PROJEKTOVÁ DOKUMENTACE

Základní škola

Pod Vodojemem 323/3A, 400 10 Ústí nad Labem

Č.PD: D1.4.c - Konektivita

MODERNIZACE UČEBNY PRO PŘÍERODNÍ VĚDY, TECHNICKÉ A ŘEMESLNÉ OBORY NA ZŠ POD VODOJEMEM, ÚSTÍ NAD LABEM

TECHNICKÁ ZPRÁVA

01/2020

PŘÍLOHA EK-01

Jednatel společnosti: Ing. Zdeněk Honska, Ing. Martin Kučera

DataSOFT, spol. s r.o., Kadaňská 2226, 430 03 Chomutov, tel.: 477012016, fax: 477012017

Obsah:

1 Základní údaje - zadavatel

akce:	*Zpracování projektové dokumentace pro část „Zajištění vnitřní konektivity“ v rámci výzvy 92 IROP „INFRASTRUKTURA ZÁKLADNÍCH ŠKOL PRO UHELNÉ REGIONY“.*
objekt:	*Základní škola, Pod Vodojemem 323/3A, 400 10 Ústí nad Labem*
část:	*E - ELEKTROINSTALACE SLABOPROUD*
charakter stavby:	*REKONSTRUKCE*
kraj:	*ÚSTECKÝ*
místo stavby:	*Ústí nad Labem*
stavební úřad:	*Ústí nad Labem*
investor:	*STATUTÁRNÍ MĚSTO ÚSTÍ NAD LABEM*
projektant:	*VARIA s.r.o., Rooseveltova 1804/2, Ústí nad Labem*
zhotovitel části:	*DATASOFT, SPOL. S R.O.*

2 Základní údaje – zhotovitel PD

obchodní jméno:	*DATASOFT, spol. s r.o.* *zapsána v Obchodním rejstříku u Krajského soudu v Ústí nad Labem, v oddíle C, složce 3660*
sídlo:	*Kadaňská 2226, 430 03 Chomutov*
telefon:	*+420477012016*
fax:	*+420477012017*
e-mail:	*honska@datasoft.cz*
IČO:	*47310405*
DIČ:	*CZ47310405*
banka:	*Komerční banka, a.s. – pobočka Chomutov*
č.ú.:	*2117860257/0100*

3 ÚVOD

Dokumentace řeší návrh vhodné infrastruktury pro Základní školu Pod Vodojemem 323/32A, Ústí nad Labem, s cílem splnit zadání výzvy č. 92 IROP – Infrastruktura základních škol pro uhelné regiony. Tato část projektové dokumentace řeší osazení aktivních prvků síťové infrastruktury tak, aby byly splněny požadavky zejména v oblasti bezpečnosti a požadované výkonové parametry.

3.1 POUŽITÉ PODKLADY

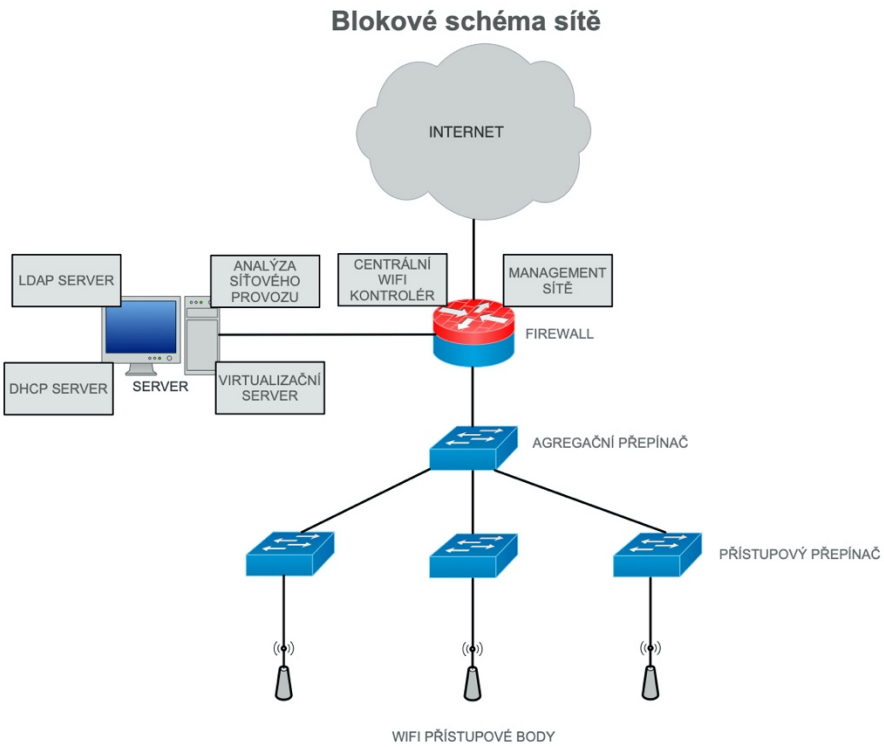
Projektová dokumentace ZŠ Pod Vodojemem 323/3A, Ústí nad Labem – STRUKTUROVANÁ KABELÁŽ V OBJEKTU č. D.1.4.b
Požadavky investora
Požadavky dle IROP č. 92

4 TECHNICKÉ ŘEŠENÍ

4.1 Popis technického řešení

Navržená síťová infrastruktura se skládá z následujících částí:

- *Firewall*
- *Agregační přepínač*
- *Přístupové přepínače*
- *Bezdrátové přístupové body*
- *Management sítě*
- *Analýza síťového provozu (virtuální appliance)*
- *Serverové a virtualizační prostředí*



Technické řešení je postaveno na síťových zařízeních, která jsou centrálně spravována. Toto řešení poskytuje funkční, centralizovanou a intuitivní správu s možností dalšího rozšiřování v budoucnu.

Každé zařízení (agregační přepínač, přístupové přepínače, bezdrátové přístupové body) bude spravováno centrálně prostřednictvím firewallu. Toto řešení poskytuje možnosti centrální správy, správu bezpečnostních politik a konfiguraci v reálném čase. Veškeré činnosti se provádějí v management konzoli firewallu, která je spuštěna v internetovém prohlížeči.

4.2 Aktivní prvky, Wi-Fi, UTM, monitoring

Navržené řešení používá pro připojení koncových klientů a zařízení centrálně řízené L3 přístupové přepínače typ 2 – 6, s podporou IPv4/IPv6, a to ve verzích s 24 nebo 48 GbE porty. Přepínače jsou také vybaveny buď čtyřmi SFP+ 10 GbE nebo čtyřmi SFP 1 GbE porty pro připojení do páteřní sítě. Přepínače podporují standard 802.3af/at pro napájení připojených zařízení, např. bezdrátových přístupových bodů nebo VoIP terminálů.

Přístupové přepínače typ 2 - 6 jsou připojeny do centrálně řízeného L3 agregačního přepínače typ 1. Jedná se o přepínač, který disponuje 24-ti SFP+ 1/10 GbE porty Jedná se o L3 přepínač s podporou směrování a dual stacku IPv4 a IPv6.

Všechny navržené přepínače umožňují klasifikaci síťového provozu až na úrovni L7.

Podrobné požadované parametry všech přepínačů jsou uvedeny ve výkazu výměru (Příloha projektové dokumentace č. EK-03).

Pro vytvoření bezdrátové infrastruktury jsou navrženy centrálně řízené přístupové body. Přístupové body jsou navrženy ve dvou variantách:

- *WIFI přístupový bod typ 1 je přístupový bod se dvěma nezávislými radiovými částmi, které pracují ve frekvenčních pásmech 5 a 2,4 GHz, 2x2:2. Zařízení podporuje standard 802.11ac (5 GHz) a 802.11n (2,4 GHz). Zároveň obsahuje radiovou část s Bluetooth. Agregovaná propustnost je max. 1,2 Gbps. Pro připojení do LAN je zařízení vybaveno jedním 10/100/1000 Base-T portem s podporou napájení PoE. Zařízení umožňuje klasifikaci síťového provozu až na úrovni L7. Max. počet klientů na jedno zařízení je 512.*
- *WIFI přístupový bod typ 2, je přístupový bod se dvěma nezávislými radiovými částmi, které pracují ve frekvenčních pásmech 5 a 2,4 GHz, 4x4:4. Zařízení podporuje standard 802.11ac (5 GHz) a 802.11n (2,4 GHz). Neobsahuje radiovou část s Bluetooth. Agregovaná propustnost je max. 2,5 Gbps. Pro připojení do LAN je zařízení vybaveno dvěma 10/100/1000 Base-T porty s podporou napájení PoE. Zařízení umožňuje klasifikaci síťového provozu až na úrovni L7. Max. počet klientů na jedno zařízení je 512.*

Podrobné požadované parametry obou typů WIFI přístupových bodů jsou uvedeny ve výkazu výměru (Příloha projektové dokumentace č. EK-03).

Pro zajištění bezpečnosti a pro připojení celé sítě k Internetu je navržen bezpečnostní prvek Next Generation Firewall s těmito funkcionalitami:

- *Firewall s hloubkovou analýzou paketů na úrovni L7 (FW, DPI)*
- *Antivirus (AV, včetně skenování archivních souborů)*
- *Intrusion Prevention System (IPS)*
- *Application Controll Systém (ACS, včetně kategorizace aplikací)*
- *Antispam (AS, s možností přidávání vlastních pravidel, whitelist/blacklist)*
- *Filtrování obsahu internetových stránek na základě jejich kategorizace*

- *Kontrola obsahu protokolů zabezpečených SSL (s možností vyloučení kontroly na základě kategorizace stránek - např. bankovnictví a zdravotní péče)*
- *Plná podpora IPv6 včetně všech výše uvedených UTM funkcionalit, a to současně s podporou IPv4 (dual stack)*
- *Podpora SSL, nebo IPSec VPN*
- *Kontrola datového toku z VPN pomocí UTM funkcí*
- *Podpora QoS*
- *Podpora VLAN (802.1Q)*
- *Podpora zabezpečení přístupu do počítačové sítě (802.1X)*
- *Podpora autentizace založené na protokolu RADIUS*
- *Podpora autentizace založené na integraci s Active Directory (SSO)*
- *Podpora autentizace zařízení prostřednictvím RADIUS serveru pomocí MAC adresy*
- *Podpora řízení průtoku dat (rate limiting, traffic shaping apod.)*
- *Podpora přenosu paketů DNSSEC (větší oproti DNS)*
- *Podpora SNMP*
- *Podpora synchronizace času NTP*

Zařízení bude vybaveno minimálně:

- *2x 10 GbE SFP+ porty*
- *18x GbE RJ45 porty*
- *8x GbE SFP porty*
- *1x USB port*
- *1x konzolový port*

Propustnost zařízení je min. 18 Gbps.

Součástí dodávky bezpečnostního prvku je Sandbox. Jedná se o cloudové řešení pro detekci hrozeb s dynamickou analýzou k identifikaci neznámého škodlivého SW.

Podrobné požadované parametry bezpečnostního prvku jsou uvedeny ve výkazu výměru (Příloha projektové dokumentace č. EK-03).

Komplexní monitoring sítě bude řešen v modulu, který je instalován jako virtuální appliance na serveru. Jedná se o zařízení pro sběr logů, analýzu a reporting provozu v LAN, integrované do jednoho uceleného systému, poskytující centralizované analýzy bezpečnostních událostí, forenzní výzkum, reporting, archivaci obsahu, těžbu dat, karanténu škodlivých souborů a posouzení zranitelnosti. Kapacita úložného prostoru pro uchování logů a ostatních dat musí dostačovat min. na 2 měsíce kontinuálního sběru všech dat a zařízení musí vyhovovat požadavkům, které jsou uvedeny v dokumentu „Prokázání a kontrola naplnění standardu konektivity ve výzvách IROP (infrastruktura základních a středních škol).“

4.3 Topologie, konfigurace

Topologie LAN je hvězda. Přesná topologie je zřejmá z blokového schématu (Příloha projektové dokumentace č. EK-02).

Přístupové přepínače typ 2 - 6 budou připojeny do optické páteře jedním SM FO uplinkem, nebo v případě UTP páteře, jedním 1000Base-T uplinkem. Pro tento účel budou v přepínačích instalovány transceivery SFP 1GbE LX nebo 1GbE TX. Transceivery budou do páteřní FO sítě připojeny prostřednictvím SM patchcordů s LC konektory. V případě UTP páteře budou použity UTP patchcordy s RJ45 konektory. V případě, že v jednom rozvaděči bude instalováno několik hraničních přepínačů, budou mezi sebou propojeny stohovacími kabely a do páteřní sítě bude připojen pouze jeden z nich.

Na přepínačích v LAN budou nakonfigurovány následující VLAN, do nichž budou zařazeny jednotlivé porty a to na základě zařízení, které k nim bude připojeno a služeb, které budou poskytovat:

- ***VLAN1** – management VLAN – pro správu a konfiguraci přepínačů. Do této VLAN budou mít přístup pouze IT správci.*
- ***VLAN9** – zaměstnanecká a pedagogická VLAN. Do této VLAN budou mít přístup pouze pedagogové a zaměstnanci školy a bude určena pro oddělení provozu od části LAN určené pro žáky a učebny.*
- ***VLAN29** – výuková VLAN – prostřednictvím této VLAN budou mít přístup do LAN koncová zařízení umístěná v učebnách (počítače, periférie, ……).*
- ***VLAN39** – žákovská VLAN – jedná se o část LAN, do které budou mít přístup žáci školy prostřednictvím svých osobních zařízení. Tato VLAN bude směrována přímo do Internetu a nebude možné skrze ni přistupovat k jakýmkoliv zdrojům v LAN školy.*
- ***VLAN49** – Guest VLAN – VLAN určená pro hosty. Přístup do VLAN pouze pro hosty, která bude směrována přímo do Internetu. Přístup do této VLAN bude řízen Captive Portalem.*
- ***VLAN59** - kamery – VLAN určená pro připojení kamer kamerového systému*
- ***VLAN69** – zařízení pro docházkový systém. V této VLAN budou zařízení, která kontrolují přístup do objektu.*
- ***VLAN99** – pro neautentifikovaná zařízení, nebo pro zařízení nepodporující autentifikaci*

Bezdrátová infrastruktura bude realizována přístupovými body typ 1 a 2. Přístupové body budou připojeny do hraničních přepínačů prostřednictvím 1000Base-T portu (RJ45) s použitím metalických UTP patchcordů. Napájení přístupových bodů bude provedeno z přístupových přepínačů prostřednictvím PoE 802.1af/at.

V bezdrátové WLAN budou nakonfigurovány následující bezdrátové sítě s názvy SSID:

- ***WIFI_ZS_POD_VODOJEMEM** – jedná se o WLAN, ze které jsou na základě ověření z RADIUS serveru uživatelé automaticky přiřazeni do konkrétních VLAN.*
- ***Host** – WLAN pro hosty. Zajistí připojení do Internetu pro hosty. Provoz z této části WLAN bude směrován přímo do Internetu, zdroje umístěné ve školní LAN budou neviditelné a tudíž nedostupné. Obsluha této WLAN bude řízena Captive Portalem z bezpečnostního prvku.*

Ve Wi-Fi síti, bude řešení poskytovat následující minimální funkcionality:

- *Centrální správa Wi-Fi sítě*
- *Centrálně spravované přístupové body*
- *Centrálně řízený upgrade firmwaru přístupových bodů*
- *Detekce stavu signálu a rušení na jednotlivých kanálech*
- *Automatické ladění kanálů a výkonu*
- *Podpora technologií usnadňujících a urychlujících přechod klientů mezi jednotlivými AP*
- *Podpora izolace klientů*
- *WPA2*
- *PoE*
- *Podpora více SSID na jednom rádiu*
- *Současný provoz AP v pásmu 2,4GHz a 5GHz*
- *Podpora standardu 802.11ad a novějších*
- *Systém správy přístupu hostů (jednorázová, krátkodobá hesla, captive portál)*

Pro ověření přístupu do sítě bude provedena konfigurace ověřování na bázi 802.1x. Pedagogičtí pracovníci, zaměstnanci školy a žáci, budou ověřeni na RADIUS serveru – Active Directory. Na serveru bude instalován OS Microsoft Windows Server Std 2019. Na tomto serveru budou uživatelské účty pedagogů, zaměstnanců a žáků školy. Ostatní entity v LAN, které se nemohou prokázat uživatelským účtem (tiskárny a ostatní periferie) se budou prokazovat svou MAC adresou a port, ke kterému budou připojeny, bude nakonfigurován pro tuto MAC adresu. Na OS Windows Server Std. 2019 bude na službě HyperV nakonfigurován virtuální stroj, na kterém bude provedena instalace modulu pro monitoring a analýzu síťového provozu celé sítě, vč. sběru logů.

Správa IP adresního prostoru a přidělování IP adres klientům bude realizováno prostřednictvím lokálního DHCP serveru, který bude zprovozněn v rámci OS MS Windows Server Std. 2019. Přidělování IP adres klientům v LAN bude prováděno dynamicky z interního IP prostoru, pro který bude na DHCP serveru alokována část neveřejné IP podsítě třídy B.

4.4 Konektivita - hodnocení

Stávající připojení k Internetu je realizováno mikrovlnným spojem. ZŠ je do Internetu připojena přenosovou rychlostí 40/20 Mbps (download/upload). Ve vztahu k doporučením Standardu konektivity, se jedná o nevyhovující hodnotu. Požadavek definovaný ve Standardu konektivity určuje, že potřebná kapacita připojení do Internetu, je v případě zavedení BYOD 128 kbps na žáka. Škola má v současné době 510 žáků. ***Potřebná kapacita je tedy 65 Mbps, což je vzhledem k aktuální kapacitě připojení nedostačující hodnota.***

5 Vnější vlivy

Prostředí v prostorách objektu dle ČSN 33 2000-3 je normální. Těmto podmínkám odpovídá i výběr jednotlivých prvků (odpovídající krytí).

5.1 Vliv na životní prostředí

Všechna zařízení navržená pro instalaci, splňují hygienické normy a nemají žádný vliv na okolní životní prostředí. Veškeré odpady vzniklé při montáži budou ekologicky zlikvidovány na náklady montážní firmy.

6 ZÁVĚR

V případě změn nebo doplňků provede dodavatel projektu na základě dodaných podkladů dodatek k projektové dokumentaci. Při provozu zařízení je uživatel povinen dodržovat pravidla a postupy uvedené v návodu k údržbě vydané výrobcem.

Při užívání systému je nutno dodržet všechny platné předpisy a normy, včetně návodů k použití zařízení, která zpracoval výrobce.