

Příloha č. 1 – TS ZŠ Dr. Hrubého

Technická specifikace

Centrální systém řízení a monitorování sítě

Vyžadován je centrální systém řízení a monitorování všech níže poptávaných komponent a to prostřednictvím jednotného webového rozhraní.

Centrální systém řízení a monitorování sítě (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Centrální systém řízení a monitorování sítě musí umožnit zabezpečenou vzdálenou správu, plnou konfiguraci a monitorování současně pro všechny poptávané komponenty sítě (bezpečnostní brány, přepínače, bezdrátové přístupové body a systém správy mobilních zařízení) a to prostřednictvím jednotného integrovaného webového rozhraní.
2.	Systém musí zajistit automatickou aktualizaci softwaru a instalaci bezpečnostních záplat do všech zařízení v systému a to v uživatelsky definovaném čase.
3.	Systém musí umožnit změny konfigurace více zařízení stejného typu současně a konfigurace nových zařízení pomocí šablon.
4.	Centrální systém řízení a monitorování sítě musí podporovat následující metody autentizace klientů LAN a WLAN infrastruktury: <ul style="list-style-type: none">- 802.1X ověření na základě údajů interní databáze systému- 802.1X ověření prostřednictvím RADIUS serveru- Webová autentizace na základě údajů interní databáze systému- Webová autentizace prostřednictvím RADIUS nebo LDAP serveru- Webová autentizace prostřednictvím Facebook účtu- Možnost vytvoření vlastního webového portálu
5.	Centrální systém řízení a monitorování sítě musí být schopen zobrazit všechny klientská zařízení připojená k síti školy během minimálně posledních 10 dnů. Výpis by měl obsahovat minimálně následující informace: <ul style="list-style-type: none">- Uživatelské jméno- IP a MAC adresa zařízení- Objem uživatelem / zařízením přenesených dat za dané období s rozpadem na jednotlivé rozpoznané aplikace
6.	Systém musí být schopen zobrazit seznam top žáků / studentů, kteří za dané období ve školní síti přenesli nejvíce dat.
7.	Systém musí být schopen zobrazit polohu a stav všech zařízení v systému v geografické mapě a také graficky zobrazit reálnou fyzickou topologii sítě školy.
8.	Systém musí být schopen zobrazit polohu všech klientských zařízení v závislosti na způsobu jejich připojení a to buď přímo v plánech jednotlivých podlaží, v geografické mapě nebo v kontextu portu příslušného LAN přepínače.
9.	Systém musí být provozován v režimu vysoké dostupnosti.
10.	Základní konektivita a přístup do Internetu musí být pro klienty zachován i v případě, že je Centrální systém řízení a monitorování sítě dočasně nedostupný.
11.	I v případě nedostupnosti Centrálního systému řízení a monitorování sítě musí být zajištěna možnost autentizace a autorizace nových klientů LAN i WLAN infrastruktury prostřednictvím 802.1x protokolu pomocí RADIUS.
12.	Systém musí umožnit rozdělení administrátorů do skupin s různými právy přístupu.
13.	Pro autentizaci administrátora přistupujícího přes webové rozhraní musí systém podporovat minimálně RADIUS protokol, SAML a dvoufaktorovou autentizaci.
14.	Systém musí být schopen odesílat správcům emailové zprávy o důležitých systémových událostech.
15.	Systém musí být schopen odesílat zprávy na vzdálený SYSLOG server.
16.	Systém musí podporovat SNMP protokol pro vzdálenou správu a monitorování.
17.	Systém musí podporovat XML API pro integraci s navazujícími systémy školy poskytující informace o připojených komponentách sítě a také klientských zařízeních.
18.	Systém musí sledovat změny konfigurace systému a zahrnutých síťových komponent – Informace musí minimálně obsahovat:

	<ul style="list-style-type: none"> - položku konfigurace - uživatelské jméno administrátora, který změnu provedl - novou hodnotu proměnné, v které ke změně došlo
19.	System musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
20.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně všech aktualizací softwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. System musí být v době prodeje výrobcem plně podporován a na žádnou jeho část nesmí být vyhlášeno ukončení prodeje.

Next-Gen Firewall, IPS a anti-malware

Zařízení určené k ochraně síťového prostředí před hrozbami na bázi pokročilých útoků. Kromě funkcí tzv. Nex.Gen FW (typicky chápané jako aplikační a identity-based FW) je schopno provádět inspekci provozu s detekcí a ochranou před útoky na úrovni síťového provozu. V oblasti ochrany proti malware je možno aktivovat analýzu souborů včetně dynamické analýzy (tzv. sandboxing) i ukládání nebezpečných souborů do karantény. Zařízení lze použít i pro URL filtraci na úrovni kategorií, konkrétních URL či podle reputace serverů v Internetu.

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Výkon a funkcionality firewallu	
Formát zařízení	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1
Minimální počet 1Gb 10/100/1000 BaseT Ethernet	8
Podporovaný počet současně otevřených spojení stavový FW/aplikační FW	Min.100000M/100000
Rychlost vytváření nových spojení přes stavový FW	Min. 10K/s
Propustnost stavového firewallu (multiprotokolový režim)	Min. 500 Mbps
Propustnost aplikačního FW (next-gen FW) – (top parametry)	Min. 450 Mbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	Min. 250 Mbps
Propustnost aplikačního FW (next-gen FW) – (transakční profil, 450B průměrná velikost paketu)	Min. 180 Mbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (transakční profil, 450B průměrná velikost paketu)	Min. 115 Mbps
VPN propustnost	Min. 175 Mbps
Současný počet VPN spojení (IPSec/SSL)	Min. 100
Podpora L2 (transparentního) módu s podporou NAT a PAT	Ano
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano
Podporovaný počet VLAN	Min. 50
Podpora stateful failover	active/standby
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	Ano
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	Ano
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	Ano
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	Ano
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 250 kontextů	Ano
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano
Podpora Policy based Routing	Ano
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž	Ano

cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	
Podpora filtrace IPv4, IPv6	Ano
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano
Podpora inspekce IPv6 provozu	Ano
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano
Podpora NAT64 a DNS64	Ano
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	Ano
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	Ano
Možnost rozšíření o funkce NextGen FW	Ano
Možnost rozšíření o funkce NextGen IPS	Ano
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano
Funkce IPS a anti-malware	
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano
Možnost obejít IPS funkcí při zahlcení nebo nedostupnosti	Ano
Podpora 802.1Q tagovaných rámců	Ano
Podpora různých IPS politik pro různé typy provozu	Ano
Inspekce pro IPv4 i IPv6	Ano
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	Ano
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano
Podpora aplikace pro psaní zákaznických filtrů	Ano
Podpora importu komunitních filtrů/signatur Snort	Ano
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	Ano
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	Ano
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano

Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	Ano
Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano
Možnost definice uživatelské vrstvy politik	Ano
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano
Různé politiky lze sdílet a aplikovat na různé senzory	Ano
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů	Ano
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	Ano
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	Ano
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	Ano
Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	Ano
Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru dodavatele jako malware je na koncových stanicích okamžitě přesunut do karantény	Ano
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	Ano
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano
Možnost automatické i manuální klasifikace stanice jako „kritické“ se zohledněním v pravidlech, reportech apod.	Ano
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano
Funkce Next-Gen FW	
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano
Podpora pasivního monitorování (TAP režim)	Ano
Podpora 802.1Q tagovaných rámců	Ano
Podporovaných aplikací	Min. 3000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano
URL kategorií	Min. 80
Kategorizovaných světových URL	Min. 280 milionů
Řízení přístupu k WWW - Web Usage Control (WCU)	Ano
Filtrace podle typů aplikací webových i ne-webových	Ano
Filtrace podle reputace serverů	Ano
SSL inspekce (dekrypce/enkrypce)	Ano
Security Intelligence database – známé uzly botnet sítí C&C	Ano
Security Intelligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano
Security Intelligence database – známé nebezpečné URL adresy a jmenné domény	Ano

Možnost integrovat vlastní reputační databáze	Ano
Podpora komunitních, otevřených standardů popisu aplikací (OpenAppID)	Ano
Filtry mohou zohlednit roli a identitu uživatele	Ano
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano
Řešení musí být schopné pasivního sběru informací o síťových zařízeních a zobrazení:	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,..) Důvod případného blokování Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní Zdroj. a cíl. port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact“ aplikace Množství přenesených dat
Správa	
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano
Přístup ke GUI http/https protokolem	Ano
Možnost vzdáleného přístupu protokolem ssh přímo do FW	Ano
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano
Možnost lokální správy v případě nasazení jednoho FW (omezené možnosti nastavení)	Ano
Možnost centrální správy při nasazení více firewallů	Ano
Při centrální správě: možnost sdílených bezpečnostních politik	Ano
Při použití clusteru se spravuje pouze jeden logický prvek	Ano
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano
Zobrazení logů a událostí v grafickém rozhraní správy	Ano
Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	Ano
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního systému (centrální dohledové konzole)	Ano
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano

Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	Ano
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	Ano
Pro reporty lze definovat template definující formát a obsah reportu	Ano
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight BMC Remedy Trustwave NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano
Podpora řízeného přístupu podle rolí administrátorů	Ano
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano
Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	Ano
Workflow pro předávání „ticketů“ mezi administrátory	Ano
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu	Ano
Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano
Zákaznický definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli	Ano

LAN L2 přepínač 24 portů PoE+

Síťový přepínač je zařízení, které umožňuje připojit koncové LAN klienty, bezdrátové přístupové body a ostatní zařízení v systému. Volitelná optická rozhraní slouží k agregaci dalších přepínačů školy.

LAN přepínač 24 portů PoE+ je inteligentní přepínač s 24x 10/100/1000Base-T porty s podporou PoE/PoE+ a 4x 1/10GE SPF porty.

LAN L2 přepínač 24 portů PoE+ (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Zařízení musí být možné nainstalovat stojanu 19".
2.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
3.	Zařízení musí mít minimálně 4x 1/10 GE SFP/SFP+ rozhraní pro uplink/downlink.
4.	Zařízení musí podporovat stohování více zařízení stejného typu pomocí dedikovaných fyzických portů s propustností minimálně 80 Gb/s.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat PoE (IEEE 802.3af-2003) na všech RJ45 rozhraní.
7.	Zařízení musí podporovat PoE+ (IEEE 802.3at-2009) na alespoň polovině RJ45 rozhraní.
8.	Zařízení musí podporovat jumbo frame 9600 bajtů.
9.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
10.	Zařízení musí podporovat minimálně 16000 MAC adres.
11.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
12.	Zařízení musí podporovat L3 funkce: statické směrování, DHCP relay.
13.	Zařízení musí podporovat 802.1x na všech rozhraních.
14.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
15.	Propustnost zařízení musí být nejméně 128 Gb/s.
16.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
17.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
18.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
19.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
20.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
21.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
22.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
23.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
24.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

LAN L3 přepínač 24 portů

LAN L3 přepínač 24 portů je inteligentní přepínač s 24x 10/100/1000Base-T porty a 4x 10G SPF+ porty.

LAN přepínač (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Zařízení musí být možné nainstalovat stojanu 19".
2.	Zařízení musí podporovat možnost fyzického stohování s propustností minimálně 80 Gb/s.
3.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
4.	Zařízení musí mít minimálně 4x 10G SFP+ rozhraní pro uplink/downlink.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.

6.	Zařízení musí podporovat jumbo frame 9600 bajtů.
7.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
8.	Zařízení musí podporovat L3 funkce a protokoly: statické směrování, dynamické směrování pomocí OSPFv2, DHCP relay/server a VRRP.
9.	Zařízení musí podporovat minimálně 16000 MAC adres.
10.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
11.	Zařízení musí podporovat 802.1x na všech rozhraních.
12.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
13.	Propustnost zařízení musí být nejméně 128 Gb/s.
14.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
15.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
16.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
17.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
19.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
20.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
21.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
22.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Bezdrátový přístupový bod

Bezdrátový přístupový bod je zařízení, které umožňuje klientům připojení do bezdrátové sítě.

Bezdrátový přístupový bod (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Zařízení musí podporovat následující Wi-Fi standardy: 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac Wave2.
2.	Zařízení musí být schopno pracovat současně v pásmu 2,4 GHz a 5 GHz.
3.	Zařízení musí v případě standardu 802.11ac podporovat šířku kanálu až 80MHz.
4.	Zařízení musí podporovat centrálně řízené automatické nastavení výběru kanálu a vysílacích výkonů a to včetně dynamické reakce na změnu prostředí.
5.	Zařízení musí podporovat 2x2:2 MU-MIMO a beamforming.
6.	Zařízení musí podporovat PoE napájení dle standardu 802.3af.
7.	Zařízení musí být dodáno s úchytem na stěnu a/nebo strop.
8.	Zařízení musí být uzamykatelné proti krádeži.
9.	Zařízení musí mít alespoň jedno 100/1000Base-T rozhraní.
10.	Zařízení musí umožnit konfiguraci minimálně 8 SSID na každém z 802.11 rádií.
11.	Zařízení musí podporovat následující bezpečnostní standardy: WEP, WPA2-PSK, WPA2-Enterprise s 802.1X autentizací.
12.	Zařízení musí podporovat šifrování AES.
13.	Zařízení musí podporovat ověřování PEAP (MSCHAPv2)
14.	Zařízení musí podporovat standardy 802.11r, 802.11k a 802.11v pro rychlý roaming klientů a rozložení zátěže mezi jednotlivými AP infrastruktury.
15.	Zařízení musí podporovat VLAN tagging (802.1Q) na jeho ethernetovém rozhraní.
16.	Zařízení podporuje principy QoS dle WMM, 802.1p a DSCP.
17.	Zařízení musí podporovat funkci rozpoznávání tříd klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.

18.	Zařízení musí být schopné omezit šířku pásma pro každé jednotlivé SSID, pro každého z klientů a také dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI).
19.	Zařízení musí umožnit QoS klasifikaci paketů dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI) pomocí DSCP a 802.1p tagu.
20.	Zařízení musí podporovat BLE (Bluetooth Low Energy) dle specifikace Bluetooth 4.0.
21.	Zařízení musí umožňovat spektrální analýzu pro detekci zdrojů rušení (non-WiFi interference) v pásmu 2,4 a 5GHz s možností zobrazení diagramů v reálném čase. Funkce spektrální analýzy nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením.
22.	Zařízení musí umožnit filtrování procházejících uživatelských dat dle cílových IP adres a/nebo UDP/TCP portů.
23.	Zařízení musí umožnit zakázat komunikaci vybraných klientů a to až dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI) a v případě http i dle DNS jména cílového serveru.
24.	Zařízení musí mít integrovanou funkci detekce a zastavení útoku na bezdrátovou infrastrukturu (wIDS/wIPS). Tato funkce musí být dostupná v reálném čase na všech kanálech (i neobsluhovaných) a nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením.
25.	Zařízení musí podporovat zachytávání klientského provozu s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
26.	Zařízení musí podporovat L3 roaming klientských zařízení mezi různými subnety školy.
27.	Zařízení musí umožnit tunelovat SSID pro návštěvy přímo na bezpečnostní bránu v DMZ školy.
28.	Zařízení musí umožnit izolaci jednotlivých uživatelských zařízení tak, aby tato zařízení nemohla komunikovat mezi sebou (v rámci celého SSID školy).
29.	Zařízení musí být v případě nedostupnosti drátové ethernet konektivity schopné jako uplink dynamicky využít jedno ze svých rádii – mesh link přes některé z okolních AP.
30.	Zařízení musí umožnit spolu s Centrálním systémem řízení a monitorování sítě lokalizaci klientských zařízení v mapě jednotlivých podlaží na základě triangulace dle síly signálu.
31.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
32.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
33.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
34.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Netflow analyzer

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 – systém pro monitorování a sběr provozně-lokačních údajů na úrovni rozhraní WAN i LAN a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců

Vlastnosti zařízení	
Rack-mount zařízení	maximální velikost 1 RU
Počet monitorovacích portů	min. 4 x 10/100/1000 Mbps (metalika - RJ45)
Management port	1x 10/100/1000 Mbps metalický
Minimální výkon na každém monitorovacím portu	1 480 000 paketů za sekundu
Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s	na metalických rozhraních
Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky	Ano

Pasivní zapojení bez vlivu na monitorovanou síť	zapojení pomocí TAPů
Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě	Ano
Přesný nezávislý autonomní zdroj NetFlow statistik	podpora IPv4, IPv6, VLAN, MPLS, GRE
Podpora monitorování MAC adres	
Podpora standardizovaných protokolů pro výměnu dat o IP tocích	NetFlow v5, v9 - RFC3954, IPFIX
Detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik	Ano
Zabezpečená vzdálená správa, dohled a konfigurace	HTTPS (GUI), SSH
Vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance)	obsahuje uživatelsky definovaný dashboard, automatickou tvorbu reportů, detekci aktivních zařízení a detailní analytické možnosti
Úložná kapacita vestavěného kolektoru	min. 500 GB
Možnost doplnit o další moduly	např. behaviorální analýza, monitoring výkonu webových aplikací
Časová synchronizace zařízení proti centrálnímu zdroji času na síti	Ano
Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména	Ano
Správa uživatelů a přístupových práv na zařízení	Ano
Podpora vzdálené autentizace uživatelů	LDAP (Active Directory)
Plná zákaznická podpora v českém jazyce	Ano

Server do racku pro DNSSEC a RADIUS

Pro zajištění služeb DNSSEC A RADIUS serveru bude instalován HW server, na kterém bude spuštěn OS plně kompatibilní s Microsoft Windows Server a bude začleněn do stávající serverové infrastruktury jako člen domény. Server musí splňovat následující kritéria:

- Jednosocketový server o velikosti 1U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely
- 1 procesor (min 4 jádra, 8 vláken), min. 8MB cache dle passmark min. 9900 bodů
- Podpora paměti DDR-4 o frekvenci 2400MHz
- Možnost maximálního rozšíření na minimálně 64GB
- min. 32GB DDR-4
- Integrovaný RAID SAS řadič s podporou RAID 0/1/5/6/10 včetně 2GB flash paměti nebo baterií zálohovanou RAM paměti
- Min. 4 pozice pro 3.5" hot-swap SAS/SATA/SSD disky
- Min. 2x 600GB 10000 otáček hotplug disky
- Min. 4 porty USB 3.0
- Možnost rozšíření až 3-mi PCI-e kartami, z toho alespoň 2x PCIe Gen3 s x8 bus
- 2x 1Gbit LAN porty
- 1x Dedikovaný management port RJ-45
- Větráčky v serveru musí být redundantní
- 2x Napájecí zdroje s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje je 450W

- Zdroje musí splňovat požadavky na certifikaci energetické účinnosti, např. ECOS Consulting 80 Plus (min. PLATINIUM), popř. je nutno doložit, že mají při napětí 230V účinnost min. 94%
- Certifikace a podpora výrobce pro OS MS Windows Server 2012 R2 a výše
- Požadovaná 5 letá servisní podpora s opravou v místě instalace serveru a s garantovanou opravou následující pracovní den od nahlášení případné závady

Software pro Server

Požadavky na operační systém pro servery:

- Licence pro serverový operační systém pro provoz 1 operačního systému na 1 fyzickém serveru, který je součástí nabídky
- Možnost downgrade verze operačního systému
- Nevázanost licence na dodaném hardware
- Operační systém musí být plně kompatibilní s provozovanými aplikacemi a současnou serverovou infrastrukturou a Active Directory
- Součástí dodávky požadujeme také 40ks licencí pro přístup uživatelů k doméně (Active Directory) kompatibilní se stávající platformou školy

Ostatní služby infrastruktury a platformy

DNSSEC resolver – zřízení DNSSEC resolveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

AD, LDAP - využití stávající AD s databází uživatelů a skupin uživatelů v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

SSO - předpokládáme instalaci SSO (Single Sign On) utility jako součást bezpečnostní brány do standardního serverového operačního systému.

RADIUS - předpokládáme instalaci RADIUS serveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

Strukturovaná kabeláž pro wifi

Pro zajištění komunikace a současně napájení wifi sítě bude dobudována strukturovaná kabeláž ke všem 42 ks wifi access pointů. Kabeláž bude uložena v existujících lištách nebo budou instalovány nové lišty dle potřeby. Strukturovaná kabeláž bude zakončena ve stávajícím centrálním datovém rozvaděči na patch panelu. Požadovaná kabeláž je min. UTP Cat 5e. Součástí dodávky bude potřebný počet patchcordu do datového rozvaděče a další vybavení rozvaděče.

Učebna IVT velká

Pro zajištění potřebného technického zázemí v učebně IVT, bude osazeno 16 PC s příslušenstvím a provedena rekonstrukce datových a napájecích rozvodů k počítačům.

Celkem bude k dispozici 20 přípojných míst strukturované sítě a 20 zásuvek s 230V přivedených do jednotlivých lavic, kam budou instalovány PC s příslušenstvím.

PC s příslušenstvím

- Case minitower se zdrojem splňujícím ENERGY STAR® certified; EPEAT® Gold
- Procesor splňující výkon min. 12000 bodů passmark
- minimálně RAM 8GB DDR4

- minimálně HDD 256GB SSD
- Mechanika DVDRW
- Klávesnice, myš
- Výstup na monitor DP nebo HDMI
- Operační systém plně kompatibilní se současným systémem školy (aktuálně Windows)
- Monitor s úhlopříčkou min. 21,5 - 22" s rozlišením min. 1920 x 1080, IPS, odezvou 5ms, 250cd, rozhraním min. 1x HDMI
- Záruka 36 měsíců onsite NBD
- PC i monitor od stejného výrobce
- Kabel na propojení PC a LCD HDMI nebo DP
- balík kancelářských aplikací plně kompatibilní s OS a systémem školy (aktuálně MS Office)

Software pro správu třídy

Pro řízení jakékoliv výuky využívající PC bude implementován systém, který umožní sledovat, ovládat a řídit všechny počítače z učitelského pracoviště.

Správa Třídy

- Zapínání a vypínání všech počítačů ve třídě z počítače učitele.
- Dálkové "Odhlášení" všech počítačů.
- Zaslání dálkového "Přihlášení" na začátku vyučovací hodiny na všechny počítače studentů.
- Ponechání obrazovek studentů prázdných k získání pozornosti.
- Zablokování myši a klávesnic studentů při podávání pokynů.
- Rozmístění tak, aby počítač učitele představoval rozmístění fyzické třídy.
- Použití profilů jednotlivých učitelů k předložení prvků, které každý z učitelů potřebuje.
- Vizualní odměňování jednotlivých studentů k povzbuzení snahy nebo chování.

Správa Tiskárny

- Brání studentům v tisku ve třídě.
- Omezení použití tiskárny počtem stránek.
- Před tiskem se požaduje schválení učitele.

Správa Zařízení

- Brání kopírování dat na nebo z USB úložiště a CDR / DVD zařízení.
- Brání tvorbě nových síťových připojení.

Registrace Studentů

- Požadavek na standardní a uživatelské informace od každého studenta na začátku vyučovací hodiny.
- Distribuce souborů na více počítačů jedním úkonem.
- Náhled na shrnutí pro studenta „najeťím myši“ na ikonu studenta.
- Použití přizpůsobených úkonů pro jednotlivé studenty nebo skupiny studentů.

Rozdávání a Sbíráání Souborů

- Transfer souborů na a ze zvoleného počítače jedním úkonem.
- Distribuce souborů na více počítačů jedním úkonem.
- Rozdávání a automatický sběr souborů s připojenými údaji každého studenta.

Pokyny v Reálném Čase (Režim Ukázky)

- Ukázání obrazovky učitele zvoleným studentům.
- Ukázání specifického počítače zvoleným studentům.
- Ukázání jen zvolené aplikace zvoleným studentům.
- Ukažte soubor Replay (předchozí nahrávka obrazovky) vybraným studentům, a výstup jak video soubor.
- Přehráání video souboru zvoleným studentům.
- Předložení prezentací optimalizovaných pro bezdrátové sítě.
- Zanechání záznamu Ukázky na počítači studenta k pozdějšímu prohlédnutí.

- Zvuková interakce se studenty během demonstrace tématu.
- Ukažte obrazovku studenta (Mód prohlížení)

Společné Prohlížení Internetu

Umožňuje učiteli otevírat zvolené webové stránky a synchronizovat je s prohlížečem na počítačích všech studentů. Když učitel naviguje webovými stránkami, počítače studentů ho následují.

Náhled na Obrazovky Studentů v Reálném Čase (Režim Monitorování)

- Monitorování celé třídy jedním pohledem.
- náhled přes studentské počítače v předem definovaných skupinách.
- Pokrytí dalšími informacemi včetně aktivní aplikace nebo aktivní webové stránky.
- Zoom pro optimalizované miniatury studentů s vysokým rozlišením.

Monitorování Instant Messengerů Sledování Klávesnic v Reálném Čase Měření a Kontrola Internetu

- Monitorování veškerého využití Internetu studenty.
- Náhled na všechny webové stránky otevřené v pozadí na všech počítačích.
- Otevírání a zavírání webových stránek na všech zvolených počítačích jedním úkonem.
- Záznam úplné historie využití Internetu pro třídu.
- Předchází přístupu na všechny nebo na omezené webové stránky.
- Povoluje pouze přístup na schválené webové stránky.

Monitorování Audia v Reálném Čase a Jazykové Nástroje Průzkumy Studentů

- Tvorba průzkumu s využitím předem dodaných nebo uživatelských odpovědí.
- Okamžité prohlédnutí všech odpovědí a shrnutí pro třídu.
- Dynamická tvorba skupin založená na odpovědích studentů.
- Publikace výsledků průzkumu všem studentům.

Zkoušení a kvízy Studentů

- Tvorba knihovny zdrojů a otázek, které lze sdílet.
- Tvorba libovolného počtu testů s využitím otázek z vaší knihovny.
- Nyní využívá 8 různých stylů otázek.
- Tvorba otázek se 2 až 4 možnými odpověďmi.
- Nastavení úrovně hodnocení zkoušek (např. přes 75% = hodnocení A).
- Sledování pokroku studentů a sledování správných nebo nesprávných odpovědí na otázky v reálném čase.
- Automatické známkování testů, aby byly výsledky dostupné okamžitě po jejich dokončení.
- Zobrazení výsledků jednotlivým studentům.
- Předložení výsledků (včetně zdůraznění správných odpovědí) třídě.
- Instalace návrháře testů na samostatném systému.

Technická konzole pro správce umožní:

- Monitorovat všechny počítače ve školní síti v jednom pohledu.
- Monitorovat využití aplikací a Internetu na počítači každého studenta.
- Přenášet soubory a složky do zvolených nebo všech počítačů.
- Seskupovat všechny počítače podle třídy / fyzického místa.
- Generovat úplné hardwarové systémové informace pro zvolené počítače.
- Generovat úplné informace o softwaru pro každý počítač včetně Hotfixů.
- Prohlížet a kontrolovat služby, procesy a aplikace běžící na každém PC.
- Poskytovat přímou technickou pomoc učiteli v libovolné třídě.
- Zapínat, vypínat, restartovat nebo se přihlásit na počítače ve třídě dálkově.
- Provádět výkonnou 1:1 dálkovou kontrolu PC na libovolně zvoleném počítači.

Zabezpečení

- Jedinečný "zabezpečovací klíč", aby byla vaše kopie nekompatibilní s ostatními kopiemi.

- Omezení konektivity pouze na systémy s odpovídající softwarovou licencí.
- Profily učitelů, z nichž každý umožňuje uživatelské úrovně funkčnosti dle požadavku.
- Použití AD profilů k omezení toho, kteří uživatelé smějí používat software učitele nebo technika.
- Použití AD profilů k vynucení konfigurací pro učitele a klienta.
- Kontrola přístupu a použití přenosných mediálních zařízení ve třídě.
- Automatická opakovaná aplikace omezení po restartování počítače studenta.

Deník Studenta

- Podrobné údaje o vyučovací hodině a cíle.
- Poznámky učitele.
- Poznámky jednotlivých studentů.
- Snímky obrazovky z prezentace (a vysvětlení).
- Virtuální obrazovky bílé tabule.
- Výsledky zkoušek jednotlivých studentů.
- URL webových stránek používaných během vyučovací hodiny.
- Kopie přepisů libovolných chatů třídy.

Učebna IVT malá

Software pro správu třídy – viz. učebna velká - identické

Montážní a implementační práce - pro splnění standardu konektivity škol

Hardware

- Doprava na místo
- Fyzická montáž do datového rozvaděče
 - Prostor připraví zákazník
 - Popis jednotlivých dodaných prvků – popisky, štítky
 - Fotodokumentace
- Zapojení, oživení do sítě zákazníka
 - Konfigurace MGMT IP adres
 - Aktualizace dle doporučení výrobce na poslední verze FW, BIOS
 - Doložení dle výrobce o aktuálnosti
- Vyvázání kabeláže
 - Popis kabelů
 - Dokumentace + fotodokumentace k zapojení
- Dodavatel zajistí všechny potřebné kabely vč. PDU
 - LAN
 - Opt.
 - Power
 - Jiné
- Instalace žákovských PC a implementace do stávající infrastruktury
- Implementace systému řízení výuky v učebnách
- Fyzická likvidace odpadu, odvoz

Software

- Virtualizační platforma
- Instalace operačních systémů
- Konfigurace všech potřebných rolí dle standardu konektivity do škol včetně RADIUS serveru
- Konfigurace operačních systémů, rolí dle doporučení výrobce
- Konfigurace MGMT reportů
 - Reportování stavů HW
 - RAID, FAN, PSU, CPU, RAM, HDD
 - Poštovní server dodá zákazník
- Instalace jednotlivých serverů / zařízení dle standardu konektivity do škol

Na WAN připojení k internetu:

- 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 rate limiting, 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.

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 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.
- 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 full duplex
- Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,...)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s full duplex
- Pátevní 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)¹ s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based 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. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou

¹ 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 architekturu přepínacího subsystému

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

Všechny body výše vychází z daného standartu, který je nutno dodržet.

- Plná integrace nového řešení do stávající infrastruktury ICT školy

Dokumentace

- Kompletní dokumentace vč. Fotodokumentace HW zapojení
 - Zálohy konfigurací na přiloženém CD
 - Obálka vč. Uživatelských jmen a hesel
 - Seznam vytvořených uživatelů vč. Vzdálených přístupů
 - Kompletní dokumentace nastavení jednotlivých rolí dle standartu
- Výstupní protokol, který prověří fungování daného standartu
- Provedení site survey wifi pokrytí – zakres do dodaných půdorysů
- Veškeré licence v tištěné i elektronické formě na přiloženém CD
- Předávací protokol o předání dokumentací

Předání

1. Zaškolení obsluhy, předání informací o celém řešení
2. Testovací provoz, který ověří funkčnost (cca 1 měsíc)