# Popis současného stavu

Hlavní technologie Integrované střední školy živnostenská se nacházejí na adrese Škroupova 13 v Plzni. Připojení školy do internetu zajišťuje Správa informačních technologií města Plzně prostřednictvím sítě CESNET.

Na straně školy se nachází firewall SonicWall NSa 2650, slouží zároveň k oddělení vnitřních sítí školy, které segmentovány a distribuovány formou VLAN (klíčové segmenty: servery, zaměstnanci, učebny, WiFi pro zaměstnance, WiFi pro veřejnost, DMZ). Strukturovaná kabeláž splňuje standard CAT6, některé části CAT5e. Kabelová síť je vybudována na switchích výrobce HPE Bezdrátovou síť zajišťují prvky HP Aruba.

Serverová infrastruktura je postavena na virtualizační technologii HyperV. Servery převážně využívají operační systém Microsoft Windows. Škola provozuje Active Directory jako identitní systém uživatelů (zaměstnanců, studentů, externích pracovníků), pracovních stanic, bezpečnostních skupin a centrálních politik.

Současný stav ICT školy neodpovídá „Standardu konektivity škol“ vydaného MŠMT (<https://edu.gov.cz/digitalizujeme/standard-konektivity-skol/>) a současným nárokům na výkon, bezpečnost a centralizovanou správu počítačové sítě. Počítačová síť byla budována postupně, je sestavena z prvků odlišného stáří a chybí hlubší provázanost jednotlivých částí.

Absence možnosti detailního řízení a sledování provozu je klíčovou překážkou ve zvýšení úrovně kybernetické bezpečnosti a realizaci preventivních opatření. Decentralizovaná, resp. roztříštěná správa sítě bez podpůrných a automatizačních nástrojů vyčerpává kapacitu správce sítě opakovanými rutinními činnostmi a nedává časový prostor pro systematický a koncepční rozvoj.

# Popis cílů projektu a specifikace předmětu plnění

V rámci projektu je řešena vnitřní konektivita školy a připojení k internetu. V rámci projektu bude řešena konektivita pouze v hlavní budově na adrese Škroupova 13, Plzeň.

Projekt zajistí zvýšení propustnosti a kybernetické bezpečnosti současné síťové infrastruktury. Současně dojde k naplnění klíčových požadavků „Standardu konektivity škol“ dle níže uvedené specifikace.

|  |  |
| --- | --- |
| **Požadavek** | **Způsob naplnění** |
| **Konektivita školy k veřejnému internetu (WAN) - povinné parametry** |
| 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 | Tento parametr škola v současné době splňuje. |
| Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy. | Tento parametr škola v současné době splňuje. |
| Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců. | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem**. |
| Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality. | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem.**  |
| Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků. | \* Tento parametr škola v současné době **splňuje a jeho udržení bude řešeno tímto projektem.** |
| Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.). | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem**. |
| Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem**. |
| Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici | \* Tento parametr škola v současné době **splňuje a jeho udržení bude řešeno tímto projektem.** |
| 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. | Tento parametr škola v současné době splňuje. |
| **Konektivita školy k veřejnému internetu (WAN) - doporučené parametry** |
| Symetrické připojení (zajištění konektivity) bez agregace a omezení | Tento parametr škola v současné době splňuje. |
| Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách. | \* Tento parametr škola v současné době **nesplňuje**, škola má zajištěné IPv6 adresy, odpovídající konfigurace prvků a systémů pro naplnění požadavků **budou řešeny v rámci tohoto projektu.** |
| 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. | Tento parametr škola v současné době splňuje prostřednictvím poskytovatele konektivity. |
| Antivirová kontrola internetového provozu | \* Tento parametr škola v současné době **splňuje a jeho udržení bude řešeno tímto projektem.** |
| **Vnitřní konektivita školy (LAN a WLAN) - společné povinné parametry** |
| 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). | Tento parametr škola v současné době splňuje. |
| Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem.**  |
| Systémy zálohování a obnovy dat serverové infrastruktury | Tento parametr škola v současné době splňuje. |
| Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů | Tento parametr škola v současné době splňuje. |
| **Vnitřní konektivita školy (LAN a WLAN) - povinné parametry pevné LAN** |
| Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex | Tento parametr škola v současné době splňuje. |
| Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex | Tento parametr škola v současné době splňuje. |
| Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) 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.]. | \* Tento parametr škola v současné době **splňuje a jeho udržení bude řešeno tímto projektem.** |
| Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.). | Tento parametr škola v současné době splňuje. |
| 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. | Tento parametr není v rámci jedné budovy relevantní |
| **Vnitřní konektivita školy (LAN a WLAN) - povinné parametry bezdrátové sítě WLAN** |
| 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. | Tento parametr škola v současné době splňuje. |
| Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu. | Tento parametr škola v současné době splňuje. |
| Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty). | Tento parametr škola v současné době splňuje. |
| Podpora mechanismu izolace uživatelů. | Tento parametr škola v současné době splňuje. |
| 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. | Tento parametr škola v současné době splňuje. |
| **Vnitřní konektivita školy (LAN a WLAN) - společné doporučené parametry** |
| Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele. | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem.** |
| Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase. | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem.** |
| Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému www.eduroam.cz). | Toto neplánujeme |
| 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). | Tento parametr škola v současné době splňuje. |
| 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]. | Tento parametr škola v současné době splňuje, využitím RADIUS serveru s ověřením proti MS AD. |
| Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku. | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem.** |
| **Doporučené bezpečnostní prvky projektu** |
| Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent) | Toto neplánujeme |
| Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie. | \* Tento parametr škola v současné době **splňuje a jeho udržení bude řešeno tímto projektem.** |
| Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management). | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem.** |
| Systémy pro monitorování funkčnosti síťové a serverové infrastruktury. | \* Tento parametr škola v současné době **nesplňuje a bude řešen tímto projektem.** |
| Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu. | \* Tento parametr škola v současné době **splňuje a jeho udržení bude řešeno tímto projektem.** |
| Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.). | Tento parametr škola v současné době nesplňuje, ani neplánujeme zavést. |
| Nástroje pro centrální správu a audit ICT prostředků. | Tento parametr škola v současné době nesplňuje, ani neplánujeme zavést. |
| Podpora vzdáleného přístupu (VPN). | \* Tento parametr škola v současné době **splňuje a jeho udržení bude řešeno tímto projektem.** |
| Zavedení více-faktorové autentizace. | Tento parametr škola v současné době nesplňuje, ani neplánujeme zavést. |

# Předmět plnění

Předmětem plnění veřejné zakázky je dodávka hardwaru, licencí, softwarových řešení, implementačních prací, které zajistí naplnění požadavků „Standardu konektivity škol“. Součástí plnění je i příprava dokumentace potřebné pro doložení splnění podmínek zmíněného Standardu konektivity škol.

Detailní specifikace předmětu plnění je uvedena níže v Technické specifikaci.

Bližší informace Standardu konektivity škol jsou uvedeny na webové stránce:
<https://edu.gov.cz/digitalizujeme/standard-konektivity-skol/#prokazani>

Zadavatel zároveň požaduje od dodavatele vyplněné čestné prohlášení, že nabídka splňuje požadavky Standardu konektivity škol (Příloha č. 4 Výzvy – Vzor prohlášení).

Součástí předání předmětu plnění bude akceptační protokol, mezi jehož kritéria patří doložení testu standardu konektivity na webu <https://www.stadardkonektivity.cz> a prokázání dle manuálu <https://www.edu.cz/digitalizujeme/standard-konektivity-skol/#prokazani>.

*Účastník je povinen předložit pouze a jen taková zařízení a výrobky, která zcela odpovídají technické specifikaci. V případě, že této specifikaci nabízené dodávky zcela nevyhoví, může toto vést k vyloučení účastníka. Změna dodávaného zboží nebo výrobků po podání nabídky by bylo možné pokládat za materiální změnu nabídky, jež není dle ZZVZ ani dle aktuální rozhodovací praxe Úřadu pro ochranu hospodářské soutěže přípustná. Proto důrazně účastníkům doporučujeme, aby případné nejasnosti v technické specifikaci řešili v době před podáním nabídky, a to formou žádosti o vysvětlení zadávací dokumentace.*

# Příloha – Technická specifikace

Na základě požadavků měření provozu sítě a odhadu budoucího nárůstu nároků na kybernetickou bezpečnost a propustnost v horizontu udržitelnosti tohoto projektu se stanovují následující minimální požadované produkty a parametry:

## 1 ks Next Generation Firewall – HA cluster

Firewall v režimu vysoké dostupnosti, dvě spolupracující nezávislá identická hardwarová zařízení v režimu aktivní/pasivní. Níže uvedené parametry se vztahují na každou unitu samostatně:

* Hardware, velikost max. 1U
* Fyzické porty min.
	+ 10x SFP+ 10Gbps (2x LAN konektivita s podporou LACP, 2x WAN konektivita)
	+ 10x RJ-45 1Gbps (LAN konektivita pro podružené systémy, např. odečty energií)
	+ 1x RJ-45 1Gbps dedikovaný management
	+ 1x RJ-45 sériová konzole
* Duální (redundantní) napájení
* Maximální spotřeba 200 W
* Podpora IPv6 (Dual stack, ICMPv6, ND, stateless auto-config)
* Podpora VLAN dle standardu 802.1Q
	+ Minimálně 100 VLAN kvůli mikrosegmentaci serverů publikovaných v DMZ a včetně příp. rozdělení sítě po jednotlivých učebnách a kabinetech
	+ Podpora více VLAN a více subnetů na jednotlivých WAN i LAN rozhraních a koexistence WAN s LAN/DMZ na jednom fyzickém rozhraní (kvůli možnosti připojení k síti Camelnet)
	+ Podpora výchozí brány pro IPv4 provoz na jiné VLAN než pro IPv6 (kvůli možnosti připojení k síti Camelnet)
	+ Nepřipouští se varianta dosažení výše uvedených VLAN funkcionalit předřazením jiného zařízení (switche/routeru) z důvodu minimalizace SPoF
* Podpora více WAN konektivit
	+ Na jednom i fyzickém rozhraní i na více fyzických rozhraních
	+ Automatický failover v případě výpadku některé z konektivit
	+ Policy based routing (kvůli možnosti připojení k síti Camelnet)
* Podpora linkové agregace
	+ LACP dle standardu 802.3ad
* Access-listy
	+ Řízení přístupových oprávnění na základě zdrojové/cílové zóny/sítě/portu
	+ Síť může být určena IP adresou, subnetem, rozsahem adres, doménovým názvem, případně i jejich skupinou
* Rate limiting
	+ QoS (podpora 802.1p a DSCP vč. mapování, aby bylo možné DSCP značkováním přenášet 802.1p informace i přes sítě, které 802.1p nepodporují – např. priorita VOIP paketů přenášených přes WAN/VPN)
	+ Bandwidth management (omezování šířky pásma)
	+ Možnost přidělování politik šíře pásma pro každé pravidlo zvlášť i možnost sdílení politiky více pravidly
	+ Možnost dodatečného omezení i pro každou IP adresu zvlášť)
* Anti-spoofing
	+ Hlídání zdrojových IP adres v komunikaci na základě směrovacích pravidel (zdrojová IP musí odpovídat subnetu zdrojového rozhraní)
	+ Hlídání vazby IP-MAC, možnost omezení konkrétních MAC na daném rozhraní
	+ DHCP server/IP relay snooping (důvěra vazby IP-MAC z DHCP serveru nebo relay)
* Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků
	+ Podpora automaticky stahovatelných seznamů IP adres (nejméně v 10minutových intervalech), které lze použít v ACL kvůli stahování centrálních škodlivých IP adres nebo naopak IP výjimek
* Antivirová kontrola internetového provozu
	+ Signaturní databáze
	+ Sandbox analýza neznámých vzorků, alespoň exe, pdf, office dokumentů
	+ Podpora TLS dekrypce s propustností min. 1 Gbps kvůli ochraně služeb v DMZ
* Propustnost IPS a Threat Protection 8 Gbps (uvažován 1 Gbps pro každou klíčovou VLAN)
* Min. 100000 souběžných spojení, s nárůstem 10000 spojení/sekundu (týká se hloubkové inspekce paketů i TLS dekrypce)
* Propustnost VPN (IPSec) min. 1 Gbps (kvůli replikacím záloh mimo hlavní budovu)
* Detekce nelegitimního provozu nebo síťových anomálií
	+ Kategorizace a selekce aplikací, blokování nežádoucích kategorií a jednotlivých aplikací
	+ Filtrování provozu z/do nežádoucích sítí (filtrování botnetů a geo-lokace)
	+ Filtrování nežádoucích domén a podezřelého DNS provozu vč. DNS tunelování
* Kontrola http a https provozu
	+ Kategorizace a selekce obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu
* Vestavěný DHCP server, DHCP relay, DNS proxy, NTP server
* Správa prostřednictvím Web GUI (TLS 1.3), SSH v2, sériové konzole a REST API s autentizací pomocí Digest algoritmu SHA256
* Ověřování uživatelů prostřednictvím protokolů LDAP, RADIUS a SAML2
* Podpora single-sign-on ke zjištění přihlášeného uživatele na pracovní stanici čtením logů z řadičů domény a pomocí protokolu WMI dotazováním se na konkrétní pracovní stanici
* Podpora IPsec site-to-site tunelů s podporou eliptických klíčů 521-bitů ve fázi 1 i 2 (PFS)
* Automatické každodenní zálohování konfigurace do cloudu
* Konfigurace zařízení musí být exportovatelná do čitelného textového formátu z auditních důvodů
* Možnost monitorování nedávného provozu přímo v rozhraní firewallu s možností filtrování na úrovni aplikace, webové stránky, uživatele a zdrojové/cílové IP adresy
* Možnost monitorování paketů přímo v rozhraní firewallu za účelem ladění provozu (např. dohledávání blokované komunikace)
* Podpora protokolů SNMP, Syslog, IPFIX a Netflow pro monitoring, sledování událostí a provozu
* Duální redundantní napájecí zdroj
* Součástí dodávky musí být odpovídající SFP(+) moduly a optická kabeláž nebo DAC
* Požadavky na komunikaci s druhým firewallem ve vysoce dostupném clusteru
	+ Detekce dostupnosti druhého firewallu, automatické převzetí aktivní role při zjištěné nedostupnosti
	+ Automatická synchronizace konfigurací a firmwaru
	+ Při identickém redundantním zapojení LAN i WAN části při přepnutí bezvýpadková změna role aktivní/neaktivní mezi oběma zařízeními (bez přerušení otevřených spojení), a to při zjištěné nedostupnosti nebo při ručním zásahu (restartu nebo vynucené změně) nebo aktualizaci firmwaru
	+ Při neredundantním zapojení alespoň synchronizace konfigurace a při výpadku zprovoznění konektivity přepojením kabeláže z jednoho firewallu do druhého
* Požadované funkčnosti musí být zalicencované minimálně po dobu udržitelnosti projektu (5 let od uzavření projektu – předpoklad - 2/2026)

## 7 ks Network switch typu A (bez PoE)

* Hardware, velikost max. 1U
* Fyzické porty min.
	+ 48x RJ-45 1Gbps
	+ 4x SFP+ 10Gbps
	+ 1x RJ-45 sériová konzole
	+ 1x USB port pro připojení ext. úložiště pro přenos firmware a konfigurace
* Neblokující architektura přepínacího subsystému (wire speed)
* Základní bezpečnostní prvky proti zneužití přístupu k síti (např. MAC based omezení port-security, např. vyhrazení portu pro určitou MAC, omezení počtu dynamických MAC)
* Podpora IPv6 (Dual stack, ICMPv6, ND, stateless auto-config)
* Podpora 802.3x (Flow control), 802.1Q (VLAN), 802.3ad (LACP), 802.1X (autentizace, s podporou guest VLAN), 802.3az (EEE), 802.1ab (LLDP, s podporou MED)
* Podpora STP (spanning-tree) 802.1d, 802.1w, 802.1s
* QoS na základě DSCP a 802.1p
* Loop guard nezávislý na STP i STP loop guard
* Podpora min. 8000 MAC adres
* Konfigurace prostřednictvím Web GUI (TLS 1.3), SSH v2 a sériové konzole
* Možnost konfigurace profilů portů dle připojení koncového zařízení, které na základě předem stanovené konfigurace nastaví na vybraném portu požadované VLAN a příp. další parametry jako např. max. počet dynamických MAC adres na daném portu, konfigurace STP edge, aby nebylo nutné tyto parametry nastavovat pro každý port zvlášť
* Součástí dodávky musí být odpovídající SFP/SFP+ moduly a optická kabeláž nebo DAC
* Požadované funkčnosti musí být zalicencované minimálně po dobu udržitelnosti projektu (5 let od uzavření projektu – předpoklad - 2/2026)

## 1 ks Network switch typu B (s PoE)

Požadavky stejné jako u switche typu A a navíc:

* Napájení koncových zařízení (PoE+) všech 48 portů, celkový výkon napájení min. 350 W
* Schopnost zachovat napájení zařízení i při restartu switche, např. při upgrade firmware
* Požadované funkčnosti musí být zalicencované minimálně po dobu udržitelnosti projektu (5 let od uzavření projektu – předpoklad - 2/2026)

## Softwarová řešení a konfigurace

* Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.
* Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení
	+ Detekce NAT událostí firewallu pomocí Syslog nebo jiným vhodným způsobem
	+ Aplikace s webovým rozhraním
	+ Snadné vyhledávání záznamů zadáním vyhledávacích kritérií (zdrojová/cílová IP adresa, vnější port po NAT maskování portu, časové rozmezí)
	+ Držení záznamů min. 3 měsíce
* Software nebo zařízení pro logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém
	+ Detekce přihlášených uživatelů v drátové síti (single-sign-on detekce přihlášených uživatelů ke stanicím pomocí čtení logů z doménových řadičů a WMI protokolem proti konkrétní stanici)
	+ Logování DHCP událostí (přidělení IP adresy DHCP serverem a DHCP IP helperem) k dohledání vazby MAC adresy k IP adrese
	+ Aplikace s webovým rozhraním
	+ Snadné vyhledávání záznamů zadáním vyhledávacích kritérií (zdrojová IP adresa, časové rozmezí, identifikovaný uživatel)
	+ Držení záznamů min. 3 měsíce
* Software nebo zařízení pro logování provozu za účelem dohledatelnosti na úroveň koncového uživatele
	+ Detekce provozu z firewallu pomocí Syslog, IPFIX nebo Netflow
	+ Aplikace s webovým rozhraním
	+ Snadné vyhledávání záznamů zadáním vyhledávacích kritérií (zdrojová/cílová IP adresa, zdrojový/cílový port, časové rozmezí, identifikovaný uživatel)
	+ Držení záznamů min. 3 měsíce
* Software nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent) a odpovídající webové rozhraní, ve kterém je možné sledování realizovat
	+ Detekce provozu z firewallu pomocí IPFIX nebo Netflow
	+ Aplikace s webovým rozhraním
	+ Snadné vyhledávání záznamů zadáním vyhledávacích kritérií (zdrojová/cílová IP adresa, zdrojový/cílový port, časové rozmezí, identifikovaný uživatel)
	+ Držení záznamů min. 3 měsíce
* Systém pro monitorování funkčnosti síťové a serverové infrastruktury
	+ Monitoring síťových prvků (firewally, switche, AP)
		- Dostupnost síťových prvků (Ping)
		- Linkový stav portů a jejich datové přenosy (in/out, datové přenosy, počty validních a chybných paketů – SNMP)
	+ Monitoring serverů
		- Hardware (iLO, iDRAC – SNMP)
			* Zatížení CPU, teplota CPU a vstupního vzduchu
			* Stav a spotřeba PSU
			* Stav diskové skupiny RAID a jednotlivých fyzických disků
		- OS Windows (SNMP nebo agentem)
			* Zatížení CPU, obsazenost paměti
			* Vytížení a obsazenost diskových svazků
			* Stav automaticky spouštěných služeb systému (s možností filtrování ignorovaných na základě jejich jména)
		- OS Linux (SSH nebo agentem)
			* Zatížení CPU, obsazenost paměti
			* Vytížení a obsazenost diskových svazků
			* Stav automaticky spouštěných služeb systému (s možností filtrování ignorovaných na základě jejich jména)
		- Virtualizační hypervisor Hyper-V, VMware a Proxmox (SNMP, SSH nebo agentem)
			* Zatížení CPU, obsazenost paměti
			* Vytížení a obsazenost diskových svazků
			* Stav virtuálních serverů (s možností filtrování ignorovaných na základě jejich jména)
	+ Monitoring webových aplikací
		- Délka odezvy, návratový HTTP kód, návratová informace
	+ Aplikace s webovým rozhraním
	+ Konfigurace monitorovacích šablon, které budou obsahovat sledované parametry (budou nastaveny dodavatelem min. pro výše uvedené typy zařízení)
	+ Správcem definovatelná kategorizace priority zařízení (min. 3 úrovně nízká/střední/vysoká)
	+ Výrobcem připravená kategorizace závažnosti událostí s možností administrátorské změny (min. 3 úrovně nízká/střední/vysoká)
	+ Detekované události odesílané emailem (alerty) dle upravitelných pravidel pro různé kombinace priorit zařízení a závažnosti událostí, možnost opakovaného zasílání kritických situací, možnost stanovení eskalací (odesílání dalším osobám) při neřešeném problému, možnost potlačení problému (bez odesílání alertů), možnost plánování periodických nebo nahodilých údržbových oken k potlačení alertů (např. plánovaný výpadek služby, ignorování zvýšení provozu na portu během zálohování)
	+ Držení historie min. 3 měsíce
	+ Licence bez omezení počtu sledovaných zařízení a jejich parametrů
* Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.
	+ Captive portál, generování dočasných hostovských účtů/hesel
	+ Může být řešeno konfigurací WiFi řešení/controlleru nebo nastavením ve firewallu
* Centrální správa dodaných switchů, splňující požadavky:
	+ Webové rozhraní pro správu
	+ Zobrazení topologie a vzájemných uplinkových portů
	+ Plánování automatického zápisu konfigurace do konfigurace pro spuštění
	+ Plánování automatického zálohování konfigurace switchů
	+ Konfigurace názvů portů, VLAN a zvolení profilu připojeného zařízení (alespoň desktop, server, VoIP telefon, kamera, WiFi AP, switch)
	+ Upgrade firmware switchů
	+ Konfigurace prostřednictvím Web GUI (TLS 1.3), SSH v2 a REST API
* Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem (použitý jako forwarder)

Navržená softwarová či hardwarová řešení musí být nejen schopna splnit požadované schopnosti a vlastnosti, ale musí být zároveň dodavatelem nakonfigurována tak, aby je plnila.

Navržená softwarová či hardwarová řešení musí zahrnovat licence, které budou uvedené schopnosti a vlastnosti obsahovat minimálně po dobu udržitelnosti projektu (5 let od uzavření projektu – předpoklad - 2/2026).

Nedílnou součástí dodávky je dokumentace naplnění kritérií Standardu konektivity v podobě, kterou akceptuje poskytovatel dotace v Závěrečné zprávě o realizaci projektu.

# Příloha – Akceptační protokol

|  |  |  |
| --- | --- | --- |
| **Požadavek** | **Splňujeano/ne** | **Komentář, parametry** |
| **Dodávka hardware** |
| 1x Firewall HA cluster |  |  |
| 7x Switch typu A |  |  |
| 1x Switch typu B |  |  |
| **Konektivita školy k veřejnému internetu (WAN) - povinné parametry** |
| Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců. |  |  |
| Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality. |  |  |
| Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků. |  |  |
| Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.). |  |  |
| Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem |  |  |
| Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici |  |  |
| **Konektivita školy k veřejnému internetu (WAN) - doporučené parametry** |
| Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách. |  |  |
| Antivirová kontrola internetového provozu |  |  |
| **Vnitřní konektivita školy (LAN a WLAN) - společné povinné parametry** |
| Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém |  |  |
| **Vnitřní konektivita školy (LAN a WLAN) - povinné parametry pevné LAN** |
| Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3) 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.]. |  |  |
| **Vnitřní konektivita školy (LAN a WLAN) - společné doporučené parametry** |
| Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele. |  |  |
| Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase. |  |  |
| Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku. |  |  |
| **Doporučené bezpečnostní prvky projektu** |
| 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. |  |  |
| Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu. |  |  |
| Podpora vzdáleného přístupu (VPN). |  |  |
| **Závěr** |
| Dokumentace projektu v podobě použitelné pro Závěrečnou zprávu o realizaci projektu. |  |  |

# Obecné podmínky

Z povahy předmětu plnění v oblasti klíčových bezpečnostních síťových zařízení zadavatel vlastní analýzou rizik dospěl k závěru, že předmět plnění nesmí být nevyhovující z hlediska informační bezpečnosti, přičemž za nevyhovující považuje jakékoli plnění, které obsahuje technologie a/nebo klíčové prvky, vůči jejichž výrobcům vydal Národní úřad pro kybernetickou a informační bezpečnost Varování NÚKIB č. j. 3012/2018-NÚKIB-E/110 ze dne 17. prosince 2018 v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, které dle analýzy představují vysoké nebo kritické riziko.

<https://uohs.gov.cz/download/sbirky_rozhodnuti/dokumenty/2021_S0207.pdf>

<https://uohs.gov.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16528.html>