**TECHNICKÁ SPECIFIKACE - část - Konektivita**

Základní škola Vizovice, příspěvková organizace

Školní 790, Vizovice 763 12

IČ: 49156683

|  |  |
| --- | --- |
|  | **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]](#footnote-1) - uvedené v příloze č.1 (dále jen Standard konektivity). Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

| Označení | Komodita | Počet |
| --- | --- | --- |
| K1 | Virtualizační platforma | 1 |
| K2 | Zabezpečení LAN a Wifi | 1 |
| K3 | Centrální logování | 1 |

* + - 1. 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.
      2. 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.
      3. 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.
      4. Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:
         1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
         2. mají plnou záruku od výrobce,
         3. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
         4. obsahují všechny nezbytné licence na používání příslušného softwaru,
         5. jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
         6. jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží čestným prohlášením distributora, popř. dodavatelovým samotným, nelze-li prohlášení distributora získat.

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.

* + - 1. 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** |

### **Specifické požadavky na technické řešení**

* + - 1. **K1 - Virtualizační platforma**
         1. Pro provoz veškerých pořízených systémů a aplikací bude pořízen jeden server vybavený interním úložištěm s vysokou kapacitou. Hardware serveru bude virtualizován a na serveru bude možno provozovat 4 virtuální servery.
         2. 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.
      2. **K2- Zabezpečení LAN a Wifi**
         1. Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby s využitím technologie 802.1X.
         2. 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).
         3. Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem (řadičem), který bude součástí firmwarů přístupových bodů.
         4. 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).
      3. **K3 - Centrální logování**
         1. 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).
         2. 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.
         3. 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.

### **Implementační služby**

* + - 1. V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K3
         1. 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.
         2. Zajištění projektového vedení realizace předmětu plnění.
         3. Provedení testů.
         4. 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 |
| * 1. Návrh a kompletní implementace serverové virtualizační platformy   2. Implementace pořízených technologií   3. Návrh vhodné struktury ActiveDirectory, její vybudování   4. Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie   5. Návrh a provedení akceptačních testů |
| K2: Zabezpečení LAN a Wifi |
| * 1. Implementace pořízených technologií   2. Provedení segmentace LAN – VLAN, adresování, routování   3. Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách   4. 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   5. Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu   6. Vybudování VPN pro vzdálený přístup uživatelů LAN   7. Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik   8. Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity |
| K3: Centrální logování |
| * 1. 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.)   1. Provedení souvisejících konfigurací monitorovaných systémů |

* + - 1. 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.

### Školení

* + - 1. Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu:
         1. běžných administrátorských činností pro implementované systémy
         2. 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 1 hodina, není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele.

### **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 | - |

* + - 1. Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.
      2. Dodavatel uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy.

### **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, nebo tower provedení |
| **CPU** | Server musí být osazen min. 1x CPU, minimálně s čtyřmí procesorovými jádry.  Hodnocení výkonu nabídnutého serveru musí být publikované na webu: <https://www.cpubenchmark.net> s minimálními parametry:   * Passmark CPU Mark, hodnota min: 9 000 |
| **RAM** | 32GB v provedení min. 2666MT/s DDR4 ECC UDIMM |
| **Diskový subsystém** | Server musí disponovat alespoň 4x 2TB 7.2K RPM NL-SAS 12Gbps 512n 2.5" Hot-plug Hard Drive, 3.5" rámeček, RAID 5 |
| **Optická mechanika** | DVD+/-RW SATA |
| **Síťové rozhraní** | * 2x 1000Base-T, onboard (nezabírající volné PCI-e sloty) |
| **Napájení** | Redundantní napájecí zdroje 230V, max. 550W |
| **Chlazení** | Možnost provozu při okolní teplotě stabilně až do 40°C (provoz chlazení čerstvým vzduchem) |
| **Podpora OS a virtualizace** | Microsoft Windows Server 2012 R2  Microsoft Windows Server 2016  Microsoft Windows Server 2019  VMware ESX 5.1 až 6.7  Citrix Xen Server 7.1  RedHatEnterprise Linux 6  RedHatEnterprise Linux 7  SUSE Linux ES 15 |
| **Podpora a servis** | Podpora na 3 roky typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru. |

|  |  |  |
| --- | --- | --- |
| **SW licence operačních systémů /AD/LDAP** | Serverové operační systémy | 2 ks licencí 64-bitového serverového operačního systému v aktuální verzi. Licence musí umožnit provoz hypervizoru a min. 2 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 celkem na 100 zařízeních. |

**Povinné parametry pro Komoditu K2 – Zabezpečení LAN a Wifi:**

|  |
| --- |
| **Firewall**  **1KS** |
| Počet 1GE metalických síťových rozhraní (RJ45 10/100/1000) pro firewallové funkce - min 4x  Počet 1GE optických síťových rozhraní (SFP) pro firewallové funkce – min. 2x  Počet management rozhraní (RJ45) – min. 1 |
| Podpora LACP (802.3ad) na min. 4 portech stejného typu  Velikost max. 1U  Lokální úložiště (nerotační technologie) – min. 128GB |
| Podpora IPv6 pro všechny funkce  Podpora NAT64/NAT46  Výkonnost FW shodná pro IPv4 i IPv6  Minimální závislost výkonu firewallu na velikosti paketů |
| Propustnost FW (stavové filtrování, UDP paket) 4 Gbps (měřeno na paketech o velikosti 1518 B) |
| Propustnost FW paketů za sekundu – min. 6 Mpps |
| Počet naráz otevřených spojení – min. 1,3 M |
| Počet nových spojení za sekundu - min. 30 000 |
| Propustnost IPSEC VPN – min.2,5Gbps |
| Propustnost SSL VPN min 200 Mbps |
| Propustnost NGFW (IPS + Applicationcontrol; traffic mix) - min 360 Mbps  Propustnost IPS (měřeno na http komunikaci) – min 1,5Gbps |
| Podpora virtualizace (na dané HW appliance) min 10  Součástí dodávky musí být licence na min. 10 virtuálních kontextů, včetně kompletní UTM funkcionality ve všech kontextech |
| Podpora ActiveActive i ActivePassive HA, full mesh HA, synchronizace stavové tabulky mezi nódy clusteru  Podpora VRRP |
| Podpora L2 (transparentní) režimu i L3 (NAT/Router) režimu |
| Podpora multicast, včetně routování a firewall funkcí (tvorba multicast FW politiky) |
| Podpora VPN: SSL (portálový režim, tunelový režim), IPSEC (IKE, manualkey, certifikát, gateway to gateway, hub and spoke, dial up konfigurace, internet browsing konfigurace, podpora více tunelů – redundantní VPN, možnost VPN v L2 – transparentním režimu ukončená na management rozhraní, podpora IPv6, podpora dynamických routovací protokolů - OSPF), PPTP, L2TP, GRE |
| Možnost nastavovat firewall politiku na základě geografických údajů  Detekce klientského zařízení, možnost nastavovat firewall politiku na základě typu klientského zařízení (telefon, tablet, PC) včetně operačního systému (Android, iPhone, …) bez nutnosti instalovat klienty na koncové stanice |
| Podpora firewall pravidel na základě identity uživatele pro MS AD prostředí – nastavení bezpečnosti uživateli na základě členství v AD skupině na doménovém kontroléru |
| Funkce LoadBalancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora healtcheck funkcí, podpora SSL offload |
| Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace |
| UTM funkce, možnost výběru mezi proxy režimem (buffer) nebo flow režimem (inspekce on-the-fly), zejména pro antivirovou/antimalware kontrolu |
| Antivirová/antimalware kontrola pro vybrané protokoly, možnost volby různých databází (např. minimální, standardní a extrémní) kvůli optimalizaci výkonnosti, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spyware, keylogger, atd). |
| Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty. |
| 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. |
| Podpora ochrany pro mobilní zařízení – funkce zajistí prohledávání datového toku i na známé signatury pro útoky na připojená mobilní zařízení (BYOD – BringYourOwnDevice).  Data LeakPrevention s funkcí documentfingerprinting (běžící pouze na firewallu, tedy bez nutnosti instalovat klientský software na koncové stanice). |
| SSL dekrypce/offload – možnost kontroly komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…). |
| DoSPolicy prevence proti základním útokům typu DoS, včetně syn proxy |
| Ověřování uživatelů proti LDAP, ActiveDirectory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu, Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. |
| Dynamické routování: |
| * RIP, BGP, OSPF |
| * Policyrouting |
| TrafficShaping (QoS, prioritizace atd.) |
| Podpora VoIP, SIP včetně zabezpečení, ratelimitingu, analýzy protokolu |
| WAN optimalizace (optimalizace vybraných protokolů, byte caching), Web Cache, Reverzní proxy, WCCP  Funkce Explicitní Proxy, včetně autentizace v síti MS AD protokolem Kerberos |
| Podpora silné autentizace uživatelů – podpora pro generátor jednorázových hesel (OTP) – Token pro dvou-faktorovou autentizaci, podpora certifikátů pro ověření uživatelů (možno jako interní součást FW nebo jako externí systém – např. RADIUS server). |
| Záruka min. 24 měsíců |

|  |  |  |
| --- | --- | --- |
| **Přístupové přepínače**  **2KS PoE** | **Parametry** | |
| * 48x 10/100/1000BaseTRJ-45 STP port | | |
| * 2x SFP port - 1Gbps, hot swap | | |
| * 2x SFP+ port - 10Gbps, hot swap | | |
| * Celková propustnost: 70 Gbps | | |
| * 19" Rackmount | | |
| * Max. výkon: 750W | | |
| * PoE: PoE+ 802.3at/af nebo pasivních 24V nastavitelné na každém portu, případně vypnuto (piny 1 a 2+; 3 a 6-) | | |
| * PoE+: automatické rozpoznání 802.3at/af, výstupní napětí 50-57V, max. výkon 34,2W/port | | |
| * Pasivní PoE 24V: manuálně konfigurovatelné, výstupní napětí 20-27V, max. výkon 17W/port | | |
| * Napájení: 100-240VAC/50-60 Hz | |
| Záruka min. 24 měsíců | | |
|  |  | | |
| **WiFi přístupové body (AP) + montáž na strop 24 ks** | 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. 24 měsíců |
|  |  |

**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, zasílaní 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 |
|  |  |

**Slaboproudé rozvody pro vnitřní konektivitu:**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID položky** | **Připojení laboratoří** | **JMN** | **KS** |
|  |  |  |  |
| **Fo - propoj do budovy laboratoří - kabel** | kabel optický SM 12vl. | KS | **50m** |
| **Fo - propoj do budovy laboratoří - vybavení** | opt.vana, pigtaily, patchcordy, spojky | KS | **1** |
| **LAN - metalická RACK + vybavení** | Nástěnný rozvaděč vč.patch panel 48 port cat 6 , vyvazovací panel, přepěťová ochrana 5x220V, propojovací patch kabely. Rozměry rack - min 12U, hloubka min. 450mm, 19", uzamykatelný. | KS | **1** |
| **LAN - metalická KABEL** | kabel UTP cat.6 | KS | **320m** |
| **LAN – instalace** | Instalace včetně dopravy | KS | **1** |

**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]](#footnote-2) nebo 512kbps/počítač[[3]](#footnote-3) nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů[[4]](#footnote-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]](#footnote-5) nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz <http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX>

1. **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 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]](#footnote-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]](#footnote-7) do federovaného systému eduroam ([www.eduroam.cz](http://www.eduroam.cz)). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.

1. **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)
* 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)

1. [↑](#footnote-ref-1)
2. *Počet studentů je definovaný celkový počet studentů školy* [↑](#footnote-ref-2)
3. *Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení* [↑](#footnote-ref-3)
4. *Definováno jako saturace šířky pásma připojení k veřejnému internetu, která ani ve špičkách nedosáhne a to ani krátkodobě 100%* [↑](#footnote-ref-4)
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.* [↑](#footnote-ref-5)
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* [↑](#footnote-ref-6)
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*](http://www.eduroam.cz/_media/cs/cz_roam_policy_v2.0.pdf) [↑](#footnote-ref-7)