

| Konektivita školy k veřejnému internetu (WAN) | |
|--|--|
| Standardy konektivity | Komentář |
| šíře pásma (bandwidth) odpovídající 0,25 Mbps/student nebo 0,5 Mbps/počítač nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů | 100/100 Mbps na 600 studentů = 600*0,125 (Mbps) = 150 nutno navýšit v rámci projektu na min 200/200 |
| symetrické připojení bez agregace a omezení (FUP) | je v současnosti i v předpokladu zajišťováno |
| vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy | IPv4 běží IPv6 není – možno řešit s poskytovatelem |
| plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack) | IPv4 běží IPv6 není – možno řešit s poskytovatelem |
| validující DNSSEC resolver na straně školy | je funkční u poskytovatele DNS |
| podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení | navrhované řešení projektu požadavku vyhovuje |
| logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.) | navrhované řešení projektu požadavku vyhovuje |
| síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality | Není řešeno |
| 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 | je řešeno přesměrováním dotazů na l-bezpecne.cz |
| možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků | Není řešeno |
| podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online | IPv6 může být řešen s poskytovatelem |
| zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX | ISP školy Wolfnet v seznamu podporující Fenix není |
| u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu | je zajištěno zárukou výrobců hardware |
| Vnitřní konektivita školy (LAN) | |
| 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 | Není řešeno |

| | |
|---|--|
| monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízení 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. | serverové řešení LDAP a AD |
| logování přístupu uživatelů do sítě umožňující dohledání vazeb <i>IP adresa – čas – uživatel</i> | zajištěno na Windows serveru |
| Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s fullduplex | Splněno, projekt předpokládá vnitřní pevné LAN konektivitu fullduplex 1Gb/s - postupná výměna aktivních prvků (všude není GB) |
| Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,...) | je v projektu předpokládána |
| Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex | veškeré servery a aktivní prvky včetně bezpečnostních zařízení včetně kabeláže předpokládají 1Gb/s fullduplex |
| Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických nebo metalických vláken | Propojení budov je pomocí optického kabelu |
| Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3) s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,... | Není řešeno |
| Podpora mechanismu izolace klientů | Není řešeno |
| 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 | topologie Wi-Fi počítá s třemi konzistentními sítěmi 2,4GHz a 5GHz pro pedagogy, studenty a zařízeními školy (tiskárny, atp) - požadavku vyhovuje |
| Centralizovaná architektura správy wifi 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) | veškerá funkcionality je řešena kontrolérem Wi-Fi sítí s detekcí rušení a automatickým přeladěním signálu, rozložením zátěže a roamingu mezi AP |
| Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...) | v navrhovaném řešení je obsažena instalace a ověřování přes MS AD |
| Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz | předpokládané řešení podporuje standard IEEE 802.11n a 802.11ac v pásmech 2,4 a 5 GHz |
| Minimálně pasivní zapojení do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů. | Možnost zapojení do Eduroam |
| Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu | navrhované řešení požadavku vyhovuje |

| Další bezpečnostní prvky | |
|---|---|
| Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů | serverové řešení LDAP a AD |
| Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.) | serverové řešení je postaveno na LDAP a AD windows serverů 2016, 2012 |
| Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokáce wifi v určitém čase) | Možnost bezdrátové sítě pro hosty existuje a řešení projektu tuto funkcionalitu dovoluje |
| Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb) | Není řešeno |
| Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow) | navrhované řešení by mělo umožňovat funkce RFC 3954 |
| Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie | Není řešeno, ideálně nějak doplnit |
| Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management) | Není řešeno, vhodné doplnit v řešení |
| Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga) | Není řešeno – dá se doplnit |
| Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk) | Není řešeno |
| Nástroje pro centrální správu a audit ICT prostředků | Není řešeno |
| Systémy zálohování a obnovy dat serverové infrastruktury | je zajištěno funkcionalitou již implementovaného řešení |
| Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů | navrhované řešení požadavku vyhovuje |
| Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp. | je zajištěno funkcionalitou již implementovaného řešení |
| Podpora vzdáleného přístupu (VPN) | VPN není, je možno nastavit |

WiFi síť ve škole není centrálně řešena – několik přístupových bodů je v některých kabinetech.

Bude využita stávající LAN síť.

Ve škole bude instalováno 62 ks wifi routerů a 10 switchů plus další potřebné vybavení k zajištění konektivity.

+ práce a materiál

WiFi síť

Technické požadavky Wi-Fi systém:

- Centralizované prostředí správy pomocí webové aplikace a/nebo aplikace pro mobilní zařízení
- Wi-Fi 6 (IEEE 802.11ax)
- High-density Wi-Fi - možnost přepojit velké množství klientů na malém místě
- Podpora 802.1x, VLAN

6. 3. 2023

Mgr. Ladislav Kuba
metodik a správce ICT školy