KONEKTIVITA

SOUHRNNÁ ZPRÁVA

TECHNICKÝ POPIS UCELENÉHO ŘEŠENÍ

IDENTIFIKAČNÍ ÚDAJE

Stavba:	Vybavení odborných učeben Základní škola Ivanovice na Hané, okres Vyškov
	Tyršova 218/4, 683 23 Ivanovice na Hané
Místo stavby:	Základní škola Ivanovice na Hané, okres Vyškov
	Tyršova 218/4, 683 23 Ivanovice na Hané
Dílčí část:	Konektivita
Stupeň dokumentace:	Dokumentace výběru dodavatele – DVD
Investor:	Základní škola Ivanovice na Hané, okres Vyškov
	Tyršova 218/4, 683 23 Ivanovice na Hané
Projektant profese:	**DESIGN 4AVI s.r.o.**, Pražská 63, 102 00 Praha 10
	Sebastian Fenyk

TECHNICKÁ SPECIFIKACE

Základní požadavky na technické řešení

(1) Cílem projektu je zvýšení bezpečnosti a související modernizace IT infrastruktury, aby implementací projektu byly naplněny Standardy konektivity škol [1] - uvedené v příloze č.1 (dále jen Standard konektivity). Dílčí cíle dle jednotlivých komodit jsou specifikovány následovně:

Označení	Komodita	Počet
K1	Virtualizační platforma	1
K2	Zabezpečení LAN a Wifi	1
K3	Centrální logování	1

(2) Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Microsoft pro zachování kompatibility se stávajícími systémy a aplikacemi. Přechod na jinou platformu by způsobil uživatelské a provozní potíže.

(3) Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.

(4) Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu, přičemž nesmí překročit předpokládanou hodnotu zakázky.

(5) Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
(b) mají plnou záruku od výrobce,
(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží čestným prohlášením distributora, popř. dodavatelovým samotným, nelze-li prohlášení distributora získat.

Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

(6) Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.

1. TECHNICKÁ SPECIFIKACE – Konektivita

1.1. Specifické požadavky na technické řešení

(1) **K1 - Virtualizační platforma**

(a) Pro provoz veškerých pořízených systémů a aplikací bude pořízen jeden server vybavený interním úložištěm s vysokou kapacitou. Hardware serveru bude virtualizován a na serveru bude možno provozovat **min 4** virtuálních serverů.

(b) Provozní zabezpečení bude tvořeno souborem non-IT technologií, které zajistí optimální podmínky pro spolehlivý chod technologií – především serveru:

(i) Záložní zdroj napájení UPS zajistí chod serveru při výpadku napájení

(c) Pro zajištění bezpečnosti a možnosti řízení provozu v síti a zajištění prokazatelného monitoringu, logování a auditu interního i externího síťového provozu bude vybudována centrální databáze identit na bázi adresářové služby. Adresářová služby umožní ukládání a přehlednou správu identit (účtů včetně metadat) učitelů, žáků i externích subjektů, ale i technických prostředků – serverů, tiskáren, pracovních stanic apod. Adresářová služba bude poskytovat službu LDAP a umožní snadné napojení autentizačních mechanismů a protokolů – radius, agenta firewallu a dalších. Adresářová služba zajistí ověřování uživatelů pro účely jejich autorizace k přístupu k síťovým prostředkům (LAN, Internet atd.) i výpočetním zdrojům (pracovní stanice, tiskárny, sdílené složky atd.). Technické provedení bude založeno min. na 1 řadiči adresářové služby. Řadič bude provozován a bude pravidelně automaticky zálohovány. Součástí řadičů budou základní síťové služby – DNS, DHCP.

(2) **K2- Zabezpečení LAN a Wifi**

(a) Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby.

(b) Řízení provozu v LAN bude realizováno vytvořením VLAN (802.1Q), segmentací sítě s routováním (přepínáním) provozu mezi VLAN na úrovni centrálního přepínače s nastavitelnými ACL. Pro řízení provozu na úrovni kvality služeb bude k dispozici technologie QoS (QualityofServices).

(c) Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem (řadičem), který bude součástí firmwarů přístupových bodů.

(d) Ověřování přístupu do WiFi sítě bude realizováno na stejném principu jako LAN. Wifi bude nabízet více SSID (učitelé, žáci, Guest), které budou obsluhovány samostatnými VLAN a budou napojeny na raduis servery. Učitelé a žáci budou prostřednictvím radius serveru ověřováni v adresářové služby. Zabezpečení vnitřních sítí (BSSID) školy bude provedeno dle 802.1i, tedy - WPA2 s AES šifrováním a konfigurováno shodně pro obě frekvenční pásma. Výjimkou bude síť určená výhradně pro hosty (GuestWiFi).

(3) **K3 - Centrální logování**

(a) Bude implementováno řešení, které umožní příjem a vyhodnocení všech požadovaných informací - může jednat o jediné zařízení, softwarový nástroj či appliance. Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze https bez nutnosti instalace klienta. Data bude ukládána do jedné databáze (nebo více integrovaných databází) tak, aby bylo možno realizovat multikriteriální vyhledávání napříč informacemi z různých zdrojů (např. přepínače/ netflow a firewall/syslog).

(b) Veškeré dále požadované informace si bude systém automaticky získávat, vyčítat z monitorovaných systémů a současně bude umožňovat příjem protokolů určených pro přenos logovacích, provozních informací, alertů a událostí. Systém bude přijímat informace standardními protokoly ze síťových a dalších aktivních zařízení a Windows server systémů.

(c) Mandatorní informace, která bude v systému vždy obsažena a uchována, je vazba IP-uživatel-čas. Tuto informaci bude systém čerpat ze securityevent-logu adresářové služby, dále z informací o probíhajících komunikacích prostřednictvím firewallu a dalších přístupových a autentifikačních systémů (např. radius logy). Dále budou získávány informace o překladu zdrojových, vnitřních IP adres na externím výstupním rozhraní firewallu, kde bude prováděn NAT. Bude se tedy jednat o informace obsažené v NAT tabulce. Spolu s tím musí být po stanovenou dobu možné zpětně dohledat i vnější provoz k vnitřnímu zařízení. Další funkcionalitou bude plnohodnotná práce se síťovými toky, jejich zpracování a archivace. Nástroje systému budou umožňovat i analytickou práci s přijímanými toky a to i zpětně.

1.2. Implementační služby

(1) V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K3

(a) Dodávka a implementace předmětu plnění musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií. Musí být v souladu s nabídkou uchazeče a se Standardem konektivity.

(b) Zajištění projektového vedení realizace předmětu plnění.

(c) Zpracování **provozní dokumentace** v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat minimálně následující oblasti:

(i) ActiveDirectory – správa uživatelů a skupin

(ii) Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace

(iii) Monitorovací a logovacího systém - vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce

(iv) LAN a Wifi - připojení zařízení uživatelských postupů pro Wifi.

(v) Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupinu

(d) Provedení akceptačních testů.

(e) Předání do plného provozu.

(2) Zadavatel dále požaduje provést minimálně následující implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

K1: Virtualizační platforma
a) Návrh a kompletní implementace serverové virtualizační platformy b) Implementace pořízených technologií c) Návrh vhodné struktury ActiveDirectory, její vybudování d) Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie e) Návrh a provedení akceptačních testů
K2: Zabezpečení LAN a Wifi
a) Implementace pořízených technologií b) Provedení segmentace LAN – VLAN, adresování, routování

c) Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách d) Návrh a implementace pro kabelovou LAN i WiFi včetně uživatelské dokumentace pro konfigurace obvyklých zařízení a jejich systémů - PC, notebooky, chytré telefony, tablety, tiskárny - Windows, Linux, MacOS, Android, IOS, embedded systémy periferií e) Návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu f) Vybudování VPN pro vzdálený přístup uživatelů LAN g) Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik h) Zajištění ostatních nezbytných činností pro naplnění Standardu konektivity
K3: Centrální logování
a) Návrh a implementace systému pro centrální logování pro naplnění požadavků Standardu konektivity, především, ale nejen: • logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.) b) Provedení souvisejících konfigurací monitorovaných systémů

(3) Akceptační testy musí pro všechny komodity vždy zahrnovat minimálně prokázání kompletnosti dodávky a požadované funkčnosti. Povinným akceptačním kritériem bude prokázání naplnění požadavků Standardu konektivity dle manuálu k postupu při prokazování a kontrole včetně úspěšného provedení a doložení testu na https://www.standardkonektivity.cz/. Prokázání naplnění požadavků poskytne dodavatel v písemné formě vhodné jako příloha k Závěrečné zprávě o realizaci projektu.

1.3. Školení

(1) Školení bude pokrývat všechna zařízení a systémy všech komodit, dodávané v rámci této veřejné zakázky, a to minimálně v rozsahu:

(a) běžných administrátorských činností pro implementované systémy

(b) standardní údržby systémů pro administrátory zadavatele

(2) Školení dále zajistí seznámení pracovníků zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.

(3) Minimální rozsah školení pro každou komoditu je 1 hodina, není-li uvedeno jinak. Školení bude probíhat v sídle zadavatele.

1.4. Popis povinných parametrů dodávaného řešení

(1) V dále uvedených tabulkách jsou uvedeny povinné parametry prvků nabízeného řešení. Dodavatel musí všechny parametry splnit, v případě nesplnění požadavku zadavatele bude nabídka dodavatele vyřazena a dodavatel bude následně vyloučen z účasti v zadávacím řízení.

(2) Dodavatel ve své nabídce uvede přesné označení nabízeného zboží formou PN, nebo přesného obchodního označení. Ze značkové specifikace nabízených dodávek PN případně z obchodního popisu bude možno určit, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.

Povinné parametry pro Komoditu K1 - Virtualizační platforma:

Parametr	
Formát serveru	Rackové provedení, min.. 1U. Pro přístup ke všem komponentám serveru není nutné nářadí. Barevně značené hot-plug vnitřní i vnější komponenty
CPU	Server musí být osazen min. 1x CPU, minimálně s šestnácti procesorovými jádry. Hodnocení výkonu nabídnutého serveru musí být publikované na webu: https://www.cpubenchmark.net s minimálními parametry: • Passmark CPU Mark, hodnota min: 25 100
RAM	128GB v provedení min. DDR4, min. 3200 MHz rozšiřitelnou minimálně na 256GB
Diskový subsystém	Server musí disponovat alespoň 4x diskovou hotswap šachtou pro disky 3,5", přístupnou zpředu. Požadujeme osazení min. dvěma SSD s kapacitou alespoň 480GB min. dvěma 8TB 7.2K RPM SATA 6Gbps
Optická mechanika	Není požadována.
Diskový řadič	• typu SAS12 • podpora hot-plug disků SAS, SSD i SATA • podpora min. RAID - 0, 1, 5, 6, 10, 50, 60 • Cache řadiče alespoň 8GB se zálohováním proti výpadku napájení na dobu min. 72 hodin • Řadič nezabírá volné PCI-e sloty
Síťové rozhraní	• 2x 1000Base-T, onboard (nezabírající volné PCI-e sloty) • 2 x 10/25GbE SFP28
Napájení	Redundantní napájecí zdroje 230V, max. 700W
Chlazení	Možnost provozu při okolní teplotě stabilně až do 40°C (provoz chlazení čerstvým vzduchem)
Interface	2 x přední, 2x zadní a 1x vnitřní USB port (alespoň jeden zadní a vnitřní s podporou USB3.0) Interaktivní LCD display indikující základní informace o systému (min. IP adresa, model, chybové stavy, atd.), možnost nastavení IP konfigurace a čtení chybových stavů z out-of-band managementu, bez potřeby připojení monitoru a klávesnice
Rozšiřující sloty	Minimálně 1x PCI-e x16 Gen 3 slot, LP – volný pro budoucí rozšiřování Dedikovaný RAID slot pro RAID kartu OCP 3.0 slot
Kolejnice	Zásuvné ližiny pro rack
Podpora OS a virtualizace	Microsoft Windows Server 2016 Microsoft Windows Server 2019 Microsoft Windows Server 2022 VMware ESX 6.7 až 8.0 RedHatEnterprise Linux 7 RedHatEnterprise Linux 8 RedHatEnterprise Linux 9 SUSE Linux ES 15 Ubuntu 20.04 LTS Ubuntu Server 22.04 LTS

Management a vzdálená správa	Management serveru nezávislý na operačním systému poskytující následující management funkce a vlastnosti: • web GUI a dedikovaná IP adresa, dedikovaný management LAN port s podporou VLAN • SW LAN adaptér pro management mapovaný prostřednictvím z předu přístupného USB portu, podpora přímého připojení USB kabelem z notebooku správce nebo servisního technika (není nutné zpřístupňovat management LAN) • Agent-less hardware FW update vč. možnosti rollback při neúspěchu • Podpora asistovaného OS Deploymentu • LifeCycle Log • sledování hardwarových sensorů (teplota, napětí, stav, chybové sensory) • erroralerty (server reset, kritické sensorové hodnoty, atd.) za použití email traps, paging, atd. • možnost failoveru management LAN portu na jinou síťovou kartu na desce serveru (LOM) • podpora IPv6 • podpora WS-MAN/SMASH-CLP • plná podpora a IPMI funkcionalita • vestavěný Unified Server Configurator GUI (není třeba asistenční/driverové nebo HW-test CD/DVD) • vzdálená konfigurace RAID, přímo v OOB managementu • server remote reset, reboot, power-on/off/cycle • power management a powercaping • integrace managementu do ActiveDirectory a dvoufaktorováauthentikace (TFA), encryption) • podpora RemotevirtualSerial support • BIOS recovery • Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru • Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashována proti zneužití (zerotouchdeployment) • Management serveru ukládá nastavení komponent do vyhrazené paměti, která je neoddělitelnou součástí chassis. Tato konfigurace je pak použitelná po výměně kterékoliv HW komponenty • Interaktivníčelníinformační panel, informující o stavu a názvu serveru s možností zobrazení názvu aktuálně spuštěných virtuálních strojů. Panel musí umožňovat kontrolu a nastavení parametrů out-of-band vestavěné správy systemu, včetně přiřazení IP adres a přístupu do HW logu • management nástroje musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích • Integrovatelnost s dohledovou konzolí OpenManage Essentials
Podpora a servis	Podpora na 3 roky typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru, možnost rozšíření záruky min. na 7 let. Podpora prostřednictvím internetu musí umožňovat stahování ovladačů a manuálů adresně pro konkrétní zadané sériové či produktové číslo každého serveru. Možnost provázání managementu serveru pro online spojení technickou podporou výrobce a automatickým otevíráním servisních požadavků včetně automatického odeslání HW a OS logů pro následný troubleshooting proces.

SW licence operačních systémů <u>NELZE použít v nabídce druhotných licencí</u>	Serverové operační systémy	**2 ks** licencí 64-bitového serverového operačního systému v aktuální verzi. Licence musí umožnit provoz hypervizoru a min. 2 virtuálních serverů stejné verze v prostředí nabízené serverové virtualizace, dále provoz všech nabízených aplikací a management nástrojů.
	Klientské licence	klientské licence pro nabízené operační systémy umožňující využívat těchto systémů uživatelům celkem na **120** zařízeních.

UPS 1x	Provedení	Provedení do racku, max. 2U, včetně montážního materiálu nebo TOWER s možností umístění ve vertikální i horizontální poloze
	Elektrické provedení	Jmenovité napětí 230 V, jednofázová na vstupu i výstupu
	Výkon (VA/W)	1000 VA / 600 W
	Technologie	Line- interaktivní
	Vstup	Zásuvka IEC C14
	Výstupy	Min. 4 zásuvek IEC C13
	Komunikační porty	USB, RJ-45
	Záruka	min. 24 měsíců

Síťové úložiště NAS 1 ks	Provedení	Tower nebo RACK pro 4x HDD 3,5“
	Výkon	1xCPU min 2500bodu v CPU MARK na https://www.cpubenchmark.net
	Rozšiřitelnost	2x USB 3.2 Gen 1
	Kapacita	Osazeno 4x HDD 4TB 256MB, SATA 6 Gb/s, 7200ot/min, stejného výrobce jako NAS (nepřipouští se HDD určené jiným účelům (desktop, kamerové systémy apod.).
	Konektivita	2x RJ-45 1GbE LAN
	RAM	min. 2GB DDR4 non-ECC SODIMM s možností rozšíření až na 6GB
	Záruka	min. 36 měsíců

Datový rozvaděče – INFRA technologie		
Specifikace	Datový rozvaděč min 19U pro INFRA technologie, hloubka min 800mm	**1 ks**
Provedení	kovové robustní provedení	
Záruka	min. 24 měsíců	

Povinné parametry pro Komoditu K2 – Zabezpečení LAN a Wifi:

NGF

Základní technické požadavky

• Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …)
• Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu záruky **3ROKY**. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
• Požadujeme dodání zařízení ve formátu HW appliance o velikosti desktop
• Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem.
• Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.

HW parametry:

• Počet síťových rozhraní copper, RJ45 10/100/1000 - min 6x
• Dedikovaný port RJ45 pro DMZ
• Konzolový port pro management
• USB 3.0 port pro zálohu konfigurace
• 120 GB SSD interní HDD pro ukládání logů
•

Výkonnostní parametry:

• Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 10000 Mbps, 10000 Mbps, 7000 Mbps
• Latence firewallu (64 B UDP paket) - max 3,5 mikro sec
• Propustnost firewall – 10.5 Mpps
• Počet naráz otevřených spojení – min 1 500 000
• Počet nových spojení za sekundu - min. 45 000
• Počet firewall pravidel až 5 000
• Podpora virtualizace (min 10 virtuálních kontextů)
• Podpora funkce bezdrátový kontrolér – až 96 AP
• Podpora funkce integrovaný switch controller – podpora až 16 switchů

• Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru
• Režim fungování L2 – transparentní režim, L3 – NAT/Router
• Podpora VLAN
• Podopora multicast, vytváření politiky pro multicast routování
• Podpora 802.3ad link aggregation
• Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading
• Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace
• Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP
• Policy-based routing
• Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky

VPN

• Funkce SSL VPN
• Podpora klientského i bezklientského (portálového) režimu
• Minimální počet současně navázaných SSL VPN tunelů: 200
• Minimální propustnost SSL VPN: 950Mbps
• Funkce IPSEC VPN
• podpora site-to-site VPN
• podpora klientských VPN
• dostupnost VPN klienta pro koncové stanice (Windows, MacOS)
• funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence.
• Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 200
• Minimální počet klientských IPSEC VPN tunelů: 2500
• propustnost IPSec VPN min. 6,5 Gbps (měřeno při AES256-SHA256)
• podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
• podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování
• podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace
• Podpora VXLAN
• Podpora L2TP, PPTP, GRE
• podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec

Funkcionality

• Funkce detekce aplikací na L7 (Application Control)
• Detekce známých aplikací na základě signatur
• Signaturový database automaticky aktualizované výrobcem
• alespoň 4000 podporovaných aplikací
• pro populárná cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci)
• možnost tvorby vlastních signatur
• detekované aplikace je možné: povolit, monitorovat, blokovat
• na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
• funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.
• Funkce detekce a potlačení narušení (IPS/IDS)
• signatury automaticky aktualizované výrobcem
• alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem
• možnost tvorby vlastních signatur
• funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
• propustnost funkce IPS včetně logování min. 1400Mbps (měřeno na komunikaci typu mix aplikací)
• Funkce antivirové kontroly
• Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem
• Signatury automaticky aktualizované výrobcem

• požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)
• možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce
• deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 900Mbps
• funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
• Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů
• Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.
• Funkce kategorizace webových stránek
• založená na centrálně spravované databázi výrobce
• minimálně 50 filtračních kategorií
• možnost definice vlastních kategorií
• možnost definice vlastních seznamů zakázaných URL
• kategorizace musí zahrnovat I české a slovenské internetové stránky
• Funkce DNS filtru
• Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu)
• Možnost definovat vlastní tzv. blacklist domén
• Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
• Možnost importu seznamu blokovaných domén do DNS filtru
• Detekce a blokování komunikace do botnet sítí
• Funkce ochrany před únikem citlivých informací (DLP)
• možností analýzy běžných typů dokumentů a protokolů
• možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum
• Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty
• Podpora SSL dekrypce/SSL inspekce s minimální propustností 700Mbps
• DoS Policy prevence proti základním útokům typu DoS

Firewall

• Možnost nastavovat firewall politiku na základě geografických údajů
• Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem
• Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud
• Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
• Viditelnost do provozu na aplikační úrovni
• Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
• Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu
• Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
• Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
• Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
• Podpora funkce reverzní proxy
• Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
• Explicit proxy podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
• podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos
• funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
• Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru
• Integrovaný controller bezdrátových (Wifi) sítí
• Wifi controller integrovaný do NGFW platformy
• Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním
• podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru
• podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru
• Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení

•	Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor)
•	On-wire rogue AP detekce a mitigace
•	Podpora fast-roamingu (802.11 k,v,r)
•	podpora více PSK u jednoho SSID
•	podpora IPSEC tunelu pro šifrování data plane (uživatelských dat)
•	podpora WPA3 šifrování

Virtualizace

•	Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.
•	Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)
•	Každý virtuální kontext je zároveň samostatným wifi controllerem
•	Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)

Management

•	FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
•	Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
•	Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)

1x Centrální přepínač 24x1000Mbps + 8x 10G SFP+ LC SM Transceiver

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Třída zařízení: přepínač	ano	
Formát zařízení do racku	ano	
Velikost zařízení: 1U	ano	
Počet 1Gbit/s metalických portů	24x 10/100/1000Mbps RJ45	
Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+)	4x	
Interní AC zdroj	ano	
Maximální spotřeba přepínače při plném zatížení	66W	
Celková přepínací propustnost přepínače	128Gbit/s	
Celkový paketový výkon přepínače	95Mpps	
Minimální paketový buffer: 8MB	ano	
Maximální hloubka přepínače: 33 cm	ano	
Vlastnosti stohování		
Podporovaný počet přepínačů ve stohu: 8	ano	
Kapacita stohovacího propojení: 80 Gbps	ano	
Stoh podporuje distribuované přepínaní paketů	ano	
Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 100m)	ano	
Redundance řídícího prvku v rámci stohu	ano	
Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port)	ano	
Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)	ano	
Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)	ano	
Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF	ano	

Součástí každého přepínače je stohovací kabel minimálně 10GE s minimální délkou 1m	ano	
Základní funkce a protokoly		
Podpora "jumbo rámců" včetně velikosti 9198 Byte	ano	
Podpora linkové agregace IEEE 802.1AX	ano	
Konfigurovatelné rozkládání LACP zátěže podle L2, L3	ano	
Počet LACP skupin/linek ve skupině: 32/8	ano	
Minimální počet záznamů v tabulce MAC adres: 16 000	ano	
Minimální počet záznamů v tabulce ARP: 8 000	ano	
Protokol pro definici šířených VLAN: MVRP	ano	
Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN	ano	
Podpora zařazování do VLAN podle standardu 802.1v	ano	
IEEE 802.1s - Multiple Spanning Tree	ano	
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ano	
Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED	ano	
Detekce jednosměrnosti optické linky (např. UDLD)	ano	
Podpora NTPv3	ano	
Statické směrování IPv4 a IPv6	ano	
Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000	ano	
Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000	ano	
Dynamické směrování OSPFv2, OSPFv3, RIP, RIPng	ano	
Podpora Layer-3 routed port	ano	
IGMP v2 a v3	ano	
IGMP snooping	ano	
MLD v1 a v2	ano	
MLD snooping	ano	
Hardware podpora IPv4 a IPv6 ACL	ano	
ACL definice na základě skupiny fyzických portů	ano	
ACL aplikovatelný na interface, LAG, VLAN	ano	
BPDU a Root guard	ano	
DHCP snooping pro IPv4 a IPv6	ano	
IPv6 RA Guard	ano	
HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps	ano	
802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	ano	
Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)	ano	
Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675	ano	
Podpora Critical VLAN	ano	
Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.	ano	
Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace	ano	
Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace	ano	
Podpora Dynamic ARP protection	ano	
Port security	ano	
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ano	
Podpora IPv4 a IPv6 QoS	ano	
IEEE 802.1p - minimální počet front: 8	ano	
SDN funkce		

Podpora technologie VXLAN	ano	
Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů	ano	
Přiřazení koncového zařízení do tunelu na základě výsledku autorizace	ano	
Analytické a automatizační nástroje		
Podpora REST API pro automatizaci nastavení sítě.	ano	
Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači	ano	
Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	ano	
Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události	ano	
Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů atp.	ano	
Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.	ano	
Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení	ano	
Kapacita interního úložiště dat pro analytické účely minimálně 14 GB	ano	
Management		
USB-C konzolový port	ano	
1xRJ45 OoB management port s podporou ethernetu	ano	
Konfigurace zařízení v člověku čitelné textové formě	ano	
Podpora automatických i manuálních snapshotů konfigurace systému	ano	
USB port pro diagnostiku, přenos konfigurace a firmware	ano	
Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth	ano	
Podpora managementu přes IPv4 i IPv6	ano	
SSHv2 a HTTPS pro IPv4 a IPv6	ano	
Podpora SNMPv2c a SNMPv3	ano	
RMON	ano	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	
Lokálně vynucené RBAC na úrovni přepínače	ano	
Dualní flash image	ano	
Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů	ano	
Podpora RADIUS včetně RADIUS CoA (RFC3576)	ano	
Podpora standardního Linux Shellu (BASH) pro debugging a skriptování	ano	
Podpora TACACS+	ano	
Podpora Secure RADIUS (RadSec)	ano	
Analýza síťového provozu sFlow podle RFC 3176	ano	
Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu	ano	
Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN	ano	
Podpora IP SLA pro měření zpoždění provozu VoIP	ano	
Podpora Zero Touch Provisioning (ZTP)	ano	
8KS 10G SFP+ LC SM Transceiver	ano	

Produkty které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,

(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,

(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt
(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží potvrzením <u>výrobce</u> tohoto zařízení:

2x ACCESS přepínač 48x1G PoE + 4xSFP+

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Třída zařízení: L3 switch	ano	
Formát zařízení do racku	ano	
Velikost zařízení: 1U	ano	
Počet 10/100/1000Mbit metalických portů	48×RJ45	
Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním	4×SFP+	
10GE interface zpětně kompatibilní s 1Gbit/s transceivery	ano	
Všechny ethernet porty jsou dostupné zepředu	ano	
Interní napájecí zdroj	ano	
Podpora PoE+ dle standardu 802.3at	ano	
Dostupný výkon pro PoE+ napájení	370W	
Podpora Energy Efficient Ethernet (802.3az)	ano	
Celková propustnost přepínače	176 Gb/s	
Celkový paketový výkon přepínače	98 mpps	
Minimálně 12MB paketový buffer	ano	
Maximální přípustná hloubka přepínače	max. 31cm	
Bez ventilátoru	ne	
Základní funkce a protokoly		
Podpora "jumbo rámců" včetně velikosti 9220 Byte	ano	
Podpora linkové agregace IEEE 802.3ad	ano	
Konfigurovatelné rozkládání LACP zátěže podle L3 a L4	ano	
Minimální počet LACP skupin/linek ve skupině: 8/8	ano	
Protokol pro definici šířených VLAN: MVRP	ano	
Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN	ano	
IEEE 802.1s - Multiple Spanning Tree	ano	
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ano	
Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED	ano	
Detekce jednosměrnosti optické linky (např. UDLD)	ano	
NTP pro IPv4 a IPv6 včetně MD5 autentizace	ano	
Statické směrování IPv4 a IPv6	ano	
IGMP v2 a v3	ano	
MLD v1 a v2	ano	
Hardware podpora IPv4 a IPv6 ACL	ano	
ACL definice na základě skupiny fyzických portů	ano	
ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN	ano	
BPDU guard a Root guard	ano	
HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu	ano	
ICMPv4 a ICMPv6 rate-limiting per port	ano	
Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port	ano	
Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)	ano	
802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN	ano	
Dynamické zařazování do VLAN	ano	
802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)	ano	

Port security - omezení počtu MAC adres na port, statické MAC	ano	
Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení	ano	
Ochrana control plane (CPU) před útoky typu DoS	ano	
Podpora IPv4 a IPv6 QoS	ano	
Minimálně 8 front pro IEEE 802.1p	ano	
Management		
CLI formou 1x USB-C Console Port	ano	
Konfigurace zařízení v člověku čitelné textové formě	ano	
Podpora automatických i manuálních snapshotů konfigurace systému	ano	
USB port pro diagnostiku, přenos konfigurace a firmware	ano	
Podpora managementu přes IPv4 i IPv6	ano	
SSHv2 a a SFTP	ano	
Podpora SNMPv2c a SNMPv3	ano	
RMON	ano	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	
Lokálně vynucené RBAC na úrovni přepínače	ano	
Dualní flash image	ano	
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů	ano	
Podpora Syslog over TLS	ano	
Podpora RADIUS včetně RADIUS CoA (RFC3576)	ano	
Podpora RADIUS IPSEC	ano	
Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem	ano	
Podpora TACACS+	ano	
Analýza síťového provozu sFlow podle RFC 3176	ano	
Port mirroring (SPAN), alespoň 4 různé obousměrné session	ano	
Podpora Zero Touch Provisioning (ZTP)	ano	
REST API pro automatizaci nastavení	ano	
Automatická konfigurace portu podle připojeného zařízení	ano	
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano	

Produkty které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,
(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt
(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží potvrzením <u>výrobce</u> tohoto zařízení:

2x ACCESS přepínač 24x1G PoE + 4xSFP+

Požadavek na funkcionalitu	**Minimální požadavky**	**Splňuje ANO/NE**

Základní vlastnosti		
Třída zařízení: L3 switch	ano	
Formát zařízení do racku	ano	
Velikost zařízení: 1U	ano	
Počet 10/100/1000Mbit metalických portů	24×RJ45	
Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním	4×SFP+	
10GE interface zpětně kompatibilní s 1Gbit/s transceivery	ano	
Všechny ethernet porty jsou dostupné zepředu	ano	
Interní napájecí zdroj	ano	
Podpora PoE+ dle standardu 802.3at	ano	
Dostupný výkon pro PoE+ napájení	370W	
Podpora Energy Efficient Ethernet (802.3az)	ano	
Celková propustnost přepínače	128 Gb/s	
Celkový paketový výkon přepínače	95 mpps	
Minimálně 12MB paketový buffer	ano	
Maximální přípustná hloubka přepínače	max. 31cm	
Bez ventilátoru	ne	
Základní funkce a protokoly		
Podpora "jumbo rámců" včetně velikosti 9220 Byte	ano	
Podpora linkové agregace IEEE 802.3ad	ano	
Konfigurovatelné rozkládání LACP zátěže podle L3 a L4	ano	
Minimální počet LACP skupin/linek ve skupině: 8/8	ano	
Protokol pro definici šířených VLAN: MVRP	ano	
Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN	ano	
IEEE 802.1s - Multiple Spanning Tree	ano	
STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	ano	
Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED	ano	
Detekce jednosměrnosti optické linky (např. UDLD)	ano	
NTP pro IPv4 a IPv6 včetně MD5 autentizace	ano	
Statické směrování IPv4 a IPv6	ano	
IGMP v2 a v3	ano	
MLD v1 a v2	ano	
Hardware podpora IPv4 a IPv6 ACL	ano	
ACL definice na základě skupiny fyzických portů	ano	
ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN	ano	
BPDU guard a Root guard	ano	
HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu	ano	
ICMPv4 a ICMPv6 rate-limiting per port	ano	
Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port	ano	
Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)	ano	
802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN	ano	
Dynamické zařazování do VLAN	ano	
802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)	ano	
Port security - omezení počtu MAC adres na port, statické MAC	ano	
Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení	ano	
Ochrana control plane (CPU) před útoky typu DoS	ano	
Podpora IPv4 a IPv6 QoS	ano	
Minimálně 8 front pro IEEE 802.1p	ano	
Management		
CLI formou 1x USB-C Console Port	ano	
Konfigurace zařízení v člověku čitelné textové formě	ano	
Podpora automatických i manuálních snapshotů konfigurace systému	ano	
USB port pro diagnostiku, přenos konfigurace a firmware	ano	
Podpora managementu přes IPv4 i IPv6	ano	
SSHv2 a a SFTP	ano	
Podpora SNMPv2c a SNMPv3	ano	
RMON	ano	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano	
Lokálně vynucené RBAC na úrovni přepínače	ano	
Dualní flash image	ano	

TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů	ano	
Podpora Syslog over TLS	ano	
Podpora RADIUS včetně RADIUS CoA (RFC3576)	ano	
Podpora RADIUS IPSEC	ano	
Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem	ano	
Podpora TACACS+	ano	
Analýza síťového provozu sFlow podle RFC 3176	ano	
Port mirroring (SPAN), alespoň 4 různé obousměrné session	ano	
Podpora Zero Touch Provisioning (ZTP)	ano	
REST API pro automatizaci nastavení	ano	
Automatická konfigurace portu podle připojeného zařízení	ano	
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano	

Produkty které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,
(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt
(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží potvrzením <u>výrobce</u> tohoto zařízení:

WiFi přístupové body (AP) INTERNI + montáž na strop
24KS

Požadavek na funkcionalitu	Minimální požadavky	Splňuje ANO/NE
Základní vlastnosti		
Třída zařízení: indoor přístupový bod	ano	
Uzavřená konstrukce bez ventilátorů	ano	
Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax	ano	
Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac	ano	

Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE	ano	
Pracovní režim AP bez kontroléru (autonomní)	ano	
Pracovní režim AP řízené kontrolérem (lightweight)	ano	
Pracovní režim AP v roli kontroléru s možností správy až 120 AP	ano	
Minimální počet portů ethernet LAN: 1x 100/1000 Mbit/s RJ45	ano	
Podpora standardů IEEE 802.3af (PoE), IEEE 802.3at (PoE+)	ano	
Podpora standardního PoE IEEE 802.3af 15W bez nutnosti redukce výkonu libovolného rádia	ano	
Podpora napájení z AC napájecího zdroje	ano	
Vestavěná interní anténa MIMO, omni down-tilt	ano	
Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz	ano	
MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2	ano	
MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2	ano	
Podpora šířky kanálu 80 MHz	ano	
HW podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO	ano	
Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP	ano	
Možnost nastavení vysílacího výkonu s krokem 0.5 dBm	ano	
Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1200 Mbps	ano	
Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 570 Mbps	ano	
Integrovaný TPM pro bezpečné uložení certifikátů a klíčů	ano	
Podpora 802.11ac explicitního beamformingu	ano	
Podpora airtime fairness	ano	
Prioritizace jednotlivých SSID na základě vysílacího času	ano	
USB port s podporou 3G/4G USB modemu jako WAN uplink	ano	
Vypínatelné indikační LED diody informující o stavu zařízení	ano	
Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno)	ano	
Detekce Rogue AP	ano	
Minimální počet inzerovaných SSID (BSSID) na radio: 16	ano	
Nastavitelný DTIM interval pro jednotlivé SSID	ano	
Mapování SSID do různých VLAN podle IEEE 802.1Q	ano	
VLAN Pooling	ano	
HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu	ano	
Podpora Layer-2 izolace bezdrátových klientů	ano	
HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz	ano	
Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)	ano	
Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček	ano	
DHCP server, směrování a NAT pro bezdrátové klienty	ano	
AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN	ano	
Automatická identifikace připojeného zařízení a jeho operačního systému	ano	
Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming	ano	
Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP	ano	
Optimalizace provozu: multicast-to-unicast konverze	ano	
Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)	ano	
Filtrování přístupu na web	ano	

Podpora RadSec (RADIUS over TLS)	ano	
802.11w ochrana management rámců	ano	
Podpora Kensington lock	ano	
Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP	ano	
Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN	ano	
Volitelně možnost spravovat AP cloud management nástrojem	ano	
CLI formou serial konsole port a serial over bluetooth	ano	
SSHv2, SNMPv2c a SNMPv3	ano	
AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem	ano	
Integrované Bluetooth 5.0 Low Energy (BLE) rádio	ano	
Integrované Zigbee 802.15.4 rádio	ano	
Podpora režimu SLEEP s max. spotřebou energie do 4W	ano	
Součástí AP je příslušenství pro montáž na zeď nebo strop	ano	

Produkty které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,
(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt
(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží potvrzením <u>výrobce</u> tohoto zařízení:

WiFi přístupové body (AP) EXTERNI + montážní kit
1KS

Požadavek na funkcionalitu	Minimální požadavek	Splňuje ANO/NE
Základní vlastnosti		
Outdoor přístupový bod	ano	
Stupeň krytí IP67, rozsah provozních teplot -40° až +65°C	ano	
Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax	ano	

Certifikace Wi-Fi Aliance: Wi-Fi CERTIFIED 6™ a WPA3™-Enterprise	ano	
Pracovní režim AP bez kontroléru (autonomní)	ano	
Pracovní režim AP řízené kontrolérem (lightweight)	ano	
Pracovní režim AP v roli kontroléru s možností správy až 120 AP	ano	
Minimální počet portů ethernet LAN: 2x 100/1000 Mbit/s RJ45	ano	
Podpora muligigabit ethernet 2.5 Gbps IEEE 802.3bz	ano	
Podpora standardů IEEE 802.3at (PoE+) a IEEE 802.3bt	ano	
Podpora standardního PoE IEEE 802.3at 30W bez nutnosti redukce výkonu libovolného rádia	ano	
Podpora linkové agregace LACP	ano	
Podpora PoE na obou ethernet portech	ano	
Antény: interní, MIMO, omni všesměrová	ano	
Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz	ano	
Minimální MIMO a počet spatial stream: 4x4:4 pro 5GHz	ano	
Podpora TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax	ano	
HW podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO	ano	
Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP	ano	
Možnost nastavení vysílacího výkonu s krokem 0.5 dBm	ano	
Max data rate: 4800 Mbit/s pro 5GHz a 574 Mbit/s pro 2,4GHz	ano	
Minimálně 16 inzerovaných BSSID na rádio	ano	
Nastavitelný DTIM interval pro jednotlivé SSID	ano	
Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP	ano	
Integrovaný TPM pro bezpečné uložení certifikátů	ano	
Podpora WPA3-CNSA, WPA3-SAE, OWE	ano	
Podpora 802.11ac explicitního beamformingu	ano	
Podpora airtime fairness	ano	
Prioritizace jednotlivých SSID na základě vysílacího času	ano	
Vypínatelné indikační LED diody informující o stavu zařízení	ano	
Prioritizace 5GHz pásma – Band Steering či obdobné	ano	
Automatická detekce Rogue AP	ano	
Mapování SSID do různých VLAN podle IEEE 802.1Q	ano	
VLAN Pooling	ano	
Podpora WiFi MESH s protokolem pro optimální výběr cesty v rámci MESH stromu	ano	
Podpora Layer-2 izolace bezdrátových klientů	ano	
Spektrální analýza v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu)	ano	
HW filtry pro filtraci intermodulačního rušení pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)	ano	
Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček	ano	
DHCP server, směrování a NAT pro bezdrátové klienty	ano	
AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN	ano	
Automatická identifikace připojeného zařízení a jeho operačního systému	ano	
Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming	ano	
Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP	ano	
Optimalizace provozu: multicast-to-unicast konverze	ano	
Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)	ano	

Podpora filtrování přístupu na web	ano	
Podpora RadSec (RADIUS over TLS)	ano	
802.11w ochrana management rámců	ano	
Podpora MAC a 802.1X autentizace Wi-Fi klientů s využitím lokální databáze v AP	ano	
AP se ověřuje před připojením do LAN pomocí 802.1X - podpora PEAP a EAP-TLS suplicant	ano	
Volitelně možnost spravovat AP cloud management nástrojem	ano	
CLI formou USB-C serial konsole port	ano	
SSHv2, SNMPv2c a SNMPv3	ano	
ZTP pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem	ano	
Integrované Bluetooth 5.0 Low Energy (BLE) rádio	ano	
Integrované Zigbee 802.15.4 rádio	ano	
Podpora režimu SLEEP s max. spotřebou energie do 4W	ano	
Součástí AP je příslušenství pro montáž na sloup a/nebo na stěnu	ano	

Produkty které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky

(a) jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,

(b) mají plnou záruku od výrobce,
(c) mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
(d) obsahují všechny nezbytné licence na používání příslušného softwaru,
(e) jsou v databázi výrobce uvedeny jako prodaná kupujícímu a určeny pro tento konkrétní projekt
(f) jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží potvrzením <u>výrobce</u> tohoto zařízení:

Kabelové rozvody včetně příslušenství pro LAN školy 65KS přípojných míst cat 6 - UTP LSOH	Popis	**Metalická část LAN:** Kabelové rozvody včetně příslušenství a souvisejících služeb pro připojení **65KS** přípojných míst školy – ukončení kabeláže do zásuvky RJ45 na jedné straně a ukončení kabeláže do patch panelu (patch panel je součástí dodávky) na druhé straně -délku trasy (povrchová montáž do lišty) a kabeláže cenit na 95m/AP **Optická část FO:** -FO páteř 10GB SM min 8vl – -délka kabelu a trasy 500m - propoj mezi 2xDR (centrální x podružné) - opt.vany/optické kazety/pigtaily/patch cordy LC/LC)

		- ukončení zavřením – 2vlákna
	Záruka	Kabelové rozvody min 5let

Kabelové rozvody včetně příslušenství pro AP 24 přípojných míst cat 6 - UTP LSOH	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb pro připojení 24KS WIFI AP -ukončení kabeláže WIFI do patch panelu (patch panel je součástí dodávky) -ukončení konektorem RJ45 – strana WIFI -délku trasy (povrchová montáž do lišty) a kabeláže cenit na 95m/AP - montáž AP – 24KS (strop)
	Záruka	Kabelové rozvody min 5let

Podružný datový rozvaděče		
Specifikace	Nástěnný datový rozvaděč min 12U (š)600x(h)495	**1 ks**
Provedení	kovové robustní provedení	
Záruka	min. 24 měsíců	

Kabelové rozvody včetně příslušenství pro učebnu IT s 26PC 26 přípojných míst Min. cat 5e - UTP LSOH	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb pro připojení **26** přípojných míst -ukončení kabeláže do patch panelu (patch panel je součástí dodávky) -ukončení v zásuvce/liste (součástí dodávky) -délku trasy (povrchová montáž do lišty) a kabeláže cenit na 95m/PM - FO propoj SM do centrálního podružného DR – kalkulace na 500m SM - Podružný DR včetně vybavení, min 9U
	Záruka	Kabelové rozvody min 5let

Kabelové rozvody včetně příslušenství pro učebnu robotika s min 10 přípojných míst Min. cat 5e - UTP LSOH	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb pro připojení **10** přípojných míst -ukončení kabeláže do patch panelu (patch panel je součástí dodávky) -ukončení v zásuvce/liste (součástí dodávky) -délku trasy (povrchová montáž do lišty) a kabeláže cenit na 95m/PM - FO propoj SM do centrálního podružného DR – kalkulace na 500m SM - Podružný DR včetně vybavení, min 9U
	Záruka	Kabelové rozvody min 5let

Kabelové rozvody včetně příslušenství pro učebnu jazyků s min 10 přípojných míst Min. cat 5e - UTP LSOH	Popis	Kabelové rozvody včetně příslušenství a souvisejících služeb pro připojení **10** přípojných míst -ukončení kabeláže do patch panelu (patch panel je součástí dodávky) -ukončení v zásuvce/liste (součástí dodávky) -délku trasy (povrchová montáž do lišty) a kabeláže cenit na 95m/PM - FO propoj SM do centrálního podružného DR – kalkulace na 500m SM - Podružný DR včetně vybavení, min 9U
	Záruka	Kabelové rozvody min 5let

Povinné parametry pro Komoditu K3 – Centrální logování:

Monitorovací a logovací systém 1x	Základní funkce	Systém pro sběr, ukládání a správu provozních a bezpečnostních informací a událostí ze sledovaných systémů
	Protokoly sběru logů	syslog, TCP, UDP, HTTP, AMQP, JSON
	Sběr síťových toků	netflow či kompatibilní dle nabízeného firewallu a centrálního přepínače
	Zdroje logů	Min. REST API, textové soubory, Radius, ActiveDirectory, MS SQL databáze, Windows Event Log - včetně rozšířených "Applications and ServicesLogs", síťové prvky - syslog a netflow, ostatní aktivní prvky - syslog, SNMP trap
	Parsování logů	Integrovaný nástroj pro parsování logů. Možnost nahrání části logu, online vytváření parseru a snadné testování výsledku. Podpora vytváření opakovaně použitelných vzorků - např. definice IP adresy regulárním dotazem apod.
	Retence	Uchovávání logů min. 6 měsíců, automatická retence logů a indexů
	Geolokace	Podpora automatické doplňování logů o informaci o lokalitě podle IP adresy
	Normalizace logů	Sjednocení názvů shodných dat z různých zdrojů logů např. pro snadné vyhledávání napříč zdroji
	Rozšíření logů	Podpora rozšíření logů o vlastní statické a dynamické (kalkulované) položky integrovaným nástrojem.
	Rozšiřitelnost	Podpora snadného rozšíření funkčnosti pomocí plug-inů nebo modulů
	Bezpečnost	Podpora šifrované komunikace se zdroji (SSL apod.), ověřování zdrojů (TLS apod.)
	Výkon	Min. 500 EPS (event per second), 5000 FPM (flows per minute)
	Dashboardy	Uživatelské vytváření dashboardů (pracovních desek) včetně možnosti využití grafických prvků (grafy, mapy, histogramy apod.) i strukturovaných dat (tabulek)
	Export dat	Export dat do csv a/nebo xls - min. výsledky hledání
	Kanály	Možnost vytváření kanálů - datových sad či toků - na základě pravidel (logických podmínek) a to i napříč různými zdroji. Podpora dalšího zpracování - tvorba alarmů, zobrazení na dashboardu, online odesílání do nadřazeného systému apod.
	Alerty, notifikace	Podpora vytváření alertů - překročení okamžitých či kumulovaných hodnot, zasílání upozornění
	ActiveDirectory	integrace s ActiveDirectory pro ověřování uživatelů, nastavení oprávnění min. administrátor a operátor
	Vyhledávání	Rychlé a intuitivní vyhledávání v záznamech napříč všemi zdroji i při velkých objemech dat (řády TB). Jednoduchý dotazovací jazyk. Rychlá vyhledávání či filtrování bez tvorby dotazů - např. výběrem v kontextovém menu vybraného pole uloženého záznamu.
	Kompatibilita	Podpora provozu v prostředí nabízené serverové virtualizace
	Ukládání dat	do databáze, případná databázová licence musí být součástí dodávky
	Výstupy	Možnost výstupů do nadřazeného systému pro účely vzdáleného expertního dohledu. Zabezpečený přenos vhodným protokolem
	Záruka	min. 24 měsíců včetně poskytnutí opravných verzí

Příloha č.1

1. Konektivita školy k veřejnému internetu (WAN)

1.1. 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 parametry v době ukončení realizace a v průběhu udržitelnosti projektu.

1.2. Povinné parametry projektu:

1.2.1. Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student[2] nebo 0,5 Mbps/koncové uživatelské zařízení[3][4] a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů[5]. Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.

1.2.2. Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.

1.2.3. Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.

1.2.4. Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.

1.2.5. Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.

1.2.6. Zajištění šifrovaného přístupu (SSL/TLS) a podepsání DNSSEC domén pro služby školy dostupné online (např. emailové služby, webové servery, studijní a ekonomické agendy atp.).

1.2.7. Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem;

1.2.8. Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.

1.2.9. Poskytovatel konektivity je schopen zajistit kontaktní bod pro komunikaci, trvalý monitoring dostupnosti konektivity, realizovat blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy na straně poskytovatele na základě požadavku školy.

1.3. Doporučené parametry projektu:

Nad rámec těchto povinných parametrů je dále doporučeno v projektu realizovat:

1.3.1. Symetrické připojení (zajištění konektivity) bez agregace a omezení, doporučujeme postupně směřovat ke kapacitě konektivity 1Gbps.

1.3.2. Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.

1.3.3. Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (anti-spoofing), funkci pro blokování nežádoucí komunikace zahlcující nebo jinak omezující konektivitu a systémy školy pro zamezení zahlcení linky (např. RTBH, FlowSpec, služby AntiDDoS řešení), detekci a zamezení amplifikačních útoků, zabezpečení směrování síťového provozu pomocí RPKI a konfigurace odmítnutí nevalidních prefixů.

1.3.4. Antivirová kontrola internetového provozu.

2. Vnitřní konektivita školy (LAN a WLAN)

[2] *Počet žáků/studentů je definovaný celkovým počtem žáků/studentů školy.*

[3] *Koncové uživatelské zařízení je počítačový systém, který je aktivně využíván uživatelem (např. žákem, studentem nebo zaměstnancem školy) ke vzdělávacím či pracovním účelům (typicky počítač, notebook, tablet apod.).*

[4] *Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení*

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

2.1. Obecný popis

Vnitřní síťové prostředí školy pořizované v rámci projektu může být řešeno pevnou sítí, bezdrátovou sítí, nebo kombinací těchto síťových technologií. Připojení je nutné zajistit v prostorách dotčených hlavním projektem, rovněž je možné pokrýt ostatní prostory školy, včetně chodeb, jídelen, internátu a dalších školských zařízení. Potřebnost a účelnost takového pokrytí musí být odůvodněna ve studii proveditelnosti.

2.2. Povinné parametry projektu (bez ohledu typ síťového připojení):

2.2.1. Systém správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).

2.2.2. Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém[6].

2.2.3. Systémy zálohování a obnovy dat serverové infrastruktury.

2.2.4. Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.

2.3. Povinné parametry projektu v oblasti pevné LAN:

2.3.1. Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex.

2.3.2. Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex.

2.3.3. Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3)[7] s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost

tvorby virtuálních sítí - VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].

2.3.4. Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).

2.3.5. Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.

2.4. Minimální parametry projektu v případě řešení bezdrátových sítí (WLAN):

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

2.4.2. Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.

2.4.3. Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).

2.4.4. Podpora mechanismu izolace uživatelů.

2.4.5. Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.

---

[6] *Počítačový systém je každý prvek informačních a komunikačních technologií využívající pro svoji činnost jak hardware, tak software. Pro účely standardů jsou rozlišována: 1. koncová uživatelská zařízení (např. osobní počítače, notebooky, tablety, mobily aj.) a 2. servery, síťové prvky, datová úložiště apod.*

[7] *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.*

2.5. Doporučené parametry projektu (bez ohledu typ síťového připojení):

Nad rámec těchto povinných parametrů je dále doporučeno v projektu realizovat:

2.5.1. Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.

2.5.2. Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.

2.5.3. Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému www.eduroam.cz).

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

2.5.5. Doporučená podpora pro ověřování uživatelů oproti databázi účtů [např. pomocí protokolu IEEE 802.1X vůči centrální evidenci uživatelů (např. LDAP, MS AD) nebo pomocí Captive portalu].

2.5.6. Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.

3. Další doporučené bezpečnostní prvky projektu

Nad rámec povinných parametrů uvedených v bodech 1 a 2 je dále doporučeno v projektu realizovat:

3.1.1. Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).

3.1.2. Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.

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

3.1.4. Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.

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

3.1.6. Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).

3.1.7. Nástroje pro centrální správu a audit ICT prostředků.

3.1.8. Podpora vzdáleného přístupu (VPN).

3.1.9. Zavedení více-faktorové autentizace.