahu popisu skutečného provedení, specifikace činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat minimálně následující oblasti:
    - Adresářová služba – správa uživatelů a skupin, zařazení počítače do domény
    - Zálohování – kontrola činnosti, obnova souborů
    - Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace
    - Logovací systém – vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce
    - LAN a Wi-Fi – připojení zařízení vč. podrobných uživatelských postupů pro Wi-Fi připojení mobilních zařízení (tablety, chytré telefony, notebooky) s operačními systémy Windows 10 a vyšší, Android, iOS a macOS.

    - Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupinu
    - Systém pro správu identit – podrobná příručka pro správce i uživatele v českém jazyce
- Zpracování dokumentu Zásady využívání ICT a přístupu k síti pro začlenění do vnitřních předpisů školy.
- Zpracování materiálů pro školení a provedení školení v rozsahu dle kapitoly Školení
- Zajištění zkušebního provozu infrastruktury v délce minimálně 3 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností maximálně do 4 hodin od nahlášení požadavku v pracovní den v době od 8 do 17 hodin.
- Provedení akceptačních testů.
- Předání do plného provozu.

Náklady na provedení implementačních služeb musí být zahrnuty v nabídkové ceně k položce (komoditě), ke které se vztahují a nelze je vyčíslit zvlášť.

Příloha 1 – STANDARD KONEKTIVITY ŠKOLY

	povinné
1.1. 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 parametry v době ukončení realizace a v průběhu udržitelnosti projektu.	x
1.2.1. Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student nebo 0,5 Mbps/koncové uživatelské zařízení a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.	řešeno změnou technologie připojení a poskytovatele mimo projekt
1.2.2. Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.	splněno - stávající stav
1.2.3. Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 6 měsíců	x
1.2.4. Síťové zařízení podporující rate limiting, antispoofing, access listy – zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.	x
1.2.5. Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.	x
1.2.6. Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).	x
1.2.7. Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem	x
1.2.8. Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.	x
1.2.9. Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.	řešeno změnou technologie připojení a poskytovatele mimo projekt

1.3.1. Symetrické připojení (zajištění konektivity) bez agregace a omezení, doporučujeme postupně směřovat ke kapacitě konektivity 1Gbps.	řešeno změnou technologie připojení a poskytovatele mimo projekt
1.3.2. Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.	x
1.3.3. Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů	řešeno změnou technologie připojení a poskytovatele mimo projekt
1.3.4. Antivirová kontrola internetového provozu.	x
2.1. Obecný popis Vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojení je nutné zajistit v prostorách dotčených hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být odůvodněna ve studii proveditelnosti.	x
2.2.1. Systém 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. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů)	x
2.2.2. Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém.	x
2.2.3. Systémy zálohování a obnovy dat serverové infrastruktury.	x
2.2.4. Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů	x
2.3.1. Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex.	x
2.3.2. Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex.	x

2.3.3. Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3)7 s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí - VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].	x
2.3.4. Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).	x
2.3.5. Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.	x
2.4.1. Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.	x
2.4.2. Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.	x
2.4.3. Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).	x
2.4.4. Podpora mechanismu izolace uživatelů.	x
2.4.5. Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.	x
2.5.1. Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.	x
2.5.2. Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.	x
2.5.3. Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému www.eduroam.cz).	volitelné
2.5.4. Centralizovaná architektura správy Wi-Fi sítě (centrální řadič, centrální management, tzv. thin access 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).	x

2.5.5. Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].	x
2.5.6. Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.	x
3.1.1. Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).	x
3.1.2. Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.	dle popisu v příslušné kapitole
3.1.3. Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).	dle popisu v příslušné kapitole
3.1.4. Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.	x
3.1.5. Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.	x
3.1.6. Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).	volitelné
3.1.7. Nástroje pro centrální správu a audit ICT prostředků.	volitelné
3.1.8. Podpora vzdáleného přístupu (VPN).	x
3.1.9. Zavedení více-faktorové autentizace.	pro správu síťových prvků

Příloha 2 – TECHNICKÁ SPECIFIKACE

Obecný popis zařízení	Kategorie	Počet kusů
Firewall		
1. Systém ochrany IPS – nejdůležitější prvek utm, tj. signatury striktně síťových útoků a vzory doprovodných anomálií, navíc konfigurovatelné pomocí zásad a senzorů. 2. Filtr obsahu v síti, který chrání před škodlivými webovými stránkami a umožňuje blokovat webové stránky kvůli nežádoucímu obsahu (např. hazardní hry, pornografie, internetové obchody atd.). 3. Ochrana elektronické pošty + Antispam 4. Podpora VPN – umožňuje vytvářet bezpečné a snadno použitelné VPN tunely (IPsec a SSL) na základě integrace s AD nebo jinými řešeními SSO 5. Antivirová ochrana proti narušení UTM – nejen pevné signatury, ale také pokročilou heuristiku, spolupráce s ochranou e-mailu a také monitoring P2P a detekce virů z webových stránek. 6. Architektura založená na využití specializovaných čipů (ASIC) pro zvýšení výkonu a bezpečnosti Technické parametry: Výkon firewallu 2.5 Gbit/s Průchodnost SSL VPN 1 Gbit/s Propustnost antimalware ochrany 2 Gbps IPS propustnost 4 Gbit/s Latence firewallu <4 µs Bezpečnostní zásady 4500 Shoda s FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB Šifrování/zabezpečení 256-bit AES, HTTPS, IPSec, SHA-256, SSL/TLS Minimálně 2x 10Gb SFP+ / GbE porty (mohou být sdílené) a 8x 1GbE RJ 45 porty, včetně 2x SFP+ 10 Gb SM modulů s LC konektorem. Podpora vysoké dostupnosti (clustering) - aktivní/pasivní, aktivní/aktivní Záruka 5 let, odeslání náhradního zařízení NBD.	WAN	1
Přídavný software a licence UTP k firewallu, pokud je třeba minimálně po dobu 5 let	WAN	1
Technická podpora pro blok Firewall v rozsahu: • implementace oprav kritických zranitelností neprodleně po jejich vydání a otestování • 1x ročně upgrade firmware • 2 hodin ročně – konzultace, změnové požadavky apod. po dobu realizace a udržitelnosti projektu.	WAN	1

Obecný popis zařízení	Kategorie	Počet kusů
Server		
2U 1CPU max 16 jader (CPU mark (PassMark) min 41 000+), 128 GB RAM 2x 10Gbit SFP+ Lan s podporou iSCSI a virtualizace VMware NetQueue, Microsoft VMQ. HW RAID SAS/NVMe řadič s cachem min 8 GB, podpora HBA i RAID (1,5,6) režimu Min. 2x SSD 480 GB SSD pro OS, min. 9x 3,8 TB SSD, všechny min. 1 DPWD Vzdálená správa s plnou podporou KVM nezávislá na OS, montážní kolejnice v ceně a 5 let záruka NBD v místě instalace.		2
2U 1CPU max 16 jader (CPU mark (PassMark) min 41 000+), 128 GB RAM 2x 10Gbit SFP+ Lan s podporou iSCSI a virtualizace VMware NetQueue, Microsoft VMQ. HW RAID SAS/NVMe řadič s cache min 8 GB, podpora HBA i RAID (1,5,6) režimu Min. 2x SSD 480 GB SSD pro OS min. 1 DPWD, min. 6x 6 TB 7200 ot/min SAS 12 Gb Vzdálená správa s plnou podporou KVM nezávislá na OS, montážní kolejnice v ceně a 5 let záruka NBD v místě instalace		1
UPS		
Rackové UPS, online technologie, výkon min. 2000 W/2000 VA, diagnostický a konfigurační displej, min. 8 výstupních zásuvek ve 2 samostatně ovládaných skupinách, LAN (web, SNMP) rozhraní pros vzdálenou správu a management, 3 roky záruka	LAN	3
Zálohování		
Racková NAS, 64 bit CPPU min. 4 jádra, 8 GB RAM, 2x LAN 10Gbit SFP+ slot, 12 diskových pozic SATA osazených min. 8x 8TB, 7200 ot/min, podpora RAID1,5 a 6, min. USB 3.0 porty pro propojení s UPS a externími disky, schopnost iSCSI target a vnitřní software pro zálohování virtuálních I fyzických serverů, záruka 5 let včetně disků. Včetně 2x SFP+ 10 Gb SM modulu s LC konektorem.	LAN	1
Vybavení rozvaděče		
KVM přepínač 4 porty pro servery	LAN	1
Monitor LCD min. 19", klávesnice, myš ke KVM, polička pro serverový rozvaděč – sada	LAN	1
Barevně rozlišené patch kabely (minimálně CAT 6A) pro zajištění funkce	LAN	400
Antivirový systém		
Komplexní antivirová a antimalwarová ochrana počítačů a serverů včetně centrální lokální a cloudové správy, na 5 let	LAN	150
Licence OS		
Windows Server Standard, aktuální verze a hypervizor pro minimálně 2 virtuální servery na jeden fyzický. Licence musí umožnit provoz virtuálních serverů stejné verze v prostředí stávající serverové virtualizace, dále provoz všech nabízených aplikací, management nástrojů a systémů.	LAN	6
Switche		

Obecný popis zařízení	Kategorie	Počet kusů
Agregační switch, 24x 10 Gbit SFP+ a 4x 10/25 Gb SFP28 portů. Typ přepínače: L2+/L3, rackový řízený. Neblokovaná architektura, kapacita přepínání: 760 Gbit/s. Podpora LACP, VLAN včetně jejich směrování na L3, 802.1X včetně přiřazování klientů do VLAN na základě ověření, zrcadlení portů, jumbo rámců, STP/RSTP, QoS, ACL. Včetně 28x SFP+ 10 Gb SM modulů s LC konektorem. Záruka 2 roky	LAN	1
Distribuční switch PoE (48) 32x 1 Gbit, 16x 2.5Gbit, a 4x 10 Gb SFP+ porty, z toho min. 32 portů PoE+ (30 W) a 16 portů PoE++ (60 W) s celkovým PoE výkonem 600 W. Typ přepínače: L2+/L3, rackový řízený. Neblokovaná architektura, kapacita přepínání: 176 Gbit/s. Podpora LACP, VLAN včetně jejich routování na L3, 802.1X včetně přiřazování klientů do VLAN na základě ověření, zrcadlení portů, jumbo rámců, STP/RSTP, QoS, ACL. Včetně 2x SFP+ 10 Gb SM modulů s LC konektorem. Záruka 2 roky	LAN	5
Distribuční switche PoE (24) 16x 1 Gbit, 8x 2.5 Gbit a 2x 10 Gb SFP+ porty, z toho min. 8 portů PoE+ (30 W) a 16 portů PoE++ (60 W) s celkovým PoE výkonem 400 W. Typ přepínače: L2+/L3, rackový řízený. Neblokovaná architektura, kapacita přepínání: 112 Gbit/s. Podpora LACP, VLAN včetně jejich routování na L3, 802.1X včetně přiřazování klientů do VLAN na základě ověření, zrcadlení portů, jumbo rámců, STP/RSTP, QoS, ACL. Včetně 2x SFP+ 10 Gb SM modulů s LC konektorem. Záruka 2 roky	LAN	7
SFP+ 10 Gb SM moduly s LC konektorem do nabízených serverů	LAN	6
WIFI		
WIFI přístupový bod (AP) WiFi 7 - podporuje 802.11 a/b/g/n/ac/ax/be, triband 2.4 GHz, 5 GHz, 6 GHz, MIMO 2×2, Mesh, Band Steering, Load Balance, Podpora WPA/WPA2/WPA3, VLAN (802.1Q), podpora vysílání min. 8 SSID, Advanced QoS, Guest Trafic Isolation, alespoň 1 x 2,5 Gb/s ethernet (RJ45) s podporou PoE+, včetně stropního držáku	WLAN	50
Samostatný HW řídící prvek umožňující správu nabízených přepínačů a WiFi AP bez licencí a poplatků, vzdálený přístup přes cloud – bez nutnosti VPN a veřejných IP adres, 8x 1 Gbit a 2x 10Gb SFP+ port, z toho min 6 portů PoE nebo PoE+. Rack mount. Včetně 2x SFP+ 10 Gb SM modulů s LC konektorem. Záruka 2 roky	WLAN	1
Software		

Obecný popis zařízení	Kategorie	Počet kusů
Systém pro správu identit – jde o nejdůležitější softwarový blok, který jednak zajistí vyhovění požadavkům „Standardu konektivity škol“ ale hlavně zařídí, že škola NEBUDE muset obsluhovat tři (s Google Workspace a docházkovým systémem pět databází uživatelů) nezávislé databáze uživatelů (lokální AD, Office365 AD a Google Workspace a splní tím podmínku jednotných IDM. (nutné vzhledem k SKŠ bod 2.2.1 a souvisící). Současně umožní škole mít synchronní databázi software Bakaláři s AD školy a nemuset tak každý rok synchronizovat tyto databáze ručně. Nárok na SW aktualizace a opravy 5 let	LAN	1
Systém pro centrální sběr a správu logů, musí umožnit jednoduše a rychle a bez nároku na speciální podporu vyhledat údaje o komunikaci jakéhokoli počítače dle specifikací SKŠ bod 2.2.2 a souvisící. Software musí tedy umožnit v množství dat shromážděných logů vyhledat požadované údaje co možno jednoduše a srozumitelně. Nárok na SW aktualizace a opravy 5 let	WLAN	1
Technická podpora pro blok Software v rozsahu 4 hod ročně (konzultace, změnové požadavky apod.) po dobu realizace a udržitelnosti projektu.	LAN/WAN	1
Office LTSC Standard 2021 - na min. 5 let – Word, Excel, Powerpoint, Outlook – on premise	LAN	80
HW – podíl nesmí dosáhnout 30 % z celkové ceny		
PC + monitor do učebny VT/PT, CPU 64 bit PassMark 20 000 bodů, 16 GB RAM DDR5, 256 GB NVMe SSD, LAN 1Gbit a WiFi 6E, min. 1x USB-C nebo Thunderbolt 4 s PD/DP, 2 současně použitelné grafické výstupy (minimálně 1x HDMI) včetně OS Windows 11 Pro + 24" (viditelná min. 23,5") full HD IPS monitor s HDMI a/nebo DP, záruka 3 roky na obojí	LAN	34
Panel dotykový/interaktivní min. 86') + motorizovaný držák (možnost psaní přes obsah z HDMI a dalších vstupů přímo v rámci OS panelu, 40 dotek, tvrzené sklo, 2x pero), možnost montáže křídel klasické keramické tabule na držák přímo od výrobce	LAN	8
Učitelské PC + monitor do učeben, CPU 64 bit PassMark 10 000 bodů, 8 GB RAM DDR5, 256 GB NVMe SSD, LAN 1Gbit a WiFi 6E, min. 1x USB-C nebo Thunderbolt 4 s PD/DP, 3 současně použitelné grafické výstupy (minimálně 1x HDMI + 1x HDMI/DP), hloubka skříně max 30 cm, včetně OS Windows 11 Pro + 22" (viditelná min. 21,5") full HD IPS monitor s HDMI a/nebo DP, záruka 3 roky na obojí	LAN	40
Chromebook konvertibilní s 360° rotací pantů, CPU 64 bit PassMark min 5400, 8 GB DDR5, 128 GB SSD, displej 12-13" 1920 × 1200 dotykový (IPS), min. 1x USB-C s podporou funkce Power Delivery 3.0 a DisplayPort™ 1.4, min. 1x HDMI, min. WiFi 6 a Bluetooth, web kamera, 3.5mm audio combo-jack, chromeOS s EDU UPGR, 2 roky záruka	LAN	16