MINISTERSTVO ŠKOLSTVA,
VEDY, VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

SWAN

Projekt: EDUNET_SK

DETAILNÝ POPIS RIEŠENIA IMPLEMENTÁCIE SLUŽIEB

Analýza a návrh

Obsah

1 Úvod

1.1 Identifikácia a určenie

Tento dokument obsahuje spracovanie detailného návrhu architektúry a funkčného riešenia projektu EDUNET_SK a tiež definovanie služieb, poskytovaných týmto riešením. DPR popisuje aj rozhrania na súvisiace informačné a komunikačné systémy.

Ministerstvo školstva, vedy, výskumu a športu SR a spoločnosť SWAN, a.s. zodpovedajú za to, že nedôjde k zneužitiu tohto Detailného popisu riešenia (DPR) projektu EDUNET_SK, resp. že neposkytnú tento DPR tretím osobám a zachovajú mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedeli pri vypracovaní tohto DPR."

1.2 Zmenový list

Verzia	Dátum	Popis zmien
1.0	12.4.2019	Vytvorenie dokumentu
1.1	7.5.2019	Zapracovanie pripomienok č. 1 až 12 zo dňa 30.4.2019
1.2	20.5.2019	Zapracovanie pripomienok zo dňa 15.5.2019
1.3	19.11.2019	Návrh zmien riešenia vo viacerých oblastiach a došpecifikovanie niektorých detailov

1.4	26.11.2019	Došpecifikovanie štruktúry a operácii nad adresárovou štruktúrou používateľov, zmenené Kapitoly 3.4 a 5

Tabuľka č. 1 Zmenový list

1.3 Skratky

Skratka	Vysvetlenie
AAA	Authentication, Authorization, and Accounting
AD	Active Directory
AD DS	Active Directoer Domain Services
ACL	Access Control List
BYOD	Bring Your Own Device
CA	Certifikačná Autorita
CPE	Customer-Premises Equipment (v tomto dokumente smerovač na lokálnej infraštruktúre školy)
DC	Dátové centrum
DEO	Digitálny edukačný obsah
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPR	Detailný popis riešenia
DUD	Digitálne učivo na dosah
FW	Firewall
IAM	Rezortný IAM
HTTP	Hypertextový prenosový protokol
HTTPS	Zabezpečený hypertextový prenosový protokol
HW	Hardvér
IAM	Identity Access Management
IKT	Informačné a komunikačné technológie
IS	Informačný systém
ISP	Poskytovateľ služieb internetu
IT	Informačné technológie
LAN	Local Area Network
MŠVVaŠ	Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky
PoE	Power over Ethernet
RIS	Rezortný informačný systém
SLA	Service Level Agreement
SM	Security Management
SSID	Service Set Identifier
SSO	Single Sign-on
SW	Softvér
TLS	Transport Layer Security
TTM	Trouble Ticket Management

Tabuľka č. 2 Použité skratky

1.4 Zoznam obrázkov

1.5 Zoznam tabuliek

1.6 Zámer riešenia

1.6.1 Biznis zámer projektu

Projekt EDUNET_SK je zameraný na poskytovanie telekomunikačných, dátových služieb a služieb centrálneho manažmentu virtuálnej privátnej siete so zadefinovanou úrovňou servisných služieb a zadefinovanými bezpečnostnými štandardami pripojenia pre základné a stredné školy, materské školy a vybrané školské zariadenia. Projekt EDUNET_SK je prioritne určený pre školy, v ktorých prebieha sústavná príprava na povolanie a ktoré vo vyučovacom procese aktívne využívajú prácu s digitálnymi technológiami a digitálnym vzdelávacím obsahom. Projekt je určený aj pre vybrané školské zariadenia, v ktorých sa aktívne využívajú digitálne technológie. Účelom projektu je podporiť distribúciu digitálneho vzdelávacieho obsahu, podporiť elektronické testovanie žiakov a zabezpečiť prístup k Internetu s centrálnym manažmentom siete. V rámci tohto projektu budú na väčšine lokalít inštalované telekomunikačné zariadenia.

1.6.2 Technologický zámer projektu

Zámerom projektu je vybudovanie vysokorýchlostnej, bezpečnej prístupovej siete a implementácia centralizovaného systému riadenia prístupu k existujúcemu digitálnemu edukačnému obsahu v IT infraštruktúre MŠVVaŠ.

1.7 Cieľ riešenia

Cieľom projektu EDUNET_SK je vybudovať jednotnú komunikačnú infraštruktúru pre materské, základné a stredné školy a vybrané školské zariadenia na Slovensku (ďalej spoločne nazývané školské lokality). Riešenie EDUNET_SK v súlade s konceptom informatizácie a digitalizácie rezortu školstva zabezpečí:

- Vytvorenie MPLS VPN siete úrovne L3 pripájajúcej lokality s cieľom zabezpečiť komunikáciu zo škôl na zdroje umiestnené v Dátovom centre rezortu školstva.
- Centralizovaný riadený spoločný prestup pre všetky školské lokality do siete Internet.
- Prístup do siete EDUNET_SK pre jednotlivé školy prostredníctvom technológie s najvyššou priepustnosťou, ktorá je dostupná v danej geografickej lokalite.
- Bezdrôtový, centrálne spravovaný prístup z mobilných zariadení prostredníctvom technológie WiFi do sietí na školách.
- Prevádzku služieb filtrovania obsahu z Internetu aplikovaných podľa definovaných politík s dynamickým manažmentom.
- Centralizované riešenie DDoS ochrany a elimináciu útokov z Internetu.
- Monitoring a reporty prevádzky do a z Internetu.
- Spoločný dohľad nad sieťami a IKT prostriedkami inštalovanými v rámci projektu EDUNET_SK na lokalitách.
- Manažment internej sieťovej prevádzky medzi školami a Dátovým centrom rezortu školstva.
- Integráciu škôl pripojených konektivitou od tretích strán (napr. SANET alebo ekvivalentných operátorov, príp. iných operátorov zazmluvnených školami).

2 Špecifikácia požiadaviek

2.1 Funkčné požiadavky

Riešenie EDUNET_SK je koncipované a navrhnuté tak, aby zabezpečovalo nasledovné funkčné požiadavky:

- Centrálny riadený prístup k digitálnym službám a digitálnemu edukačnému obsahu podľa role pridelenej jednotlivým používateľom.
- Centrálne riadenie a možnosti integrácie a prepojenia rezortných a medzirezortných zdrojov.
- Centrálne riadenie základnej bezpečnosti na školách.
- Registrovanie a zapojenie inštitucionálnych zariadení, ktoré budú môcť využívať prístupy k zdrojom v rámci riešenia EDUNET_SK.
- Sprístupnenie zdrojov a konektivity pre vlastné digitálne zariadenia oprávnených používateľov v rozsahu riešenia EDUNET_SK.
- Centrálny riadený prístup k digitálnym službám z Internetu na základe pridelenej role jednotlivým používateľom.

2.2 Technické požiadavky

Pre splnenie funkčných požiadaviek bolo riešenie EDUNET_SK technologicky koncipované ako centralizované riešenie s vysokou dostupnosťou, bezpečnosťou a otvorenosťou pre požiadavky na rozšíriteľnosť. Kapitola detailnejšie popisuje požiadavky na nasledovné časti:

- Komunikačná infraštruktúra riešenia EDUNET_SK.
- Centrálna časť EDUNET_SK.
- Integrácia na IS systémy mimo EDUNET_SK.
- Pripojenie koncových lokalít do EDUNET_SK.

2.2.1 Komunikačná infraštruktúra riešenia EDUNET_SK

Technické požiadavky v časti komunikačná infraštruktúra pokrývajú hlavne nasledovné kľúčové oblasti a služby poskytované v rámci riešenia EDUNET_SK:

- Poskytnutie zabezpečeného pripojenia do komunikačnej infraštruktúry EDUNET_SK s garantovanou úrovňou poskytovania služieb (ďalej len „SLA“) pre školy.
- Zabezpečenie dátovej komunikácie s Dátovým centrom rezortu školstva.
- Poskytnutie centralizovaného, riadeného, zabezpečeného a monitorovaného prístupu do siete Internet.

Základným funkčným stavebným prvkom EDUNET_SK architektúry je virtuálna privátna VPN MPLS sieť L3 úrovne prepájajúca Dátové centru rezortu školstva, školy (primárne základné a stredné, s možnosťou pripojenia materských škôl a vybraných školských zariadení) a Centrálnu časť EDUNET_SK.

Primárny dôraz pri návrhu a implementácií komunikačnej infraštruktúry riešenia EDUNET_SK je kladený hlavne na:

- bezpečnosť riešenia,
- vysokú mieru dostupnosti poskytovaných služieb,
- rozšíriteľnosť riešenia.

Dátové pripojenie Centrály EDUNET_SK do MPLS VPN EDUNET_SK je na úrovni 20 Gbit/s s možnosťou rozšírenia na 40 Gbit/s. Dátové pripojenie Centrály EDUNET_SK do Internetu je na úrovni 10 Gbit/s s možnosťou rozšírenia podľa vyťaženia na 40 Gbit/s.
Pre každú pripojenú lokalitu je rezervovaná v centrálnom IPv4 NAT systéme jedna verejná IPv4 adresa.

2.2.2 Centrálna časť EDUNET_SK

Riešenie je koncipované ako centralizované. Z toho dôvodu Centrálna časť poskytuje kľúčovú funkcionalitu potrebnú pre prevádzku a poskytovanie služieb garantovaných projektom EDUNET_SK. Centrálna časť je umiestnená v lokalitách poskytovateľa služby a spĺňa minimálnu dostupnosť 99,9 %.

Funkcionalita poskytovaná Centrálnou časťou zabezpečuje nasledovné služby:

- Centrálne riadenie sieťovej prevádzky.
- Overovanie prístupu do siete EDUNET_SK.
- Centrálne riadenie WiFi prístupu.
- Centrálny monitoring IKT prostriedkov zabezpečujúcich prevádzku služieb riešenia EDUNET_SK.
- Centrálne zbieranie udalostí o aktivitách jednotlivých popoužívateľov siete EDUNET_SK
- Centrálna správa IKT prostriedkov zabezpečujúcich prevádzku služieb riešenia EDUNET_SK na koncovej lokalite.
- Riešenie na zabezpečenie podpory a zber nových požiadaviek (Service Desk).

2.2.2.1 Centrálne riadenie sieťovej prevádzky

Využitím centrálneho komponentu na riadenie sieťovej prevádzky je možné riadiť a kontrolovať celú dátovú prevádzku smerujúcu z a do siete EDUNET_SK. Dátová prevádzka ukončovaná alebo smerovaná mimo sieť EDUNET_SK je vždy riadená, filtrovaná a zabezpečovaná viacerými spôsobmi. Zároveň sa zbierajú štatistiky a záznamy využiteľné pre spätné vyhodnotenie udalostí.

Riadenie dátovej prevádzky umožňuje reguláciu poskytovanej šírky prenosového pásma na základe typu prevádzky, časového obdobia a profilu prideleného pre jednotlivé školy.

Filtrovanie dátovej prevádzky umožňuje sprístupňovanie alebo obmedzenie zdrojov na základe typu zdroja (web stránka), časového obdobia, WiFi SSID a profilu prideleného jednotlivému používateľovi.

Zabezpečenie dátovej prevádzky umožňuje odfiltrovanie detekovateľnej škodlivej činnosti s využitím systému IPS (detekcia na základe black listov, detekcia a mitigácia známych útokov).

2.2.2.2 Overovanie prístupu do siete EDUNET_SK

Prístupy do siete EDUNET_SK sú overované voči systému prevádzkovanému MŠVVaŠ SR, ktorý zabezpečuje jednotné prihlasovanie do informačných systémov rezortu (ďalej len „IAM“). Na základe atribútov používateľa je pridelený profil dátovej prevádzky a dátová prevádzka je následne realizovaná v súlade s pravidlami nastavenými v rámci profilu (dostupné dátové zdroje, spôsob filtrovania dátovej prevádzky).

2.2.2.3 Centrálne riešenie WiFi prístupu do EDUNET_SK

Riešenie EDUNET_SK je koncipované ako centralizované. Centralizácia zahŕňa aj správu a riadenie WiFi koncových zariadení v pripojených lokalitách z centrálnej časti EDUNET_SK. Riešenie má nasledovné vlastnosti:

- Riadiaci systém je dimenzovaný na maximálnu kapacitu 15 000 bezdrôtových prístupových bodov.
- Riadiaci systém WiFi koncových zariadení nesmeruje dátovú prevádzku, stará sa iba o funkcionality relevantné k riadeniu WiFi koncových zariadení. V riadiacom systéme sú uchovávané a spracovávané len štatistické informácie potrebné k prevádzke a tvorbe reportov o prevádzke.
- Komunikácia medzi riadiacim systémom a bezdrôtovým bodom je kryptovaná protokolom AES 256 a vyšším pre potreby konfigurácie, prenos sieťových štatistík a update firmwaru bezdrôtových prístupových bodov a je oddelená od dátovej prevádzky.
- Dostupnosť riadiaceho systému je na úrovni minimálne 99,9 %.
- V prípade dostupnosti novej funkcionality dodanej výrobcom na WiFi prístupových bodoch a v prípade ak nová funkcionalita nebude negatívne ovplyvňovať funkčnosť EDUNET_SK riešenia bude táto funkcionalita sprístupnená používateľom systému.
- Aktualizácia WiFi prístupových bodov je realizovaná centralizovane na diaľku.
- Riadiaci systém zabezpečuje funkciu monitoringu a zberu štatistických údajov v granularite jednotlivých užívateľov a realizovanej dátovej prevádzky vrátane lokalizačných služieb a ich vyhodnocovania aj z pohľadu bezpečnosti.
- V procese overovania prístupu do systému EDUNET_SK riadiaci systém zabezpečí autentifikáciu užívateľa a nastaví mu príslušný prevádzkový profil. Overovanie používateľov EDUNET_SK je realizované cez AAA server, ktorý je integrovaný na identity server v Dátovom centre rezortu školstva.
- Typ a spôsob autentifikácie vyžadovaný pre využívanie systému EDUNET_SK je nastavený v riadiacom systéme a zohľadňuje vstupný bod používateľa (SSID, pevné pripojenie a pod.).
- Relácia používateľa počas doby jej platnosti nevyžaduje autorizáciu voči riadiacemu systému a funkčnosť dátovej komunikácie počas tejto doby zostáva neovplyvnená (vrátane roamovania a bezpečnostných politík) výpadkom autorizačného servera.

2.2.3 Dátové centrum rezortu školstva (DCRŠ)

Dátové centrum rezortu školstva poskytuje aplikácie a digitálny edukačný obsah pre školy a zabezpečuje testovanie. V rámci riešenia EDUNET_SK bude Dátové centrum rezortu školstva pripojené do MPLS VPN EDUNET_SK prístupom 10 Gbps s možným rozšírením na 4 x 10 Gbps.

2.2.4 Pripojenie lokalít do EDUNET_SK

Vzhľadom na počet používateľov na jednotlivých lokalitách (školách) sú lokality rozdelené do kategórií A, B, C, D, E, F a X. V nasledujúcej tabuľke sú uvedené požadované minimálne garantované rýchlosti pripojenia do MPLS VPN EDUNET_SK:

Typ pripojenia	Odhadovaný počet užívateľov	Druh lokality	Symetrický prístup do MPLS – Požadovaná šírka pásma prenosového (minimálna) (Mbit/s)	Asymetrický prístup do MPLS – Požadovaná šírka prenosového pásma (minimálna) (Mbit/s)
A	viac ako 600	ZŠ, SŠ, špec. škola	400	400/20
B	401-600	ZŠ, SŠ, špec. škola	200	200/10
C	251-400	ZŠ, SŠ, špec. škola	75 (alt.50)	75/5 (alt.50/5)
D	51-250	ZŠ, SŠ, špec. škola	30 (alt.20)	30/2 (alt.20/2)
E	do 50	ZŠ, SŠ, špec. škola	10	10/1
F	-	Materská škola, školské zariadenie, ...	10	10/0,5
X	Lokalita cez SANET, iný operátor	ZŠ, SŠ, špec. škola		-

Tabuľka č. 3 Typové rozdelenie lokalít a minimálne rýchlosti pripojenia do MPLS VPN

2.2.4.1 Pripojenie Typ F do EDUNET_SK

Pripojenie lokality typu F do siete EDUNET_SK MPLS VPN sa realizuje prostredníctvom CPE zariadenia zabezpečujúceho:

- smerovanie dátovej prevádzky,
- základnú sieťovú bezpečnosť v rámci lokality (zabezpečiť prístup na implementované zariadenia, zakázanie nepotrebných služieb ako sú ident, finger, MOP, PAD, TCP a UDP small servers, implementácia VLAN sietí v rámci lokality a filtrov na zamedzenie/reštrikciu komunikácie medzi nimi),
- QoS pre Internet a Intranet aplikácie,
- DHCP server pre lokálnych používateľov (kapacita min. 100 IP adries),
- minimálne 4 LAN porty (100BaseT).

2.2.4.2 Pripojenie Typ A - E do EDUNET_SK

Pripojenie lokality typu A - E do siete EDUNET_SK MPLS VPN sa realizuje prostredníctvom CPE zariadenia, ktorého typ závisí od prístupovej technológie. CPE zariadenie zabezpečuje:

- smerovanie dátovej prevádzky,
- základnú sieťovú bezpečnosť v rámci lokality (zabezpečiť prístup na implementované zariadenia, zakázanie nepotrebných služieb ako sú ident, finger, MOP, PAD, TCP a UDP small servers, implementácia VLAN sietí v rámci lokality a filtrov na zamedzenie/reštrikciu komunikácie medzi nimi, implementácia BPDU a STP Root Guard),
- QoS pre Internet a Intranet aplikácie,
- DHCP server pre lokálnych používateľov.

Na každej lokalite je umiestnený LAN prepínač, ktorý zabezpečuje:

- pripojenie WiFi prístupových bodov,
- prepojenie na už vybudované siete LAN na školách.

Správa LAN prepínača a WiFi je realizovaná spoločne prostredníctvom centrálneho riešenia. WiFi prístupové body budú umiestnené pre každú lokalitu samostatne, pričom pred implementáciou sa uskutoční obhliadka miesta, ktorá určí optimálne umiestnenie AP.

2.2.4.3 Integrácia lokalít s pripojením Typ X do EDUNET_SK

V súčasnosti je časť lokalít pripojená do siete Internet prostredníctvom SANETu a iných alternatívnych poskytovateľov. V rámci projektu je riešená ich integrácia do Centrály EDUNET_SK prostredníctvom koncového zariadenia na lokalite, ktoré zabezpečí:

- šifrovaný tunel (na úrovni protokolu AES256 alebo ekvivalentného) do Centrály EDUNET_SK, kde musí byť tento tunel ukončený na koncentrátore VPN,
- smerovanie dátovej prevádzky pre používateľov na lokalite k aplikáciám poskytovaných prostredníctvom DC RŠ,
- prístup k centrálnemu riadiacemu systému pre WiFi.

LAN prepínač, umiestnený na každej lokalite, zabezpečuje:

- pripojenie WiFi prístupových bodov,
- prepojenie na už vybudované siete LAN na školách.

Správa LAN prepínača a WiFi je realizovaná spoločne prostredníctvom Centrálneho riešenia. WiFi prístupové body budú umiestnené pre každú lokalitu samostatne, pričom pred implementáciou sa uskutoční obhliadka miesta, ktorá určí optimálne umiestnenie AP.

2.2.5 Centrálny monitoring IKT prostriedkov zabezpečujúcich prevádzku služieb riešenia EDUNET_SK

Monitoring aktívnych IKT prostriedkov zabezpečujúcich prevádzku služieb riešenia EDUNET_SK umožňuje sledovanie stavu jednotlivých prostriedkov, ich aktuálnych vlastností

a stavu vyťaženia. Tieto údaje sú následne aktívne využívané v rámci monitorovacích postupov na rýchlu detekciu stavu služby a v prípade detekcie problémov na rýchlu identifikáciu a následnú nápravu vzniknutých problémov. Detekcia neštandardných stavov je založená na konfigurovateľných automatizovaných akciách, ktorých výstupom sú eskalačné procesy nastavené podľa závažnosti problému.
Údaje zozbierané monitorovacím systémom sú využívané okrem aktuálneho monitoringu stavu siete aj pre štatistické a reportovacie účely a sú sprístupnené v rámci monitorovacej platformy.

2.2.6 Centrálne zbieranie udalostí o aktivitách jednotlivých používateľov siete EDUNET_SK

Informácie o aktivitách využívajúcich systémy z centrálnej časti EDUNET_SK sú ukladané pre štatistické a reportovacie účely v reportingovom systéme. Systém umožňuje vytváranie reportov, ktoré vychádzajú zo zozbieraných dát ako napr. 10 najviac využívaných AP, štatistiky pre jednotlivé SSID ako aj štatistiky samotného správania jednotlivých používateľov. Prístup k týmto dátam bude kontrolovaný a sprístupnený oprávneným osobám podľa požiadaviek MŠVVaŠ.

2.2.7 Centrálna správa IKT prostriedkov zabezpečujúcich prevádzku služieb na koncovej lokalite riešenia EDUNET_SK

IKT prostriedky zabezpečujúce služby, ktoré sú umiestnené na koncovej lokalite, budú nastavované a aktualizované centrálne bez nutnosti fyzického zásahu priamo na lokalite (výnimku robia prípady, keď chyba je povahy neumožňujúcej vzdialenú úpravu).

2.2.8 Riešenie na zabezpečenie podpory a zber nových požiadaviek (Service Desk)

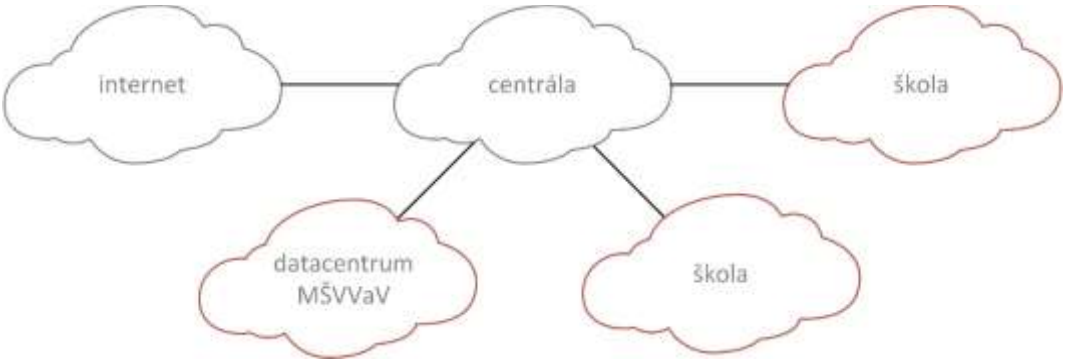
Oprávnení používatelia riešenia EDUNET_SK môžu zadávať požiadavky na zabezpečenie podpory ako aj nové požiadavky cez EDUNET Portál podporujúci proces prijímania požiadaviek a ich spracovanie.

2.2.9 Požiadavky na parametre kvality služby – Quality of Service

Požadované 2 triedy kvality poskytovanej služby popísané v podkladoch na obstarávanie boli v riešení EDUNET_SK rozšírené na 3 triedy (CoS 1, 3 a 6) kvôli lepšej diferenciácií podľa typu prihlásenia a obdobia (normálna alebo mimoriadna prevádzka). Trieda kvality služby 3 a 6 je využívaná v období normálnej prevádzky, trieda kvality CoS 1 je určená pre obdobie mimoriadnej prevádzky najmä počas elektronického testovania žiakov. Týmto rozdelením na 3 triedy bude možné poskytovať kvalitnejšie služby hlavne v kritických obdobiach.

3 Technická a systémová architektúra

Táto kapitola poskytuje popis jednotlivých technických komponentov riešenia, spôsobu komunikácie a integračnej stránky riešenia.



Obrázok č. 1 Prepojenie Lokalít

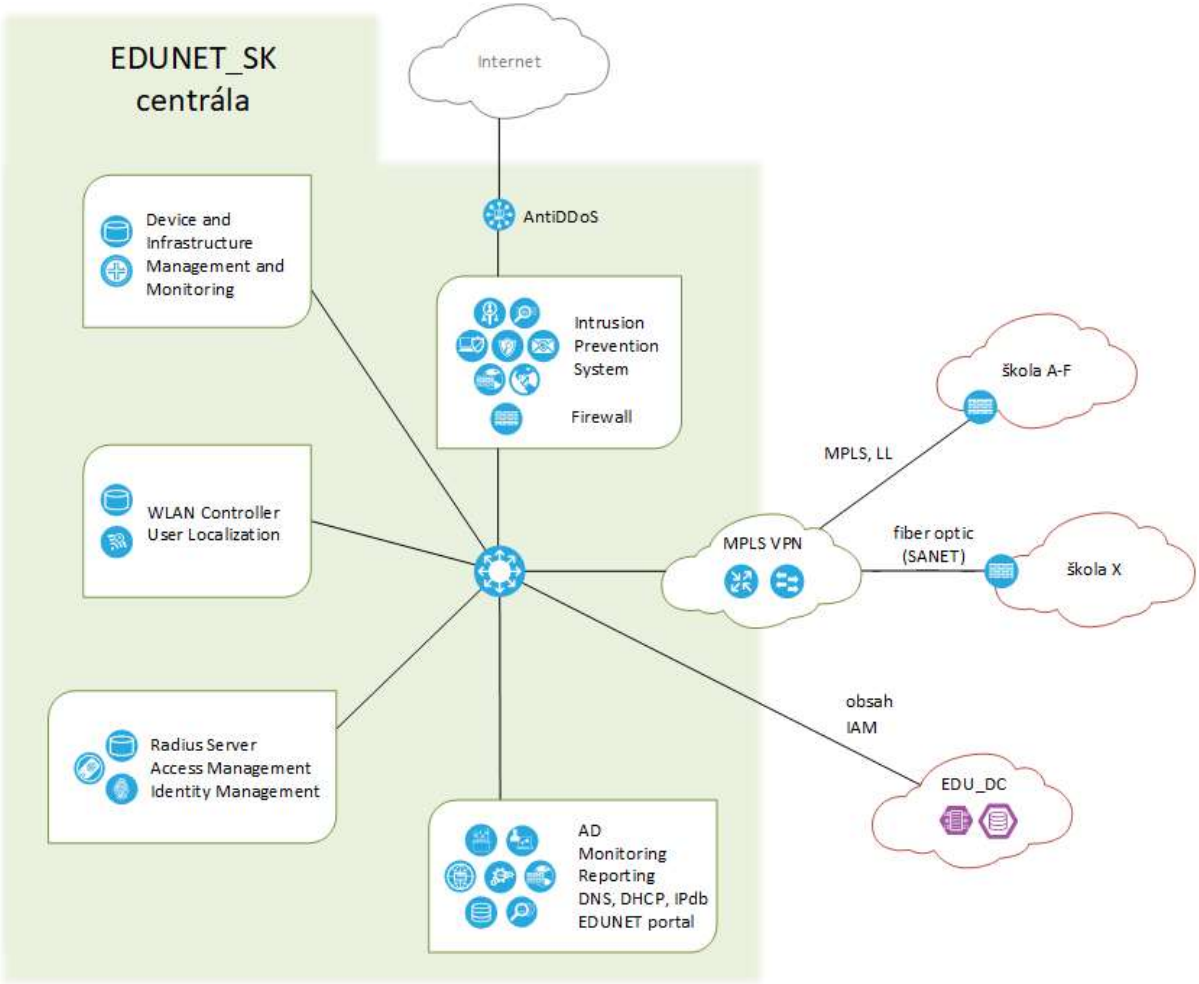
Centrálna časť: je potrebná pre riadne fungovanie celej siete EDUNET_SK. Centralizovane poskytuje všetky požadované služby, to znamená, že každá škola má vytvorené spojenie výlučne do centrálnej časti, odkiaľ môže komunikovať ďalej v rámci ďalších častí siete alebo do verejnej siete Internet.

Lokality alebo tiež školy: týmto názvom sú jednotne pomenované všetky základné školy, stredné odborné školy, gymnáziá, konzervatóriá, materské školy aj školy pre deti a žiakov so špeciálnymi výchovno-vzdelávacími potrebami. V každej škole bude inštalovaný smerovač (CPE), ktorý zabezpečí pripojenie, oddelenie jednotlivých častí siete a ich oddelenú komunikáciu voči Centrálnej lokalite. V školách bude inštalovaný tiež prepínač (switch) podľa objednávky, z ktorého budú pripojené časti siete cez Ethernet, a taktiež jednotlivé WiFi prístupové body (access pointy) podľa objednávky.

Dátové centrum MŠVVaŠ: voči tomuto dátovému centru bude zriadený prepoj z Centrálnej časti, ktorý bude slúžiť pre správu používateľov a poskytovanie Digitálneho edukačného obsahu. Prepojenie Dátového centra MŠVVaŠ je detailnejšie popísané v časti 5.2

Všetky zariadenia a softvérové riešenia, ktoré sú súčasťou architektúry Centrálneho bodu EDUNET_SK a jednotlivých lokalít spĺňajú požiadavku najnovšieho modelového radu, respektíve verzie aby bola zabezpečená ich podpora výrobcami. Použité technológie spĺňajú všetky požadované parametre, definované v Rámcovej zmluve projektu EDUNET_SK, dokonca niektoré výrazne prevyšujú.

3.1 Centrála EDUNET_SK



Obrázok č. 2 Architektúra Centrálneho bodu

EDUNET SK Centrála sa skladá zo softvérovej časti, ktorá obsahuje všetky aplikácie pre bezpečnosť, riadenie a správu zariadení a z hardvérovej časti pre prístup do EDUNET_SK siete a jej ochranu. Softvérová časť pozostáva zo systémov Device and Infrastructure Management a Monitoring, Radius Server, Access Management a Identity management, AD DS, Monitoring, Reporting, DNS, DHCP, IPdb a EDUNET Portál. Hardvérová časť sa skladá zo zariadení AntiDDOS, Firewall, Centrálneho riadiaceho systému pre WiFi (nazývaného tiež Access Point Controller) a MPLS VPN. Všetky súčasti EDUNET_SK centrály sú internými systémami spoločnosti SWAN, ktoré zabezpečujú poskytovanie služieb EDUNET_SK.

Radius Server, Access Management a Identity management je systém pre autentifikáciu a autorizáciu používateľov, ktorí sú definovaní v IAM MŠVVaŠ. Tento modul obsahuje hlavný centrálny radius server, ktorý na základe bezpečnostných politík nastaví prístup používateľovi do siete EDUNET_SK.

AD DS je štrukturovaná databáza všetkých používateľov definovaných v IAM MŠVVaŠ s ich príslušnými atribútmi.

Monitoring a Reporting je modul zabezpečujúci zbieranie prevádzkových dát, ich vyhodnocovanie.

DNS je modul pre DNS záznamy.

DHCP je server pre prideľovanie management IP adries prístupových bodov. DHCP server pre používateľov bude umiestnený na koncových smerovačoch z dôvodu rozdelenia záťaže.

IPdb je systém na udržiavanie IP databázy všetkých systémov a zariadení v EDUNET_SK sieti.

EDUNET Portál je informačný a Service Desk portál pre sieť EDUNET_SK.

Device and Infrastructure Management a Monitoring je modul určený na centralizovanú správu, dohľadávanie a monitorovanie koncových zariadení.

Access point controller je hardvérové zariadenie, ktorého primárna funkcia je riadenie a správa prístupových bodov. V tomto module je aj umiestnený systém na lokalizáciu používateľských zariadení.

AntiDDOS je systém na ochranu centrálnych služieb pred DDoS útokmi.

Firewall má na starosti centrálnu bezpečnosť siete EDUNET_SK. Obsahuje funkcionality Intrusion Prevention and Detection System (IPS), web content filter a application control. Na základe používateľských skupín a ich oprávnení povoľuje prístup do internetu.

MPLS VPN je koncentrátor pre prístup všetkých koncových smerovačov do siete EDUNET_SK.

Funkcie týchto komponentov sú detailnejšie rozpísané v ďalších kapitolách.

3.2 Interné systémy MŠVVaŠ SR

Identity and Access Management (IAM): Modul pre autentifikáciu a autorizáciu používateľov a zariadení, ktoré sú evidované pre prístup do vyhradenej siete MŠVVaŠ. Jednotlivé identity majú pridelené technické parametre, ktoré obsahujú informácie potrebné pre aplikáciu nastavení podľa bezpečnostnej politiky na prístupovej a prestupovej časti siete.

AD – Active Directory je databáza používateľov, ktorá je naplnená a pravidelne aktualizovaná z relevantných zdrojov dát, ktorými sú IAM a RIS.

Digitálny Edukačný Obsah (DEO): Z dátového centra MŠVVaŠ bude prístupný používateľom digitálny edukačný obsah podľa nastavenia ministerstva.

3.3 Informačný a komunikačný systém EDUNET_SK

Súčasťou projektu EDUNET_SK je Informačný systém / Komunikačné prostredie EDUNET Portál, ktorý bude slúžiť pre poverené osoby Objednávateľa a jednotlivých škôl, na prístup k aktuálnym aj archívnym údajom o projekte. Súčasťou Informačného systému sú:

- Service Desk prístup pre poverené osoby Objednávateľa a jednotlivých škôl, komunikačné prostredie pre zasielanie požiadaviek Poskytovateľovi
- Informačný systém pre poverené osoby objednávateľa s informáciami o priebehu projektu

3.4 Súčinnosť MŠVVaŠ SR

Pre korektnú implementáciu a prevádzku projektu EDUNET_SK je potrebné poskytnúť súčinnosti zložiek MŠVVaŠ SR v nasledujúcich oblastiach :

- Zabezpečenie prepoja v dátovom centre Datacube medzi technológiou MŠVVaŠ SR a SWAN
  - inštalácia SFP modulov
  - zriadenie fyzického prepoja v rámci dátového centra Datacube
  - sieťová konfigurácia aktívnych prvkov

- Plnenie Active directory (AD) Site domény edunet.sk z modulov IAM/RIS
  - IP plán pre deployment modulu IAM/RIS pre plnenie AD edunet.sk
  - IP plán pre deployment integrácie SWAN systému webových služieb SOAP API IAM/RIS pre dopĺňanie atribútov AD edunet.sk
  - Povolenie komunikačnej matice na sieťovej infraštruktúre MŠVVaŠ SR site SWAN všetkých potrebných modulov a systémov prepojenia AD edunet.sk a RIS modulov a webových služieb
  - Súčinnosť administrátora modulu RIS na sieťovej infraštruktúre MŠVVaŠ SR pri pridávni používateľov do domény edunet.sk na sieťovej infraštruktúre SWAN
  - Vytvorenie servisných kont v IAM/RIS pre webové služby SOAP API
  - Vytvorenie práv v IAM/RIS
  - Zadefinovanie potrebných práv pre správu operačného systému a služby domain controler pre novú AD Site edunet.sk
  - Úvodné naplnenie pre používateľov 400 škôl do AD edunet.sk s potrebnými atribútmi
  - integrácia s IAM/RIS
    - úvodné naplnenie pre používateľov do AD Edunet.sk s potrebnými atribútmi
    - pravidelná synchronizácia databázy
    - súčinnosť pri integrácii na webové služby SOAP API pre obohatenie atribútov používateľa AD edunet.sk
  - vygenerovanie testovacích prihlasovacích údajov do IAM

- správa IAM prihlasovacích údajov – reset hesla, odblokovanie, zablokovanie, pridanie, vymazanie konta
- sprístupnenie testovacieho prostredia RIS/IAM pre integráciu SWAN systému pri integrácii na webové služieb SOAP API
- sprístupnenie produkčného prostredia RIS/IAM pre integráciu SWAN systému pri integrácii na webové služieb SOAP API
- testovanie správnej integrácie RIS na edunet.sk s webovými službami
- pravidelné kontroly funkčnosti integrácie RIS na AD edunet.sk

- Správa DNS záznamov
  - pre EDUNET Portál infoportal.edunet.sk
  - pre informačnú stránku www.edunet.sk
  - prístup k DEO

- Generovanie certifikátov pre doménu edunet.sk
  - Úvodné generovanie SSL cerifikátov
  - Regenerovanie certifikátov na základe požiadaviek SWAN.

- Definovanie politík pre prístup k aplikáciám a webovému obsahu
  - Web content filtering
  - Aplikačná kontrola

3.5 Systémy využívané MŠVVaŠ SR v rámci projektu EDUNET_SK

EDUNET Portál - Informačný systém / Komunikačné prostredie určené slúžiť pre poverené osoby Objednávateľa a jednotlivých škôl na prístup k aktuálnym aj archívnym údajom o projekte. Súčasťou Informačného systému sú moduly Service Desk a Informačný systém.

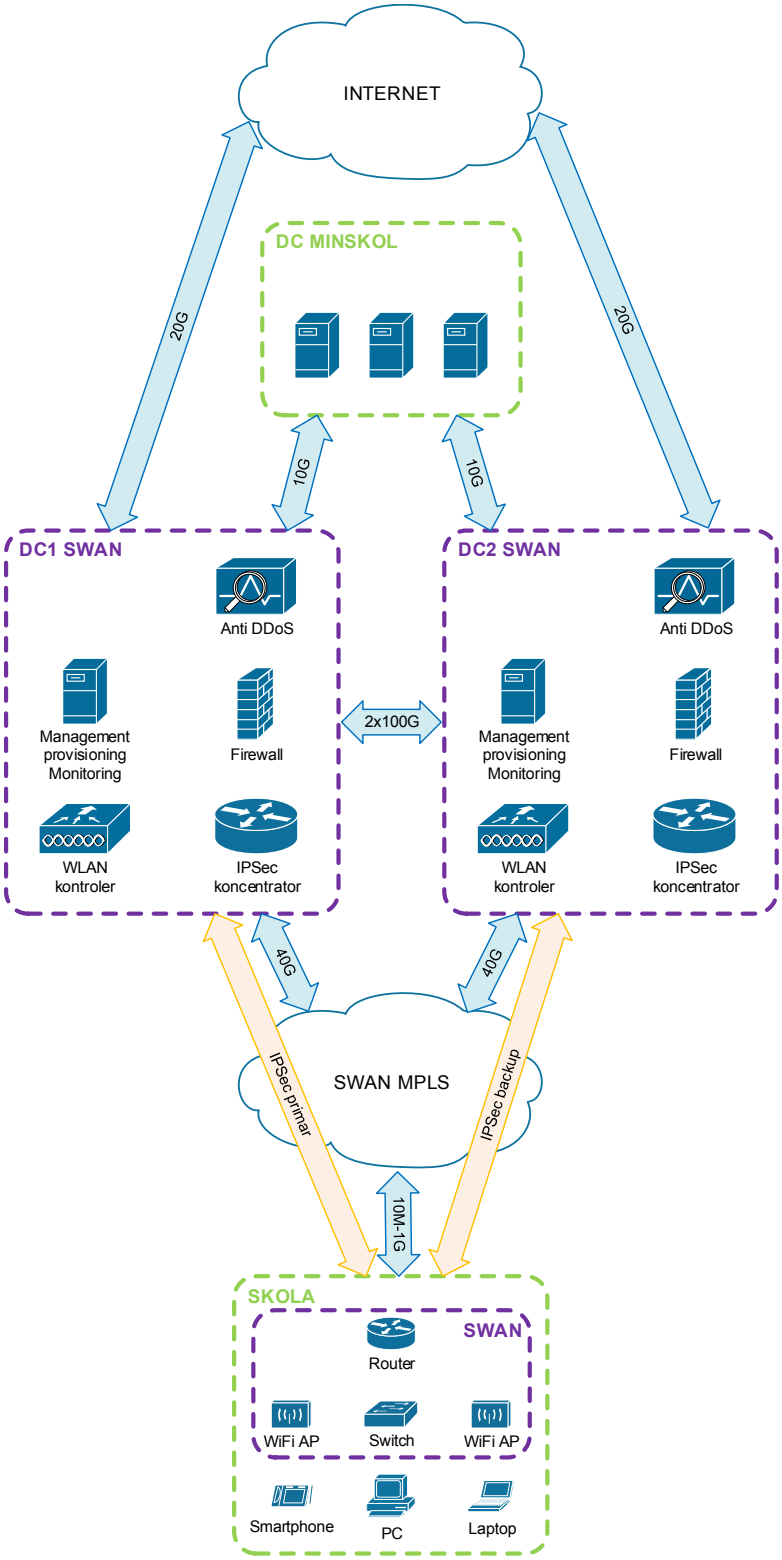
4 Technická infraštruktúra

Táto kapitola poskytuje popis technickej infraštruktúry a slúži ako podklad pre prípravu, inštaláciu a konfiguráciu technickej infraštruktúry produkčného systému.

4.1 Komunikačná architektúra

Pre zabezpečenie riadeného a bezpečného prístupu jednotlivých škôl k službám EDUNET_SK je potrebné zabezpečiť obojsmernú komunikáciu všetkých častí riešenia. Jednotlivé časti riešenia sú riadené prvkami Centrálneho bodu, ktorý zabezpečuje, na základe identifikácie koncového používateľa, adekvátny prístup podľa príslušného autorizačného oprávnenia prostredníctvom bezpečnostných politík a centrálneho riadenia bezpečnosti.

Škola je prostredníctvom prístupovej siete pripojená podľa požadovanej kapacity do MPLS siete SWANu. Z CPE je vybudované primárne a záložné kryptované spojenie v rámci redundancie do dvoch paralelných EDUNET_SK Centrálnych bodov na IPSec koncentrátory, odkiaľ je dátová prevádzka smerovaná na centrálne firewally. Firewally zabezpečujú overovanie/povoľovanie/blokovanie spojení na základe konfigurovaných pravidiel a oprávnení. Z firewallov je riadený prestup do internetu cez anti-DDoS zariadenia.



Obrázok č. 3 Komunikačná architektúra

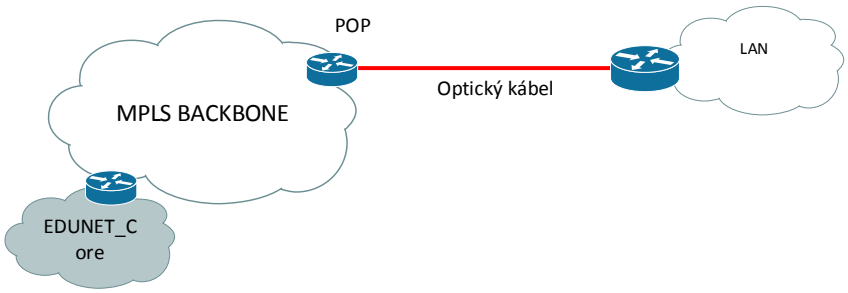
4.1.1 Prepojovacia sieť

Dátové centrum MŠVVaŠ SR nachádzajúce sa v priestoroch Datacube bude vo finálnom riešení prepojené do dátových centier SWAN EDUNET_SK pomocou dvoch nezávislých optických trás, každá o kapacite 10 GB s možnosťou rozšírenia každej trasy na 40GB. Prepoje budú slúžiť na prístup k DEO Ministerstva školstva a tretích strán ako aj k overovaniu používateľských identít z prístupového systému ministerstva. Obe optické trasy budú zrealizované pri akceptácii obsahu prvej objednávky. V úvodnej konfigurácii bude redundancia EDUNET_SK Centrálneho bodu v jednom dátovom centre s prípravou pre plánovaný presun do druhého dátového centra. Druhé dátové centrum bude zrealizované po príprave potrebnej infraštruktúry dátového centra.

4.1.2 Prístupová sieť

Pre každú z pripojených škôl bude budovaná posledná míľa prístupovej siete na základe kapacitných požiadaviek a dostupnej technológie. Predpokladá sa využitie nasledovných technológií pre vybudovanie poslednej míle prístupovej siete:

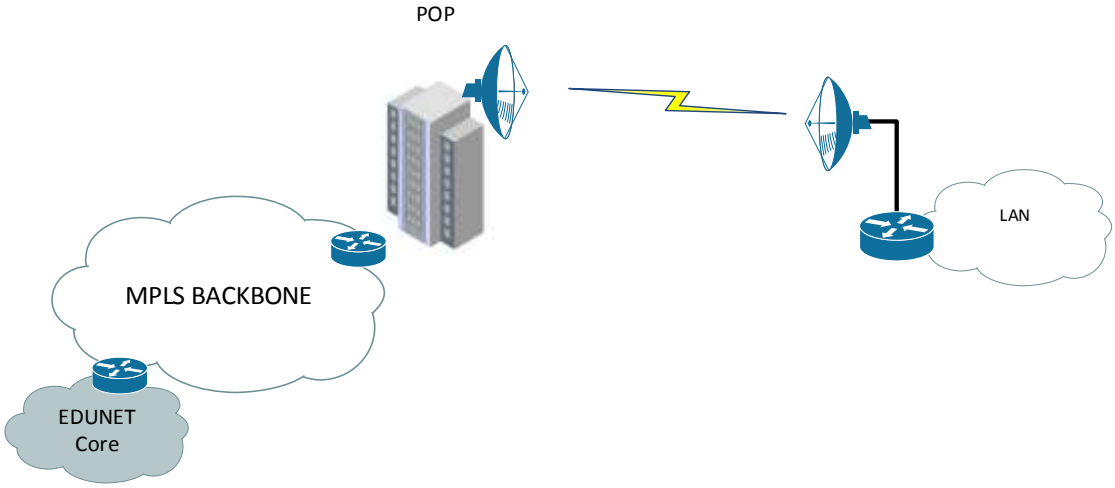
- Optické pripojenie
  Optické pripojenie je prístupová technológia pripojenia zákazníka pomocou optického kábla. SWAN má vybudovanú širokú a hustú infraštruktúru prístupových bodov, z ktorý je možné pripojiť školu optickým káblom. V prípade, že je možné z najbližšieho prístupového bodu siete realizovať výkop ku škole, je možné priviesť a realizovať pripojenie pomocou optického kábla.
  Technológia pripojenia optickým káblom umožňuje poskytovať široké spektrum služieb s pripojením podľa požiadaviek zákazníka.



Obrázok č. 4 Optické pripojenie

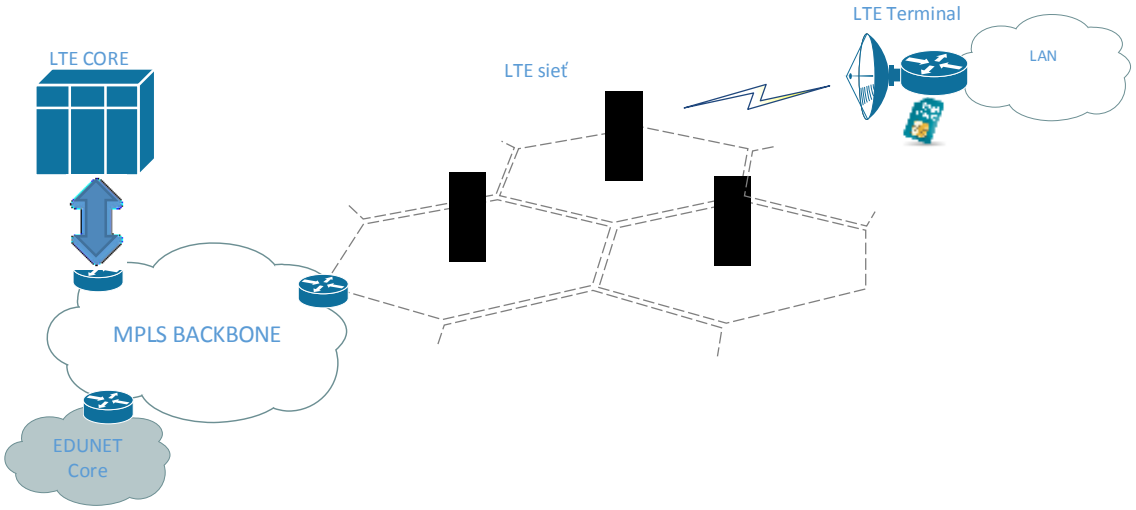
- Rádio-reléový spoj
  Rádio-reléový spoj (ďalej len RR spoj) je bezdrôtová P2P (bod-bod) prístupová technológia pre pripojenie škôl do chrbticovej (nazývanej tiež backbone) siete. Pre pripojenie zákazníkov sa využíva licencované frekvenčné pásmo 13, 18, 23, 26, 32 alebo 38 GHz. Použité frekvenčné pásmo je navrhnuté podľa vzdialenosti od základňovej stanice (protibodu). SWAN má vybudovanú širokú a hustú infraštruktúru prístupových bodov, z ktorý je možné pripojiť zákazníka.
  Na prístupovom bode siete je umiestnená vysielacia anténa, ktorá je nasmerovaná na bod pripojenia školy, pričom na budove školy je pevne umiestnená na vonkajšej

strane budovy a nasmerovaná na protibod. Technológia sa skladá z vonkajšej parabolickej antény s rádiovou jednotkou a koaxiálnym káblom je prepojená s vnútornou jednotkou, na ktorej je terminovaná služba a je umiestnená v požadovanom mieste ukončenia.



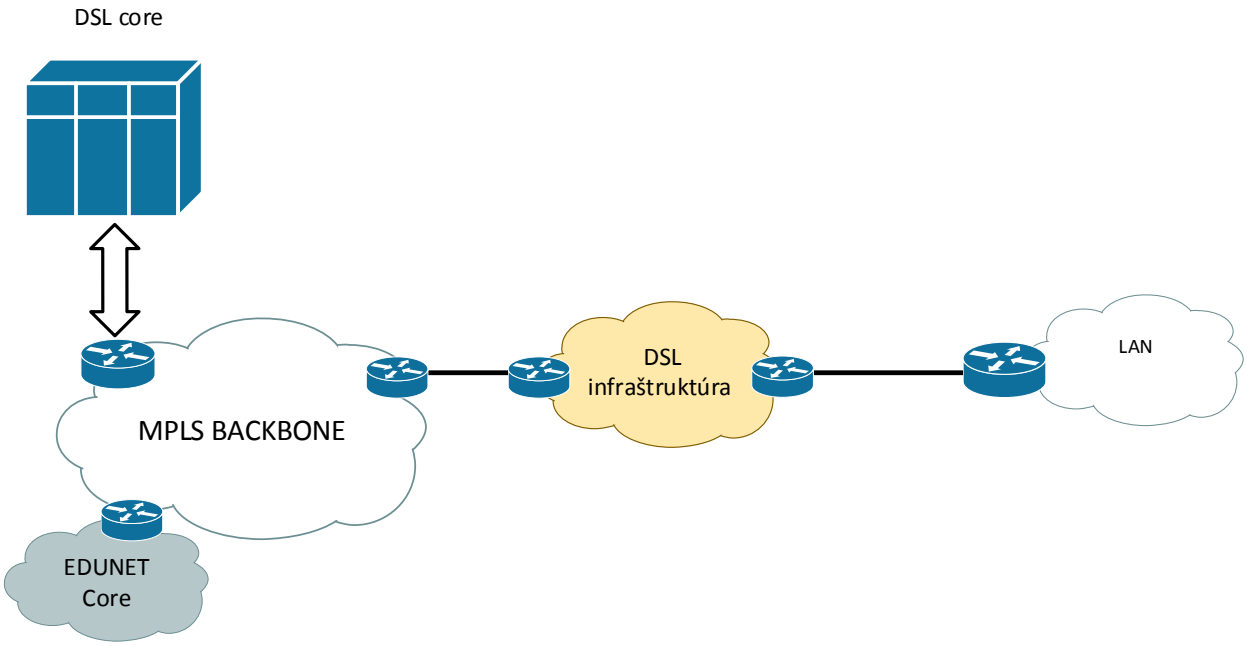
Obrázok č. 5 Rádio-reléový spoj

- FWA P2MP
  Bezdrôtová P2MP (bod-multibod) prístupová technológia pre pripojenie zákazníkov do siete je využívaná v štandarde LTE. Pre pripojenie škôl bude využité licencované frekvenčné pásmo 3,7 GHz, ktorého výlučným používateľom je SWAN.
  LTE technológia je centralizovaná technológia, ktorej služby sú riadené z centrálneho bodu. Na LTE koncovom terminály je ukončená prístupová časť LTE spojenia. LTE terminál je fixne umiestnený na vonkajšej strane budovy a nasmerovaný na niektorú zo základňových staníc.



Obrázok č. 6 LTE Pripojenie

- DSL technológia (aDSL alebo VDSL) je káblová prístupová technológia, pre ktorej realizáciu je využívaná sieťová infraštruktúra majoritného vlastníka DSL infraštruktúry, ktorý pre SWAN ako veľkoobchodného partnera pripraví pripojenie na páre metalického kábla v mieste pripojenia a dátovú prevádzku nasmeruje do spoločného prepoja s infraštruktúrou SWAN.
  DSL je centralizovaná technológia, ktorej služby sú riadené a nastavované z centrálneho bodu SWAN a danému pripojeniu zákazníka je odovzdaná požadovaná služba. Rýchlosť pripojenia je závislá aj na dĺžke a stave metalického páru vlastníka infraštruktúry DSL.



Obrázok č. 7 DSL pripojenie

4.2 Komponenty technickej infraštruktúry

Komponenty technickej infraštruktúry sú rozdelené do troch hlavných častí riešenia:

- centrálny bod,
- centrálny monitoring a reporting,
- lokálna infraštruktúra.

4.2.1 Centrálny bod

Centrálny bod EDUNET_SK zabezpečuje sieťové služby centrálneho pripojenia škôl cez VPN sieť, rôzne typy ochrany a prestupu do Internetu, centrálne riadenie WiFi služby a riadenie prístupov a autentifikácie.
V rámci celkovej funkčnosti a služieb poskytovaných prostredníctvom riešenia VPN siete EDUNET_SK je potrebné zabezpečiť aj komunikáciu mimo VPN siete, konkrétne do siete Internet a do prepojených sietí.
Centrálne pripojenie do Internetu a iných sietí poskytuje:

- vysoko dostupné a zabezpečené pripojenie do Internetu prostredníctvom Centrály EDUNET_SK,
- centrálny IPv4 NAT pre lokality EDUNET_SK,
- DNS služby pre lokality pripojené v EDUNET_SK,
- centrálny firewall pre dátovú komunikáciu, ako aj web content filtering a application control služby,
- IPS (Intrusion Prevention System),
- anti-DDoS ochranu,
- ucelený prehľad o správaní používateľov v rámci celej siete a z toho vyplývajúci jednotný reporting.

Centrálne riadenie WiFi siete poskytuje:

- zabezpečené pripojenie WiFi access pointov do Centrály EDUNET_SK
- centrálnu konfiguračnú správu WiFi SSID EDUNET_SK
- optimálne riadenie vysielacieho výkonu
- synchronizované riadenie prideľovania kanálov
- roaming používateľov pri prechode medzi jednotlivými bránami (WiFi access pointami)
- rozdelenie záťaže access pointov v lokalite
- sledovanie pohybu používateľov
- jednotný reporting WiFi siete

Centrálne riadenie prístupov a autentifikácie zabezpečuje:

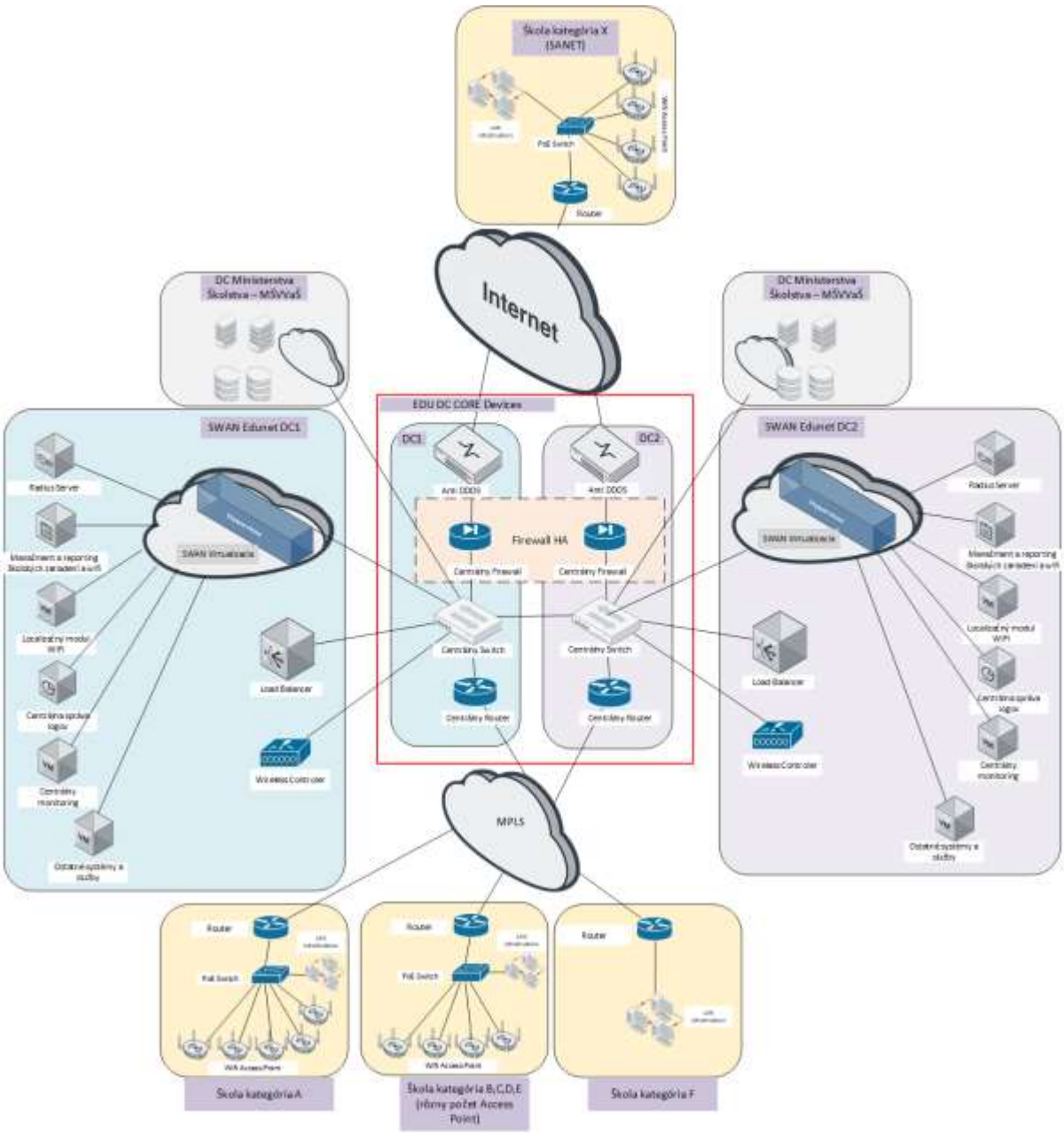
- vytváranie a presadzovanie zásad zabezpečenia na koncových zariadeniach
- centrálna správa identít a politík
- autorizovanie prístupov WiFi, Captive portal
- správa certifikátov
- správa WiFi portálov
- ucelený prehľad o správaní používateľov v rámci celej siete a z toho vyplývajúci jednotný reporting

Prestup do sietí mimo EDUNET_SK je vykonávaný centrálnym firewallom a je to kontrolovaný prestup s IPS ochranou a s aplikáciou firewallových, web content filteringových a application control pravidiel na báze používateľa alebo skupiny používateľov.
V rámci prestupu do siete Internet je zabezpečený cez centrálny IPv4 NAT preklad, ktorý umožňuje nielen dynamický preklad adries, ale aj statický preklad adries pre zabezpečenie rôznych služieb pre lokality a používateľov v sieti EDUNET_SK.

4.2.1.1 High level dizajn zapojenia EDUNET_SK

Centrála EDUNET_SK je koncipovaná s možnosťou geolokácie v dvoch datacentrách DC Perpetuus (DC1) a DC SWAN (DC2). Jednotlivé komponenty Centrály EDUNET_SK sú redundantné. Hlavné komponenty anti-DDoS, centrálny smerovač, firewall, prepínač, loadbalancer a Access point controller tvoria spoločne hlavné hardvérové zariadenia tzv.

Centrálnej časti. Ostatné hlavné komponenty ako rádius server, portálové služby, ktoré umožňujú virtualizáciu, sú umiestnené na v dedikovanej virtuálnej infraštruktúre. Centrálna časť sa prepája s jednotlivými celkami do Internetu, dedikovanej MPLS VPN siete pre EDUNET_SK a s s Dátovým centrom MŠVVaV.



Obrázok č. 8 High level dizajn zapojenia EDUNET_SK

4.2.1.2 NAT pre lokality EDUNET_SK

Prestupy zo siete z interných zdrojov v sieti EDUNET_SK, ale taktiež zo zdrojov v sieti Internet, bude realizovaný na centrálnom firewalle. Dynamické preklady smerom do Internetu za stanovené verejné IP sú v odsúhlasenom IP pláne. Zároveň každá škola má rezervovanú jednu verejnú IP na statické preklady z Internetu.
NAT preklady IP na lokalitách nie sú plánované, komunikácia v rámci lokality a v rámci MPLS bude smerovaná. Jediné NAT preklady realizuje centrálny firewall.

4.2.1.3 Použitie IPv6

V rámci riešenia EDUNET_SK bude pre všetky lokality ako aj pre celkovú dátovú komunikáciu zabezpečená plnohodnotná podpora IPv6. Pre zachovanie funkčnosti všetkých služieb však plánujeme využívanie IPv4 v celej sieti EDUNET_SK, pre služby v koncových lokalitách ako aj pre služby a nastavenia Centrály EDUNET_SK.

4.2.1.4 Verejné IP adresy

V rámci požiadaviek na verejné IP adresy EDUNET_SK je pripravená rezervácia v počte minimálne jedna verejná IPv4 adresa pre každú lokalitu.

4.2.1.4.1 Dynamické preklady adries

Dynamické preklady adries pre lokality budú zabezpečované centrálne na firewalloch Centrály EDUNET_SK. Nakoľko kompletná dátová komunikácia bude povinne smerovaná cez systém pre filtrovanie a kontrolu obsahu až na úroveň používateľa, bude centrálny preklad komunikácie na základe zdrojového IP adresného rozsahu jednoducho aplikovateľný.
Každá lokalita a jej priradené privátne rozsahy IP adries pre jednotlivé LAN a WiFi siete, budú prekladané na verejné IP adresy.

4.2.1.4.2 Statické preklady adries

Statické preklady adries pre každú lokalitu budú zabezpečované centrálne na firewalloch Centrály EDUNET_SK.
Statické preklady adries budú zabezpečovať funkčnosť doplnkovej služby pre lokality EDUNET_SK, ktorou je statický preklad na báze portov pre servery a zariadenie v DMZ LAN sieti.
Pre doplnkové služby statických NAT prekladov je potrebné zabezpečiť zo strany MŠVVaŠ SR jednoznačný proces schvaľovania požiadaviek lokalít na zabezpečenie týchto služieb. V rámci procesného postupu musia byť jasne špecifikované typy služieb a parametre QoS pre tieto služby tak, aby boli v súlade so stratégiou a bezpečnostnou politikou stanovenou pre EDUNET_SK.
Použitie statických IP adries je bližšie popísané v kapitole 4.2.3.2.

4.2.1.5 DNS služby pre lokality pripojené v EDUNET_SK

DNS služby pre EDUNET_SK, ktoré budú implementované v rámci projekt EDUNET_SK je potrebné rozdeliť na dve kategórie :

- DNS služby pre interné potreby EDUNET_SK (portálové služby, servery a služby bežiace v rámci domény edunet.sk) a pre siete priamo prepojené do EDUNET_SK

- DNS služby pre prístup do verejného Internetu

V rámci služieb EDUNET_SK sa nepredpokladá zabezpečovanie služieb registrátora DNS. Pre služby EDUNET_SK sa implementuje vlastné DNS riešenie, ktoré bude dostatočne robustné pre potreby všetkých používateľov pripojených do siete EDUNET_SK.

Riešenie DNS služieb EDUNET_SK bude prepojené na interné DNS servery MŠVVaŠ SR, ktoré budú zabezpečovať korektné preklady doménových mien domény iedu.sk, respektíve dc.iedu.sk na IP adresy. Toto prepojenie je nevyhnutné vzhľadom na poskytovaný digitálny edukačný obsah, ktorý je zabezpečovaný z interných serverov a datacentrových zdrojov MŠVVaŠ v rámci neverejnej siete EDUNET_SK.

Autoritatívne DNS servery

Ako platforma pre poskytovanie služby autoritatívnych menných serverov je použitý PowerDNS Authoritative Server. Je to univerzálny menný server, ktorý podporuje veľký počet typov backendov. Backend je datastore DNS servera obsahujúci záznamy DNS a meta dáta. Tieto backendy môžu byť buď obyčajné textové súbory so zónami alebo sa môže použiť dynamickejší typ backendu, ako je databáza. PowerDNS je Open Source produkt distribuovaný pod licenciou GPL General Public License verzie 2.
Autoritatívne menné servery PowerDNS, budú zabezpečovať poskytovanie služby DNS pre internú sieť EDUNET_SK a aj pre požiadavky zo siete Internet. PowerDNS servery budú inštalované vždy ako dvojica serverov v konfigurácii master - master s použitím vysokodostupného backendu. Vzhľadom na výkony PowerDNS deklarované vývojármi sa nepredpokladá potreba rozširovania počtu autoritatívnych serverov na viac ako dva pre interné požiadavky a dva pre externé požiadavky. PowerDNS Authoritative Server obsahuje plnú podporu konfigurácie a zhromažďovania štatistických údajov pre potreby monitoringu cez REST API.

Rekurzívne DNS servery

Ako platforma pre poskytovanie služby rekurzívnych menných serverov je použitý PowerDNS Recursor. PowerDNS Recursor je vysokovýkonný rekurzívny menný server. Využitím viacerých procesorov a podporou skriptovania, poskytuje PowerDNS Recursor špičkový výkon pri zachovaní flexibility moderných nasadení DNS služieb. Recursor bude poskytovať cache pre DNS požiadavky z internej siete EDUNET_SK. Zároveň bude Recursor preposielať požiadavky pre vybrané domény na autoritatívne servery.
Škálovanie výkonnosti v prípade PowerDNS Recursora sa vykonáva do šírky, teda zvyšovaním počtu Recursorov a použitím vhodného Load Balancera, napríklad PowerDNS dnsdist. PowerDNS Recusor obsahuje plnú podporu konfigurácie a zhromažďovania štatistických údajov pre potreby monitoringu cez REST API.

DNS loadbalancing

PowerDNS dnsdist je vysokovýkonný DNS loadbalancer, ktorý je schopný rozkladať DNS požiadavky na autoritatívne alebo rekurzívne DNS servery na základe dostupnosti a času odozvy DNS serverov. Dnsdist je možné konfigurovať aj ako ochranu DNS serverov pred rôznymi typmi útokov na DNS služby ako sú DoS útoky a definovaním prístupových oprávnení na DNS servery. PowerDNS dnsdist podporuje zhromažďovanie štatistických údajov pre potreby monitoringu cez SNMP.

4.2.1.6 Služby DHCP

Pre zabezpečenie Dynamického prideľovania IP adries je zvolená platforma ISC KEA. Je to DHCP server novej generácie, podporujúci DHCPv4 a DHCPv6. KEA je navrhnutá tak aby ju bolo možné rozšíriť pridaním voliteľných knižníc. Pomocou knižníc a definovaními závislosťami je možné napríklad kontrolovať, ako sa budú IP adresy priraďovať a ako sa budú generovať dynamické DNS záznamy pre priradené IP adresy. Pridávanie, zmeny podsietí a oblastí je možné bez nutnosti reštartovania KEA. Ako datastore pre DHCP lease bude použitá vysoko dostupná databáza. KEA server je možné plne konfigurovať cez REST API.

4.2.1.7 Centrálny firewall a web-content filtering pre dátovú komunikáciu

EDUNET_SK zabezpečuje kapacitne dostatočne škálovaný, bezpečný a riadený prístup, ktorý umožní používateľom s využitím najmodernejších technológií flexibilne pristupovať k rôznym digitálnym zdrojom a nástrojom vo výchovno-vzdelávacom procese, podporí využívanie zdrojov MŠVVaŠ SR a ich tvorbu v rámci interného (rezortného) prostredia. Súčasťou konceptu EDUNET_SK ako prístupu k digitálnym službám je taktiež ich využitie pre riadenie základnej digitálnej bezpečnosti na školách.

Služby EDUNET_SK v rámci centrálneho firewallu a content-filteringu umožňujú a zabezpečujú:

- riadenie prístupov k portfóliu digitálnych služieb na úrovni používateľa podľa pridelenej roly,
- oprávneným používateľom digitálnych služieb školy používanie inštitucionálnych (inventárnych) aj nimi vlastnených digitálnych zariadení (koncept BYOD), cez ktoré budú využívať digitálne služby EDUNET_SK,
- centrálne riadenie prístupov k službám a digitálnemu obsahu tretích strán (umožní jednoduché, bezpečné a riadené prepojenie so zdrojmi tretích strán)
- kontrolovaný prístup ku zdrojom, ktoré podliehajú napríklad spoplatňovaniu alebo je potrebné pri nich individuálnym spôsobom uplatňovať autorské práva,
- centralizované riadenie základnej digitálnej bezpečnosti na školách.

Filtrovanie webového obsahu rovnako ako aplikačná kontrola sa kvôli objemu používateľov aplikuje nad skupinami používateľov podľa AD, ktoré je možné upravovať a napĺňať používateľmi podľa potreby (aj na úroveň jednotlivej školy). Týmto spôsobom je možné nastaviť pravidlá aj individuálne pre jednotlivého používateľa respektíve PC. Manažment

samostatného nastavovania bezpečnostných politík nad používateľmi by bol obtiažne udržovateľný.

4.2.1.7.1 Centrálny firewall

V rámci riešenia Centrály EDUNET_SK je centrálny firewall systém významným zabezpečovacím prvkom, ktorý má za úlohu nielen chrániť sieť EDUNET_SK "zvonku" ale aj "zvnútra".
V riešení centrálneho firewall systému sú okrem základných firewall funkcionalít implementované aj funkcie kombinovaného zabezpečenia s využitím funkcionalít IPS/IDS, web content filtering a aplikačnej kontroly.
Základné funkcionality firewallu, ktoré sú nevyhnutné pre zabezpečenie prestupov zo siete EDUNET_SK do iných sietí vrátane verejného Internetu, sú opísané nižšie:

Klasifikácia do úrovne aplikačnej vrstvy pre real-time dátovú prevádzku :

- identifikácia aplikácie na základe jednoznačne rozpoznateľných znakov
- využitie aplikačnej vrstvy a nie portu ako základu pre výber správnej bezpečnostnej politiky a aplikáciu bezpečnostných opatrení (allow, deny, schedule, inspect a aplikuj traffic-shaping alebo content-filtering)
- kategorizácia neidentifikovaných aplikácií pre nastavenie policy control, forenznú analýzu

Ochrana proti známym a neznámym hrozbám

- blokovanie na základe databáz známych hrozieb, vrátane expoitov, malware a spyware na všetkých portoch a bez ohľadu na spôsob alebo metódu prieniku
- limitovanie a obmedzovanie neautorizovaného prenosu súborov alebo iných typov dát vrátane HTTP a HTTPS prenosov webového obsahu
- identifikácia neznámych typov malware na základe aplikácie analytických nástrojov

Routing

- OSPFv2/v3 with graceful restart, BGP with graceful restart, Static routing
- Policy-based routing
- Multicast : PIM-SM, PIM-SSM, IGMPv1, v2, andv3
- Bidirectional Forwarding Detection (BFD)

IPv6

- support

IPsec VPN

- Key exchange : Manual key, IKEv1 and IKEv2 (pre-shared key, certificate-based authentication)
- Encryption : 3DES, AES (128-bit,192-bit,256-bit)
- Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512

VLANs

- 802.1q VLAN tags per device: 4,094 / 4,094
- Aggregate interfaces (802.3ad), LACP

Network Address Translation (NAT)

- NAT modes (IPv4) : static IP, dynamic IP, dynamic IP and port (port address translation)
- NAT64, NPTv6
- Additional NAT features : Dynamic IP reservation, tunable dynamic IP and port oversubscription

High Availability Modes

- Active/Active, Active/Passive
- Failure detection: Path monitoring, interface monitoring

4.2.1.7.2 Centrálny web-content filtering

Filtrovanie podozrivého webového obsahu je potrebné realizovať centrálne pre zachovanie integrity a nediskriminačného aspektu poskytovania služieb. Filtrovanie obsahu je potrebné realizovať primárne pre zdroje obsahu umiestnené mimo siete EDUNET_SK a to najmä v sieti Internet.
Technológia filtrovania webového obsahu umožňuje:

- explicitne povoliť web stránky / zdroje elektronického obsahu, ktoré sú dôveryhodné a tie ponechať bez inšpekcie
- vytvoriť zoznamy s web stránkami alebo URL alebo špeciálnych výrazov, ktoré budú podliehať inšpekcii
- použiť preddefinované kategórie filtrov obsahu a podkategórie a tie podľa určenia blokovať alebo povoľovať

Generálne nastavenie filtrovania obsahu bude realizované spôsobom tzv. black-list prístupu k filtrovaniu, teda nevhodný a nedôveryhodný obsah bude zakázaný na základe dodaných black-list URL podľa požiadaviek MŠVVaŠ. Takto nastavený proces filtrovania je možné škálovať a nastavovať pre skupiny z RADIUS/ AD DS servera.

4.2.1.7.2.1 Kategórie web filtrov

Kategórie filtrov obsahu sú dostupné nasledovné:

Hlavné kategórie	Pod kategórie	Popis pod kategórie
Adult / Mature Content	Abortion	Websites pertaining to abortion data, information, legal issues, and organizations.
	Advocacy Organizations	This category caters to organizations that campaign or lobby for a cause by building public awareness, raising support, influencing public policy, etc.
	Alcohol	Websites which legally promote or sell alcohol products and accessories.

	Alternative Beliefs	Websites that provide information about or promote religions not specified in Traditional Religions or other unconventional, cultic, or folkloric beliefs and practices. Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, satanic or supernatural beings.
	Dating	Websites that allow individuals to make contact and communicate with each other over the Internet, usually with the objective of developing a personal, romantic, or sexual relationship.
	Gambling	Sites that cater to gambling activities such as betting, lotteries, casinos, including gaming information, instruction, and statistics.
	Lingerie and Swimsuit	Websites that utilizes images of semi-nude models in lingerie, undergarments and swimwear for the purpose of selling or promoting such items.
	Marijuana	Sites that provide information about or promote the cultivation, preparation, or use of marijuana.
	Nudity and Risque	Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse.
	Other Adult Materials	Mature content websites (18+ years and over) that feature or promote sexuality, strip clubs, sex shops, etc. excluding sex education, without the intent to sexually arouse.
	Pornography	Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.
	Sex Education	Educational websites that provide information or discuss sex and sexuality, without utilizing pornographic materials.
	Sports Hunting and War Games	Web pages that feature sport hunting, war games, paintball facilities, etc. Includes all related clubs, organizations and groups.
	Tobacco	Websites which legally promote or sell tobacco products and accessories.
	Weapons (Sales)	Websites that feature the legal promotion or sale of weapons such as hand guns, knives, rifles, explosives, etc.
Bandwidth Consuming	File Sharing and Storage	Websites that permit users to utilize Internet servers to store personal files or for sharing, such as with photos.
	Freeware and Software Downloads	Sites whose primary function is to provide freeware and software downloads. Cell phone ringtones/images/games, computer software updates for free downloads are all included in this category.
	Internet Radio and TV	Websites that broadcast radio or TV communications over the Internet.
	Internet Telephony	Websites that enable telephone communications over the Internet.
	Peer-to-peer File Sharing	Websites that allow users to share files and data storage between each other.
	Streaming Media and Download	Websites that allow the downloading of MP3 or other multimedia files.
General Interest - Business	Armed Forces	Websites related to organized military and armed forces, excluding civil and extreme military organizations.
	Business	Sites sponsored by or devoted to business firms, business associations, industry groups, or business in general. Information Technology companies are excluded in this category and fall in Information Technology.
	Charitable Organizations	Sites for organizations that are set up with a mission that serves a public purpose, and are philanthropic in nature. This category excludes advocacy or political organizations.

	Finance and Banking	Financial Data and Services -- Sites that offer news and quotations on stocks, bonds, and other investment vehicles, investment advice, but not online trading. Includes banks, credit unions, credit cards, and insurance. Mortgage/insurance brokers apply here as opposed to Brokerage and Trading.
	General Organizations	Sites that cater to groups, clubs or organisations of individuals with similar interests, either professional, social, humanitarian or recreational in nature. Social and Affiliation Organizations: Sites sponsored by or that support or offer information about organizations devoted chiefly to socializing or common interests other than philanthropy or professional advancement.Not to be be confused with Advocacy Groups and Political Groups.
	Government and Legal Organizations	Government: Sites sponsored by branches, bureaus, or agencies of any level of government, except for the armed forces, including courts, police institutions, city-level government institutions. Legal Organizations: Sites that discuss or explain laws of various government entities.
	Information Technology	Information Technology peripherals and services, cell phone services, cable TV/Internet suppliers.
	Information and Computer Security	Sites that provide information about or free downloadable tools for computer security, but not ordinary Freeware and Software downloading.
	Online Meeting	Sites that enable hosting of meetings, screen sharing and collaboration of documents across the Internet.
	Remote Access	Sites that facilitate authorized access and use of computers or private networks remotely across the Internet.
	Search Engines and Portals	Sites that support searching the Web, news groups, or indices/directories. Sites of search engines that provide info exclusively for shopping or comparing prices, however, fall in Shopping and Auction.
	Secure Websites	Sites that institute security measures such as authentication, passwords, registration, etc.
	Web Analytics	Sites that are used to collect and assess web traffic data.
	Web Hosting	Sites of organizations that provide hosting services, or top-level domain pages of Web communities.
	Web-based Applications	Sites that mimic desktop applications such as word processing, spreadsheets, and slide-show presentations.
General Interest - Personal	Advertising	Sites that provide advertising graphics or other ad content files, including ad servers (domain name often with 'ad.', such as ad.yahoo.com). If a site is mainly for online transactions, it is rated as Shopping and Auctions. Includes pay-to-surf and affiliated advertising programs.
	Arts and Culture	Websites that cater to fine arts, cultural behaviors and backgrounds including conventions, artwork and paintings, music, languages, customs, etc. Also includes institutions such as museums, libraries and historic sites. Sites that promote historical, cultural heritage of certain area, but not purposely promoting travel.
	Auction	Websites that feature on-line promotion or sale of general goods and services such as electronics, flowers, jewelry, music, etc, excluding real estate. Also includes on-line auction services such as eBay, Amazon, Priceline.
	Brokerage and Trading	Sites that support active trading of securities and management of investments. Real estate broker does not apply here, and falls within Shopping and Auction. Sites that provide supplier and buyer info/ads do not apply here either since they do not provide trading activities.
	Child Education	Websites developed for children age 12 and under. Includes educational games, tools, organizations and schools. Note that children's hospitals are rated as Health.

Content Servers	Websites that host servers that distribute content for subscribing websites. Includes image and Web servers.
Digital Postcards	Sites for sending/viewing digital post cards.
Domain Parking	Sites that simply are place holders of domains without meaningful content.
Dynamic Content	URLs that are generated dynamically by a Web server.
Education	Educational Institutions: Sites sponsored by schools, other educational facilities and non-academic research institutions, and sites that relate to educational events and activities. Educational Materials: Sites that provide information about, sell, or provide curriculum materials. Sites that direct instruction, as well as academic journals and similar publications where scholars and professors submit academic/research articles.
Entertainment	Sites that provide information about or promote motion pictures, non-news radio and television, music and programming guides, books, humor, comics, movie theatres, galleries, artists or review on entertainment, and magazines. Includes book sites that have personal flavor or extra-material by authors to promote the books.
Folklore	UFOs, fortune telling, horoscopes, fen shui, palm reading, tarot reading, and ghost stories.
Games	Sites that provide information about or promote electronic games, video games, computer games, role-playing games, or online games. Includes sweepstakes and giveaways. Sport games are not included in this category, but time consuming mathematic game sites that serve little education purpose are included in this category.
Global Religion	Sites that provide information about or promote Buddhism, Bahai, Christianity, Christian Science, Hinduism, Islam, Judaism, Mormonism, Shinto, and Sikhism, as well as atheism.
Health and Wellness	Sites that provide information or advice on personal health or medical services, procedures, or devices, but not drugs. Includes self-help groups. This category includes cosmetic surgery providers, children's hospitals, but not sites of medical care for pets, which fall in Society and Lifestyle.
Instant Messaging	Sites that allow users to communicate in real-time over the Internet.
Job Search	Sites that offer information about or support the seeking of employment or employees. Includes career agents and consulting services that provide job postings.
Meaningless Content	This category houses URLs that cannot be definitively categorized due to lack of or ambiguous content.
Medicine	Prescribed Medications: Sites that provide information about approved drugs and their medical use. Supplements and Unregulated Compounds: Sites that provide information about or promote the sale or use of chemicals not regulated by the FDA (such as naturally occurring compounds). This category includes sites of online shopping for medicine, as it is a sensitive category separated from regular shopping.
News and Media	Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines, or other media. This category includes TV and Radio sites, as long as they are not exclusively for entertainment purpose, but excludes academic journals. Alternative Journals: Online equivalents to supermarket tabloids and other fringe publications.
Newsgroups and Message Boards	Sites for online personal and business clubs, discussion groups, message boards, and list servers; includes 'blogs' and 'mail magazines.'
Personal Privacy	Sites providing online banking, trading, health care, and others that contain personal privacy information.

	Personal Vehicles	Websites that contain information on private use or sale of autos, boats, planes, motorcycles, etc., including parts and accessories.
	Personal Websites and Blogs	Private web pages that host personal information, opinions and ideas of the owners.
	Political Organizations	Sites that are sponsored by or provide information about political parties and interest groups focused on elections or legislation. This is not to be confused with Government and Legal Organizations, and Advocacy Groups.
	Real Estate	Websites that promote the sale or renting of real estate properties.
	Reference	Websites that provide general reference data in the form of libraries, dictionaries, thesauri, encyclopedias, maps, directories, standards, etc.
	Restaurant and Dining	Websites related to restaurants and dining, includes locations, food reviews, recipes, catering services, etc.
	Shopping	Websites that feature on-line promotion or sale of general goods and services such as electronics, flowers, jewelry, music, etc, excluding real estate. Also includes on-line auction services such as eBay, Amazon, Priceline.
	Social Networking	A social networking site is a platform to build social networks or social relations among people who share similar interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social network sites are web-based services that allow individuals to create a public profile, create a list of users with whom to share connections, and view and cross the connections within the system.
	Society and Lifestyles	This category contains sites that deal with everyday life issues and preferences such as passive hobbies (gardening, stamp collecting, pets), journals, blogs, etc.
	Sports	Includes sites that pertain to recreational sports and active hobbies such as fishing, hunting, jogging, canoeing, archery, chess, as well as organized, professional and competitive sports.
	Travel	Websites in this category feature travel related resources such as accommodations, transportation (rail, airlines, cruise ships), agencies, resort locations, tourist attractions, advisories, etc.
	Web Chat	Sites that host Web chat services, or that support or provide information about chat via HTTP or IRC.
	Web-based Email	Sites that allow users to utilize electronic mail services.
Potentially Liable	Child Abuse	Websites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is available at http://www.iwf.org.uk/.
	Discrimination	Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.
	Drug Abuse	Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc.
	Explicit Violence	This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc.
	Extremist Groups	Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs.
	Hacking	Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites.
	Illegal or Unethical	Websites that feature information, methods, or instructions on fraudulent actions or unlawful conduct (non-violent) such as scams, counterfeiting, tax evasion, petty theft, blackmail, etc.

	Plagiarism	Websites that provide, distribute or sell school essays, projects, or diplomas.
	Proxy Avoidance	Websites that provide information or tools on how to bypass Internet access controls and browse the Web anonymously, includes anonymous proxy servers.
Security Risk	Dynamic DNS	Sites that utilize dynamic DNS services to map a Fully Qualified Domain Name (FQDN) to a specific IP address or set of addresses under the control of the site owner; these are often used in cyber attacks and botnet command & control servers.
	Malicious Websites	Sites that host software that is covertly downloaded to a user's machine to collect information and monitor user activity, and sites that are infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse.
	Newly Observed Domain	Domains that are newly configured or newly active, but not necessarily newly registered.
	Newly Registered Domain	Domains that were very recently registered.
	Phishing	Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.
	Spam URLs	Websites or webpages whose URLs are found in spam emails. These webpages often advertise sex sites, fraudulent wares, and other potentially offensive materials.
Unrated	Not Rated	Sites not yet analyzed/categorized are considered unrated.

Tabuľka č. 4 Kategórie web filtrov obsahu

Kategórie a podkategórie filtrov sa môžu zmeniť v závislosti na firmware centrálneho firewallu. Pre potrebu aktualizácie firmware centrálneho firewallu kvôli napríklad bezpečnostným, funkčným chybám alebo pridaným novým funkciám sú možné zmeny štruktúry kategórií a podkategórií.

4.2.1.7.2.2 Možnosti web filtrov

Systém poskytuje funkcionalitu vytvárania vlastných filtrov pre web filtering obsahu na základe požiadaviek MŠVVaŠ.
Základné filtre pre HTTP/HTTPS inšpekciu sú pravidelne aktualizované zo zdrojov verejne dostupných aj zo zdrojov so spoplatneným prístupom, zároveň však umožňujú manuálne úpravy. Filtre sú granulárne a dovoľujú vhodne kombinovať vstupné kritériá, ako aj granulárne zvoliť akciu, čo spraviť s kontrolovaným obsahom.

Akcie kategórie filtra sú:

- Block – Blokovanie URL – používatelia, ktorí sa pokúšajú získať prístup k zablokovanému webu, dostanú správu vysvetľujúcu, že prístup k stránkam je zablokovaný.
- Allow – Povolenie URL.
- Monitor – Povolenie URL ako Allow s rozdielom, že každá session bude zalogovaná počas zostavenia, zároveň je možné nastaviť kvótu pre maximálny čas strávený na stránke alebo maximálny objem prenesených dát danej kategórie.

- Warning – Upozornenie používateľa správou pred zobrazením obsahu, ktorá mu umožňuje pokračovať, ak potvrdí upozornenie.
- Authenticate – Overenie totožnosti – Pred zobrazením webu sa vyžiada, aby sa používateľ overil so svojím menom a heslom z IAM, po autentifikácií používateľa sa overia jeho oprávnenia. Ak povoľujú prístup do kategórie alebo skupiny kategórií používateľovi sa sprístupní daná kategória.

Odporúčame kvôli jednoduchosti konfigurácie použitie Block a Alow.

Ďalšia možnosť upravovania filtrov je použitím kombinácie kategórie filtrov obsahu, statického URL filtra dodaných URL na základe požiadaviek MŠVVaŠ a kontroly web obsahu na základe obsahu web stránky obsahujúcej špecifické slová (string) alebo pattern.

Statický URL filter má možnosti definovania URL ako:

- textový reťazec v alebo z URL,
- regulárny výraz,
- URL so zástupnými znakmi.

Statický URL filter má možnosti akcie URL ako:

- Block – Blokovanie URL – používatelia, ktorí sa pokúšajú získať prístup k zablokovanému webu, dostanú správu vysvetľujúcu, že prístup k stránkam je zablokovaný.
- Allow – Povolenie URL
- Monitor – Povolenie URL ako Allow s rozdielom, že každá session bude zalogovaná počas zostavenia.
- Exemption – URL je považovaná ako dôveryhodná

Jednotlivé statické URL budú na základe požiadaviek MŠVVaŠ SR pridané do preddefinovaných kategórií centrálneho FW, migrované do preddefinovaných kategórií alebo pridané do nových kategórií. Výhodou použitia nových kategórií je, že v porovnaní so statickým URL filtrom umožňujú aj akcie Monitor, Warning a Authenticate.
Dodatočné funkcionality pri aplikácii filtrovania obsahu sú nasledujúce:

- monitoring filtrovania sieťovej komunikácie do Internetu až na úroveň používateľa,
- extenzívne reportovacie vlastnosti a možnosť prepojenia s externými reportovacími systémami,
- filtrovanie a blokovanie nevhodného obsahu podľa:
    - času,
    - podľa typu LAN siete alebo WiFi SSID,
    - podľa iných parametrov z RADIUS / AD DS
    - podľa zdrojovej IP adresy alebo rozsahu adries,
- regulácia šírky prenosového pásma – traffic shaping, pre aplikácie nesúvisiace s procesom výučby.

Dodatočné funkcionality a možnosti nastavenia:

- Regulácia maximálneho počtu prenesených dát kategórie alebo podkategórie a individuálne nastavovanie podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne a zaradenia používateľa v IAM resp. AD DS skupine.
- Regulácia pre maximálny čas strávený na stránke kategórie a alebo pod kategórie a individuálne nastavovanie podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne a zaradenia používateľa v IAM resp. AD DS skupine.

4.2.1.8 Centrálna aplikačná kontrola

Aplikačná kontrola skúma sieťovú prevádzku generovanú aplikáciami. Jednotlivé aplikácie je možné povoľovať, blokovať alebo obmedziť prístup na určitú dobu. Aplikačná kontrola umožňuje jemne doladiť pravidlá filtrovania webového obsahu použitím typu aplikácie a pomocou kategórií aplikácií. Optimalizuje využitie šírky pásma v sieti tým, že uprednostňuje, obmedzuje alebo blokuje prevádzku na základe kategórie aplikácií alebo konkrétnej aplikácie. Filtrovanie aplikácií je potrebné realizovať primárne pre zdroje obsahu umiestnené mimo siete EDUNET_SK a to najmä v sieti Internet.

Technológia aplikačnej kontroly umožňuje:

- explicitne povoliť kategórie aplikácie a ich komunikáciu na zdroje elektronického obsahu, ktoré sú dôveryhodné a tie ponechať bez inšpekcie
- explicitne zakázať kategórie aplikácie a ich komunikáciu na zdroje elektronického obsahu, ktoré sú nedôveryhodne alebo nežiadane pre komunikáciu siete EDUNET_SK do Internetu
- vytvoriť profily nastavení aplikačnej kontroly na základe požiadaviek MŠVVaŠ SR a uplatniť ich až do úrovne a zaradenia používateľa v IAM resp. AD DS skupine.

Generálne nastavenie filtrovania obsahu bude realizované spôsobom tzv. black-list prístupu k aplikáciám, teda neznáme aplikácie a aplikácie zadefinované ako bezpečnostné riziko so stupňom „critical“ budú zakázané na základe požiadaviek MŠVVaŠ SR. Ostatný obsah bude štandardne povolený. Takto nastavený proces filtrovania je možné škálovať a individuálne nastavovať podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne zaradenia používateľa v IAM resp. AD DS skupine.

4.2.1.8.1.1 Kategórie aplikačných filtrov

Kategórie aplikačných filtrov obsahu sú nasledovné:

Kategória	Popis kategórie
Botnet	Škodlivé aplikácie, ktoré sa používajú na distribúciu škodlivého softvéru, útokov DDoS a iných škodlivých účelov
Business	Aplikácie súvisiace s podnikaním, ako sú napr. Office balíky
Cloud.IT	Cloud aplikácie
Collaboration	Aplikácie používané na zdieľanie pracovnej plochy, vzdialené stretnutia a inú spoluprácu
Email	Aplikácie na odosielanie / prijímanie a spracovanie e-mailov
File.Sharing	Aplikácie používané na zdieľanie súborov

Game	Hry
General.Interest	Nástroje všeobecného záujmu, aplikácie
IM	Instant Messaging aplikácie
Industrial	Priemyselné aplikácie
Mobile	Komunikácia mobilných aplikácií
Network.Service	Aplikácie používané pre sieťové služby a komunikáciu
P2P	Peer-to-Peer aplikácie používané na zdieľanie súborov
Proxy	Proxy a VPN aplikácie
Remote.Access	Aplikácie na vzdialený prístup na prenos súborov alebo na diaľkové ovládanie
Social.Media	Online aplikácie sociálnych médií
Special	Špeciálne aplikácie
Storage.Backup	Aplikácie na online ukladanie súborov a fotografií
Update	Komunikácia na aktualizáciu serverov pre rôzne aplikácie
Video/Audio	Zdieľanie videa, streamovanie a vysielacie aplikácie
VoIP	Aplikácie Voice over IP
Web.Others	Webový prehliadač a ďalšie nástroje pre prehľadávanie webu
Web.Client	Klientské aplikácie založených na protokole HTTP
Unknown	Ostatné aplikácie, ktoré nespadajú do žiadnej inej kategórií aplikácií

Tabuľka č. 5 Kategórie aplikačných filtrov

Kategórie filtrov sa môžu zmeniť v závislosti na firmware centrálneho firewallu. Pre potrebu aktualizácie firmware centrálneho firewallu kvôli napríklad bezpečnostným, funkčným chybám alebo pridaným novým funkciám sú možné zmeny štruktúry kategórií a podkategórií. Aplikácie sú rozpoznávané pomocou aplikačných signatúr.

4.2.1.8.1.2 Možnosti aplikačných profilov

V systéme je možné vytvárať separátne aplikačné profily na základe požiadaviek MŠVVaŠ SR. Základné profily pre aplikačnú kontrolu umožňujú manuálne úpravy. Filtre sú granulárne a umožňujú vhodne kombinovať vstupné kritériá, ako aj granulárne zvoliť akciu, čo spraviť s kontrolovaným obsahom. Akcie kategórie filtra sú:

- Block – Blokovanie aplikácie – ak sa snaží aplikácii alebo aplikácia v kategórii komunikovať je prístup zablokovaný.
- Allow – Povolenie, akcia umožňuje cielenej aplikácii alebo kategórii pokračovať cez centrálny firewall.
- Monitor - akcia umožňuje pokračovanie cielenej aplikácie pokračovať cez centrálny firewall, ale zaznamenáva sa komunikácia a analyzuje sa.

Ďalšie možnosti upravovania filtrov a kategórií je použitím kombinácie kategórie aplikácií, výnimiek pre konkrétnu aplikáciu a výnimiek pre danú kategóriu na základe požiadaviek MŠVVaŠ SR.

Výnimka alebo prepis pre konkrétnu aplikáciu je možná definovaním mena aplikácie a zmeny predefinovanej akcie (Allow, Block, Monitor), ktorá prepíše nastavenia aplikácie na rozdiel od kategórie.

4.2.1.9 Centrálna IPS ochrana

Ochrana založená na anomáliách sa používa, keď samotná sieťová prevádzka je zneužitá a napríklad hostiteľ môže byť zaplavený oveľa väčším počtom požiadaviek, ako je schopný zvládnuť, čím sa stáva nedostupný. Ochrana na základe signatúr sa používa proti známym útokom alebo pri známych zraniteľnostiach. Útočník v tomto prípade používa konkrétne príkazy alebo sekvencie príkazov premenných na získanie prístupu. IPS signatúry zahŕňajú tieto príkazové sekvencie, ktoré umožňujú centrálnemu firewallu identifikovať a zastaviť útok. Tieto signatúry sú pravidelne aktualizované alebo v prípade vzniku novej hrozby sa posielajú na centrálny firewall, aby sa zabránilo aj najnovším typom útokov hneď pri ich detekcii. IPS signatúry sú zlučované do prednastavených profilov inšpekcie komunikácie, ktoré sa aplikujú na komunikácie alebo skupiny komunikácií na centrálnom firewalle.

4.2.1.10 Centrálna ochrana proti DDoS

DDoS ochrana poskytuje efektívnu, inovatívnu ochranu proti útokom DDoS. Pomáha chrániť infraštruktúru pred hrozbami a nedostupnosti služieb odstránením útokov DDoS v sieťovej a aplikačnej vrstve. Bráni kritickú infraštruktúru pred útokom, pričom legitímnej dátovej prevádzke umožní pokračovať ďalej. Tieto škálovateľné vysokovýkonné zariadenia prinášajú osvedčenú ochranu proti DDoS.

DDoS ochrana v rámci riešenia EDUNET_SK má tieto vlastnosti:

- poskytuje viditeľnosť a kontrolu nad sieťou a automaticky detekuje a robí mitigáciu útoku,
- online zapojenie a transparentná mitagácia útokov, ktorá umožňuje jednoduché nasadenie a riadenie prevencie proti DDoS útokom,
- schopnosť sledovať stovky tisíc parametrov súčasne,
- ochrana DDoS založená na správaní, ktorá eliminuje potrebu signatúr,
- ochrana DNS prostredníctvom špecializovaných nástrojov,
- minimalizácia falošných detekcii prostredníctvom priebežného hodnotenia hrozieb.

4.2.1.11 Systém centrálneho riadenia WiFi

Systém centrálneho riadenia WiFi sa používa na centralizované riadenie a správu lightweight WiFi prístupových bodov. Predstavuje vysoko škálovateľnú, odolnú a flexibilnú platformu s bohatou ponukou služieb bezdrôtovej siete budúcej generácie v stredne veľkých až veľkých nasadeniach. Manažment zariadení a preposielanie overovacích údajov prebieha cez Control and Provisioning of Wireless Access Points (CAPWAP) tunel, ktorý je šifrovaný použitím Datagram Transport Layer Security (DTLS) protokolu. Prihlasovacie údaje sa overujú na centrálnom rádius serveri s ktorým komunikuje systém centrálneho riadenia WiFi. Vstavané nástroje pre bezdrôtové siete pripájajúce BYOD (Bring-Your-Own-Device) zariadenia umožňujú klasifikovať klientské zariadenia a aplikovať bezpečnostné politiky založené na skupinách používateľov. Pri redundantnom zapojení ponúka stabilné pripojenie klientských

zariadení, kde v prípade výpadku primárneho centrálneho systému riadenia WiFi sa preklopí celá prevádzka do jednej sekundy na redundantný systém. Vďaka správe RF sa proaktívne identifikuje a zmierňuje rušenie signálu pre zabezpečenie najlepšieho možného výkonu prístupových bodov. Jednou z podstatných výhod použitia centrálneho riadenia WiFi je roaming klientských staníc pri vybudovaní topológie s viacerými prístupovými bodmi na školách, kde pri pohybe klienta sa jeho zariadenie automaticky prepne na prístupový bod, ktorý má najvyššiu úroveň signálu.

4.2.1.12 Centrálny rádius server

Slúži na spravovanie politiky zabezpečenia. Spája a automatizuje kontrolu prístupu na vynútenie politiky prístupu do siete a ku sieťovým zdrojom na základe rolí a jej dodržiavaní. Je to softvérovo definovaný bezpečnostný regulátor. Umožňuje jednoducho definovať pravidlá prístupovej politiky a pružne reagovať na stále sa meniace potreby. Správa sa realizuje z centralizovaného miesta, ktoré prerozdeľuje výkon činností v celej sieti a bezpečnostných infraštruktúrach. IT správcovia môžu centrálne definovať politiku, ktorá bude rozlišovať medzi používateľmi - hosťami (guest users) a zariadeniami registrovaných používateľov. Bez ohľadu na prístupové miesto, používatelia a koncové body budú mať povolený prístup na základe svojho kontextu.
Poskytuje model politiky na báze pravidiel a atribútov slúžiaci na vytváranie flexibilných politík kontroly prístupu. Umožňuje vytvárať diferencované politiky extrakciou atribútov z preddefinovaných slovníkov, ktoré obsahujú informácie o používateľovi a identite koncového bodu, overenie posture, overovanie protokolov, profilovanie identity alebo ďalšie zdroje externých atribútov. Atribúty môžu byť vytvárané dynamicky a uložené na neskoršie použitie.
Ponúka schopnosť integrácie s viacerými externými poskytovateľmi identít, ako sú Microsoft Active Directory, AD DS, RADIUS, RSA jednorazové heslo (OTP) a certifikované úrady pre overovanie a povolenia.
Používa RADIUS, štandardný protokol na overovanie, povolenia a účtovania (AAA). Podporuje širokú škálu overovacích protokolov vrátane (no nie výhradne) PAP, MS-CHAP, Extensible Authentatication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) a EAP-Tunneled Transport Layer Security (TTLS). RADIUS server podporuje EAP prepájanie stroja a používateľských poverení.
Poskytuje komplexné overovanie a autorizáciu voči multiforestným doménam Microsoft Active Directory. Môže zoskupiť viaceré nesúvislé domény do logických skupín pre zjednodušenie konfigurácie zložitých topológií Active Directory za účelom podpory neustále sa meniaceho prostredia.

Pre korektnú impementáciu centrálneho radius serveru je navrhované využitie SSL certifikátu
radius.edunet.sk

- certifikát slúži na 8021x EAP autentifikáciu
- certifikát a doménové meno slúži ako trusted certifikát pre prihlásenie do SSID EDU_CERTIFIKAT, EDU_SPEC, EDU_PRIHLASENIE, aby nedochádzalo ku certificate warning pri prihlasovaní do SSID, resp. k nefunkčnosti služby

- certifikát bude umiestnený na centrálnom radius servery
- Proces použitia certifikátu:
    - Kientské zariadenie sa prihlási do SSID EDU_PRIHLASENIE, EDU_SPEC, EDU_CERTIFIKAT
    - Vyžiadaná je 802.1x autentifikácia, pričom sa použije PEAP alebo EAP. Radius server sa autentifikuje certifikátom radius.edunet.sk
- Loadbalancing komunikácie:
    - Každá radius session je pridelovaná na jeden z viacerých radius serverov, napr. radius11.edunet.sk
    - Na akceptáciu daného certifikátu klientom je potrebný SAN záznam v certifikáte radius.edunet.sk

4.2.1.13 Portálové služby Centrály EDUNET_SK

V rámci projektu EDUNET_SK budú v Centrálnej časti implementované portály

- BYOD
- Captive portál

4.2.1.13.1 BYOD Portálové služby Centrály EDUNET_SK

4.2.1.13.1.1 Inštalácia nových certifikátov

Implementácia konceptu BYOD v rámci projektu EDUNET_SK znamená pripájanie širokej škály zariadení vrátane stolných počítačov, notebookov, netbookov, smartfónov, tabletov, elektronických čítačiek a mobilných zariadení. Je pravdepodobné, že niektoré zariadenia budú vlastnené a riadené školami, zatiaľ čo iné zariadenia môžu byť zamestnanecké. Aby pripájanie nových zariadení bolo jednoduché a v ideálnom prípade samoobslužné, sú v rámci riešenia použité aplikácie na samoinštalovanie certifikátov do zariadení.

SSID určené pre BYOD bude fungovať v dvoch krokoch:

1. Auto inštalácia alebo zápis BYOD certifikátu do zariadenia v rámci prvého prihlásenia a zamedzenie prístupu do siete bez platného certifikátu.
2. Overenie BYOD certifikátom a prístup do siete podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne zaradenia používateľa v IAM resp. AD DS skupine.

Prvý mód slúži pre automatickú inštaláciu alebo zápis BYOD certifikátu cez auto-enrollment portál (v prípade operačného systému iOS) alebo BYOD „auto-enrollment“ aplikáciu do klientského zariadenia. Používateľ pristúpi do SSID EDU_CERTIFIKAT na základe svojho mena a hesla a overí sa voči RADIUS serveru. Ak sa používateľ úspešne overí dostane autorizáciu na prístup do SSID EDU_CERTIFIKAT. Následne je pri pokuse zobrazenia web stránky presmerovaný na web stránku BYOD portál - certificate-enrollment na adrese portalXY.swan.sk.. Ostatné komunikácie sú blokované okrem komunikácií na DNS, DHCP, portály centrály Edunet_SK a Google play pre stiahnutie BYOD certificate auto enrollment aplikácie do Android terminálu., Ostatné webové stránky sú vždy presmerované na BYOD

portál certificate-enrollment. BYOD portál vyžaduje zadanie ľubovoľného názvu zariadenia pre prípadnú neskoršiu identifikáciu pri správe certifikátov. Následne je podľa typu operačného systému potrebné nainštalovať a spustiť auto-enrollment aplikáciu do klientského zariadenia a nasledovať jednoduché kroky popísané v aplikácii. Pre zariadenia s operačným systémom Windows, Android a MacOS je potrebná inštalácia aplikácie, ktorá automaticky po krokoch nainštaluje potrebné certifikáty a urobí zmeny nastavenia WIFI pre ďalšie prihlásenie s použitím certifikátu.. Pre zariadenia s iOS je potrebné len potvrdenie inštalácie profilu a certifikátov priamo z portálu bez nutnosti inštalácie akejkoľvek aplikácie. Operačné systémy založené na iných platformách nie sú podporované v rámci auto-enrollment procedúry. (Pre tieto zariadenia je nutné vygenerovať certifikát cez portál pre správu certifikátov popísaný v ďalšej kapitole a po jeho stiahnutí ho manuálne nainštalovať do zariadenia.) Po úspešnom dokončení inštalácie certifikátu je možné opätovné prihlásenie do SSID s certifikátom.
(Internetové prehliadače, ktoré používajú rozšírenie http protokolu pre striktnú transportnú bezpečnosť Strict Transport Security (HSTS) znemožnia zobrazenie BYOD portál web stránky, preto je potrebné použiť iný a taký, ktorý ochranu nepoužíva.) V prípade, že je použitá web stránka, ktorá používa ochranu HSTS, klientovi je zobrazená chybová hláška s neplatným certifikátom pre dané HTTPS.

Druhý mód slúži pre pristúpenie do SSID EDU_CERTIFIKAT s nainštalovaným certifikátom vydaným v predchádzajúcom móde. Pri overení platným BYOD certifikátom dostane oprávnenie v sieti na základe príslušnosti v AD DS až do úrovne a zaradenia používateľa v IAM.
Po úspešnej autentifikácii BYOD portál nie je zobrazovaný, používateľ pokračuje k pôvodnej URL adrese a môže pristupovať k webovým zdrojom na základe jeho oprávnení.

Generovanie certifikátov bude zabezpečené internou certifikačnou „self-signed“ autoritou. Certifikačná autorita je v edunet.sk doméne a je spravovaná prostredníctvom modulu centrálneho riadenia prístupov a autentifikácie v rámci Centrálneho bodu EDUNET_SK.
Požiadavky na generovanie certifikátov sa vytvárajú automaticky prostredníctvom BYOD portálu, aplikácie, ktorá je súčasťou modulu centrálneho riadenia prístupov a autentifikácie. Následne sú vygenerované certifikáty automaticky naimportované do klientskej pracovnej stanice podľa popisu vyššie.

Parametre certifikátov :

- RSA
- 2048 Bytes
- Platnosť 3652 dní

4.2.1.13.1.2 Generovanie certifikátov BYOD

Tento portál sa nachádza na certifikat.edunet.sk. Cez tento portál sa manuálne generujú a inštalujú certifikáty v prípade zlyhania alebo nekompatibility samoinštalačnej aplikácie a pre nepodporované operačné systémy v rámci auto-enrollmentu.

4.2.1.13.1.3 Správa certifikátov BYOD

Tento portál sa nachádza na byod.edunet.sk. Tento portál sa používa po úspešnej registrácií zariadenia na vykonanie operácií so zariadeniami ako je odstránenie alebo označenie za stratené. Na pozadí sa udeje zneplatnenie (tzv. revoke) certifikátu.

4.2.1.13.2 Captive portál Centrály EDUNET_SK

Na získanie identity z nemanažovateľných častí LAN sietí a uplatnenie s oprávnení v sieti na základe príslušnosti v AD DS až do úrovne a zaradenia používateľa v IAM sa vyvoláva Captive portál a jeho https URL captive.edunet.sk. Portál je zobrazený iba pri pokuse na komunikáciu do Internetu. V rámci LAN sietí školského zariadenia nie je vyvolávaný.

Klientské zariadenie pri pokuse o prístup na internetovú stránku je automaticky presmerované na web stránku Captive portál vyžaduje zadanie mena a hesla používateľa a potvrdenie. Pokiaľ sa používateľ úspešne neoverí zadaním mena a hesla je stále presmerovaný na Captive portál stánku pre akúkoľvek požiadavku na web, ostatné komunikácie sú blokované okrem komunikácií na DNS, portály centrály Edunet_SK. Po úspešnej autentifikácii používateľ pokračuje k pôvodnej URL adrese a môže pristupovať k webovým zdrojom na základe jeho oprávnení.

Captive portál je uplatnený iba pre LAN siet LAN1 učiteľ na prechode cez centrálny bod EDUNET_SK. V LAN školského zariadenia sa vyžaduje priame pripojenie do prepínača a jej broadcast domény, bez možnosti zapojenia alebo zreťazenia ďalších sieťových prvkov (ako smerovač, firewall, WiFi prístupový bod, WiFi extender a podobne). Pre prípad potreby rozšírenia siete je možné použiť prepínač s prednastavenou rovnakou VLAN alebo nemanažovaný prepínač. Prepínač sa nemôže využiť na prepojenie ďalšej LAN prepínača, z dôvodu vzniku tzv. spanning tree slučky (napríklad pre LAN1 a LAN2). Pokiaľ dôjde ku NAT klientskej komunikácie v LAN alebo školskej infraštruktúre pred EDUNET prepínačom/smerovačom na vlastnom zariadení ako smerovač, firewall, WiFi prístupový bod, WiFi extender a podobne, je prvý užívateľ vyzvaný ku autentifikácii cez Captive portál iba prvý krát a ostatné zariadenia pristupujú s oprávnením daného užívateľa.
Internetové prehliadače, ktoré používajú rozšírenie HTTPS protokolu pre striktnú transportnú bezpečnosť Strict Transport Security (HSTS) znemožnia presmerovanie na Captive portál captive.edunet.sk. Preto je potrebné použiť inú web stránku takú, ktorý ochranu nepoužíva. Pokiaľ je použitá web stránka, ktorá používa ochranu HSTS, klientovi je zobrazená chybová hláška s neplatným certifikátom pre dané HTTPS URL

4.2.1.13.2.1 Možnosti nastavenia výnimiek Captive portálu

Captive portál ponúka nasledujúce možnosti vytvorenia výnimky overovania cez Captive portál na základe:

- zdrojovej adresy
- cieľovej adresy
- špecifikácie konkrétnych cieľových aplikácií použitím aplikačnej kontroly firewallu
- servisov s kombináciou zdrojovej adresy alebo cieľovej adresy

Nastavenie výnimiek je možné nahlásením zdrojovej IP adresy terminálu, PC, serveru administrátorom školy alebo na základe požiadaviek MŠVVaŠ SR pre konkrétnu možnosť vytvorenia výnimky overovania cez Captive portál. Globálne výnimky odporúčame nastaviť na základe cieľových IP adries pre zdroje DEO alebo iných vopred definovaných zdrojov na základe cieľovej IP adresy prípadne doménového mena. Cieľové zdroje DEO je potrebné definovať v požiadavke MŠVVaŠ SR. Pri výnimkách je potrebné dbať na to, že cieľové IP, cieľové aplikácie, zdrojové zariadenia prípadne skupiny zdrojových zariadení budú uplatnené pre všetkých používateľov a LAN EDUNET_SK.

4.2.1.13.3 Portál karantény Wifi zariadení

Portál na URL blacklist.edunet.sk

- portál pre informácie, že zariadenie sa nachádza v karanténe pre WiFi pripojenie. v prípade že dôjde k takejto situácii je automaticky otvorená stránka (redirect) s oznámením o dôvode zablokovania prístupu.
- certifikát a doménové meno slúži na informovanie používateľa, že zariadenie sa nemôže dostať na sieť kvôli tomu, že sa nachádza v karanténe (napr. kvôli WiFi útokom alebo viacnásobnej autentifikácii a nadmerného zaťažovania centrály)
- certifikát bude umiestnený na centrálnom radius serveri
- Prístup k sieti je blokovaný kôli neoprávnenému prístupu.
- Iné dôvody s informáciou alebo s možnosťou prekliku na externy informačný web

4.2.2 Centrálny monitoring , manažment zariadení, služieb, reporting

4.2.2.1 Centrálny monitoring

Pre Centrálny monitoring všetkých častí Centrály EDUNET_SK a Lokálnej infraštruktúry na školách bude použitý monitoring softvér Zabbix. Zabbix je softvér, ktorý monitoruje množstvo parametrov siete, zdravie a integritu prvkov siete. Zabbix používa flexibilný mechanizmus oznamovania, ktorý umožňuje používateľom konfigurovať výstrahy založené na e-mailoch prakticky pre každú udalosť. To umožňuje rýchlu reakciu na vzniknuté problémy. Zabbix ponúka vynikajúce funkcie prehľadov a vizualizácie dát na základe uložených dát. To robí Zabbix ideálnym nástrojom pre plánovanie kapacít.
Všetky správy a štatistiky služby Zabbix, ako aj konfiguračné parametre, sú prístupné prostredníctvom webového rozhrania. Webové rozhranie zabezpečuje, že stav siete a zdravie monitorovaných zariadení možno vyhodnotiť z ľubovoľného miesta.

Centrálny monitoring je interný systém Poskytovateľa, ktorý je využívaný pre zabezpečenie nasledujúcich požiadaviek na Centrálu EDUNET_SK.

- monitoring a manažment všetkých aktívnych zariadení v Centrálnom bode EDUNET_SK
- monitoring a manažment všetkých aktívnych zariadení v rámci lokálnej infraštruktúry škôl projektu EDUNET_SK
- korelácie udalostí z jednotlivých aktívnych zariadení v sieti Centrálnom bode a v rámci lokálnej infraštruktúry škôl projektu EDUNET_SK
- analýzu prvotnej príčiny incidentu

- správu zoznamu zariadení

V prípade požiadavky MŠVVaŠ SR je možné pripraviť výstup a report zo systému centrálneho monitoringu.

4.2.2.1.1 Zabbix Agent

Natívny Zabbix Agent vyvinutý v programovacom jazyku C môže byť prevádzkovaný na rôznych podporovaných platformách, vrátane Linux, UNIX, Windows a ďalších typoch operačných systémov a zhromažďuje dáta ako vyťaženie CPU, RAM, SWAP, sieťových adaptérov a lokálnych diskov.
Vďaka centralizovanej konfigurácii Zabbix agentov cez Zabbix server je možné jednoduchým spôsobom upravovať konfiguráciu zhromažďovaných metrík.
Zabbix agent je schopný zhromažďovať metriky pasívnym a aktívnym systémom. V prípade pasívneho systému si Zabbix server, prípadne Zabbix Proxy, vyžiada informácie o predmetnej metrike. V prípade aktívneho systému server posiela Zabbix Agentovi informácie o požadovaných metrikách a intervaloch, v akých má byť predmetná metrika zbieraná a Zabbix Agent následne posiela potrebné metriky na Zabbix Server, prípadne na Zabbix Proxy.
Zabbix Agent môže byť rozšírený o metódy zásuvných modulov, používateľsky nastavených parametrov a Zabbix Sender.
Zabbix Sender je súčasťou inštalácie Zabbix Agenta a na rozdiel od Zabbix Agenta, ktorý posiela nazhromažďované dáta na základe požiadavky Zabbix Servera alebo na základe nakonfigurovaných intervalov, Zabbix Sender odosiela dáta primárne na základe vzniknutej udalosti.

4.2.2.1.2 SNMP a IPMI agent

Zabbix server umožňuje zhromažďovanie údajov zo zariadení cez SNMP protokol. Porporuje verzie SNMP v1, v2 a v3. SNMP agentom je možné zhromažďovať údaje hlavne zo sieťových zariadení, ale aj ďalších zariadení pripojených na sieť ako UPS, PDU a ďalších.
Zber údajov je možný SNMP Poliingom alebo prijímaním SNMP Trapov cez SNMP Traptrap daemon. Zabbix Server podporuje štandard SNMP MIB-2, čo zjednodušuje prácu s SNMP zariadeniami.
IPMI agent zabezpečuje zber údajov o hardvéri postavenom na Intel architektúre. Metriky dostupné cez IPMI protokol sú rôzne pre každý typ zariadenia. Prevažne však poskytujú informácie o stave hardvéru ako teploty CPU a mainboard, rýchlosti ventilátorov, systémových napätiach a celkovom stave hardvéru.

4.2.2.1.3 Monitoring bez použitia agenta

V prípade, že je potreba monitorovania zariadenia, ktoré nie je možné monitorovať cez SNMP alebo IPMI a zároveň nie je možné na zariadenie nainštalovať ani Zabbix Agenta, je možné použiť monitoring bez použitia agenta. V takomto prípade, je možné monitorovať napríklad dostupnosť a otvorenosť TCP portu a čas odozvy.

Ak zariadenie neposkytuje ani žiadnu službu vo forme TCP portu, je možné monitorovať zriadenie pomocou ICMP protokolu. Tak ako v prípade TCP portu sa jedná o dostupnosť cez ICMP a čas odozvy.
Ďalším spôsobom zberu údajov je vykonávanie príkazov na vzdialených systémoch cez SSH, alebo Telnet protokol.

4.2.2.1.4 Používateľské metódy

Ako rozšírenie vstavaných metód Zabbix Agenta je možné vytvoriť vlastné skripty ako používateľské parametre. Zabbix Agent je potom schopný spúšťať tieto skripty a zozbierané údaje následne odoslať na Zabbix Server alebo Zabbix Proxy.
V prípade potreby kontroly z externých systémov je možné spúšťať používateľské skripty priamo zo Zabbix servera alebo Zabbix Proxy.

4.2.2.1.5 Kalkulácie a agregácie

Pomocou aritmetických funkcií nad zozbieranými metrikami je možné vytvárať virtuálne metriky, ktoré sú následne uložené a umožňujú generovanie grafov, vytváranie alarmov a posielanie notifikácii.
Agregované metriky sú virtuálne metriky, vytvorené na základe aritmetických funkcií minimum, maximum a priemer z viacerých zariadení. Typickým príkladom použitia je výpočet priemeru používanej RAM na databázovom clusteri.

4.2.2.1.6 Detekcia vzniknutých problémov

4.2.2.1.6.1 Detekcia incidentov

Následne po zozbieraní údajov rôznymi metódami, ktoré umožňuje Zabbix, nasleduje vyhodnocovanie údajov a porovnanie s konfigurovanými hraničnými hodnotami. V prípade, že je naplnená podmienka, Zabbix server vyvolá alarm a následne aktivuje zasielanie notifikácií podľa nakonfigurovaných pravidiel.

4.2.2.1.6.2 Závažnosť incidentov a eskalácia

Zabbix umožňuje definovať pre jednotlivé návratové hodnoty zozbierané zo zariadení, rôzne úrovne závažnosti incidentu. V prípade konfigurácie alarmu ako eskalačného je možné zvyšovanie závažnosti na základe nasledujúcich hodnôt z meraní. Napríklad v prípade zostávajúceho voľného miesta na disku je možné definovať vyvolanie prvého alarmu pri prekročení minimálneho zostávajúceho priestoru 20% ako upozornenie, v prípade prekročenia hranice 10% vyvolať alarm so závažnosťou vážna a v prípade prekročenia 5% vyvolať alarm ako vysoká hrozba.

4.2.2.1.6.3 Predikcia, hysteréza, závislosti

Na vyhodnocovanie zozbieraných údajov je možné použiť rôzne aritmetické a časovo definované funkcie.
Navyše Zabbix ponúka definovanie alarmov na základe predikcie. V takomto prípade sa vyhodnocujú zozbierané údaje s ohľadom na prechádzajúce obdobie za časový úsek a tým

pádom je možné vyhodnotiť, kedy je predpoklad že v budúcnosti nazbierané hodnoty nadobudnú istú prahovú hodnotu.
Hysteréza je funkcia, kedy zozbierané dáta oscilujúce okolo prahovej hodnoty nie sú vyhodnocované ako pozitívny alarm okamžite po prekročení prahovej hodnoty, ale až po prekročení hodnôt počas definovanej periódy. Rovnako môťe byť definovaný aj návrat metriky do normálneho stavu.
Zabbix server umožňuje vyvolanie alarmu na základe závislosti viacerých metrík z jedného, alebo rôznych zariadení. Navyše je možné kombinácia viacerých parametrov, ako napríklad v prípade že monitorujeme zariadenie s dvomi napájacími zdrojmi, je vyvolaný alarm až v prípade že príde ku zlyhaniu oboch zdrojov. Druhým prípadom môže byť monitoring databázového clustera, kedy je alarm aktivovaný až v prípade nedostupnosti oboch databázových serverov

4.2.2.1.7 Zabbix WEB

Zabbix WEB je centrálny nástroj pre konfiguráciu celého systému Zabbix a zobrazovanie meraných metrík, konfiguráciu a zobrazovanie grafov z nameraných hodnôt. Tieto grafy je možné vytvárať ad-hoc alebo ako preddefinované s možnosťou nastavenia časového rozsahu.
Zabbix WEB ďalej umožňuje vytváranie obrazoviek, na ktorých je možné definovať grafy z rôznych zariadení, sieťové mapy a slideshow, kde je možné rotovať v časových intervaloch rôzne obrazovky. Táto funkcionalita je vhodná hlavne pre dohľadové centrá. Zabbix WEB je UTF-8 kompatibilný a lokalizovaný do množstva jazykov.

4.2.2.1.8 Upozornenia, eskalácie a korelácie

Zabbix je možné konfigurovať na zasielanie upozornení pre zodpovedné osoby v prípade vzniku alarmu na základe rôznych používateľsky definovaných podmienok. Medzi vstavané metódy patrí zaslanie e-mailu, správy cez SMS, JABBER a ExTexting. Navyše však umožňuje spustenie používateľských skriptov, ktorými je možné vyvolať akciu na externom zariadení alebo na zavolanie externej oznamovacej služby.
Vykonanie akcie na externom zariadení je možné cez Zabbix Agenta, cez SSH alebo Telnet. Ako príklad je možné vyvolať reštart servera v prípade vyvolania alarmu z daného servera.
Eskalácia umožňuje definovanie scenára, kedy je v prípade vyvolania alarmu zaslané upozornenie zodpovednej osobe v prvom rade. Následne v prípade pretrvávania problému dlhšie ako stanovený čas je informovaná osoba v druhom rade a tak ďalej.
Na základe definovaných značiek je možné vyvolať upozornenie na základe globálnych korelácií udalostí alebo na základe korelácií alarmov z jedného zariadenia.

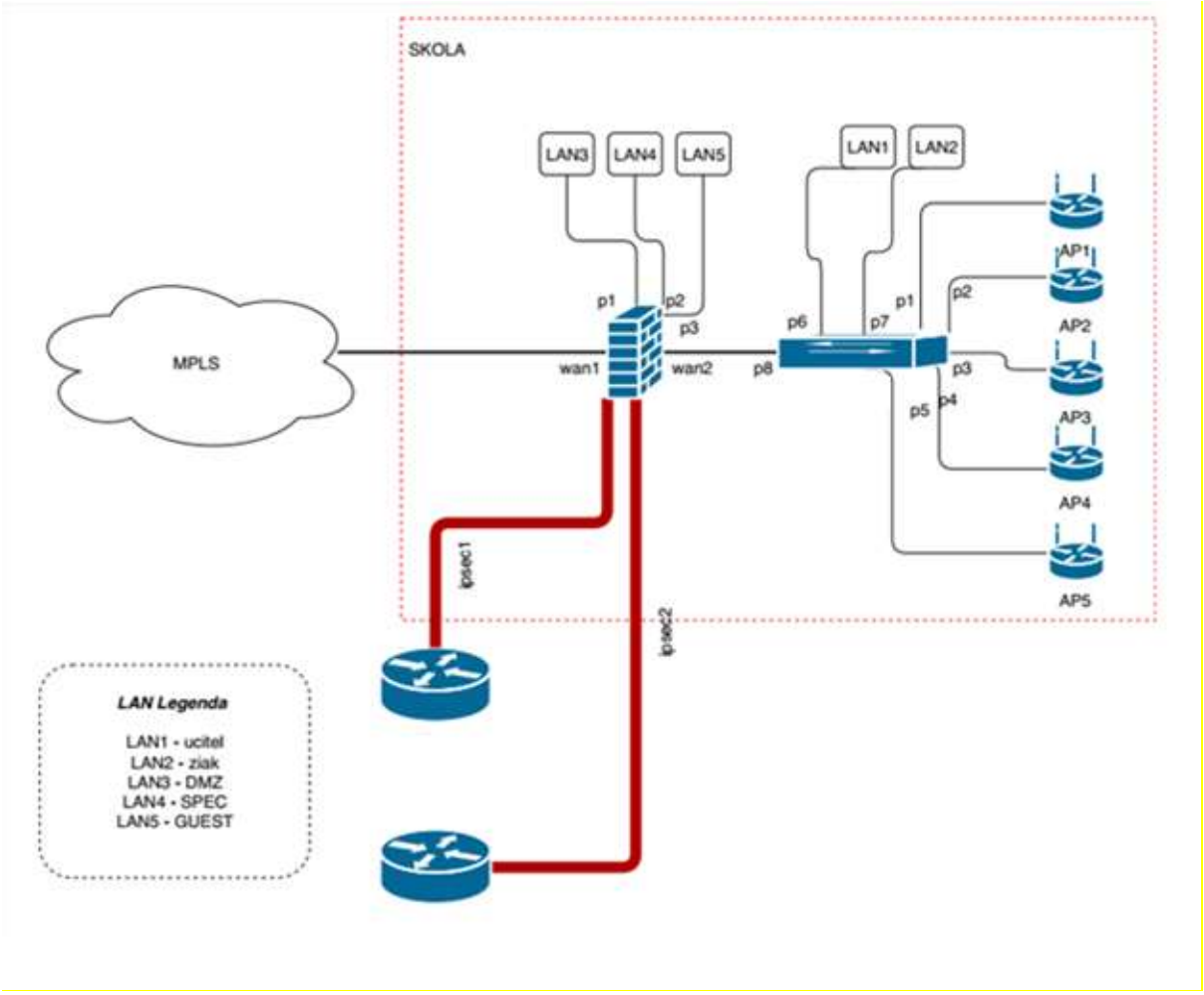
4.2.2.2 *Reporting*

Pri tvorbe reportov bude databázový systém automatizovane kompletizovať dáta z dvoch parciálnych dohľadových a reportingových systémov. Dáta týkajúce sa WiFi ako TOP 10 SSID, TOP 10 AP, štatistiky pre SSID a podobne budú poskytované centrálnym riadiacim systémom WiFi, štatistiky týkajúce sa správania používateľov budú čerpané zo security časti Centrály automatizovaným analytickým systémom nad údajmi z centrálneho firewallu.

4.2.3 Lokálna infraštruktúra škôl

Lokálna LAN/WiFi infraštruktúra závisí od typu školy podľa počtu žiakov a existujúceho typu pripojenia. Súčasťou lokálnej infraštruktúry sú zariadenia

- Smerovač (CPE)
- Prepínač
- Prístupový bod (AP)



Obrázok č. 9 Lokálna infraštruktúra škôl

Popis smerovačov (CPE):

Školy typu X:

IPsec priepustnosť do 1Gbit/s
- Zariadenie riadené z centrálneho riadiaceho systému.
- Porty: 8x 10/100/1000 BaseT Ethernet, 2x SFP Gigabit Ethernet uplink
- Podpora 4096 VLAN, minimálne 8000 MAC adries, podpora PoE na všetkých portoch.
- Podpora 802.1x, DHCP snooping, ARP inspection a port security

Školy typu A, B,C:

IPsec pri zapnutých QoS priepustnosť do 420Mbit/s
- Zariadenie riadené z centrálneho riadaceho systému.
- Porty: 8x 10/100/1000 BaseT Ethernet, 2x SFP Gigabit Ethernet uplink
- Podpora 4096 VLAN, minimálne 8000 MAC adries, podpora PoE na všetkých portoch.
- Podpora 802.1x, DHCP snooping, ARP inspection a port security

Školy typu D,E,F:
IPsec pri zapnutých QoS priepustnosť do 100Mbit/s
- Zariadenie riadené z centrálneho riadiaceho systému.
- Porty: 8x 10/100/1000 BaseT Ethernet, 2x SFP Gigabit Ethernet uplink
- Podpora 4096 VLAN, minimálne 8000 MAC adries, podpora PoE na všetkých portoch.
- Podpora 802.1x, DHCP snooping, ARP inspection a port security

Prepínač (switch):
- Zariadenie je riadené z centrálneho riadiaceho systému.
- Porty: 8x 10/100/1000 BaseT Ethernet, 2x SFP Gigabit Ethernet uplink
- Podpora 4096 VLAN, minimálne 8000 MAC adries, podpora PoE na všetkých portoch.
- Podpora 802.1x, DHCP snooping, ARP inspection a port security.

WiFi prístupový bod (access point):
- Zariadenie vyhovuje norme ETSI a má povolenie na prevádzku v Slovenskej republike
- Zariadenie plne manažovateľné centrálnym riadiacim systémom.
- 1×10/100/1000BASE-T
- Maximálny počet pripojených klientov: 200 pre každé frekvenčné pásmo (400 dohromady)
- Podpora WiFi štandardov IEEE 802.11ac Wave 2, IEEE 802.11n, IEEE 802.11a, IEEE 802.11g, IEEE 802.11b (až do 866 Mbps pre 5GHz pásmo a 300Mbit/s pre 2,4GHz pásmo), 2×2 MIMO technológia, podpora DFS, 20 aj 40 MHz kanály
- Integrované antény so ziskom 2dBi pre 2,4 GHz pásmo a 4dBi pre 5 GHz pásmo
- Podpora šifrovaného bezdrôtového prenosu: AES 128 bit
- Podpora PoE podľa štandardu 802.3af/at
- Podpora 802.1X, RADIUS authentication, authorization, and accounting (AAA), 802.11r, 802.11i
- LED indikácia operačného stavu

Na lokálnych CPE bude umiestnený SSL certifikát firewall.edunet.sk

- Certifikát bude slúžiť na **redirect pre prípad, že sa používateľ dostal do karantény** (automaticky otvorená stránka (redirect) s oznámením o dôvode zablokovania) (napr. kvôli DDoS alebo iného útoku na centrálny bod EDUNET_SK), prípadne na účely captive portálu na lokalitných CPE (rovnako ako portál captive.edunet.sk)
- Slúži aj ako redirect pre ostatné služby centrálneho firewallu HTTPS

4.2.3.1 *WiFi služby EDUNET_SK*

Bezdrôtové pripojenie používateľov k sieti EDUNET_SK bude zabezpečovať alternatívu k pevnému LAN pripojeniu. Pre plnohodnotnú funkcionalitu porovnateľnú s kvalitou

a parametrami pevného pripojenia k LAN sieti je potrebná aplikácia príslušných nastavení pre bezpečnosť a kvalitu služieb WiFi.

4.2.3.1.1 SSID WiFi sietí

Pre zabezpečenie ekvivalentného pripojenia ako pri pevnom LAN pripojení je potrebné zachovať obdobné nastavenia a rozdelenia dátovej prevádzky. Preto je v rámci riešenia potrebné konfiguračne rozdeliť dátovú prevádzku do jednotlivých sietí, čo pri WiFi technológiách znamená aplikovať nastavenia pre jednotlivé SSID nasledovne:

- SSID EDU_PRIHLASENIE - ekvivalent k LAN 1 a LAN 2
- SSID EDU_CERTIFIKAT - ekvivalent k LAN 1 a LAN 2
- SSID EDU_SPEC - ekvivalent k LAN 4
- SSID EDU_HOST - špeciálny prístup pre návštevníkov

SSID „EDU_HOST“

Primárnou funkciou SSID EDU_HOST je pripojenie k sieti EDUNET_SK a sprístupnenie základného rozsahu digitálneho edukačného obsahu podľa špecifikácií uvedených pre Centrálu EDUNET_SK.

Účelom tejto siete je sprostredkovať žiakom a návštevníkom školy bez nutnosti autentifikácie a autorizácie bezpečný prístup k všeobecne dostupnému digitálnemu edukačnému obsahu ako sú interné zdroje MŠVVaŠ SR, stránky IAM, a podobne.

Pri prihlasovaní do WiFi SSID EDU_HOST bude používateľovi zobrazený oznam o obmedzenom rozsahu dostupných webových služieb a ostatných dátových služieb dostupných prostredníctvom siete EDU_HOST v sieti EDUNET_SK.

Toto SSID je možné podľa na požiadanie školy alebo školského zariadenia selektívne vypnúť.

Overovanie	OPEN + DISCLAIMER
Povolená komunikácia	LEN vybrané zdroje dostupné cez HTTP/HTTPS, ostatné porty a komunikačné protokoly zakázané
Traffic shaping	max. 64 kbps na session, max. 1 Mbps na SSID na lokalite
IP adresný rozsah	spoločný pre celú sieť EDUNET_SK, max. 250 IP adries pre jednu školu
Max. čas prihlásenia	60 min
Security	povolený prístup z SSID EDU_HOST k vybraným zdrojom v EDUNET_SK a v sieti Internet zakázaný prístup z SSID EDU_HOST do ostatných WiFi sietí a LAN sietí mapovanie celej dátovej prevádzky do samostanej virtuálnej LAN pre transport v sieti EDUNET_SK
QoS	QoS 6, CoS 6
Komunikácia v rámci SSID	Oddelená od ostatnej komunikácie, klienti nevedia komunikovať medzi sebou navzájom.

Tabuľka č. 6 SSID EDU_HOST

SSID EDU_PRIHLASENIE

Primárnou funkciou SSID EDU_PRIHLASENIE je autentifikácia, autorizácia a následné pripojenie používateľa k sieti EDUNET_SK. Autentifikácia bude prebiehať prostredníctvom mena a hesla.

Aplikácia bezpečnostných profilov a nastavení prebieha vždy až po autentifikácii a autorizácii používateľa. Samotný proces beží podľa štandardu 802.1X a to najmä z dôvodu zachovania možnosti oddeľovania a tagovania používateľov do samostatných VLAN pre ďalší transport v sieti na základe jednoznačnej autentifikácie a autorizácie.

Pre plnú funkčnosť je požadovaná schopnosť oddeľovať/tagovať používateľov po autentifikácii na základe autorizačných profilov.

Overovanie	WPA/WPA2-Enterprise s podporou EAP-TLS / EAP-TTLS
Povolená komunikácia	podľa security-group
Traffic shaping	podľa security-group
IP adresný rozsah	jedinečný pre lokalitu, max. 500 IP adries pre jednu lokalitu
Max. čas prihlásenia	180 min
Security	bezpečnostné limitácie pre prístup k sieti podľa príslušnej security group povolený prístup k vybraným zdrojom v EDUNET_SK a v sieti Internet podľa profilu pre security group
QoS	Security group Učiteľ - QoS 3, CoS 3 Security group Žiak- QoS 3, CoS 3
Komunikácia v rámci SSID	Oddelená od ostatnej komunikácie, klienti nevedia komunikovať medzi sebou navzájom. Možnosť pristupovať k zdieľaným zariadeniam v LAN sieťach pre skupinu klientov

Tabuľka č. 7 SSID EDU_PRIHLASENIE

SSID EDU_CERTIFIKAT

Primárnou funkciou SSID EDU_CERTIFIKAT je autentifikácia a pripojenie používateľského zariadenia k sieti EDUNET_SK. Autentifikácia bude prebiehať prostredníctvom certifikátu zariadenia cez funkcionalitu BYOD sprostredkovanú Centrálou EDUNET_SK.

Aplikácia bezpečnostných profilov a nastavení prebieha vždy až po autentifikácii a autorizácii používateľského zariadenia.

Samotný proces bude bežať prostredníctvom štandardu 802.1X, a to najmä z dôvodu zachovania možnosti oddeľovania a tagovania používateľov/zariadení do samostatných VLAN pre ďalší transport v sieti.

Pre plnú funkčnosť je požadovaná schopnosť oddeľovať/tagovať používateľov/zariadenia po autentifikácii na základe autorizačných profilov.

Overovanie	WPA/WPA2-Enterprise s podporou EAP-TLS / EAP-TTLS / 802.1X
Povolená komunikácia	podľa security-group
Traffic shaping	podľa security-group

IP adresný rozsah	jedinečný pre lokalitu, max. 500 IP adries pre jednu lokalitu
Max. čas prihlásenia	480 min
Security	bezpečnostné limitácie pre prístup k sieti podľa príslušnej security group povolený prístup k vybraným zdrojom v EDUNET_SK a v sieti Internet podľa profilu pre security group
QoS	Security group Učiteľ - QoS 3, CoS 3 Security group Žiak- QoS 3, CoS 3
Komunikácia v rámci SSID	Oddelená od ostatnej komunikácie, klienti nevedia komunikovať medzi sebou navzájom. Možnosť pristupovať k zdieľaným zariadeniam v LAN sieťach pre skupinu klientov

Tabuľka č. 8 SSID EDU_CERTIFIKAT

SSID EDU_SPEC

Primárnou funkciou SSID EDU_SPEC je autentifikácia a pripojenie používateľského zariadenia k sieti EDUNET_SK. Toto SSID bude využívané v špeciálnom režime, teda bude sprístupňované na vyžiadanie pre účely elektronických testovaní, ako aj pre iné špecifické účely podľa potrieb MŠVVaŠ SR a jeho organizácií. Mimo špeciálneho režimu (tzv. kritickej prevádzky) bude toto SSID vypnuté.

Autentifikácia bude prebiehať prostredníctvom mena a hesla alebo certifikátu zariadenia.

Aplikácia bezpečnostných profilov a nastavení prebieha vždy až po autentifikácii a autorizácii používateľa alebo zariadenia. Samotný proces bude bežať prostredníctvom štandardu 802.1X.

Overovanie	WPA/WPA2-Enterprise s podporou EAP-TLS/EAP-TTLS /802.1X
Povolená komunikácia	podľa security-group
Traffic shaping	podľa security-group
IP adresný rozsah	250 IP adries pre jednu školu
Max. čas prihlásenia	variabilný
Security	bezpečnostné prístupové limitácie minimálne na základe MAC adries, aplikácia bezpečnostných obmedzení na základe 802.1X, povolený prístup z SSID EDU_SPEC len k vybraným zdrojom v EDUNET_SK zakázaný prístup z SSID EDU_SPEC do WiFi sietí a LAN sietí.
QoS	QoS 1, CoS 1
Komunikácia v rámci SSID	Oddelená od ostatnej komunikácie, klienti nevedia komunikovať medzi sebou navzájom.

Tabuľka č. 9 SSID EDU_SPEC

4.2.3.2 *LAN služby EDUNET_SK*

Pre realizáciu pripojenia pevnej LAN siete školskej lokality je potrebná inštalácia CPE v kombinácii s LAN prepínačom, na ktorých sú pre pripojenie pevnej siete dostupné 4 fyzické metalické porty s rýchlosťou minimálne 100 Mbps, teda minimálne štandard FastEthernet.
Na každej lokalite budú terminované LAN 1 – 4 pripadne len LAN 5. Každá LAN bude určená pre špecifický účel nasledovne:

LAN 1

LAN sieť školského zariadenia pre pripojenie "učiteľskej" infraštruktúry, do ktorej budú mať oprávnenie pristupovať len zamestnanci školského zariadenia s príslušným zaradením do security-group. Táto LAN sieť bude zároveň dostupná príslušným používateľom na úrovni "učiteľ" alebo „zamestnanec" aj z WiFi SSID EDU_PRIHLASENIE a EDU_CERTIFIKAT. Zároveň bude možné z tejto LAN siete pristupovať k prostriedkom v sieťach LAN 2, LAN 3 a k digitálnemu edukačnému obsahu v sieti EDUNET_SK a mimo nej na úrovni podľa príslušného zaradenia do security-group

Overovanie	CAPTIVE portál, výnimka z Captive portál na základe definovania IP adresy alebo žiadne
Povolená komunikácia	podľa security-group a zóny na lokálnom firewalle
Garancia prenosového pásma	podľa typu lokality v zmysle QoS a CoS
IP adresný rozsah	jedinečný pre každú lokalitu s rozsahom min. 64 IP adries podľa typu školy; IP rozsah je špecifický podľa typu školy
Max. čas prihlásenia	802.1X alebo sa neuplatňuje, pri type BYOD a CAPTIVE portál sa rieši na globálnej úrovni
Security	aplikácia bezpečnostných limitácií pre prístup k sieti minimálne na základe MAC adries možnosť aplikácie bezpečnostných obmedzení na základe 802.1X podľa možností zariadení v LAN sieti školskej lokality, povolený prístup z LAN 1 do LAN 2, LAN 3 a do EDUNET_SK, na základe lokálnych zónových pravidiel
QoS	QoS 3, CoS 3
Komunikácia s LAN	klient je oddelený od ostatných LAN sietí využitím zónového firewallu alebo access-listami tak, že je možná komunikácia z LAN 1 do LAN 2 a LAN 3, ale nie naopak.
	Povolený prístup do LAN 1 je len pre používateľov priamo pripojených v LAN 1 alebo pripojených cez WiFi s autorizáciou na úrovni "učiteľ" alebo „zamestnanec" alebo vyššou.

Tabuľka č. 10 LAN 1

Pre prípad žiadneho overovania nie je možné zabezpečiť overenie používateľa, centrála EDUNET_SK nemá informáciu o identite. Nedochádza k obohacovaniu logov centrálneho riešenia o identitu a nedokáže prideliť zabezpečenie priradenia správneho oprávnenia používateľa pre web content filtering, aplikačnú kontrolu a firewall pravidlá, podľa group a nastavovať ich podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne a zaradenia používateľa v IAM resp. AD DS.

LAN 2

LAN sieť školského zariadenia pre pripojenie učební a zdieľanej výpočtovej techniky, ktorá je dostupná aj žiakom. Z tejto siete bude možné pristupovať k vybraným prostriedkom v sieti LAN 3, ako aj k digitálnemu edukačnému obsahu v sieti EDUNET_SK a mimo nej na úrovni podľa príslušného zaradenia do security-group. Táto LAN sieť je zároveň dostupná príslušným používateľom na úrovni "učiteľ" alebo „zamestnanec" aj z WiFi SSID EDU_PRIHLASENIE a EDU_CERTIFIKAT.

Overovanie	bez overovania ale s možnosťou navýšenia oprávnení pre filtrovanie webového obsahu pre používateľov s úrovňou uprávnení „učiteľ" alebo „zamestnanec"
Povolená komunikácia	podľa security-group a zóny na lokálnom firewalle
Garancia prenosového pásma	podľa typu lokality v zmysle QoS a CoS
IP adresný rozsah	jedinečný pre každú lokalitu s rozsahom min. 128 IP adries a podľa typu školy; IP rozsah je špecifický podľa typu školy
Max. čas prihlásenia	neuplatňuje sa žiadne obmedzenie
Security	aplikácia bezpečnostných limitácií pre prístup k sieti minimálne na základe MAC adries povolený prístup z LAN 2 do LAN 3 a do EDUNET_SK zakázaný prístup z LAN 2 do WiFi sietí.
QoS	QoS 3, CoS 3
Komunikácia s LAN	Komunikácia pripojených klientov je oddelená od ostatných LAN sietí využitím security zonácie alebo access-listami tak, že je možná komunikácia z LAN 2 do LAN 3, ale nie naopak. Povolený prístup do LAN 2 je len pre používateľov priamo pripojených v LAN 1 a LAN 2 alebo pripojených cez WiFi s autorizáciou na úrovni "učiteľ" alebo "zamestnanec".

Tabuľka č. 11 LAN 2

Pre túto sieť bez overovania nevieme zabezpečiť overenie používateľa, centrála EDUNET_SK nemá informáciu o identite. Nedochádza k obohacovaniu logov centrálneho riešenia o identitu a nedokáže prideliť zabezpečenie priradenia správneho oprávnenia používateľa pre web content filtering, aplikačnú kontrolu a firewall pravidlá, podľa group a nastavovať ich podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne a zaradenia používateľa v IAM resp. AD DS.

LAN 3

LAN sieť školského zariadenia so špecifikáciou DMZ. Táto LAN sieť má primárne slúžiť na pripojenie serverov alebo zdieľaných zariadení, ktoré budú dostupné všetkým používateľom v LAN 1, LAN 2, ako aj používateľom pripojených k WiFi sieťam okrem SSID EDU_HOST. Táto LAN sieť je zároveň dostupná príslušným používateľom na úrovni "učiteľ" a "zamestnanec" aj z WiFi SSID EDU_PRIHLASENIE a EDU_CERTIFIKAT. Z tejto LAN siete je možná komunikácia len k vybraným zdrojom údajov v sieti EDUNET_SK a mimo nej podľa individuálnych požiadaviek (napr. aktualizačné servery a podobne).

Overovanie	žiadne
Povolená komunikácia	DMZ
Garancia prenosového pásma	podľa typu lokality v zmysle QoS a CoS
IP adresný rozsah	jedinečný pre každú lokalitu s rozsahom min. 64 IP adries podľa typu školy; presný IP rozsah je špecifický podľa typu školy
Max. čas prihlásenia	neuplatňuje sa žiadne obmedzenie
Security	aplikácia bezpečnostných limitácií pre prístup k sieti minimálne na základe MAC adries povolený prístup z LAN 3 k vybraným zdrojom v EDUNET_SK a v sieti Internet zakázaný prístup z LAN 3 do WiFi sietí
QoS	QoS 3, CoS 3
Komunikácia s LAN	Pre komunikáciu v LAN 3 sieti školského zariadenia je potrebné uplatňovať pravidlá a best-practices určené pre siete typu DMZ

Tabuľka č. 12 LAN 3

LAN 4

LAN sieť školského zariadenia pre pripojenie zariadení, ktoré budú využívané v špeciálnom režime, teda budú sprístupňované na vyžiadanie pre účely elektronických testovaní, ako aj pre iné špecifické účely podľa potrieb MŠVVaŠ SR a jeho organizácií.

Overovanie	CAPTIVE portál, výnimka z Captive portál na základe definovania IP adresy alebo žiadne 802.1X alebo žiadne overovanie
Povolená komunikácia	CoS 1/QoS 1
Garancia prenosového pásma	CoS 1/QoS 1
IP adresný rozsah	jedinečný pre každú lokalitu s rozsahom min. 64 IP adries podľa typu školy; presný IP rozsah je špecifický podľa typu školy
Max. čas prihlásenia	802.1X alebo podľa požiadavky
Security	aplikácia bezpečnostných limitácií pre prístup k sieti minimálne na základe MAC adries možnosť aplikácie bezpečnostných obmedzení na základe 802.1X podľa možností zariadení v sieti školskej lokality povolený prístup z LAN 4 len k vybraným zdrojom v EDUNET_SK zakázaný prístup z LAN 4 do WiFi sietí a ostatných LAN na škole
QoS	CoS 1/QoS 1
Komunikácia s LAN	Pre komunikáciu v LAN 3 sieti školského zariadenia je potrebné uplatňovať pravidlá a best-practices určené pre siete typu DMZ

Tabuľka č. 13 LAN 4

Pre prípad zvolenia žiadneho overovania nevieme zabezpečiť overenie používateľa, centrála EDUNET_SK nemá informáciu o identite. Nedochádza k obohacovaniu logov centrálneho riešenia o identitu a nedokáže prideliť zabezpečenie priradenia správneho oprávnenia používateľa pre web content filtering, aplikačnú kontrolu a firewall pravidlá, podľa group a nastavovať ich podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne a zaradenia používateľa v IAM resp. AD DS.

Podľa požiadavky je riešenie pripravené tak, že každá LAN je terminovaná na samostatnom rozhraní prepínača alebo smerovača. Pre potreby testovania (využitie LAN 4) sa predpokladá fyzické pripojenie eternet kábla do určeného rozhrania na prepínači. V prípade požiadavky je možné

- Poskytnutie trunk rozhrania na prepínači.

- Prekonfigurovanie rozhrania s LAN 2 na LAN4 (v móde tzv. access). Vzhľadom na objem prevádzky a počet pripojených lokalít budú tieto zmeny uskutočnené v dávkach podľa skupín (ktoré vieme definovať podľa potreby).

LAN 5

LAN sieť školského zariadenia, ktorá umožňuje prístup na určité materiály MŠVVaŠ SR, nepoužíva žiadne overovanie, maximálne reštrikcie na prístup do internetu. Predpokladáme jej využitie len v špeciálnom prípade ak školské zariadenie nevie prejsť na systém LAN 1 – 4.
Riešenie z dôvodu popísanej nemožnosti nastavenia štandardov 802.1X ponúka využitie tzv.: LAN siete LAN5 a WiFi SSID EDU_HOST, ktoré umožňuje prístup na určité materiály MŠVVaŠ SR, nepoužíva žiadne overovanie a sú uplatnené maximálne reštrikcie na prístup do internetu, pre každého používateľa rovnako, bez možností vytvorenia výnimiek a detekovanie používateľa/identitu. Takéto pripojenie nezabezpečuje overenie používateľa, centrála EDUNET_SK nemá informáciu o identite. Nedochádza k obohacovaniu logov centrálneho riešenia o identitu a nedokáže prideliť zabezpečenie priradenia správneho oprávnenia používateľa pre web content filtering, aplikačnú kontrolu a firewall pravidlá, podľa group a nastavovať ich podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne a zaradenia používateľa v IAM resp. AD DS.

Overovanie	žiadne
Povolená komunikácia	vybrané zdroje dostupné cez HTTP/HTTPS, ostatné porty a komunikačné protokoly zakázané
Garancia prenosového pásma	v zmysle špecifikácie QoS a CoS
IP adresný rozsah	jedinečný pre každú lokalitu s rozsahom min. 64 IP adries podľa typu školy; IP rozsah je špecifický podľa typu školy
Max. čas prihlásenia	podľa požiadavky
Security	povolený prístup z LAN 5 k vybraným zdrojom v EDUNET_SK a v sieti Internet, zakázaný prístup z LAN 5 do ostatných WiFi sietí mapovanie celej dátovej prevádzky do samostatnej virtuálnej LAN pre transport v sieti EDUNET_SK
QoS	CoS 6/QoS 6

Tabuľka č. 14 LAN 5

Pre lokality so špecifickými zdôvodnenými požiadavkami na pripojenie do siete internet je možné po dohode upraviť oprávnenia až na úroveň nefiltrovaného internetu.

4.2.3.2.1 Prestupy medzi sieťami v rámci lokality

len smer →	SSID EDU_PRIHLASENIE	WiFi učiteľ	WiFi žiak	SSID EDU_CERTIFIKAT	WiFi učiteľ	SSID EDU_SPEC	SSID EDU_HOST	LAN1 - učiteľ	LAN2 - žiak	LAN3 - DMZ	LAN4 - spec	LAN5 - internet	EDU_DC	Internet	BYOD portal
SSID EDU_PRIHLASENIE															
WiFi učiteľ		X	X		X			X	X	X			X	X	
WiFi žiak													X	X	
SSID EDU_CERTIFIKAT															X
WiFi učiteľ		X	X		X			X	X	X			X	X	X
SSID EDU_SPEC													X		
SSID EDU_HOST														X	
LAN1 - učiteľ		X	X		X			X	X	X			X	X	
LAN2 - žiak									X	X			X	X	
LAN3 - DMZ										X			X	X	
LAN4 - spec											X		X		
LAN5 - internet										X		X	X	X	
n/a															
zakázané															
povolené	X														

Tabuľka č. 155 prestupy medzi sieťami v rámci lokality

4.2.3.2.2 Súčasné LAN siete v školských lokalitách

Pre tie lokality siete EDUNET_SK, ktoré nie sú pripravené na aplikáciu technicky náročnejšieho riešenia s využívaním L2 služieb na úrovni VLAN alebo s prípadným nasadením štandardu 802.1X, je navrhnuté riešenie aplikovateľné aj na lokalitách, kde infraštruktúra a najmä aktívne prvky lokálnej siete neumožňujú využívanie vyššie uvedených štandardov.

Riešenie umožňuje na lokalitách s vyhovujúcou infraštruktúrou nasadenie štandardov 802.1X s MŠVVaŠ SR, prípadne umožňuje po dohode v dodatku zmluvy o doplnenie ďalších prepínačov s možnosťou rozšírenia VLAN resp. nasadenia 802.1x.

Riešenie ráta pre vybrané LAN 1-4 siete s autentifikáciou používateľov cez Captive portál v Centrálnej časti na zabezpečenie získania identity a oprávnenia na základe skupín a nastavovať podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne a zaradenia používateľa v IAM resp. AD DS skupine opísaných v časti“ Captive portál Centrály EDUNET_SK. Overením používateľa sa zabezpečí obohatenie logov centrálneho riešenia o identitu a zabezpečenie priradenia správneho oprávnenia používateľa pre web content

filtering, aplikačnú kontrolu a firewall pravidlá. Pre jednotlivé LAN hlavne pre LAN3 určené pre DMZ môžu byť definované výnimky z Captive portál autentifikácie.
Riešenie z dôvodu popísanej nemožnosti nastavenia štandardov 802.1X ponúka vyžitie tzv.: LAN siete LAN5 a WiFi SSID EDU_HOST, ktoré umožňuje prístup na určité materiály MŠVVaŠ SR, nepoužíva žiadne overovanie a sú uplatnené maximálne reštrikcie na prístup do internetu, pre každého používateľa rovnako, bez možností vytvorenia výnimiek. Používa sa len v špeciálnom prípade ak školské zariadenie nie je ochotné prejsť na systém tzv.: LAN 1 – 4, popísané v časti: „Všeobecný funkčný popis riešenia LAN“. Takéto pripojenie nezabezpečuje overenie používateľa. Nedochádza k obohacovaniu logov centrálneho riešenia o identitu a nedokáže prideliť zabezpečenie priradenia správneho oprávnenia používateľa pre web content filtering, aplikačnú kontrolu a firewall pravidlá, podľa grúp a nastavovať ich podľa bezpečnostných nastavení skupín z RADIUS/AD DS servera až do úrovne a zaradenia používateľa v IAM resp. AD DS.

4.2.3.2.3 Komunikácia z LAN do internetu a LAN iných školských zariadení

Komunikácia LAN lokality do internetu na LAN inej školskej lokality alebo zdrojov MŠVVaŠ SR je ošetrená tak, aby bol zabezpečený prechod všetkých komunikácií cez centrálny firewall EDUNET_SK a aby boli uplatnené dostupné security profily a ochrany. Komunikácie medzi rôznymi LAN školských zariadení sú kvôli bezpečnosti v predvolenom nastavení zakázané na centrálnom Firewalle EDUNET_SK a nie sú umožnené, s výnimkou LAN3 (DMZ), ako je popísané v časti „Komunikácia z internetu a iných školských zariadení do DMZ“.

4.2.3.2.4 Komunikácia z internetu a iných školských zariadení do DMZ

Komunikácie z Internetu a iných školských lokalít do LAN sietí školskej lokality sú zakázané. Môžu byť povolené iba za účelom sprístupnenia LAN3 a špecifického DMZ servera, akým je napríklad WEB server danej školy. Pridávanie povolení pre DMZ server sa realizuje na základe požiadavky od školy alebo školského zariadenia, špecifikáciou IP adresy, doménového mena, cieľového portu transportnej vrstvy IP modelu.

Vo všetkých LAN beží DHCP serverová služba zabezpečovaná routrom, pričom pridávanie pevných IP je zakázané s výnimkou DMZ. V každej DMZ sieti je totiž vyhradený rozsah IP ktorý je možné prideliť výlučne staticky podľa uváženia sieťového administrátora školy: každej škole je pridelený jeden subnet s maskou /26 (z celého DMZ rozsahu 10.176.0.0/14), pričom prvá polovica tohto subnetu (/27) je dedikovaná práve pre statické IP, druhá polovica je prideľovaná službou DHCP. V prípade nedostatočného počtu IP adries pre konkrétnu školu je možné pridať ďalší subnet /26.
Všetky webové a iné dátové služby hostované v rámci siete školy, ktoré majú byť dostupné zvonka, je preto potrebné presťahovať do dedikovanej LAN DMZ. Každá škola má pridelenú jednu verejnú IPv4 adresu, pre ktorú je pre potreby prístupu z verejného internetu do DMZ siete predkonfigurovaná služba NAT s prekladom 1:1 na prvú statickú adresu pre zariadenia z privátneho subnetu určeného pre DMZ (napr. pre pridelený subnet 10.176.1.0/26 je adresa routra 10.176.1.1 a prvá statická adresa pre zariadenie je 10.176.1.2). V prípade potreby nastavenia NAT prekladu špecifikovaných portov na ďalšie adresy v DMZ je potrebné o túto zmenu požiadať.

V prípade potreby je možnosť požiadať o vytvorenie reverzného DNS záznamu na verejnú IP adresu pre potreby prístupu cez FQDN.

4.2.3.2.5 Spôsob odovzdávania služieb/terminácie služieb na fyzických rozhraniach prepínača

Návrh ráta s viac LAN sieťami podľa jednotlivého určenia ako je možné ukončiť na portoch LAN prepínača, z tohto dôvodu je potrebné niektoré LAN terminovať aj na CPE. Terminovanie LAN na prepínači a na CPE má nasledujúce limitácie:

- Ukončenie jedenej LAN siete (VLAN) nie je možné terminovať na CPE a zároveň LAN prepínač, ale iba na jednom z daných zariadení.
- Na prepínači je možné ľubovoľné odovzdanie LAN móde trunk alebo Access VLAN.
- Na CPE je možné terminovať jednu LAN sieť (VLAN) na viacerých portoch buď v móde trunk alebo Access, kombinácia nie je možná.
- WiFi AP je možné terminovať iba na LAN prepínači kvôli podpore funkcie PoE+.

Lokality typu A,B,C,X

Pri terminácii na týchto lokalitách je ukončenie LAN služieb na fyzických portoch prepínača v režime Access VLAN. Uplink porty prepínača slúžia na prepojenie s CPE.
Využitie fyzických portov na LAN prepínači je nasledovné:

- LAN port 1 až LAN port 5 – pripájanie WiFi AP s využitím PoE,
- LAN port 6 – terminácia LAN rozhrania LAN 1
- LAN port 7 – terminácia LAN rozhrania LAN 2
- LAN port 8 – Uplink porty pre prepojenie s CPE.

Využitie fyzických portov na CPE LAN port 1 – terminácia LAN rozhrania LAN 3

- LAN port 2 – terminácia LAN rozhrania LAN 4
- LAN port 3 – terminácia LAN rozhrania LAN 5
- LAN port 4-7 a port DMZ rezervácia pre ďalšie použitie
- LAN port WAN2 – prepoj na LAN prepínač
- WAN port WAN1 – prepoj do MPLS

Lokality typu D,E

Pri terminácii na týchto lokalitách je ukončenie LAN služieb na fyzických portoch prepínača v režime Access VLAN. Uplink porty prepínača slúžia na prepojenie s CPE.
Využitie fyzických portov na LAN prepínači je nasledovné:

- LAN port 1 až LAN port 5 – pripájanie WiFi AP s využitím PoE,
- LAN port 6 – terminácia LAN rozhrania LAN 1
- LAN port 7 – terminácia LAN rozhrania LAN 2
- LAN port 8 – Uplink porty pre prepojenie s CPE.

Využitie fyzických portov na CPE

- LAN port 1 – terminácia LAN rozhrania LAN 3

- LAN port 2 – terminácia LAN rozhrania LAN 4
- LAN port 3 – terminácia LAN rozhrania LAN 5
- LAN port 4 – prepoj na LAN prepínač
- WAN prepoj do MPLS

Lokality typu F

Nie je inštalovaný LAN prepínač, pri terminácii na lokalitách typu F je ukončenie služieb na fyzických portoch CPE ako Access VLAN. Následné prepojenie jednotlivých LAN portov s lokálnou sieťou je individuálne.

Využitie fyzických portov na CPE

- LAN port 1 - terminácia LAN rozhrania LAN 1
- LAN port 2 – terminácia LAN rozhrania LAN 5
- LAN port 3-4 rezervácia pre ďalšie použitie
- WAN prepoj do MPLS

4.2.3.2.6 Spôsob odovzdávania služieb/terminácie služieb na logickom rozhraní prepínača

Terminácia na logickom rozhraní prepínača bude výhradne s využitím funkcionalít 802.1q a 802.1x.

Samotný prepínač bude terminovať VLAN len v Access móde pre LAN rozhrania a vo VLAN trunk móde pre Uplink rozhrania bude zabezpečovať len ich transport a mapovanie prevádzky na základe 802.1q a 802.1x.

Logické rozhrania jednotlivých sietí pre WiFi a LAN budú terminované na CPE.

4.2.3.2.7 Mapovanie dátovej prevádzky pre riadenie šírky pásma

Všetky dáta mapované v príslušnej triede CoS zdieľajú spoločnú šírku pásma pre LAN pripojenia a pre WiFi pripojenia.

V rámci riadenia šírky pásma nie sú obmedzované šírky dátového pásma v rámci lokality – teda nie je limitovaný prístup k lokálnym zdrojom dát, ale sú limitované iba prístupy k dátam mimo lokality školského zariadenia – teda dáta tečúce cez sieť EDUNET_SK.

4.3 Parametre kvality služby – Quality of Service

Globálne nastavenia bezpečnosti sú nastavenia pre komunikáciu v rámci VPN siete EDUNET_SK, pravidlá pre prístup k obsahu v tejto sieti, ako aj pravidlá pre prístup k zdrojom umiestneným mimo siete EDUNET_SK.

Lokálne nastavenia bezpečnosti sú nastavenia aplikované priamo na zariadeniach inštalovaných v lokalite školského zariadenia (CPE, prepínač a WiFi AP). Tieto nastavenia priamo ovplyvňujú riadenie bezpečnosti komunikácie v rámci školského zariadenia, teda najmä prestupy a prístupy používateľov k lokálnym sieťam a sieťovým prostriedkom.

Navrhnuté QoS riešenie obsahuje 3 triedy QoS a CoS, tak aby vyhovelo požiadavkám MŠVVaŠ na riadenie kvality služieb ako v lokálnej časti tak aj globálnej časti. Z pôvodných 2.tried QoS a CoS (Cos 1 a 2) sa rozšírilo na 3 triedy (Cos 1, 3 a 6), aby sme vedeli garantovať dostupnosť kritických služieb v sieti EDUNET_SK počas elektronického testovania žiakov (CoS

1), tak aj počas výučbového procesu prístup k výučbovým materiálom definováným MŠVVaŠ (CoS 3) ako v globálnej tak aj lokálnej časti.

4.3.1 Globálne nastavenia kvality služby

Globálna kvalita služieb definuje pravidlá riadenia kvality služieb pre transportnú časť siete EDUNET_SK a pre centrálu EDUNET_SK.
Globálne riadenie kvality služieb definuje pravidlá pre riadenie transportu dátových tokov a celkovú kvalitu dostupnosti služieb, ako aj ich technických parametrov pre kvalitu prenosu dát medzi lokalitami a centrálou EDUNET_SK. Okrem transportnej časti siete sú globálne nastavenia pre kvalitu aplikované aj na prestupových prvkoch centrály EDUNET_SK, kde je priamo riadený prestup do iných sietí a k iným zdrojom dát (dáta v DCRŠ, Internet, iné zdroje dát). Globálne QoS využiva 3 triedy na mapovanie a prioritizáciu komunikácie medzi lokaklitami v sieti EDUNET_SK, su to QoS 1, QoS 3 a QoS 6. Detailný popis daných riešení je uvedený nižšie. QoS 6 slúži ako best-effort čiže všetká komunikácia, ktorá nebude využívať QoS 1 a 3 automaticky spadá do QoS 6.

4.3.2 Lokálne nastavenia kvality služby

Lokálna kvalita služieb definuje pravidlá pre riadenie kvality služieb v rámci dátových tokov v lokalite školského zariadenia, najmä však rieši prioritizáciu dátových tokov medzi jednotlivými LAN a WiFi sieťami tak, aby bolo možné garantovať prístupy k lokálnym dátovým zdrojom a riadený prístup ku globálnym dátovým zdrojom. Lokálne nastavenia bezpečnosti sú priamo aplikované na LAN a WiFi prvkoch v lokalitách. Lokálne QoS využívajú 3 triedy CoS a to CoS 1, 3 a 6. CoS 6 slúži ako best-effort, čiže všetka komunikácia, ktorá nespadá pod CoS 1 a 3 je automaticky mapovaná ako CoS 6. Detailný popis riešenia je uvedený nižšie.

Na lokálnom CPE prípadne Firewall zariadení sa zapnú tieto bezpečnostné funkcie:

- Dynamic ARP inspection pre zabránenie preposielania neplatných ARP dotazov a odpovedí na porty prepínača v rovnakej VLAN
- DHCP snooping pre ochranu nechceného DHCP servera v LAN sieťach lokalít, dôveryhodný DHCP server je považovaný iba centrálny EDUNET_SK
- IGMP Snooping pre podporu multicastov
- STP spanning tree ochranu pre L2 slučkami
- Storm control ochrana proti zahlteniu siete nadmernými počtom broadcast, multicast nebo neznámymi unicast paketmi
- ochrana proti MAC flooding - proti útoku pomocou zahlteniu MAC adresami pre možnosť vyčerpať pamäte prepínača alebo CPE

Triedy QoS

<u>QoS 1 pre služby mapované podľa CoS 1</u>

- dôležitá dátová prevádzka s vysokou prioritou určená pre služby s vysokou prioritou dátového prenosu v sieti EDUNET_SK
- primárne využitie pre účely zabezpečenia prístupu k aplikáciám a dátovým zdrojom pri online testovaniach žiakov v sieti EDUNET_SK,

- mapovanie prevádzky do CoS 1 bude realizované na lokalitách školských zariadení pre prevádzku v sieti EDUNET_SK,
- kvalitatívne parametre v sieti EDUNET_SK:
    - latency: < 100 ms,
    - packet loss: <1%,
    - jitter: <30 ms,
    - šírka pásma pre služby triedy CoS 1 bude dynamický prideľovaná to znamená ak sa daná služba nebude využívať, bude možné použiť toto garantované pásmo na iné triedy QoS ako CoS 3 CoS 6.
    - pri symetrickom a asymetrickom pripojení bude garantovaná kapacita podľa požiadavky MŠVVaŠ SR a typu školy môže byť garantovaná až do 100% kapacity linky. V prípade použitia asymetrického zapojenia školy sa kapacita vypočítava z uplinkovej rýchlosti daného pripojenie

<u>QoS 3 pre služby mapované podľa CoS 3</u>

- dátová prevádzka so strednou prioritou, určená pre služby nutné pre zabezpečenie bežnej školskej prevádzky,
- primárne využitie pre účely zabezpečenia plynulosti učebného procesu, teda pre prístup učiteľov, žiakov a zamestnancov školských zariadení, na zariadenia definované MŠVVaŠ SR
- mapovanie prevádzky do CoS 3 bude realizované na lokalitách školských zariadení v sieti EDUNET_SK
- kvalitatívne parametre v sieti EDUNET_SK:
    - latency: < 100ms,
    - packet loss < 1%,
    - jitter: < 30 ms,
    - šírka pásma pre služby triedy CoS 3 bude dynamický prideľovaná to znamená ak sa daná služba nebude využívať bude možné použiť toto garantované pásmo na triedu CoS 6.
    - pri symetrickom a asymetrickom pripojení bude garantovaná kapacita podľa požiadavky MŠVVaŠ SR a podľa typu školy. V prípade použitia asymetrického zapojenia školy sa kapacita vypočítava z uplinkovej rýchlosti daného pripojenie.

<u>QoS 6 pre služby mapované podľa CoS 6</u>

- dátová prevádzka v kvalite best-effort, určená pre všetku dátovú prevádzku, ktorá nespadá pod CoS 1 a CoS 3,
- primárne využitie pre prístup žiakov a učiteľov k dátovým zdrojom, ktoré priamo nesúvisia s výučbovým procesom,
- mapovanie prevádzky do CoS 6 bude realizované na lokalitách školských zariadení,
- kvalitatívne parametre v EDUNET_SK:
    - latecny: < 150 ms
    - packet loss: < 3 %

- jitter: < 50 ms
- šírka pásma pre služby triedy CoS 6 bude využívať zvyšnú časť dostupnej kapacity lokálnej siete pre školskú lokalitu
- trafika, ktorá nebude označená QoS 1 a 3 bude automaticky spadať pod danú triedu QoS

4.3.3 Lokálne nastavenia pre riadenie kvality služieb

CoS 1

Pre triedu Cos 1 bude mapovanie prebiehať nasledovným kľúčom:
Lokálne zdroje

- mapovanie podľa zdrojovej a cieľovej IP adresy
- využívanie CoS 1 pre lokálne zdroje dát nie je definované.

Zdroje v sieti EDUNET_SK

- mapovanie podľa zdrojovej a cieľovej IP adresy a označkovanie danej komunikácie
- mapovanie prevádzky z LAN 4 a WiFi SSID EDU_SPEC smerujúcej k vybraným zdrojom v EDUNET_SK,
- zdroje v EDUNET_SK budú definované zo strany MŠVVaŠ SR.

Zdroje mimo siete EDUNET_SK

- mapovanie podľa zdrojovej a cieľovej IP adresy a označkovanie danej komunikácie
- mapovanie prevádzky z LAN 4 a WiFi SSID EDU_SPEC smerujúcej k vybraným zdrojom mimo EDUNET_SK,
- zdroje mimo EDUNET_SK budú definované zo strany MŠVVaŠ SR.

CoS 3

Pre triedu Cos 3 bude mapovanie prebiehať nasledovným kľúčom:
Lokálne zdroje

- mapovanie podľa zdrojovej a cieľovej IP adresy
- využívanie CoS 3 pre lokálne zdroje dát nie je definované

Zdroje v sieti EDUNET_SK

- mapovanie podľa zdrojovej a cieľovej destinácie a následne označenie danej dátovej prevádzky pod CoS 3
- mapovanie prevádzky z LAN 1, LAN 2, LAN 3 a autentifikovaných používateľov z WiFi smerujúcej k vybraným zdrojom digitálneho edukačného obsahu v EDUNET_SK,
- zdroje digitálneho edukačného obsahu v sieti EDUNET_SK budú definované zo strany MŠVVaŠ SR

Zdroje mimo siete EDUNET_SK

- mapovanie podľa zdrojovej a cieľovej IP adresy a označkovanie danej komunikácie
- mapovanie prevádzky z LAN 1, LAN 2, LAN 3 a autentifikovaných používateľov z WiFi smerujúcej k vybraným zdrojom digitálneho edukačného obsahu v EDUNET_SK
- zoznam dôveryhodných zdrojov mimo siete EDUNET_SK je definovaný pravidlami pre filtrovanie obsahu podľa typu autentifikovaného používateľa v centrále EDUNET_SK.

CoS6

Pre triedu CoS 6 (best-effort) bude mapovanie prebiehať nasledujúcim spôsobom.
Lokálne zdroje

- celá komunikácia ktorá nebude používať CoS 1 a CoS 3, automaticky bude označená ako CoS 6

Zdroje v sieti EDUNET_SK

- celá komunikácia, ktorá nebude mapovaná v CoS 1 a CoS 3 bude automaticky označená ako CoS6

Zdroje mimo siete EDUNET_SK

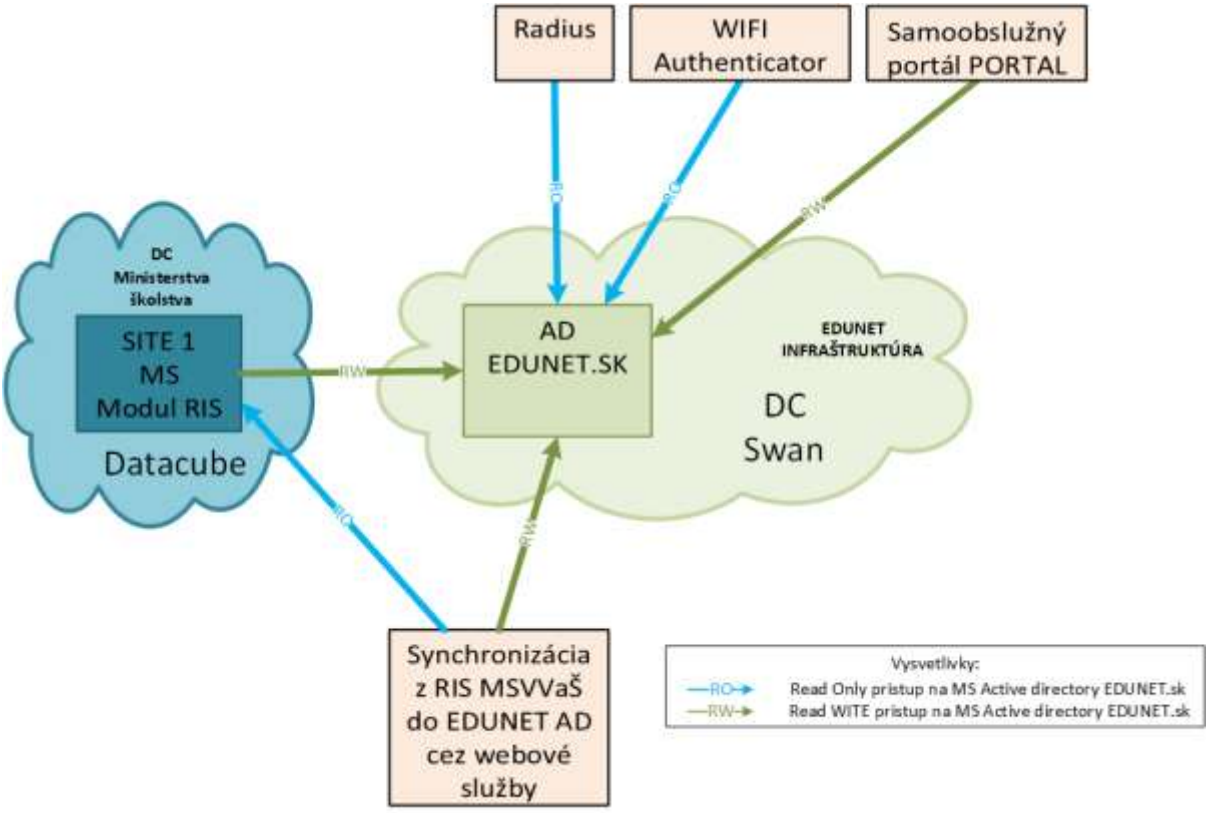
- celá komunikácia, ktorá nebude mapovaná v CoS 1 a CoS 3 bude automaticky označená ako CoS6

5 Integrácia systémov

5.1 Prepojenie systémov IAM a Active Directory

Jedným zo základných predpokladov pre nasadenie akýchkoľvek centrálne manažovaných služieb v sieti EDUNET_SK je centrálny manažment používateľov. MŠVVaŠ SR v rámci svojich interných systémov disponuje databázou používateľov, ktorú je možné využiť pre potreby overovania používateľov, poskytovania doplnkových údajov k používateľom a k prideľovaniu oprávnení pre týchto používateľov.

Základným prvkom pre centrálny manažment používateľov je Active Directory databáza používateľov, ktorá je naplnená a pravidelne aktualizovaná z relevantných zdrojov dát, ktorými sú IAM a RIS.



Obrázok č. 10: Integračná schéma pripojenia IAM do EDUNET_SK

Na obrázku vyššie je schematicky znázornené prepojenie AD databáz a jednotlivých komponentov EDUNET_SK riešenia. V rámci projektu EDUNET_SK bude vytvorená doména edunet.sk. Vznik domény je nutný z dôvodu potreby servisných účtov a security skupín pre podporné systémy Centrály EDUNET_SK (DNS, Virtualizácia, EDUNET portál, zabbix,

správcovské VPN, autentifikácia network core zariadení). Správa bude prebiehať prostredníctvom domain controlleru spoločnosti SWAN.

Centrála EDUNET_SK bude používať jednu prevádzkovú Active Directory databázu EDUNET.sk, nezávislú od dc.iedu.sk. Prevádzková databáza edunet.sk bude použitá ako hlavná na autentifikáciu používateľov a overovanie príslušnosti do security group a atribútov používateľov pre systémy a služby.
AD edunet.sk bude použitá pre prihlásenie používateľov a modifikáciu členstva v skupine (group membership) na podporné systémy.
Jednotlivé komponenty (centrálny Firewall, lokálne smerovače/firewally, centrálny radius/portal server a centrálne riadenie WiFi) budú pristupovať ku AD edunet.sk pre autentifikáciu, autorizáciu a zistenie príslušnosti do Active Directory - Security group. Firewall kvôli Captive portalu, Radius server kvôli AAA WiFi a portálovým službám. Centrálne riadenie WiFi kvôli zistovaniu príslušnosti do group a obohacovanie radius accounting o informáciu o príslušnosti do Active directory - Security group. Prístup do edunet.sk je v móde read only, prístup do EDUNET.sk v read write.

Zdrojová referenčná databáza identity je modul RIS. Pre riešenie replikácie používateľských účtov do novej domény EDUNET je navrhnuté použitie modulu RIS a ostatných súčastí iných modulov v rámci modulu RIS pre replikácie identít. RIS a jeho súčasti umožnia potrebný zápis používateľských prihlasovacích údajov a ich atribútov zo zdrojových systémov do cieľového systému AD edunet.sk. Systém RIS musí zabezpečiť sledovanie zmeny v rámci zdrojových systémov a aplikovať zmeny nad AD edunet.sk automaticky prípadne manuálnym zásahom. Zápis do AD edunet.sk bude v móde read write operácie, kedy budú vkladané preddefinované dáta, ktoré bude možné upravovať iba prostredníctvom modulov RIS.

Očakávané hodnoty zápisu modulu RIS do AD edunet.sk budú podľa nasledujúcich atribútov.

Názov atribútu v AD	Význam atribútu	Typ
objectGuid	Identifikátor	reťazec
objectSid	Security identifikátor	reťazec
givenName	Meno	reťazec
sn	Priezvisko	reťazec
mail	Email	reťazec
<<custom>> EDUID	Jednoznačný biznisový identifikátor	reťazec
<<custom>> birthdate	Dátum narodenia	dátum
<<custom>>UcitelEDUID	Zoznam EDUID škôl, kde je učiteľom	reťazec
sAMAccountName	Názov účtu	reťazec
displayName	Meno + priezvisko	reťazec
userPassword	Heslo	reťazec

Tabuľka č. 16 AD štruktúra group

Horeuvedená tabuľka a jej hodnoty sú požadované hodnoty pre zápis modulom RIS MŠVVaŠ SR do AD edunet.sk.

Na základe zapisovaných atribútov v AD databáze používateľov je možné cez AD DS rozhranie pripojiť centrálne systémy EDUNET_SK a poskytovať im údaje o jednotlivých identitách v nasledovnej štruktúre:

Názov atribútu v AD	Význam atribútu	Typ
objectGuid	Identifikátor	reťazec
objectSid	Security identifikátor	reťazec
givenName	Meno	reťazec
sn	Priezvisko	reťazec
mail	Email	reťazec
title	učiteľ, žiak, zamestnanec	reťazec
sAMAccountName	login	reťazec
displayName	Meno + priezvisko	reťazec
userPassword	Heslo	reťazec
<<custom>> EDUID	Jednoznačný biznisový identifikátor	reťazec
<<custom>> birthdate	Dátum narodenia	dátum
<<custom>>UcitelEDUID	Zoznam EDUID škôl, kde je učiteľom	reťazec
sAMAccountName	Názov účtu	reťazec
userPrincipalName	login@edunet.sk	dátum
distinguishedName	CN=login,OU=niečo,OU=niečo,DC=edunet,DC=sk	reťazec
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=edunet,DC=sk	reťazec
memberOf	príslušnosť skupiny alebo viacerých skupín	reťazec

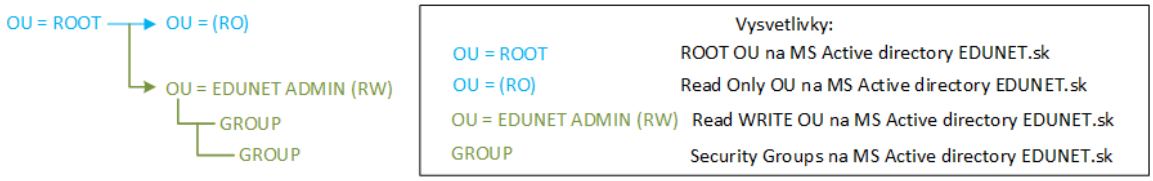
Tabuľka č. 17 AD štruktúra group

Voči doméne EDUNET.sk sa budú autentifikovať a autorizovať zariadenia a systémy Centrálny Rádius, Authentifikator a Firewall s právom domain user, ktoré slúžia ako používatelia pre firewall a identity management.
MŠVVaŠ SR a modul RIS bude mať v AD edunet.sk admin používateľa a bude sa používať pre integračné nástroje a má možnosť plniť užívateľov a meniť ich atribúty v dohodnutej OU.

Nasledujúci obrázok zobrazuje logickú organzačnú štruktúru OU. Jednotlivé zariadenia Firewall, Radius, Autentifikátor budú pristupovať a mať read only práva do dohodnutej OU sprístupnenej a plnenej MŠVVaŠ SR. Do dohodnutej OU (označenej modrou farbou) budú plnení MŠVVaŠ RIS modulom jednotliví používatelia. RIS bude do dohodnutej OU pristupovať s oprávnením Read write. Interný systém bude cez webové služby z MŠVVaŠ SR pomocou SOAP API obohacovať hlavne atribút „title“ o hodnoty žiak, učiteľ, zamestnanec prípadne iné, kvôli identifikácií úrovne oprávnenia v rámci EDUNET_SK. Interný systém bude cez webové služby z MŠVVaŠ SR pomocou SOAP API obohacovať aj iné pomocné

potrebné atribúty potrebné počas prevádzky. Ostatné OU ako napríklad OU=Edunet_admin (označených zelenou farbou) security group budú vytvorené pre interné prevádzkové účely dodávateľa. Do daných security group bude mať práva iba dodávateľ. Integrácia RIS voči domain controllerom AD edunet.sk a webových služieb SOAP API bude cez vybudovanú infraštruktúru dodávateľa a DC MŠVVaŠ SR.

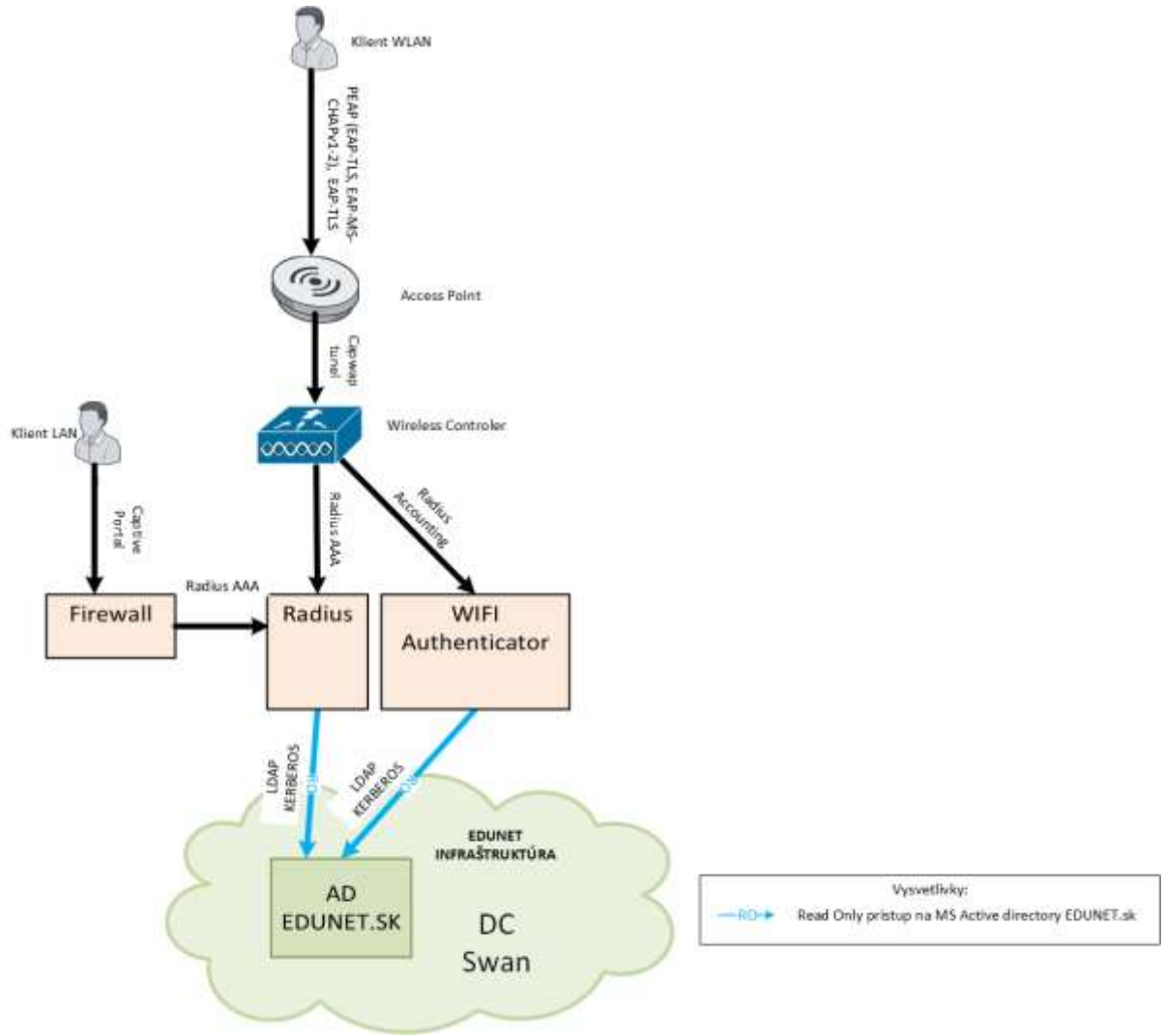
Z dôvodu potreby napríklad blokovania používateľov, budú použité RW (read-write) operácie iba nad dohodnutou OU (organization unit) v doméne edunet.sk. Všetky požiadavky budú smerovať na domain controller v Centrálnom bode EDUNET_SK. Operácie RW nebudú použité na vytváranie a modifikáciu organizačnej jednotky, ale iba na zmeny (pridávanie a odoberanie) členstva v skupine (security group).



Obrázok č. 11: Organizačná štruktúra EDUNET_SK

V ostatných organizačných jednotkách napr. OU=EDUNET_custom_group, nachádzajúcej sa v doméne edunet.sk budú bezpečnostné skupiny (group) - typ skupiny Global, do ktorých sa bude meniť príslušnosť globálnych skupinách na základe rozhodnutia administrátora zo strany dodávateľa riešenia. Organizačné skupiny v tejto jednotke sa budú priebežne pridávať. Prvá bude s názvom EDU_karanténa. Pridávanie do security skupín v OU=EDUNET_custom_group bude vykonávané administrátormi EDUNET_SK. Systémy dodávateľa po prihlásení do Active directory obohatí alebo vyradí skupinu v OU=EDUNET_custom_group o potrebného používateľa. Organizačná jednotka OU=Edunet_admin bude iba v správe dodávateľa.

Autorizácia používateľov bude prebiehať na úrovni prístupovej sieti. Proces autorizácie pre používateľa znamená zadanie prihlasovacích údajov pre LAN do Captive portál a pre WLAN na úrovni Access point a cez rádius server sa overí voči Active Directory. Autorizácia do siete záleží od návratových atribútov používateľa z Active directory a príslušnosti ku security group. Rádius server následne podľa politík pridelí oprávnenia.



Obrázok č. 12: Proces autorizácie používateľov

Používatelia sa v systéme delia na základe bezpečnostných skupín (žiak, učiteľ, zamestnanec, atď.) a podľa stupňa (1. stupeň základnej školy, 2. stupeň základnej školy, stredná škola). Ďalej sa rozlišujú aj pomocou AD atribútov (EDUID školy). Používatelia budú pridávaní do bezpečnostných skupín podľa nasledujúcich kritérií:

- žiak, učiteľ, zamestnanec, ...,
- stupeň: 1. stupeň základnej školy, 2. stupeň základnej školy, stredná škola
- identifikátor EDUID školy

Tieto údaje budú zabezpečené cez synchronizáciu z RIS MSVVaŠ do EDUNET AD cez webové služby.

Centrála EDUNET_SK podporuje SOAP, RESTful API rozhrania a SAML služby. Primárny zdroj pre všetky používateľské účty je Active Directory.

5.2 Synchronizácia z RIS MSVVaŠ do EDUNET AD cez webové služby

5.2.1 Koncept riešenia

Navrhnutá synchronizácia medzi RIS a AD EDUNET replikuje základné údaje o používateľoch (podľa tabuľky č.16). Pre funkčnosť portálu EDUNET je potrebná kategorizácia každého používateľského účtu a jeho synchronizácia.
Pre doplnenie chýbajúcich údajov do internej databázy AD EDUNET z RIS MSVVaŠ bude použitý komponent synchronizácie údajov. Jedná sa o komponent, ktorý bude pre svoju potrebu pristupovať k údajom integračných služieb RIS ako aj AD EDUNET.

5.2.1.1 Zdrojový systém

Ako zdrojový systém na získanie informácii bude slúžiť integračné rozhranie služieb RIS. Predpokladá sa použite API rozhrania na báze SOAP.
Na základe dokumentácie budú volané funkcie

- prihlásenie sa menom a heslom
- odhlásenie
- vyhľadanie objektov podľa zadaných kritérií
- poskytnutie aktuálnych údajov objektu

Obsah požadovaných oprávnení je iba na čítanie.

5.2.1.2 Cieľový systém

Ako cieľový systém na uloženie informácií slúži AD EDUNET. Komunikačný protokol je LDAP.
Obsah požadovaných oprávnení je na čítanie aj zápis.

5.2.2 Chýbajúce údaje

5.2.2.1 Zaradenie používateľského účtu.

Pre správnu identifikáciu prístupu v rámci EDUNET siete je nutné jednoznačne určiť zariadenie používateľského účtu podľa typu alebo ročníka používateľa. Tieto údaje nebudú synchronizované prostredníctvom RIS modulu.

5.2.3 Aktualizácia údajov

Systém EDUNET nie je notifikovaný o zmenách jednotlivých používateľov vo svojej databáze, teda nevie efektívne posúdiť, ktoré atribúty sa od poslednej synchronizácie zmenili. Preto bude aktualizácia údajov prebiehať byť inkrementálne alebo celkovo.

5.2.3.1 Inkrementálna synchronizácia údajov

Synchronizačný modul z AD EDUNET zistí všetkých používateľov, ktorí nespĺňajú kritériá. Na základe získaného EDUID sa z RIS získajú potrebné záznamy, ktoré sa zapíšu do EDUNET AD.
Tento postup reflektuje iba novozaložených používateľov. Zmeny atribútov už existujúcich používateľov nie sú reflektované.

5.2.3.2 Celková synchronizácia

Pri celkovej synchronizácii sa z AD EDUNET načítajú všetky používateľské kontá. Pre každý záznam sa získa aktuálny záznam z RIS systému. Pokiaľ sú údaje v nesúlade, upraví sa databáza AD EDENET.

5.2.3.3 Poznámky

Vzhľadom na očakávaný počet používateľských účtov (rádovo 100 tisíc) a frekvencie (nízka) ich zmeny sa odporúča inkrementálna synchronizácia v kratších časových intervaloch, celkovo v dlhšej perióde. Aktuálne nie sú známe systémové nároky na synchronizačný komponent ani jeho dopady na jednotlivé systémy, takže tieto budú doladené následne po vzájomnom odsúhlasení na technickej úrovni.

5.3 Dočasné naplnenie AD edunet.sk

Vzhľadom na očakávané medzi obdobie nasadenia integrácie konceptu naplňovania modulu RIS na AD edunet.sk a integráciu webových služieb SOAP API a plnenia potrebných atribútov pre jednoznačné určenie úrovne zabezpečenia je potrebné naplnenie AD edunet.sk pracovníkmi MŠVVaŠ SR pre užívateľov prvých cca 400 škôl manuálnym importom do AD edunet.sk vo formáte:

Názov atribútu v AD	Význam atribútu	Typ
objectGuid	Identifikátor	reťazec
objectSid	Security identifikátor	reťazec
givenName	Meno	reťazec
sn	Priezvisko	reťazec
mail	Email	reťazec
title	ucitel, zamestnanec, ziak_ZS_1st, ziak_ZS_2st, ziak_SS	reťazec
sAMAccountName	login	reťazec
displayName	Meno + priezvisko	reťazec
userPassword	Heslo	reťazec
<<custom>> EDUID	Jednoznačný biznisový identifikátor	reťazec
<<custom>> birthdate	Dátum narodenia	dátum
<<custom>>UcitelEDUID	Zoznam EDUID škôl, kde je učiteľom	reťazec
sAMAccountName	Názov účtu	reťazec
userPrincipalName	login@edunet.sk.sk	dátum
distinguishedName	CN=login,OU=niečo,OU=niečo,DC=edunet,DC=sk	reťazec
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=edunet,DC=sk	reťazec

Tabuľka č. 18 štruktúra AD pre prvotný import

Pre atribút title hodnoty ziak_ZS_1st znamená žiak základnej školy prvého stupňa, hodnota ziak_ZS_2 st znamená žiak základnej školy druhého stupňa, ziak_SS znamená žiak strednej školy.

5.4 Prepojenie Dátového centra MŠVVaŠ

Prepojenie bude vo finálnej architektúre realizované cez 10 GB optické prepoje:

1. DC Datacube – strana MŠVVaŠ SR a SWAN DC1
2. DC Datacube – strana MŠVVaŠ SR a SWAN DC2

Ukončenie optického prepoja v DC SWAN v EDUNET Centrálnych prepínačoch, cez 10 GB Single mode SFP, ER (40 km)

Pre tento účel budú na Centrálnych prepínačoch pripravené nasledujúce porty a navrhované VLAN:

- VLAN 30 pre prepoj 1), určený rozsah 172.31.130.0/29 , fyzicky a L2 ukončené na EDUNET Centrálny prepínač dcp-edu-core-sw-01, port eth1/10, IP L3 ukončené na zariadení EDUNET Firewall (dcp-edu-core-fw-01)
- VLAN 31 pre prepoj 2), určený rozsah 172.31.130.8/29 , fyzicky a L2 ukončené na EDUNET Centrálny prepínač dcud-edu-core-sw-01, port eth1/10, IP L3 ukončené na zariadení EDUNET Firewall (dcud-edu-core-fw-01)

Smerovanie oboch rozsahov cez protokol BGP.

- BGP AS strany SWAN je AS64999, strany BGP AS Ministerstva Školstva AS 65500
- VLAN 30, 172.31.130.0/29, primárna linka
    - Smerovač/Firewall Ministerstva Školstva .6
    - EDUNET Firewall (dcp-edu-core-fw-01) .1

- VLAN 31, 172.31.130.8/29, backup linka
    - Smerovač/Firewall Ministerstva Školstva .14
    - EDUNET Firewall (dcud-edu-core-fw-01) .9
    - Znevýhodnenie linky cez AS prepend

Oznamované siete zo strany SWAN EDUNET_SK budú:

- 10.32.0.0/11
- 10.64.0.0/10
- 10.128.0.0/10
- 10.192.0.0/10
- 192.168.128.0/17
- Prípadne ďalšie podľa potreby

Oznamované siete zo strany Ministerstva Školstva budú:

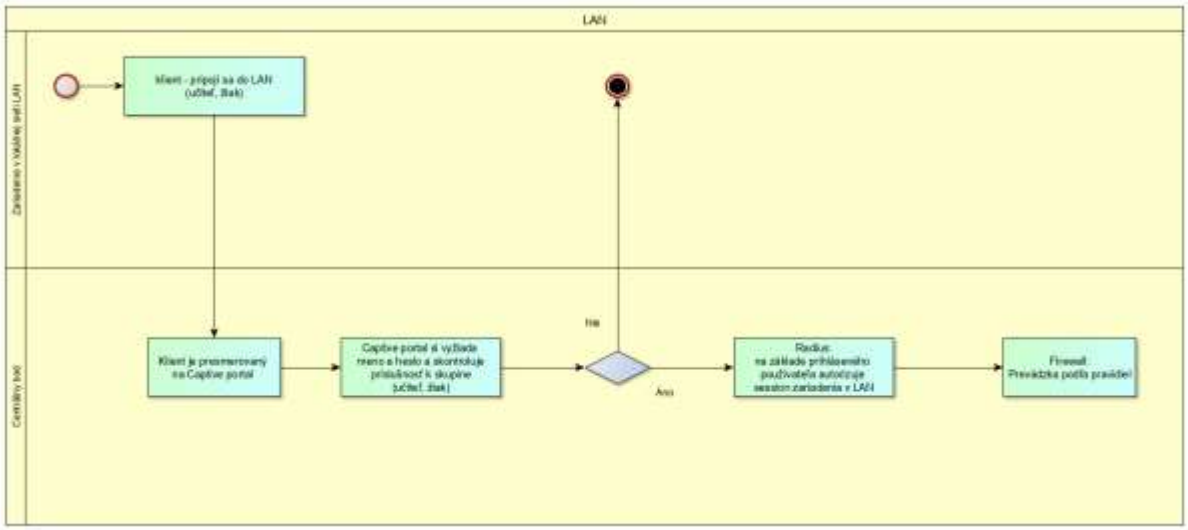
- 10.0.0.0/11
- Prípadne ďalšie podľa potreby

6 Používateľský proces

Používatelia služieb EDUNET_SK budú pristupovať k sieti a obsahu prostredníctom Wifi prístupových bodov alebo LAN siete Centrálny bod zároveň poskytuje možnosť pripojenia vlastného zariadenia prostredníctvom BYOD procesu.

6.1 Prihlásenie cez LAN sieť

Obrázok č. 13 zobrazuje interakciu používateľa pri prihlásení do siete EDUNET_SK prostredníctvom LAN siete.



Obrázok č. 13: Diagram – Prihlásenie do LAN siete

Používatelia zariadení pripojených do do LAN1 učiteľ a LAN4 spec sú pri pokuse o prístup na akúkoľvek internetovú stránku presmerovaní na Captive portal na URL **captive.edunet.sk** . Po prihlásení svojim IAM kontom bude umožnené vytvorenie pripojenia do internetu.
Návštevník školy sa svojím zariadením pripojí na SSID EDU_HOST bez zadania mena a hesla. Pri pokuse o prístup na akúkoľvek internetovú stránku sa prostredníctvom presmerovania prehliadača zobrazí tzv. Disclaimer (súhlas s podmienkami používania) na URL **portalXY.edunet.sk**.

Tabuľka č. 17 zobrazuje popis jednotlivých scenárov v prípade prihlásenia používateľa s platným, respektíve neplatným IAM kontom na zariadenia pripojené cez LAN konektivitu pomocou zadania prihlasovacích údajov (meno, heslo).

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Úžívateľ zadal platné prihlasovacie údaje	Používateľ je prihlásený do infraštruktúry EDUNET_SK s pridelenými oprávneniami
negatívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Používateľ zadal neplatné prihlasovacie údaje	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Úžívateľ so zadanými prihlasovacími udajmi nie je evidovaný v systéme IAM	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Používateľ zadal neplatné prihlasovacie heslo	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Používateľ zadal viac ako povolený počet opakovaní nesprávne prihlasovacie údaje a konto bolo zablokované v EDUNET_SK AD	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.

Tabuľka č. 19 Scenáre – Prihlásenie do LAN siete s IAM kontom

6.2 Prihlásenie používateľa prostredníctvom WiFi

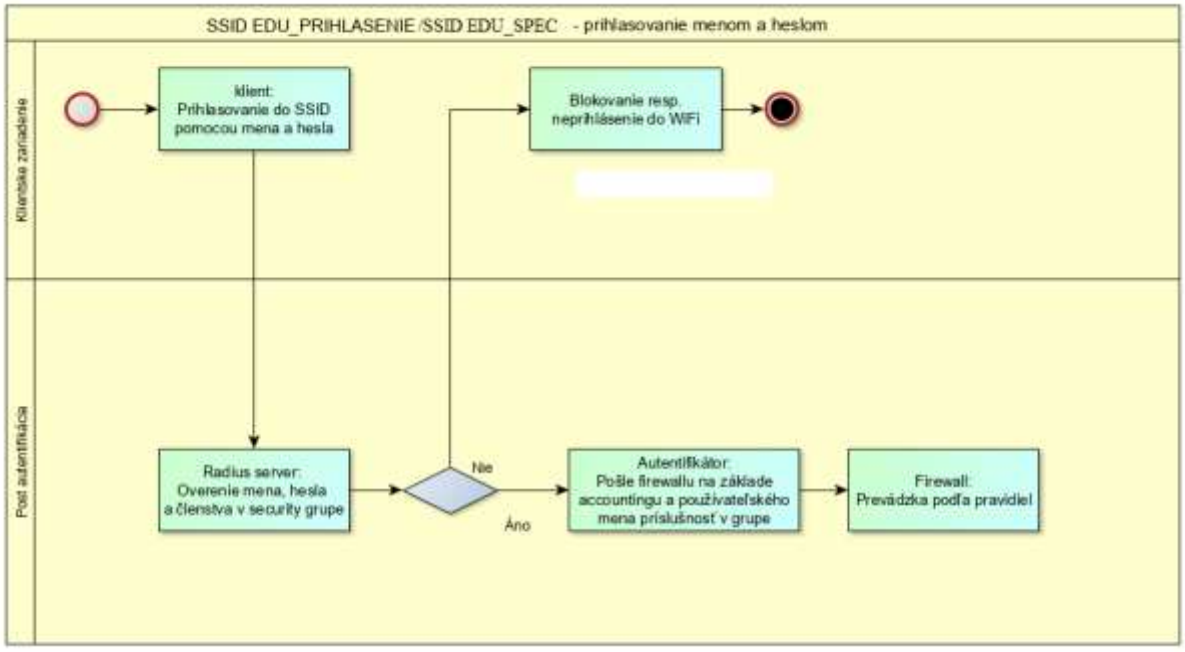
V rámci riešenia EDUNET_SK je konfiguračne rozdelená dátová prevádzka do jednotlivých SSID nasledovne:

- SSID EDU_PRIHLASENIE
- SSID EDU_CERTIFIKAT
- SSID EDU_SPEC
- SSID EDU_HOST

6.2.1 SSID EDU_PRIHLASENIE a SSID EDU_SPEC

Primárnou funkciou SSID EDU_PRIHLASENIE a SSID EDU_SPEC je autentifikácia, autorizácia a následné pripojenie používateľa k sieti EDUNET_SK a k relevantnému obsahu. Autentifikácia bude prebiehať prostredníctvom mena a hesla.

Obrázok č. 14 zobrazuje interakciu používateľa pri prihlásení do siete EDUNET_SK prostredníctvom SSID EDU_PRIHLASENIE a SSID EDU_SPEC



Obrázok č. 14: Diagram – Prihlásenie do SSID EDU_PRIHLASENIE/EDU_SPEC

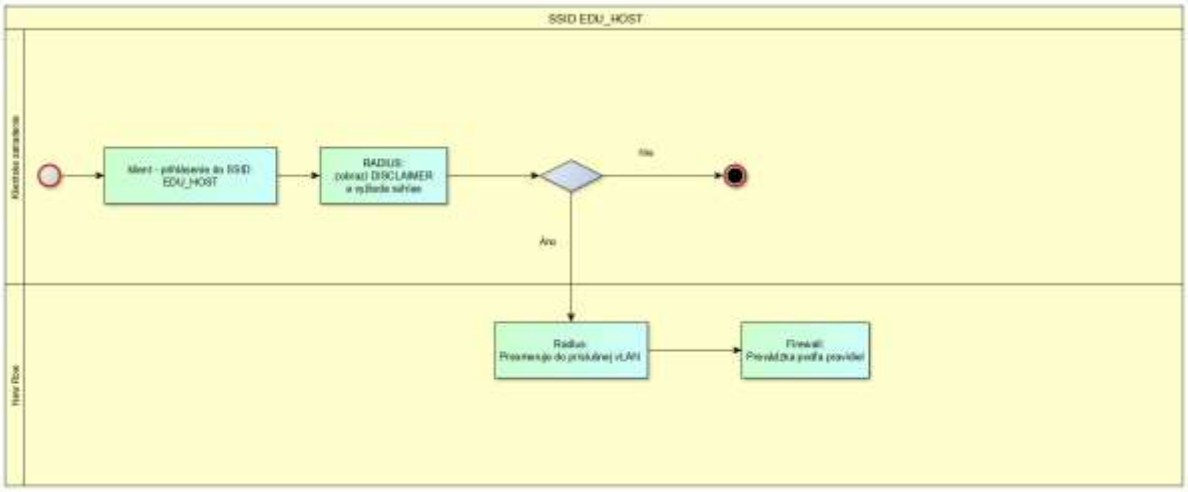
Tabuľka č. 17 zobrazuje popis jednotlivých scenárov v prípade prihlásenia používateľa s platnými respektíve neplatným IAM kontom prostredníctvom zadania prihlasovacích údajov (meno, heslo) do WiFi infraštruktúry cez SSID EDU_PRIHLASENIE a SSID EDU_SPEC

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Úžívateľ si nastavil WiFI so SSID EDU_PRIHLASENIE a SSID EDU_SPEC a systém mu zobrazil prihlasovaciu stránku	Úžívateľ zadal platné prihlasovacie údaje	Používateľ je prihlásený do infraštruktúry EDUNET_SK v sieti WIFI SSID SSID EDU_PRIHLASENIE a SSID EDU_SPEC s pridelenými oprávneniami
negatívny	Úžívateľ si nastavil WiFi so SSID EDU_PRIHLASENIE a SSID EDU_SPEC a systém mu zobrazil prihlasovaciu stránku	Používateľ zadal neplatné prihlasovacie údaje	Používateľ vidí v prihlasovacom formulári informáciu Neplatné prihlasovacie údaje. V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Úžívateľ si nastavil WiFi so SSID EDU_PRIHLASENIE a SSID EDU_SPEC a systém mu zobrazil prihlasovaciu stránku	Úžívateľ so zadanými prihlasovacími udajmi nie je evidovaný v systéme IAM	Používateľ vidí v prihlasovacom formulári informáciu Neplatné prihlasovacie údaje. V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Úžívateľ si nastavil WiFi so SSID EDU_PRIHLASENIE a SSID EDU_SPEC a systém mu zobrazil prihlasovaciu stránku	Používateľ zadal neplatné prihlasovacie heslo	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Úžívateľ si nastavil WiFi so SSID EDU_PRIHLASENIE a SSID EDU_SPEC a systém mu zobrazil prihlasovaciu stránku	Používateľ zadal viac ako povolený počet opakovaní nesprávne prihlasovacie údaje a konto bolo zablokované v EDUNET_SK	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.

Tabuľka č. 20 Scenáre – Prihlásenie do SSID EDU_PRIHLASENIE

6.2.2 SSID EDU_HOST

Účelom tejto siete je sprostredkovať žiakom a návštevníkom školy bez nutnosti autentifikácie a autorizácie bezpečný prístup k všeobecne dostupnému digitálnemu edukačnému obsahu ako sú interné zdroje MŠVVaŠ SR, stránky IAM, a podobne.
Obrázok č. 15 zobrazuje interakciu používateľa pri prihlásení do siete EDUNET_SK prostredníctvom SSID EDU_HOST



Obrázok č. 15: Diagram – Prihlásenie do SSID EDU_HOST

Návštevník školy sa svojím zariadením pripojí na SSID EDU_HOST bez zadania mena a hesla. Pri pokuse o prístup na akúkoľvek internetovú stránku sa prostredníctvom redirectu prehliadača zobrazí tzv. Disclaimer (súhlas s podmienkami používania) na URL **portalXY.edunet.sk**.

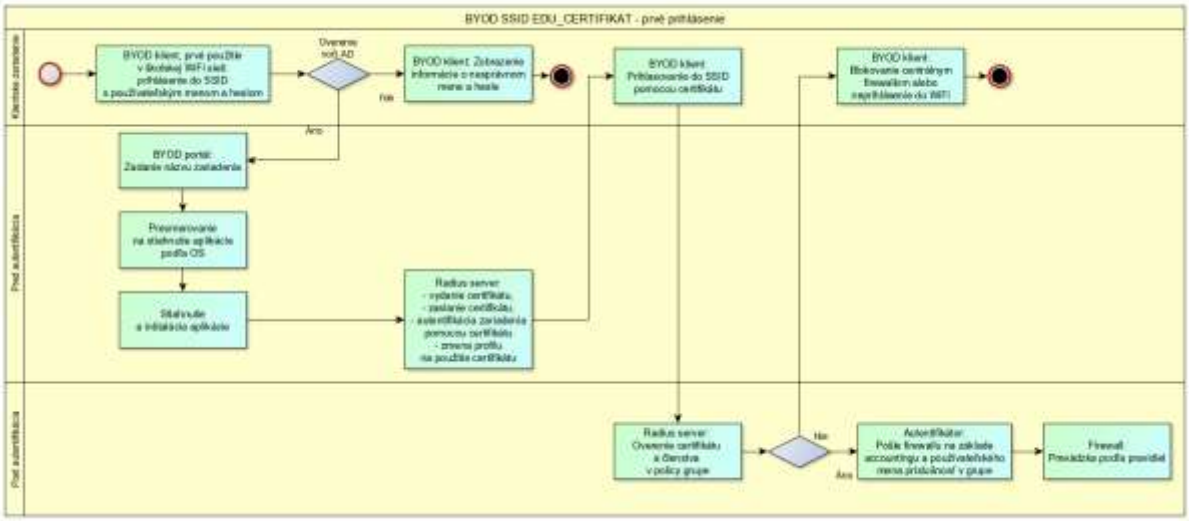
Tabuľka č. 19 zobrazuje popis jednotlivých scenárov v prípade prihlásenia používateľa do EDUNET_SK infraštruktúry cez WiFi rozhranie s SSID EDU_HOST.

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Úžívateľ si nastavil WiFI so SSID EDU_HOST a systém mu zobrazil informačnú stránku s nutnosťou potvrdenia akceptácie podmienok používania siete EDUNET_SK (disclaimer)	Používateľ potvrdil súhlas s podmienkami používania siete EDUNET_SK na informačnej stránke	Používateľ je prihlásený do infraštruktúry EDUNET_SK v sieti WIFI SSID EDU_HOST s prístupovými oprávneniami prislúchajúcimi tomuto prístupu
negatívny	Úžívateľ si nastavil WiFi so SSID EDU_HOST a systém mu zobrazil informačnú stránku s nutnosťou potvrdenia akceptácie podmienok používania siete EDUNET_SK (disclaimer)	Používateľ nepotvrdil súhlas s podmienkami používania siete EDUNET_SK na informačnej stránke	Používateľ vidí v informačnej stránke informáciu o zamietnutí prístupu a nie je mu umožnený prístup k žiadnemu zdroju v rámci siete EDUNET_SK

Tabuľka č. 21 Scenáre – Prihlásenie do SSID EDU_HOST

6.2.3 SSID EDU_CERTIFIKAT

Funkciou SSID EDU_CERTIFIKAT je autentifikácia a pripojenie používateľského zariadenia k sieti EDUNET_SK. Obrázok č. 16 zobrazuje interakciu používateľa pri prihlásení do siete EDUNET_SK pre prípad prvého prihlásenia používateľského zariadenia



Obrázok č. 16: Diagram – Prihlásenie do SSID EDU_CERTIFIKAT - prvé

Používateľské zariadenie sa pri prvom prihlásení na SSID EDU_CERTIFIKAT – overuje IAM menom a heslom do SSID. Následne je automaticky presmerované na URL **portalXY.edunet.sk** podľa load ballancerom prideleného radius serveru. Portál využíva SSL certifikát **portal.edunet.sk.** Podľa detekovaného typu zariadenia sú možné nasledujúce presmerovania :

- iOS zariadenie : portal.edunet.sk ponúkne možnosť vygenerovania nového self-signed certifikátu vystaveného radius serverom. Nasleduje import do zariadenia (stiahnutie certifikátu, inštalácia do správneho repozitára, nastavenie profilu SSID). Aplikácia sa následne pripája na radius server, ktorý sa prezentuje certifikátom **portalXY.edunet.sk**
- Windows a MacOS zariadenie : portal.edunet.sk ponúkne možnosť stiahnutia aplikácie priamo z prideleného radius serveru. Aplikácia po inštalácii požiada radius server o vygenerovanie nového self-signed certifikatu. Nasleduje import do zariadenia (stiahnutie certifikátu, inštalácia do správneho repozitára, nastavenie profilu SSID). Aplikácia sa následne pripája na radius server, ktorý sa prezentuje certifikátom **portalXY.edunet.sk**
- Android zariadenie : proces rovnaký ako pre Windows a MacOS s rozdielom, že aplikácia nie je stiahnutá priamo z radiusu, ale cez zobrazený odkaz na službe Google Play. Aplikácia sa následne pripája na radius server, ktorý sa prezentuje certifikátom **portalXY.edunet.sk**
- Iné zariadenie (nie je podporovaná funkcionality certificate auto-enrollment – typicky OS linux, Windows phone a podobne). Je potrebné požiadať helpdesk o o vydanie certifikátu, ktorý certifikát vygeneruje a dodá prostredníctvom portálu **certifikat.edunet.sk** . Nasledne si používateľ manuálne importuje certifikát do klientského zariadenia. Procedúra bude súčasťou používateľského manuálu.

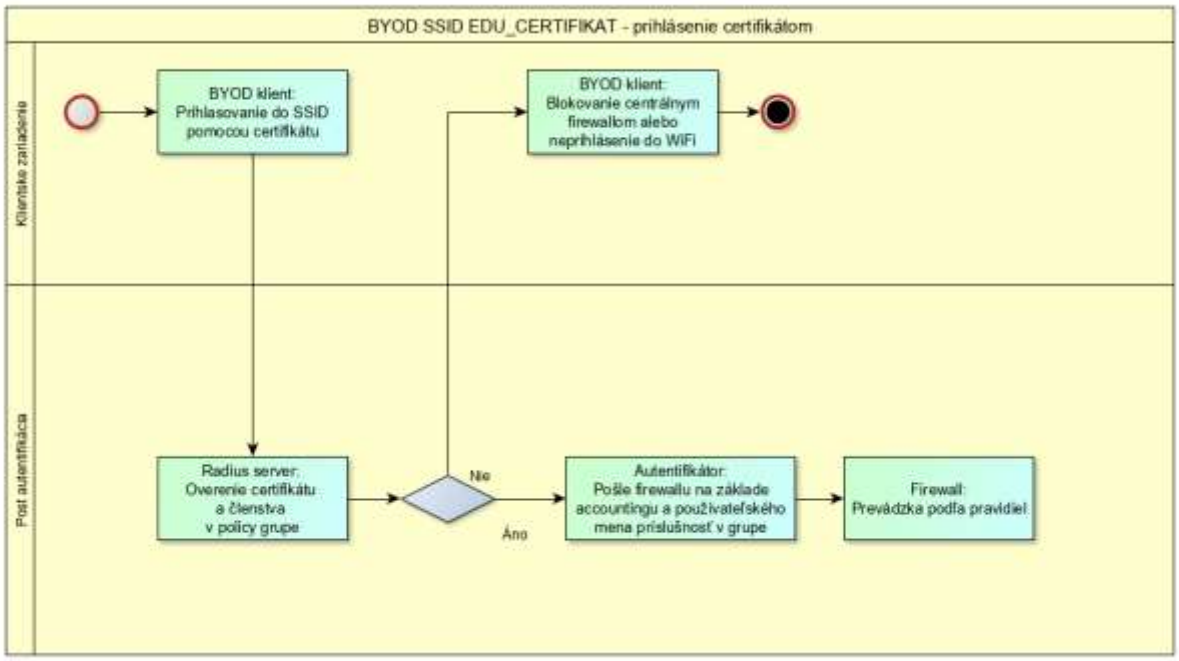
Vygenerovanie self signed certifikátu zabezpečuje implementácia radius serveru prostredníctvom integrovaného CA modulu.

Tabuľka č. 20 zobrazuje popis jednotlivých scenárov v prípade prvého prihlásenie používateľa do siete EDUNET_SK s využitím WIFI pripojenia na SSID EDU_CERTIFIKAT s nutnosťou inštalácie prístupových certifikátov.

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Po zadaní platných prihlasovacích údajov je používateľ navigovaný na stránky informujúce o postupe inštalácie prístupových certifikátov na základe použitého operačného systému (v niektorých prípadoch je vyžadovaná inštalácia aplikácie)	Používateľ má nainštalovaný na počítači prístupový certifikát oprávňujúci ho na prístup do siete EDUNET_SK cez WiFi pripojenie so SSID EDU_CERTIFIKAT
negatívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Používateľ zadal neplatné prihlasovacie údaje	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Úžívateľ so zadanými prihlasovacími udajmi nie je evidovaný v systéme IAM	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Používateľ zadal neplatné prihlasovacie heslo	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.
negatívny	Používateľ na počítači aktivuje prihlasovací formulár (prvým sieťovým prístupom mimo lokálnu sieť)	Používateľ zadal viac ako povolený počet opakovaní nesprávne prihlasovacie údaje a konto bolo zablokované v EDUNET_SK	Používateľ vidí v prihlasovacom formulári informáciu "Neplatné prihlasovacie údaje". V sieti EDUNET_SK nemá žiadne sprístupnené informačné zdroje.

Tabuľka č. 22 Scenáre – Prvé prihlásenie do SSID EDU_CERTIFIKAT

Obrázok č. 17 zobrazuje interakciu používateľa pri prihlásení do siete EDUNET_SK pre prípad prihlásenia používateľského zariadenia s korektným certifikátom nainštalovanom na používateľskom zariadení.



Obrázok č. 17: Diagram – Prihlásenie do SSID EDU_CERTIFIKAT“ – s certifikátom

Tabuľka č. 20 zobrazuje popis jednotlivých scenárov v prípade prihlásenia používateľa do EDUNET_SK s využitím WiFi pripojenia na SSID EDU_CERTIFIKAT s platným certifikátom nainštalovanom na zariadení.

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Používateľ prípojí zariadenie do EDUNET_SK Wifi SSID EDU_CERTIFIKAT	Používateľ s platným certifikátom a aktívnym IAM účtom si na zariadení nastaví sieťové pripojenie na WiFi SSID EDU_CERTIFIKAT	Používateľ je pripojený do siete EDUNET_SK s oprávneniami prislúchajúcimi jeho profilu
negatívny	Používateľ prípojí zariadenie s nainštalovaným certifikátom do EDUNET_SK WiFi SSID EDU_CERTIFIKAT	Používateľ s nainštalovaným certifikátom a neaktívnym alebo neexistujúcim IAM účtom si na zariadení nastaví sieťové pripojenie na WiFi SSID EDU_CERTIFIKAT	Používateľovi je zamietnutý prístup do WIFI siete SSID EDU_CERTIFIKAT

Tabuľka č. 23 Scenáre – Prihlásenie s platným certifikátom

Na portáli **byod.edunet.sk** bude k dispozícii portál s manažmentom certifikátov pre používateľské zariadenia. Je prístupná pre používateľov v SSID EDU_CERTIFIKAT.
Tabuľky č. 22, 23, 24 zobrazujú popis jednotlivých scenárov pri správe certifikátov cez portál byod.edunet.sk pre prípad, že uživateľ má IAM účet a platný certifikát nainštalovaný na zariadení.

- Pridanie nového BYOD zariadenia a zrušenie existujúceho BYOD zariadenia používateľom pomocou BYOD portálu

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Používateľ sa na novom zariadení pripojí na WiFi SSID EDU_CERT a zobrazí sa mu prihlasovací formulár	Po zadaní platných prihlasovacích údajov je používateľ navigovaný na stránky informujúce o postupe inštalácie prístupových certifikátov na základe použitého operačného systému (v niektorých prípadoch je vyžadovaná inštalácia aplikácie)	Používateľ má na zariadení nainštalovaný prístupový certifikát oprávňujúci ho na prístup do siete EDUNET_SK cez WIFI pripojenie so SSID EDU_CERT. Na portáli byod.edunet.sk sa pridané zariadenie zobrazuje v zozname používateľových BYOD zariadení v stave Pending a po dokončení inštalácie certifikátu a registrácie zariadenia v stave Registered (Zaregistrované).
pozitívny	Používateľ sa na inom zariadení alebo počítači pripojí do niektorej SSID a prihlási sa so svojim používateľským menom a heslom do portálu byod.edunet.sk	Po zadaní platných prihlasovacích údajov sa používateľovi zobrazí stránka s bezpečnostným upozornením a po jej potvrdení tlačidlom Accept sa zobrazí stránka pre pripojenie do siete s tlačidlom Continue. Následne sa používateľovi zobrazí zoznam jeho BYOD zariadení, kde môže podľa MAC adresy alebo názvu zakliknutím vybrať zariadenie. Vybrané zariadenie potom zruší (odstráni) kliknutím na tlačidlo Delete (Odstrániť).	Odstránené zariadenie sa nezobrazuje v zozname používateľových zariadení na portáli byod.edunet.sk a na tomto zariadení už nie je možné pripojenie do WiFi so SSID EDU_CERT.

Tabuľka č. 24 Scenáre – Pridanie/Zrušenie BIOD zariadenia

- Označenie používateľovho BYOD zariadenia ako stratené a znovu registrácia tohto zariadenia pomocou BYOD portálu

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Používateľ sa na inom zariadení alebo počítači pripojí do niektorej SSID a prihlási sa so svojim používateľským menom a heslom do portálu byod.edunet.sk	Po zadaní platných prihlasovacích údajov sa používateľovi zobrazí stránka s bezpečnostným upozornením a po jej potvrdení tlačidlom Accept sa zobrazí stránka pre pripojenie do siete s tlačidlom Continue. Následne sa používateľovi zobrazí zoznam jeho BYOD zariadení, kde môže podľa MAC adresy alebo názvu zakliknutím vybrať zariadenie. Vybrané zariadenie potom označí ako stratené kliknutím na tlačidlo Lost (Stratené).	Zariadenie sa na portáli byod.edunet.sk zobrazuje v zozname používateľových zariadení v stave Lost (Stratené). Na tomto zariadení už nie je možné pripojenie do WiFi so SSID EDU_CERT.
pozitívny	Používateľ sa na inom zariadení alebo počítači pripojí do niektorej SSID a prihlási sa so svojim používateľským menom a heslom do portálu byod.edunet.sk	Po zadaní platných prihlasovacích údajov sa používateľovi zobrazí stránka s bezpečnostným upozornením a po jej potvrdení tlačidlom Accept sa zobrazí stránka pre pripojenie do siete s tlačidlom Continue. Následne sa používateľovi zobrazí zoznam jeho BYOD zariadení, kde zakliknutím vyberie zariadenie v stave Lost (Stratené), ktoré chce reaktivovať a potom klikne na tlačidlo Reinstate. Na tomto zariadení sa potom používateľ pripojí do WiFi SSID EDU_CERT a dokončí štandardný proces inštalácie certifikátu.	Zariadenie sa na portáli byod.edunet.sk zobrazuje v zozname zaregistrovaných používateľových zariadení. Na zariadení je nainštalovaný prístupový certifikát umožňujúci prístup do siete EDUNET_SK cez WIFI pripojenie so SSID EDU_CERT.

Tabuľka č. 25 Scenáre – Nová registrácia cez BIOD portál-Stratené

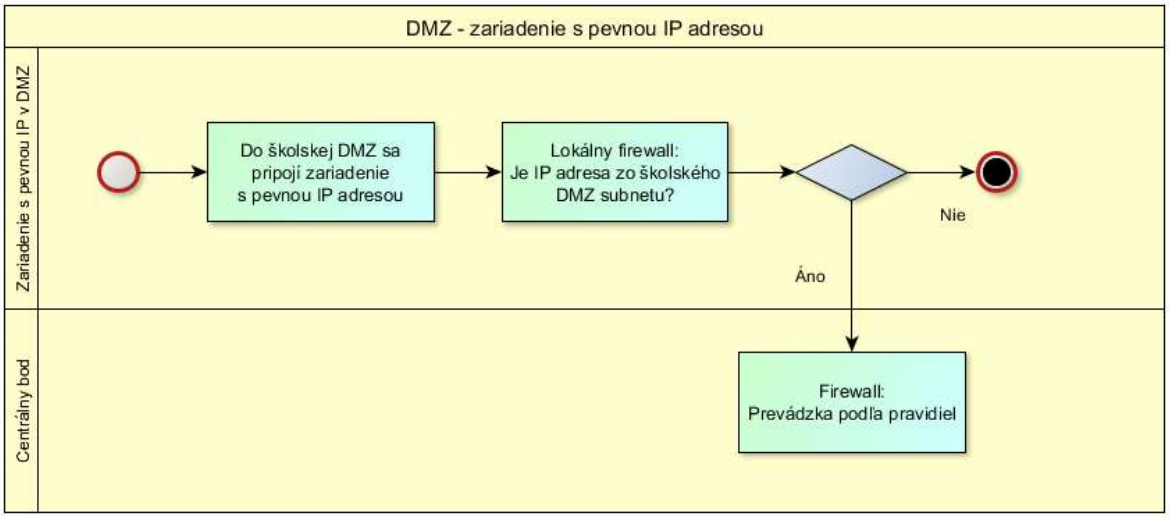
- Označenie používateľovho BYOD zariadenia ako odcudzeného a znovu registrácia tohto zariadenia pomocou BYOD portálu

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Používateľ sa na inom zariadení alebo počítači pripojí do niektorej SSID a prihlási sa so svojim používateľským menom a heslom do portálu byod.edunet.sk	Po zadaní platných prihlasovacích údajov sa používateľovi zobrazí stránka s bezpečnostným upozornením a po jej potvrdení tlačidlom Accept sa zobrazí stránka pre pripojenie do siete s tlačidlom Continue. Následne sa používateľovi zobrazí zoznam jeho BYOD zariadení, kde môže podľa MAC adresy alebo názvu zakliknutím vybrať zariadenie. Vybrané zariadenie potom označí ako odcudzené kliknutím na tlačidlo Stolen (Odcudzené).	Zariadenie sa na portáli byod.edunet.sk zobrazuje v zozname používateľových zariadení v stave Stolen (Odcudzené). Zariadeniu bol automaticky odňatý certifikát a nie je možné pripojenie do WiFi so SSID EDU_CERT.
pozitívny	Používateľ sa na inom zariadení alebo počítači pripojí do niektorej SSID a prihlási sa so svojim používateľským menom a heslom do portálu byod.edunet.sk	Po zadaní platných prihlasovacích údajov sa používateľovi zobrazí stránka s bezpečnostným upozornením a po jej potvrdení tlačidlom Accept sa zobrazí stránka pre pripojenie do siete s tlačidlom Continue. Následne sa používateľovi zobrazí zoznam jeho BYOD zariadení, kde zakliknutím vyberie zariadenie v stave Stolen (Odcudzené), ktoré chce reaktivovať a potom klikne na tlačidlo Reinstate. Na tomto zariadení sa potom používateľ pripojí do WiFi SSID EDU_CERT a dokončí štandardný proces inštalácie certifikátu.	Zariadenie sa na portáli byod.edunet.sk zobrazuje v zozname zaregistrovaných používateľových zariadení. Na zariadení je nainštalovaný prístupový certifikát umožňujúci prístup do siete EDUNET_SK cez WIFI pripojenie so SSID EDU_CERT.

Tabuľka č. 26 Scenáre – Nová registrácia cez BYOD portál-Odcudzené

6.3 Pripojenie zariadenia do LAN DMZ

Obrázok č. 18 zobrazuje proces pripojenia zariadenia do LAN siete 3 určenej pre pripojenie serverov alebo zdieľaných zariadení.



Obrázok č. 18: Diagram – Prihlásenie do DMZ

Tabuľka č. 25 zobrazuje popis jednotlivých scenárov v prípade sprístupnenia siete EDUNET_SK s príslušným profilom pre školské zariadenie na základe pevne priradenej IP adresy

Scenáre			
Typ	**Východzí stav**	**Popis**	**Výsledný stav**
pozitívny	Zariadenie s pridelenou pevnou IP pripojené do LAN na infraštruktúru EDUNET_SK	Zariadenie má pridelenú platnú IP adresu v rámci IP subnetu pre pevné IP pre príslušnú lokalitu a je pripojené do LAN siete v infraštruktúre EDUNET_SK	Zariadenie má prístup do siete EDUNET_SK s pridelenými oprávneniami. Zariadenie nie je viazané na konkrétneho používateľa v IAM.
negatívny	Zariadenie s pridelenou pevnou IP pripojené do LAN na infraštruktúru EDUNET_SK	Zariadenie má pridelenú IP adresu mimo rozsahu pre pevné IP pre príslušnú lokalitu a je pripojené do LAN siete v infraštruktúre EDUNET_SK	Zariadenie nemá prístup do siete EDUNET_SK.

Tabuľka č. 27 Scenáre – Sprístupnenie siete – pevná IP adresa

6.4 Správa IAM konta

Používateľské prístupové údaje prístupu do siete EDUNET_SK sú uložené v systéme IAM spravovanom MŠVVaŠ SR. Tabuľka č. 26 zobrazuje popis jednotlivých scenárov pri správe IAM konta.

Scenáre		
Východzí stav	**Popis**	**Výsledný stav**
Požiadavka na zablokovanie IAM účtu	Používateľ požaduje zablokovať IAM konto	Požiadavka zaslaná na Centrum podpory prevadzky MŠVVaŠ SR
Požiadavka na odblokovanie IAM účtu	Používateľ požaduje odblokovať IAM konto	Požiadavka zaslaná na Centrum podpory prevadzky MŠVVaŠ SR
Požiadavka na zmenu hesla	Používateľ požaduje zmeniť heslo na IAM konte	Požiadavka zaslaná na Centrum podpory prevadzky MŠVVaŠ SR
Požiadavka na pridanie používateľa s IAM kontom.	Zástupca školy požaduje pridanie nového používateľa s IAM kontom	Požiadavka zaslaná na Centrum podpory prevadzky MŠVVaŠ SR
Požiadavka na vymazanie IAM konta	Zástupca školy požaduje vymazanie IAM konta	Požiadavka zaslaná na Centrum podpory prevadzky MŠVVaŠ SR
Požiadavka na zmenu údajov v IAM konte	Používateľ požaduje zmenu údajov IAM konta	Požiadavka zaslaná na Centrum podpory prevadzky MŠVVaŠ SR

Tabuľka č. 28 Scenáre – Správa IAM konta

7 IP plán pre riešenie EDUNET_SK

Táto kapitola obsahuje popis IP plánu pre projekt EDUNET_SK.

IP plán je rozdelený na typy: LAN a WiFi SSID, WAN infraštruktúrne, manažment infraštruktúrne, MŠVVaŠ SR, Centrála EDUNET_SK a rozsahy pre rezervu ďalšieho použitia. Návrh rozsahov používa iba privátne IPv4 rozsahy podľa RFC1918 a RFC 6598.

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
- 100.64.0.0 - 100.127.255.255 (100.64/10 prefix)

Rozdelenie a vyhradenie jednotlivých typov je nasledovné:

Školské LAN a WiFi SSID	10.0.0.0/8
WAN infraštruktúrna a Manažment infraštruktúrna	172.16.0.0/12
Centrála EDUNET_SK	192.168.0.0/16 100.64.0.0/10
MŠVVaŠ SR a iné zdroje obsahu	nutné definovať vopred

Tabuľka č. 29 Rozdelenie IP rozsahov podľa typov

Privátne IPv4 rozsahy MŠVVaŠ SR prípadne ďalšie, ktoré navzájom kolidujú s navrhovaným, je treba dopredu definovať a navrhnúť rezerváciu a zmeny IP plánu pred rolloutom školských zariadení. Prípadné zmeny počas trvania projektu nebude možné realizovať.

7.1 IP plán školských zariadení pre LAN a WiFi

IP plán zohľadňuje hlavne oddelenie jednotlivých LAN 1-5 a WiFi SSID, aby bolo možné na CPE alebo Firewall zariadení školskej lokality, ale aj v centrále EDUNET_SK ich jednoznačné rozlíšenie a určenie pre uplatnenie sieťových politík. LAN rozsahy je potrebné ďalej rozdeliť podľa typu účelu používania.

Rozdelenie LAN a WiFi rozsahov je nasledovné:

Určenie	VLAN a TYP
[LAN] učiteľ	VLAN 10 - učiteľ [LAN1]
	VLAN 11 - učiteľ [WiFi]
[LAN] žiak	VLAN 20 - žiak [LAN2]
	VLAN 21 - žiak [WiFi]
[LAN] DMZ	VLAN 30 - DMZ [LAN3]
[LAN] SPEC	VLAN 40 - SPEC [LAN4]
	VLAN 41 - SPEC [WiFi]
[LAN] HOST	VLAN 50 - Host [LAN5]
	VLAN 51 - Host [WiFi]
[LAN] BYOD	VLAN 61 – BYOD [WiFi]

Tabuľka č. 30 Rozdelenie VLAN rozsahov podľa typov účelu používania

IPplan.xlsx

Tabuľka č. 31 Rozdelenie IP rozsahov podľa typov účelu používania
(tabuľka v priloženom dokumente)

Veľkosti poolov adries pre jednotlivé LAN siete sa prideľujú na základe nasledovného kľúča podľa typu pripojenia danej školy:

LAN sieť	Typ A	Typ B	Typ C	Typ D	Typ E	Typ F	Typ X
LAN učiteľ	/24	/24	/24	/25	/25	/25	/24
WiFi učiteľ	/24	/24	/24	/25	/25		/24
LAN žiak	/24	/24	/24	/25	/25		/24
WiFi žiak	/23	/23	/23	/24	/25		/23
DMZ	/26	/26	/26	/26	/26		/26
LAN SPEC	/24	/24	/24	/25	/25		/24
WiFi SPEC	/24	/24	/24	/25	/25		/24
LAN host (LAN5)	/23	/23	/23	/24	/25		/23
WiFi host	/23	/23	/23	/24	/25		/23

Tabuľka č. 32 Veľkosti adresných rozsahov pre školy

Adresné pooly použité pre jednotlivé LAN siete sa následne prideľujú z daných supernetov:

LAN sieť	Spernet 1	Supernet 2	Supernet 3
LAN učiteľ	10.32.0.0/13	10.40.0.0/13	10.48.0.0/13
WiFi učiteľ	10.128.0.0/14	10.132.0.0/14	10.136.0.0/14
LAN žiak	10.140.0.0/14	10.144.0.0/14	10.148.0.0/14
WiFi žiak	10.104.0.0/13	10.112.0.0/13	10.120.0.0/13
DMZ	10.176.0.0/14		
LAN SPEC	10.164.0.0/14	10.168.0.0/14	10.172.0.0/14
WiFi SPEC	10.152.0.0/14	10.156.0.0/14	10.160.0.0/14
LAN host (LAN5)	10.56.0.0/13	10.64.0.0/13	10.72.0.0/13
WiFi HOST	10.80.0.0/13	10.88.0.0/13	10.96.0.0/13

Tabuľka č. 33 Supernety pre školy

8 Služby centrálneho nahlasovania a správy servisných prípadov Service Desku

8.1 Nahlasovanie Incidentov a požiadaviek

Pre nahlásenie požiadavky je možné využiť tieto komunikačné kanály **(prevádzka 24/7/365):**

- Telefón – bezplatné telefónne číslo **0800 60 60 60**
- E-mail **edunet@swan.sk**
- EDUNET Portál **infoportal.edunet.sk**

8.1.1 Telefonické nahlásenie Incidentov a požiadaviek

- Kontaktné číslo 0800 60 60 60
- Poskytnutie operátorovi identifikačné údaje (EDUID, názov školy, adresa školy alebo označenie služby).
- Pre rýchle a efektívne riešenie oznamovateľ poskytne presný popis požiadavky.
- Operátor vytvorí v zákazníckom systéme požiadavku s identifikačným číslom, v ktorej bude prebiehať ďalšie riešenie.

8.1.2 E-mailové nahlásenie Incidentov a požiadaviek

- Požiadavku a Incident je možné odoslať na e-mailovú adresu edunet@swan.sk.
- V mailovej správe je potrebné identifikovať konkrétnu školu (EDUID, názov školy, adresa školy) a zároveň uviesť identifikačné údaje k službe s presným popisom požiadavky alebo incidentu.
- Zaslanie potvrdenia o vytvorení oficiálnej požiadavky v Service Desku s prideleným identifikačným číslom.
- Pri spätnej komunikácii nie je možné meniť predmet správy. E-mail sa automaticky priradí k už vytvorenej požiadavke.

8.1.3 Nahlásenie požiadavky cez zákaznícky portál

- Po vytvorení prístupu do EDUNET Portálu infoportal.edunet.sk je možné vytvárať požiadavky a nahlasovať incidenty priamo pod dotknutou službou.
- Operátor dopisuje potrebné informácie do vytvorenej požiadavky.
- Pri doplnení informácií od operátora bude zaslaná notifikácia na e-mailovú adresu

8.1.4 Sledovanie stavu servisných prípadov

EDUNET Portál infoportal.edunet.sk je slúži taktiež na :

- sledovanie stavu riešenia aktuálnych servisných prípadov
- sledovanie histórie uzavretých servisných prípadov za účelom kontroly a analýzy poskytovaných služieb

8.2 Riadenie Incidentov

Incidentom sa rozumie každé neplánované prerušenie služby alebo zníženie kvality služby. Eventom (udalosťou) rozumieme informáciu, upozornenie alebo výstrahu o zmene prichádzajúcej od služby, konfiguračnej položky alebo monitorovacieho nástroja. Eventy tvoria súbor informácií, ktoré umožňujú predchádzanie alebo včasnú identifikáciu Incidentu.

8.2.1 Práca s Eventami a Incidentami

Eventy (udalosti v systéme) sa zbierajú do monitorovacích a dohľadovacích aplikácií, kde sú nastavené pravidlá na vyhodnocovanie jednotlivých Eventov alebo súborov Eventov tak, aby notifikácie zasielané na dohľadové pracoviská umožnili včasnú reakciu na predídenie alebo odstránenie Incidentu.

Každý Incident, ktorý sa vyskytne na službe, zariadení alebo technológii v sieti Prevádzkovateľa musí byť zaznamenaný v ticketovom systéme Service Desk ako tzv. tiket so správnymi údajmi a informáciami:

a. priradený na riadenie konkrétnemu človeku alebo oddeleniu
b. priradený do správnej kategórie typu Incidentu
c. stanovená priorita – Prioritu stanovuje poskytovateľ na základe závažnosti incidentu
d. zaznamenané preverenie so zákazníkom
e. po kontrole a odsúhlasení zákazníkom bude tiket uzatvorený s vysvetlením riešenia incidentu
f. každý záznam vrátane začatia a ukončenia Incidentu má v systéme časovú značku

8.2.2 Stav Incidentu

Stav Incidentu vyjadruje, v ktorej časti cyklu riešenia sa Incident práve nachádza. Jednotlivé stavy na seba nadväzujú a jednoznačne identifikujú, či a čo sa s Incidentom dialo alebo má diať.

Jednotlivé zmenové stavy určujú stav, v akom sa práve proces riešenia Incidentu nachádza. Zmenu stavu Incidentu vykonáva pracovník oddelenia telefonického centra na základe vykonaných úkonov pri riešení Incidentu.

Stavy incidentu

- Nový – novozaložený incident
- V spracovaní - Incident v riešení. Prebieha identifikácia problému a rieši sa odstránenie incidentu
- Vyriešený - Technicky vyriešený incident
- Zatvorený - Vyriešenie incidentu potvrdené zástupcom školy

8.2.3 Identifikácia Incidentu

Incident je porucha, chyba alebo nefunkčnosť služby, hardvér alebo softvér, alebo také zníženie kvality parametrov služby, že znemožňuje ďalšie plnohodnotné použitie zákazníkom.

Incidenty sú identifikované buď pomocou správy z monitorovacích systémov, alebo požiadavkou od zákazníka a to buď mailom, telefonicky alebo cez EDUNET Portál.

8.2.4 Automatické systémy

Monitorovacie systémy sledujú dostupnosť služby alebo koncových zariadení na službe, alebo parametre služby a po určenom znížení parametrov služby, alebo nemožnosti komunikovať s koncovým zariadením, vyhodnotia situáciu ako Incident a o tomto zasielajú informáciu na oddelenie Service Desk. Na základe komunikácie so zákazníkom Service Desk vyhodnotí situáciu a založí servisný prípad na riešenie Incidentu.

Automatické systémy primárne zbierajú Eventy a logy z jednotlivých zariadení a technológií, ktoré vyhodnocujú podľa dostupnosti a požadovaných kvalitatívnych parametrov služieb.

8.2.5 Manuálne nahlásenie incidentu

Incident môže nahlásiť na Service Desk oddelenie aj poverený zamestnanec školy respektíve Prevádzkovateľa pri zistení problému so službou. V tomto prípade Service Desk oddelenie overuje s nahlasovateľom parametre nahlásenej nefunkčnej služby a zakladá Incident.

8.3 Zaznamenávanie Incidentov

Incidenty sa zaznamenávajú v Service Desk. Tu sú zaznamenané aj zmenové požiadavky, ako aj požiadavky na informáciu o službách.

Incidenty môžu vznikať v systéme troma spôsobmi:

- zadané technikom L1 na základe volania zákazníka
- zadané systémom Prevádzkovateľa
- automaticky – zaslaním emailu
- zákazníkom cez EDUNET Portál

8.4 Informovanie zákazníka

Poverený zástupca školy, respektíve nahlasovateľ incidentu bude notifikovaný emailom v prípadoch :

- registrácia servisného prípadu,
- pridelenie riešiteľskému tímu,
- riešenie servisného prípadu/zmena stavu servisného prípadu,
- vyriešenie servisného prípadu,
- akceptácia zo strany ohlasujúceho a uzatvorenie nahláseného servisného prípadu. (Zástupca školy je informovaný o vyriešení incidentu aj telefonicky)

9 Informačný systém EDUNET Portál

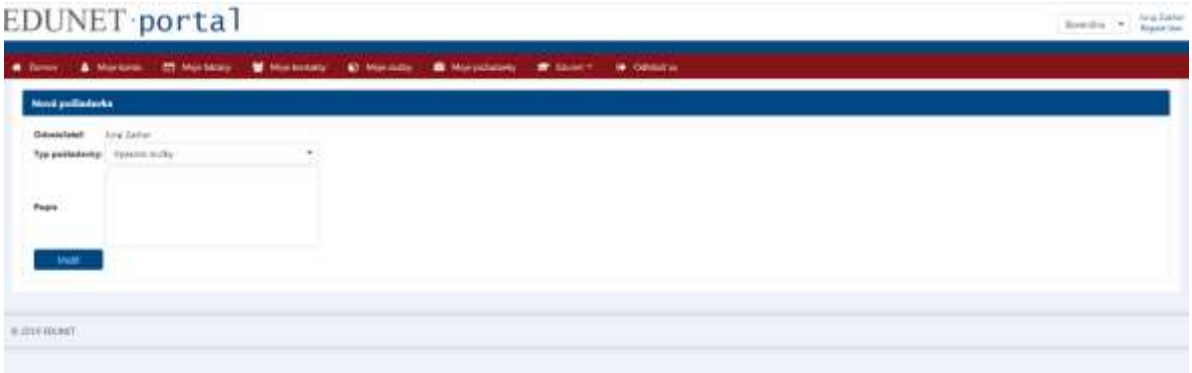
Informačný systém / Komunikačné prostredie bude slúžiť pre poverené osoby Objednávateľa a jednotlivých škôl na prístup k aktuálnym aj archívnym údajom o projekte. Súčasťou Informačného systému sú:

1. Service Desk prístup pre poverené osoby Objednávateľa a jednotlivých škôl, komunikačné prostredie pre zasielanie požiadaviek Poskytovateľovi
2. Informačný systém pre poverené osoby objednávateľa s informáciami o priebehu projektu

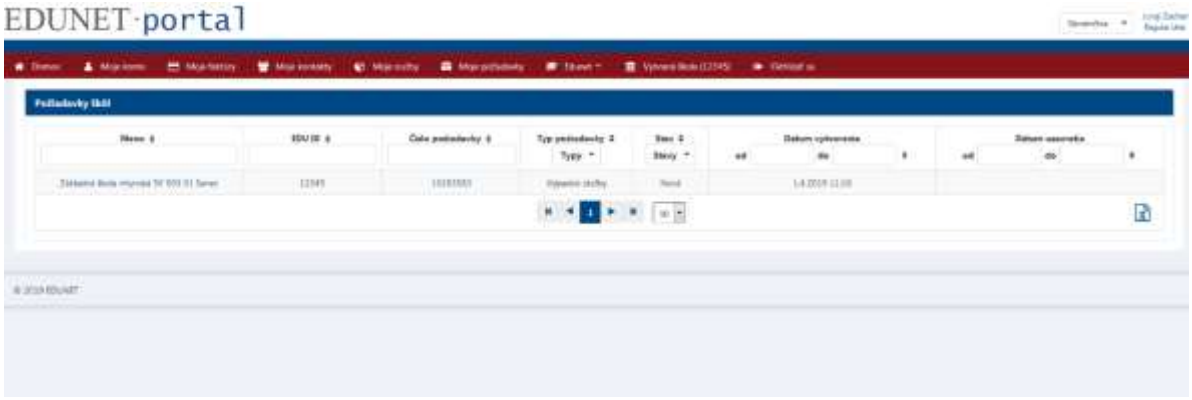
9.1 Service Desk

Poverená osoba školy vie vykonávať nasledujúce úkony:

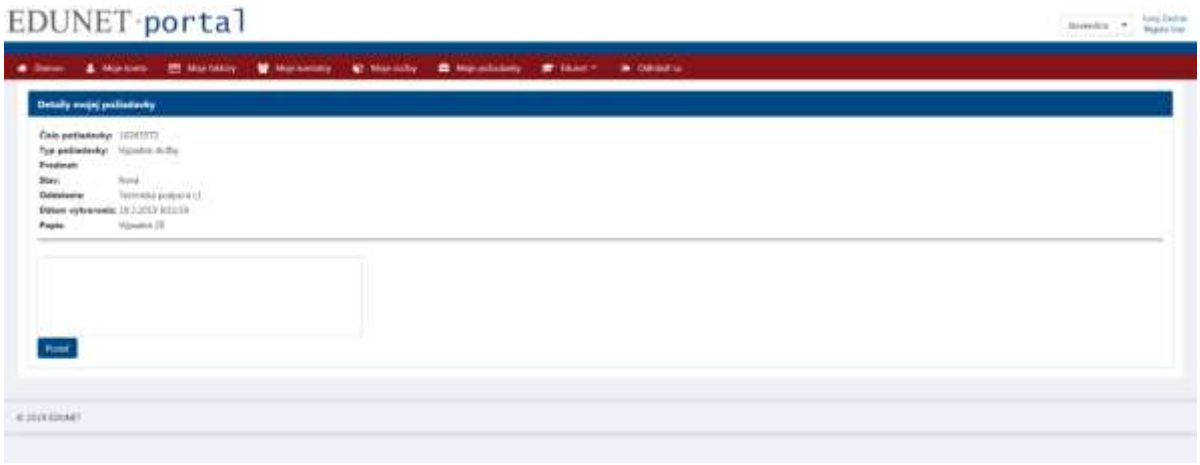
- Zadanie incidentu / zmenovej požiadavky
- Sledovanie stavu vybavenia incidentu / zmenovej požiadavky
- Komentovanie incidentu / zmenovej požiadavky
- Informácia o ukončení riešenia incidentu / zmenovej požiadavky



Obrázok č. 19 Zadanie požiadavky



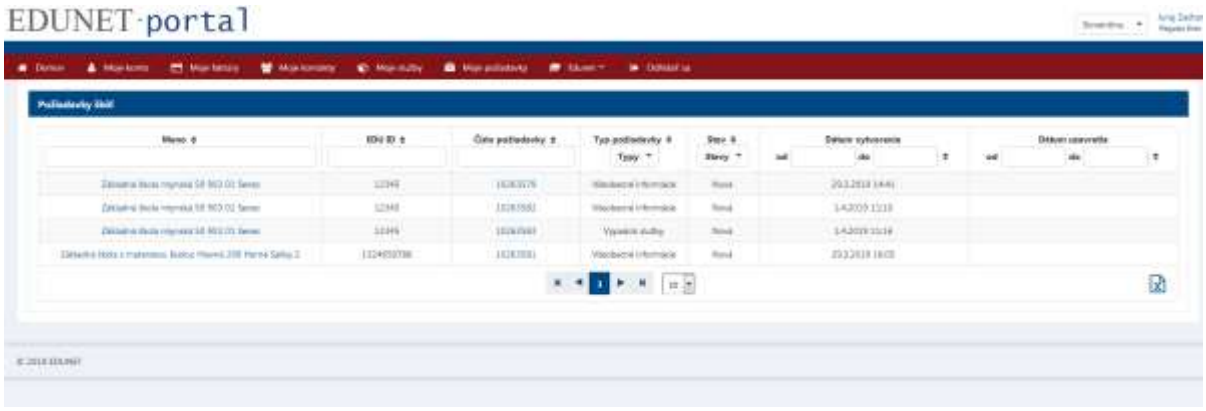
Obrázok č. 20 Zoznam požiadaviek školy



Obrázok č. 21 Detail požiadavky / incidentu

Poverené osoby Objednávateľa vedia vykonávať nasledujúce úkony:

- Zadanie incidentu / zmenovej požiadavky
- Sledovanie stavu vybavenia incidentu / zmenovej požiadavky
- Komentovanie incidentu / zmenovej požiadavky
- Informácia o ukončení riešenia incidentu / zmenovej požiadavky
- Sledovanie/filtrovanie/exportovanie všetkých incidentov/zmenových požiadaviek jednotlivých škôl



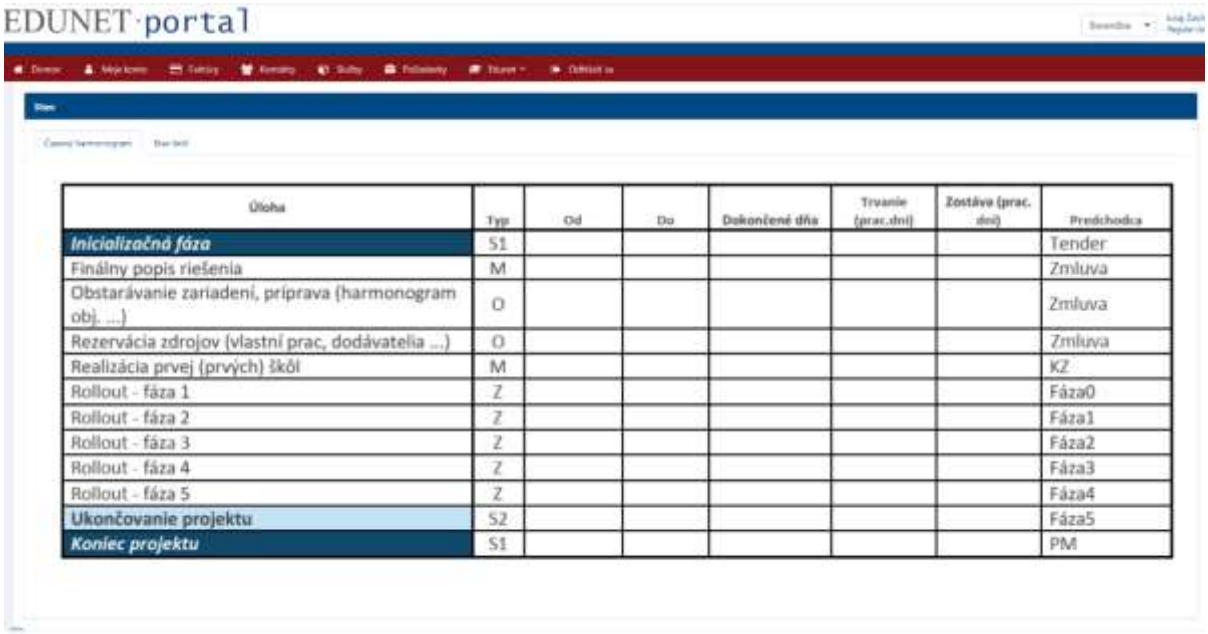
Obrázok č. 22 Sumárne sledovanie stavu požiadaviek / incidentov všetkých škôl

9.2 Informačný systém /Komunikačné prostredie – EDUNET Portál

Poverené osoby Objednávateľa vedia vykonávať nasledujúce úkony :

- sledovanie plnenia časového harmonogramu projektu

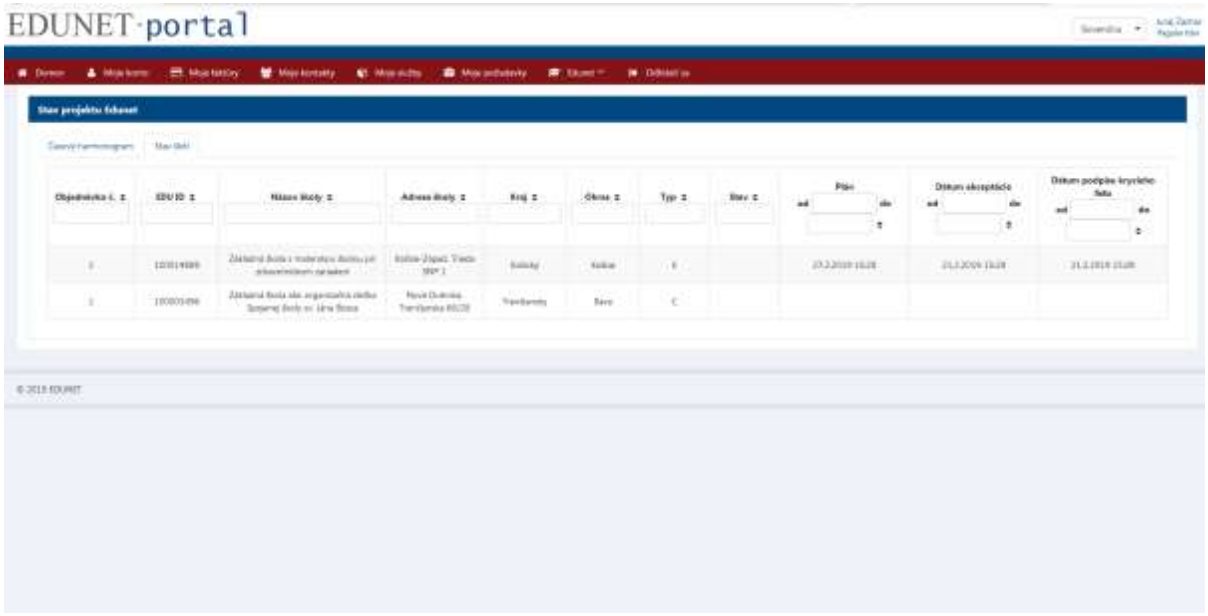
- sledovanie zapájania lokalít/ škôl do siete EDUNET_ SK (možnosť filtrovania a prezerania zoznamu zapojených škôl, plánovaných na zapojenie s termínom zapojenia),
- sledovanie historických údajov o jednotlivých lokalitách (od zapojenia do siete EDUNET, cez všetky vykonané zmeny a žiadosti o zvýšenie rýchlosti, o prekládku, o dodatočné IKT zariadenia, o služby administrátorov (IT, WiFi, LAN a server), až po prípadné zrušenie školy, resp. odpojenie zo siete EDUNET_SK,
- kontrolu údajov pre účely verifikácie oprávnenosti faktúr (filtrovanie zoznamov škôl podľa typu pripojenia a pravidelného mesačného poplatku, s možnosťou filtrovania zvoleného časového obdobia),
- vytváranie exportov štatistických údajov podľa zvolených kritérií, štatistiky a filtrované údaje bude možné vyexportovať do súboru excel,
- archívne úložisko všetkých vystavených a uhradených/neuhradených faktúr
- archívne úložisko elektronických verzií preberacích protokolov,
- archiváciu údajov o lokalitách EDUNET_SK, zodpovedný pracovník Objednávateľa bude mať možnosť údaje len prezerať, filtrovať a exportovať.



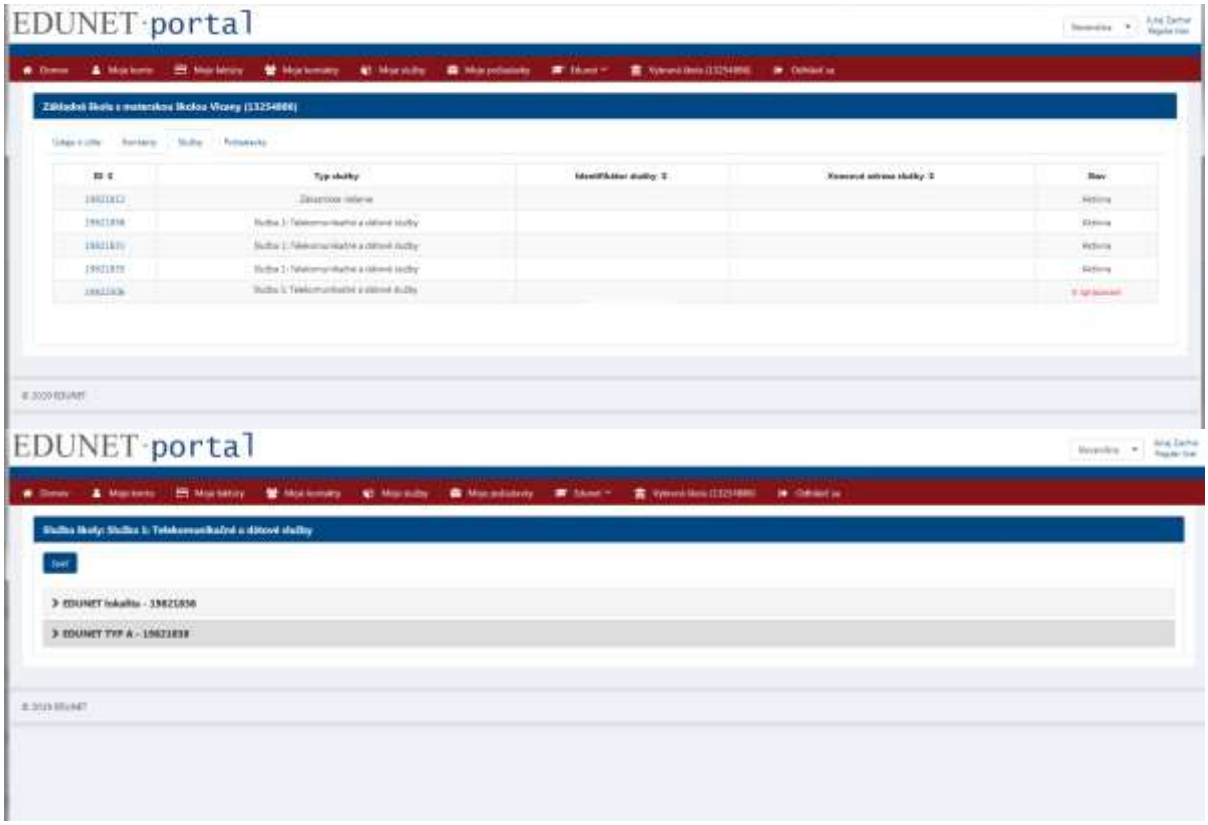
Úloha	Typ	Od	Do	Dokončené dňa	Trvanie (prac.dni)	Zostáva (prac. dni)	Predchodca
Inicializačná fáza	S1						Tender
Finálny popis riešenia	M						Zmluva
Obstarávanie zariadení, príprava (harmonogram obj. ...)	O						Zmluva
Rezervácia zdrojov (vlastní prac, dodávatelia ...)	O						Zmluva
Realizácia prvej (prvých) škôl	M						KZ
Rollout - fáza 1	Z						Fáza0
Rollout - fáza 2	Z						Fáza1
Rollout - fáza 3	Z						Fáza2
Rollout - fáza 4	Z						Fáza3
Rollout - fáza 5	Z						Fáza4
Ukončovanie projektu	S2						Fáza5
Koniec projektu	S1						PM

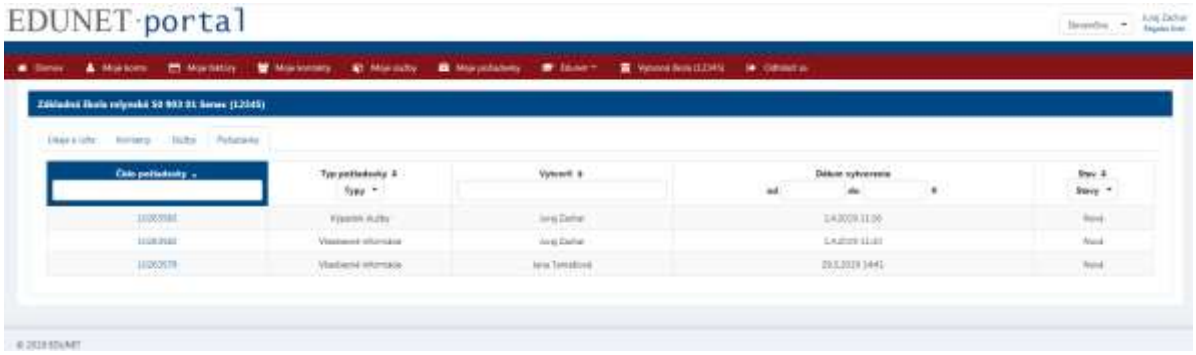
Obrázok č. 23 Projektový harmonogram

Sledovanie zapájania lokalít do siete EDUNET_SK (možnosť filtrovania a prezerania zoznamu zapojených škôl, plánovaných na zapojenie s termínom zapojenia)

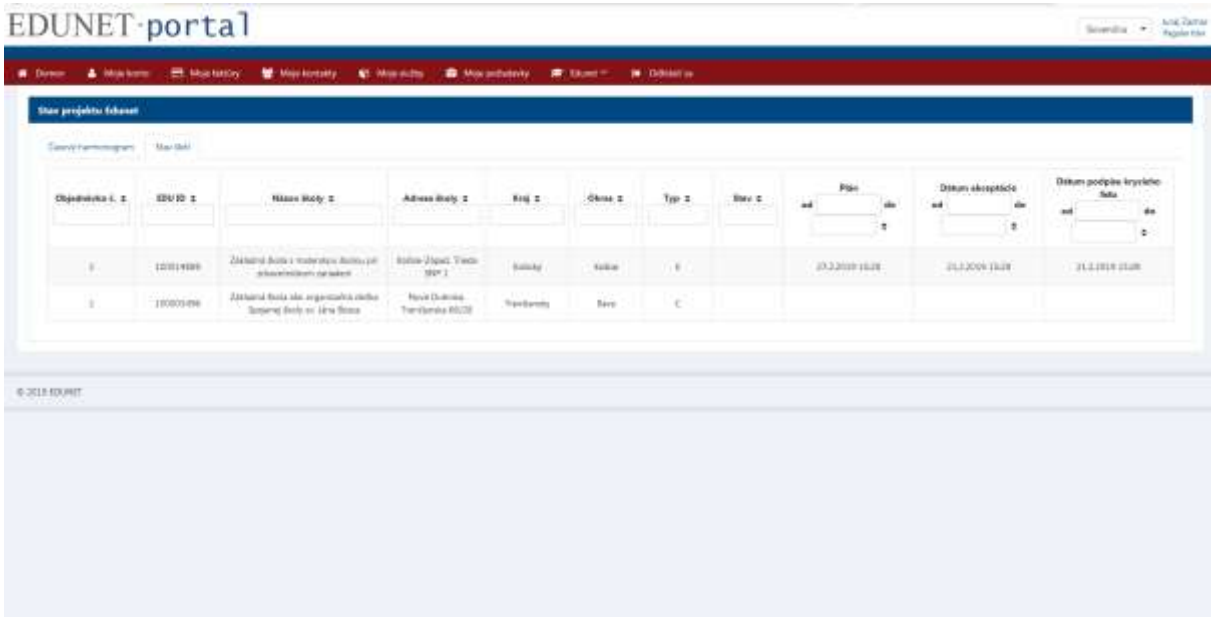


Obrázok č. 24 Stav pripájania lokalít/ škôl do siete EDUNET_ SK

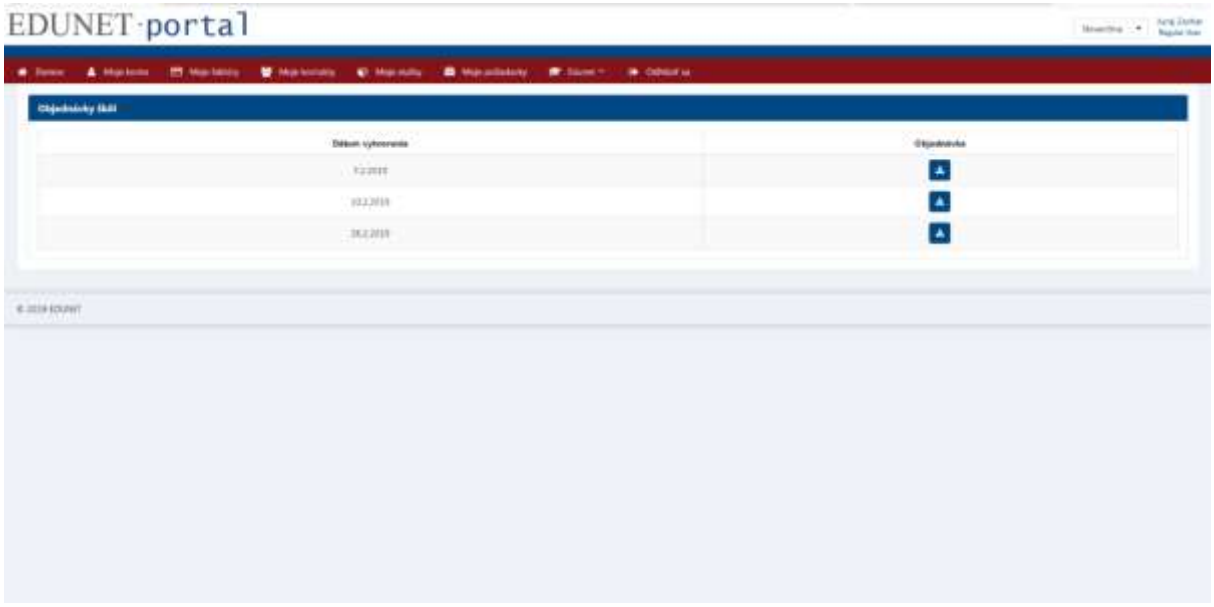




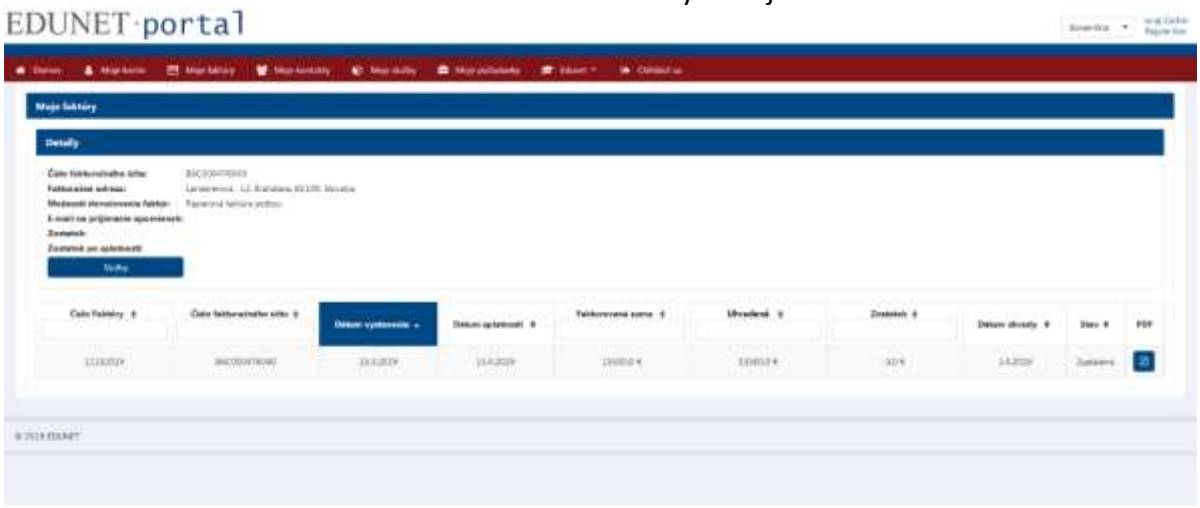
Obrázok č. 25 Historické údaje o službách a požiadavkách jednotlivej školy



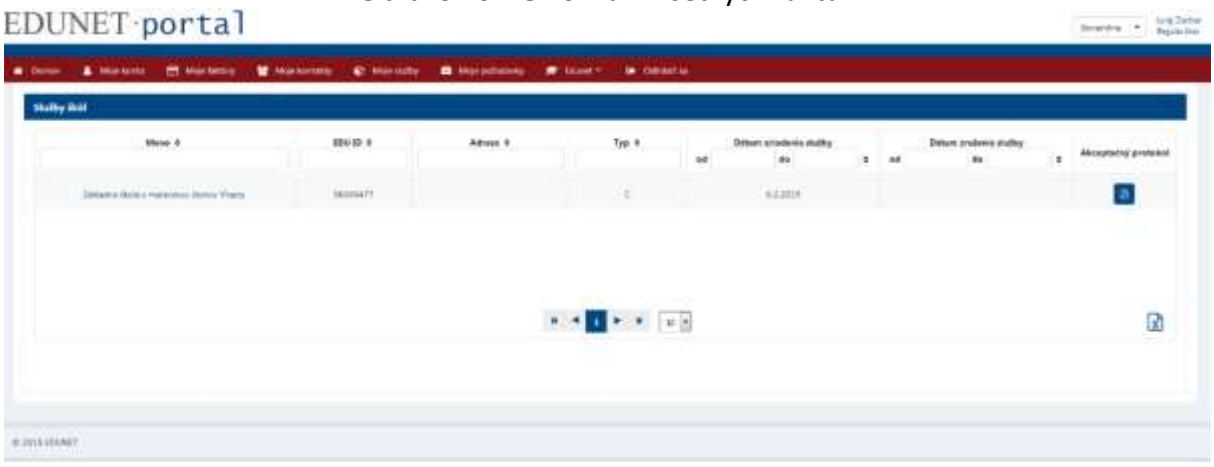
Obrázok č. 26 Zoznam škôl podľa typu pripojenia, počtu zapojených škôl



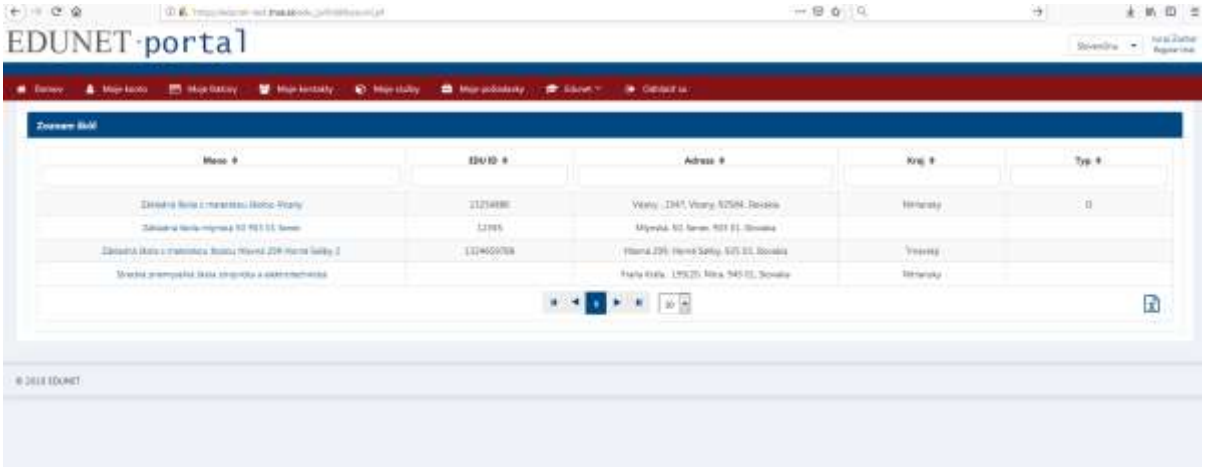
Obrázok č. 27 Zoznam všetkých objednávok



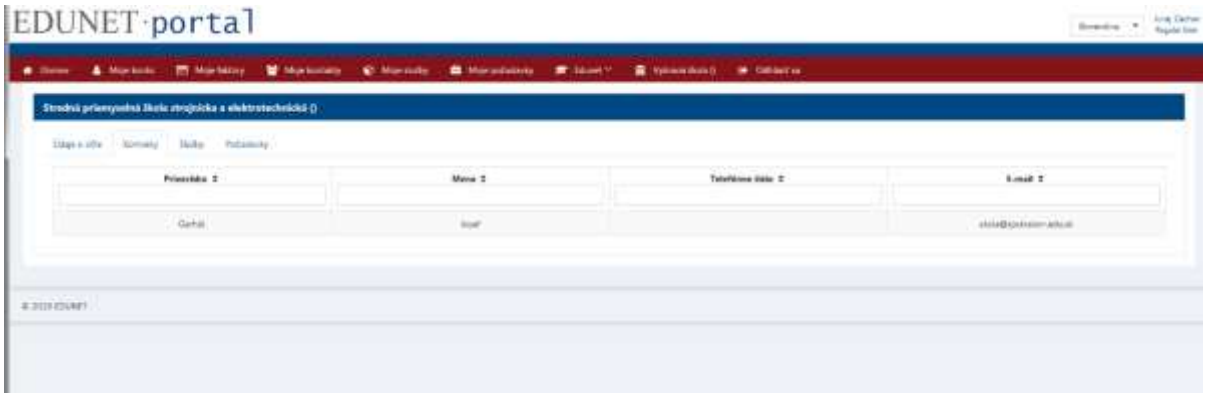
Obrázok č. 28 Zoznam všetkých faktúr



Obrázok č. 29 Zoznam všetkých preberacích protokolov



Obrázok č. 30 Zoznam všetkých škôl zapojených do projektu



Obrázok č. 31 Zoznam všetkých kontaktov na škole

10 Harmonogram projektu EDUNET_SK

Harmonogram projektu Edunet, sa operatívne prezentuje na pravidelných stretnutiach projektového manažmentu.