EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

INTEGROVANÝ REGIONÁLNÍ OPERAČNÍ PROGRAM

Prokázání a kontrola naplnění standardu konektivity ve výzvách IROP (infrastruktura základních a středních škol)

verze k 30. 6. 2017

Tento dokument definuje princip ověření a kontroly naplnění standardu konektivity v projektech IROP SC 2.4 zaměřených na zvýšení kvality a dostupnosti infrastruktury pro vzdělávání a celoživotní učení v oblasti zajištění vnitřní konektivity škol a připojení k internetu - rozvoj vnitřní konektivity v prostorách škol a školských zařízení a připojení k internetu. Dokument nemá žádnou právní závaznost, a byl vydán jako informativní příručka pro žadatele a příjemce v SC 2.4 IROP.

Kontrola parametrů konektivity je relevantní pouze v případě, když v rámci projektu na podporu infrastruktury základních, středních nebo vyšších odborných škol je tato aktivita realizována.

Obecně příjemce **prokazuje** naplnění standardu konektivity v rámci Závěrečné zprávy o realizaci projektu (ZZoR). Jakýkoliv projekt může být následně **zkontrolován** administrativním ověřením nebo kontrolou na místě pracovníky CRR nebo Řídicího orgánu IROP. Výčty příkladů aplikace ověření na místě jsou demonstrativní. V případě nenaplnění všech bodů standardu konektivity hrozí odebrání celé dotace na projekt!

Všechny povinné body standardu konektivity je nutné plnit po celou dobu udržitelnosti projektu.

UPOZORNĚNÍ:

Do MS2014+ se vkládá ZZoR ve formě textového pole, ovšem je možné přikládat přílohy. V tomto směru je doporučeno, aby pro doložení naplnění jednotlivých bodů standardu konektivity byl použit systém příloh, kdy „páteřní příloha“ bude strukturovaně popisovat naplnění jednotlivých bodů, a z této přílohy pak bude odkazováno na další jednotlivé přílohy (prinstcreeny apod.) prokazující naplnění jednotlivých bodů standardu konektivity.

Samozřejmě je na žadateli, jak tento systém pojme – je samozřejmě možné z textu ZZoR odkazovat na jednotlivé části jediné přílohy, kde bude vše potřebné zahrnuto (např. podrobná komplexní dokumentace k vnitřní konektivitě školy).

U příloh žadatel vždy uvede, k jakému datu byl daný stav zachycen.

Pro ověření některých parametrů standardu bude využíván nástroj na adrese www.standardkonektivity.cz s těmito funkcionalitami:

1. Rychlost, kvalita a typ připojení

- Podpora IPv4: ANO/NE
- IPv4 adresa
- Podpora IPv6: ANO / NE
- IPv6 adresa
- DNSSEC RSA: ANO/NE
- DNSSEC ECDSA: ANO/NE
- Připojeno do sítě FENIX[1]: ANO/NE
- Down-load: hodnota
- Up-load: hodnota
- Rozdíl Up-load a Down-rychlostí
- Ping

2. Podpora služeb

- Zadání URL (např. www.zsjizni.cz)
- IPv4 DNS záznam (A): ANO/NE
- IPv6 DNS záznam (AAAA): ANO / NE
- Zabezpečení domény DNSSEC: ANO / NE
- HTTPS: ANO/NE

Aby škola splňovala standard konektivity jako celek, je potřeba u všech sledovaných dílčích parametrů s možnostmi ANO/NE dosáhnout hodnoty ANO (✓), kromě parametru „Připojeno do sítě FENIX“, který může být vyhodnocen negativně, a přesto projekt splní standard konektivity (viz poznámka pod čarou).

[1] V rámci nástroje je ověřováno pouze připojení prostřednictvím ISP zapojeného do projektu FENIX. Negativní vyhodnocení tohoto kritéria však automaticky nemusí znamenat nesplnění podmínek Standardu konektivity škol, který umožňuje splnění podmínek i bez přijetí za člena projektu FENIX.

MANUÁL KE ZPŮSOBU OVĚŘENÍ JEDNOTLIVÝCH BODŮ STANDARDU

Zapracování zásad využívání ICT a přístupu k síti do vnitřních předpisů školy, v případě, že je tato aktivita realizována v rámci projektu IROP.

Prokázání:

- příjemce uvede, kdy a jakým způsobem byly zásady využívání ICT a přístupu k síti zapracovány do vnitřních předpisů školy. Příjemce povinně doloží k ZZoR příslušnou pasáž/směrnici.

1. **Konektivita školy k veřejnému internetu (WAN)**

Obecný popis: pro základní způsobilost projektu naplňujícího opatření „vnitřní konektivita škol" musí příslušná škola zajistit kvalitní připojení ke službám veřejného internetu, a to i v případě, že vybavení pro připojení k internetu není předmětem projektové žádosti. Za toto připojení je považováno zajištění konektivity splňující následující minimální parametry nejpozději ke dni ukončení realizace projektu:

Šíře pásma (bandwidth) odpovídající 128kbps/student[2] nebo 512kbps/počítač[3] nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů[4]

Prokázání:

- příjemce si ověří šíři pásma nástrojem na webu www.standardkonektivity.cz a přiloží export výsledku k ZZoR, nebo
- smlouva s providerem musí být nastavena tak, aby poskytovaná šíře pásma neomezovala běžný školní provoz, příjemce přiloží smlouvu k ZZoR, nebo
- příjemce v ZZoR (kapitola 6. Informace o zajištění provozu / údržby výstupů projektu po jeho ukončení) slovně popíše a vypočítá, že v rámci jeho parametrů (počet studentů, počet počítačů, počet zařízení přistupujících k internetu) dané připojení nijak neomezuje provoz zařízení a uživatelů

Symetrické připojení bez agregace a omezení (FUP)

Prokázání:

- příjemce ověří nástrojem na webu www.standardkonektivity.cz a přiloží export výsledku k ZZoR

Vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy

Prokázání:

---

2 *Počet studentů je definovaný celkový počet studentů školy*

3 *Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení*

4 *Definováno jako saturace šířky pásma připojení k veřejnému internetu, která ani ve špičkách nedosáhne a to ani krátkodobě 100%*

- příjemce ověří nástrojem na webu www.standardkonektivity.cz a přiloží export výsledku k ZZoR, společně s doprovodným XML otiskem databáze RIPE

Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)

Prokázání:

- příjemce ověří nástrojem na webu www.standardkonektivity.cz a přiloží export výsledku k ZZoR

Validující DNSSEC resolver na straně školy

Prokázání:

- příjemce ověří nástrojem na webu www.standardkonektivity.cz a přiloží export výsledku k ZZoR

Ověření na místě:

- Kontrolor se připojí zařízením do Wifi sítě a připojí se na stránky www.standardkonektivity.cz.

Podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení

Prokázání:

- příjemce přiloží k ZZoR záznam logu, a popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy)

Ověření na místě:

- v případě prověření na místě (pokud to v ZZoR nebude průkazné), bude přivolán technik a kontrolor ověří, že příjemce ukládá logy po deklarovanou dobu (namátkový záznam logu)

Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)

Prokázání:

- příjemce přiloží k ZZoR záznam logu DHCP, a popíše, jaký mechanismus logování používá (jak loguje a jak dlouho ukládá záznamy)

Ověření na místě:

- v případě prověření na místě (pokud to v ZZoR nebude průkazné), bude přivolán technik a kontrolor ověří, že příjemce ukládá DHCP logy po deklarovanou dobu (namátkový záznam logu – kontrola, kam který uživatel přistupoval v určitý časový okamžik)

Síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality

Prokázání:

- příjemce přiloží buď smlouvu, ze které bude patrná podpora rate limitingu, antispoofingu a ACL/xACL, nebo datasheet zařízení, ze kterého to bude patrné
- příjemce dále slovně obhájí, že rozhraní obsahuje všechny potřebné komponenty a licence a popíše jaké

Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu

Prokázání:

- příjemce popíše, jakým způsobem je realizováno – jak kategorizuje, jak selektuje apod., u antiviru popíše, jak ho používá a jak často ho a jakým způsobem aktualizuje. Zároveň doloží prinstcreen nastavení blokovaných adres v zařízení

Ověření na místě:

- kontrolor může chtít na požádání zablokovat ad hoc URL

Možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků

Prokázání:

- příjemce popíše, jakým způsobem je realizováno

Ověření na místě:

- kontrolor může chtít na požádání blokaci určitého rozsahu

Podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online

Prokázání:

- příjemce ověří nástrojem na webu www.standardkonektivity.cz a přiloží export výsledku k ZZoR

Zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX[5] nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX

Prokázání:

- příjemce ověří nástrojem na webu www.standardkonektivity.cz a přiloží export výsledku k ZZoR, nebo
- příjemce doloží čestným prohlášením, že, jeho poskytovatel je členem FENIX, nebo

příjemce doloží čestným prohlášením, že jeho poskytovatel jej propaguje do projektu FENIX prostřednictvím jiného operátora -člena FENIX

U software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.

Prokázání:

- příjemce popíše, jak tento bod zajišťuje (smlouva, zaplacené aktualizace, komunitní open source SW nebo další relevantní dokument, ve kterém je to ošetřeno)

2. Vnitřní konektivita školy (LAN)

Obecný popis: vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojením je nutné pokrýt prostory dotčené hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být zdůvodněna ve studii proveditelnosti.

Povinné minimální bezpečnostní parametry projektu (bez ohledu na typ síťového připojení):

- ***Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) – systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců***
- ***Povinné řešení systému správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD, apod.) a její využití pro autentizaci uživatelů***

[5] *V případě, kdy má ISP přidělené IP adresy od člena FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné adresy jsou v rámci FENIX propagovány. V případě, kdy má ISP vlastní ASn a není přímý člen FENIX, musí být součástí projektu prohlášení ISP, ze kterého bude patrné, že příslušné ASn propaguje do FENIX na základě smluvního vztahu některý ze členů FENIX.*

(žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. síťovým službám.

- ***logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel***

Prokázání:

- Příjemce detailně popíše, jak je tento bod standardu naplňován

Ověření na místě:

- Kontrolor může ad hoc ověřit výpis konkrétního provozu (zachycení pohybu uživatele na určité adrese v určitém čase)

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

- ***Minimální konektivita stanic a dalších koncových zařízení 100Mbit/s fullduplex***
- ***Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…)***
- ***Technická specifikace řešení LAN, žadatel popíše co používá***
- ***Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex***
- ***Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických nebo metalických vláken***
- ***Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)[6] s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,…***

Prokázání:

- Příjemce detailně popíše technickou specifikaci řešení LAN, co všechno využívá, a ideálně doloží smlouvami nebo datasheety

Ověření na místě:

- Kontrola infrastruktury, popř. datasheetů

V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:

Podpora mechanismu izolace klientů

Prokázání:

[6] *Požadavek se týká prvků, přes které je veden veškerý provoz, resp. jde o centrální prvky. Podružné přepínače (chodbové, učebnové) musí splňovat pouze požadavek na neblokující architekturou přepínacího subsystému*

- Příjemce detailně popíše technickou specifikaci řešení, jak je to nakonfigurováno a ideálně doloží smlouvami nebo datasheety

Ověření na místě:

- Kontrolor se připojí 2 zařízeními do wifi sítě, mezi zařízeními by neměl projít žádný provoz

Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů

Prokázání:

- Příjemce detailně popíše technickou specifikaci řešení, doloží dokumentaci provedení (mapa, model pokrytí)

Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)

Prokázání:

- Příjemce detailně popíše technickou specifikaci řešení, doloží technickou specifikaci řešení

Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD …)

Prokázání:

- Příjemce detailně popíše technickou specifikaci řešení a doloží datasheety

Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz

Prokázání:

- Příjemce detailně popíše technickou specifikaci řešení a doloží datasheety

Minimálně pasivní zapojení[7] do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam, pro zajištění národní i mezinárodní mobility žáků a učitelů.

Prokázání:

- Příjemce doloží potvrzení od CESNET, že u něj funguje min. pasivní zapojení do eduroam,kontaktní adresa: eduroam-IROP@cesnet.cz

Ověření na místě:

- Kontrolor se svým eduroam účtem připojí do sítě příjemce a ověří, že se připojí např. na stránku www.standardkonektivity.cz.

Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

Prokázání:

- Příjemce detailně popíše technickou specifikaci řešení a doloží datasheety

3. Další bezpečnostní prvky

Obecný popis: v rámci projektů je možné realizovat další aktivity naplňující principy bezpečného využívání IT prostředků. Pokud příjemce v rámci projektu uplatnil způsobilé výdaje na některé z bodů uvedených níže, je třeba prokázat v ZZoR následující:

Identity management system (IDM) – systém správy identit, řízení životního cyklu uživatelů, integrace do provozních a bezpečnostních systémů

Prokázání:

- Příjemce detailně popíše systém IDM, počet identit, a pro co všechno je to využíváno, jak je řízen životní cyklus identity

Centralizovaný autentizační systém napojení na systém správy identit (např. na bázi LDAP, AD, studijní a personální agendy apod.)

Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty, blokace wifi v určitém čase)

[7] *Pasivním zapojením se rozumí poskytování služeb sítě eduroam na úrovni poskytovatele zdrojů – viz. http://www.eduroam.cz/_media/cs/cz_roam_policy_v2.0.pdf*

Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací a zpřístupnění jejich služeb)

Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3954 nebo ekvivalent (NetFlow))

Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie

Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management)

Systémy pro monitorování funkčnosti síťové a serverové infrastruktury (např. Nagios / Icinga)

Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk)

Nástroje pro centrální správu a audit ICT prostředků

Systémy zálohování a obnovy dat serverové infrastruktury

Systémy pro antivirovou ochranu zařízení, antispamovou ochranu poštovních serverů

Zabezpečení přístupových protokolů (SSL/TLS) služeb (např. emailové služby, webové servery, studijní a ekonomické agendy) atp.

Podpora vzdáleného přístupu (VPN)

Prokázání:

- Příjemce detailně popíše implementaci a design daného systému / nástroje, doloží datasheety

!!!DOPORUČENÍ: ideální je mít vše ohledně konektivity podrobně zdokumentováno a pak z jednotlivých bodů jen odkazovat na dokumentaci, přiloženou k ZZoR!!!