**Technická specifikace nabídky**

|  |
| --- |
| **1. Identifikační údaje zakázky** |
| Označení zakázky | **„ZŠ Nová Ves u Chotěboře - vnitřní konektivita školy a připojení k internetu “** |
| Zadavatel zakázky | Obec Nová Ves u Chotěboře, Nová Ves u Chotěboře 63, 582 73 |
| **2. Základní identifikační údaje o uchazeči** |
| Název: |  |
| Sídlo/místo podnikání: |  |
| IČ/DIČ: |  |
| Osoba oprávněna jednat za uchazeče: |  |
| Kontaktní osoba: |  |
| Tel.:  |  |
| E-mail: |  |
| **3. Technická specifikace nabídky** |
| **Parametr****Minimální hodnoty požadované zadavatelem****Uchazeč musí splnit tyto požadavky beze zbytku.** | **Vaše nabídka:** **uveďte bližší parametry Vaší nabídky – zda splňuje požadavek, technické parametry, název produktu, výrobce, typové označení, modelové označení, tam kde je to relevantní** |
| Security Gateway PRO, EU - **1 ks*** WAN – SFP/RJ45 1x Gigabit
* LAN – RJ45 4x Gigabit
* Propustnost 1Gbps/port
* Správa přes centrální software / dohledaní provozu, přípojení, vytížení
* CLI ovládání
* Podpora VLAN
* Aktivní FIREWALL
* Provedení RACKmount
 |  |
| Switch, L2/L3 - **1 ks*** 24x Gbps port
* 2x SFP+ 10Gbps port
* POE+ min. 500W
* Podpora VLAN
* Provedení RACKmount
 |  |
| AP 300+867 Mbps 2,4+5 Ghz, 802.11a/b/g/n/ac, 2x2 MIMO - **2 ks*** Operační mod AP
* Frekvence 2,4GB+5GB
* Normy 802.11a/b/g/n/AC
* MULTI SSID
* Správa přes centrální software
* Šifrování WEP,WPA-PSK, WPA – Enterprise (WPA/WPA2, TKIP/AES)
* LAN PORT 1x RJ45 – 1Gbps
* Napájení POE 802.3af
* LED indikace
 |  |
| HW Server – min. 3GHz CPU, HDD 512Gb, RAM 8Gb |  |
| Nástěnný rozvaděč jednodílný min. 12U - 1 ks |  |
| NAS Server min. 1,3GHz 512Mb RAM, 2x SATA - 1 ks |  |
| HDD 4TB NAS 128MB SATAIII 7200r - 2 ks |  |
| Zprovoznění, montáž centrálního směřovače, switchů, firewallu |  |
| Kabel CAT 6 LSOH Šířka pásma:min 250 MHz - 300 m |  |
| Veřejné IP adresy 4x IPv4 |  |
| Elektroinstalační lišta 40x40 - 20 m |  |
| Datová zásuvka - 20 ks |  |
| keystone cat6 - 40 ks |  |
| Patch panel 24p. CAT6 1U,4x6 LSA, 19“ – 1 ks |  |
| Montážní práce, tažení kabelů, zapojení zásuvek |  |
| Montáž do rozvaděče, 12U - 1ks |  |
| Zatažení optického kabelu do ochranné trubky - 50 m |  |
| Terminál ONT GPON 1 ks |  |
| Průrazy 10 ks |  |
| Svár opt. vlákna - 4 vl.  |  |
| Optický kabel 12 vl. - SM - 50 m |  |
| Optická vana 1U - 12 pozic - 4 ks |  |
| Antivirový software pro 25 stanic na 5 roků |  |
| Materiál - lišta 40x20 - 50 m |  |
| ochrana sváru - 4 ks |  |
| **Celkový soulad a standard konektivity** |  |
| Nabídka je v souladu s technickým popisem požadovaného řešení, který je uveden dále v této příloze, a umožní dosažení všech cílových parametrů, které jsou v tomto popise uvedeny.Zajištění vnitřní konektivity školy musí splňovat Standard konektivity škol Integrovaného regionálního operačního programu - viz popis v další části této přílohy. |  |
| **Ostatní požadavky** |
| Bezpečnostní předpisy | Musí vyhovovat všem platným bezpečnostním normám a předpisům. |  |
| Doprava a manipulace | Součástí dodávky bude doprava, vyložení/složení, manipulace, dopravení zboží do určených učeben.  |  |
| Montáž a instalace u objednatele včetně uvedení do provozu | Součástí dodávky bude montáž, instalace, konfigurace, uvedení do provozu dodávaného zboží včetně všech potřebných prací. Součástí dodávky bude zapojení všech prvků do relevantních školních sítí, odzkoušení všech funkcí.  |  |

V ……….........………..dne ..........................

 ………………………………............ Podpis, razítko

 Titul, jméno, příjmení

**technickÝ POPIS POŽADOVANÉHO ŘEŠENÍ**

**Technické parametry výchozího a cílového stavu školní síťové infrastruktury ZŠ Nová Ves u Chotěboře**

**Aktuální stav konektivity**

Připojení do WAN – nyní v počítačové učebně –bezdrátový spoj wi-fi 5,4 GHz.

LAN v učebně řešena 15x 100Mbit – Cat5 - více než deset let stará kabeláž.

Dále do některých zásuvek vedou kabely Cat5 – jeden kabel na 2 RJ45 zásuvky, degradace sítě.

Po škole jsou malé switche 5/8port zajišťující možnost připojení do sítě LAN.

Wifi síť je tvořena osmi přístupovými body, které jsou zabezpečeny jen WPA2 heslem bez možnosti zaznamenání o připojení a malou propustností sítě do 10 Mb.

Škola nemá doménový server ani firewall.

**Navrhované řešení**

Připojení do WAN – modernizace na připojení optikou technologii GPON včetně podpory protokolu IPv6 (řešeno mimo projekt)

Zajištění monitoringu IP, datových toků pomocí hardwarového firewallu na úrovni LAN i WAN. (centrální databáze identit AD, logování přístupů do sítě)

Splnění parametrů projektu: minimální konektivita stanic 50Mbps, minimální konektivita serveru 1Gbps, páteřní rozvody mezi budovami pomocí optický vláken či Cat.6, Aktivní prvky splňující parametry projektu. Podpora 802.1Q VLAN, podpora 802.1X, podpora radius based MAC autentizace

WI-FI splňující parametry projektu:

současná funkce AP v pásmu 2,4 a 5 Ghz, multi SSID, PoE, WPA2, ACL.

**Cílový stav konektivity dle standardu IROP**

**a) Konektivita školy k veřejnému internetu (WAN)**

|  |  |
| --- | --- |
| **Parametr dle standardu**  | **Způsob naplnění parametru**  |
| podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení | Řešeno v rámci projektu pořízením nového firewallu.  |
| logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)  | Řešeno v rámci projektu pořízením nového zařízení pro správu přístupu do sítě |
| síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality | Řešeno v rámci projektu pořízením nového zařízení pro správu přístupu do sítě. |
| 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 | Bude splněno pořízením nového firewallu s odpovídajícími parametry/funkcemi.  |
| možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků | Řešeno v rámci projektu pořízením nového zařízení pro správu přístupu do sítě. |

**b) Vnitřní konektivita školy (LAN)**

|  |  |
| --- | --- |
| **Parametr dle standardu**  | **Způsob naplnění parametru**  |
| **Povinné minimální bezpečnostní parametry (bez ohledu na 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 | Řešeno v rámci projektu pořízením nového zařízení pro správu přístupu do sítě. |
| 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. | Řešeno v rámci projektu pořízením nového zařízení pro správu přístupu do sítě. |
| logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel | Řešeno v rámci projektu pořízením NAS serveru. |
| **Povinné minimální parametry v oblasti pevné LAN** |
| Minimální konektivita stanic a dalších koncových zařízení 100Mbit/s fullduplex | Bude instalována kabeláž typu CAT 6 LSOH Šířka pásma:min 250 Mhz a nový switch. |
| Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…) | Bude instalována kabeláž typu CAT 6. |
| Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex | Řešeno v rámci projektu pořízením nového switche. |
| Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ) | Rozvody budou realizovány prostřednictvím optických a metalických vláken (kabelů).  |
| Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[[1]](#footnote-1) s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,… | Bude pořízen nový firewall a switch. |
| **Povinné minimální parametry v oblasti bezdrátových sítí (wifi)** |
| Podpora mechanismu izolace klientů | Zabezpečí nové zařízení pro správu přístupu do sítě |
| Návrh topologie wifi 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 | Viz návrh topologie. Signálem wi-fi bude pokryta celá budova školy. Konzistence bude dosaženo prostřednictvím nového zařízení pro správu přístupu do sítě. |
| 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) | Zabezpečí nové zařízení pro správu přístupu do sítě |
| Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …) | Bude zajištěno prostřednictvím serveru. |
| Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz | Budou zabezpečovat nové AP. |
| Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu | Budou zabezpečovat nové AP. |
| **Doporučené parametry** |
| Minimálně pasivní zapojení[[2]](#footnote-2) 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. |  |

**3) Další bezpečnostní prvky**

|  |  |
| --- | --- |
| **Parametr dle standardu**  | **Způsob naplnění parametru**  |
| Identity management systémy (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů | Umožní nový server. |
| Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)  | Umožní nový server. |
| Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase) | Umožní nové zařízení pro správu přístupu do sítě |
| 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)) | Řešeno v rámci projektu pořízením nového zařízení pro správu přístupu do sítě |
| Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie | Umožní nové zařízení pro správu přístupu do sítě |
| Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management) | Umožní nové zařízení pro správu přístupu do sítě. |
| Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga) | Umožní nové zařízení pro správu přístupu do sítě. |
| Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk) | Umožní nové zařízení pro správu přístupu do sítě. |
| Nástroje pro centrální správu a audit ICT prostředků | Umožní nové zařízení pro správu přístupu do sítě. |
| Systémy zálohování a obnovy dat serverové infrastruktury | Umožní nové zařízení pro správu přístupu do sítě. |
| Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů | Umožní nové zařízení pro správu přístupu do sítě. |
| Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp. | Umožní nový firewall. |
| Podpora vzdáleného přístupu (VPN) | Umožní nové zařízení pro správu přístupu do sítě. |

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 architekturou přepínacího subsystému* [↑](#footnote-ref-1)
2. *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-2)