**TECHNICKÁ SPECIFIKACE - část - Konektivita**

Základní škola Komenského Slavkov u Brna, příspěvková organizace

# 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  |

1. 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.
2. 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.
3. 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.
4. Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:
	1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
	2. mají plnou záruku od výrobce,
	3. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
	4. 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.

1. 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

1. 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 provozování **min 4** virtuálních serverů.
2. 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

1. 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

1. Bude implementováno řízení přístupů k mediu (síti) na základě rolí a členství v uživatelské skupině adresářové služby.
2. 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).
3. Architektura WiFi bude založena na řešení s centrální správou prováděnou virtuálním kontrolerem (řadičem), který bude součástí firmwarů přístupových bodů.
4. 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 logovacích informací - bude se jednat se o jediné zařízení, HW apliance . Řešení umožní správu z jedné grafické konzole, přístupné nativně skrze https. 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).

### 1.2. Implementační služby

1. V rámci implementace předmětu plnění dodavatel realizuje pro všechny nabízené komodity K1 až K3
	1. 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.
	2. Zajištění projektového vedení realizace předmětu plnění.
	3. 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:
		1. ActiveDirectory – správa uživatelů a skupin
		2. Hypervizor – ovládání virtuálních serverů, změna jejich konfigurace
		3. Monitorovací a logovacího systém - vyhledávání činnosti uživatelů a systémů, běžná správa a kontrola funkce
		4. LAN a Wifi - připojení zařízení uživatelských postupů pro Wifi.
		5. Firewall – blokování stránek, dohledání činnosti uživatele, práce s kategoriemi stránek, zablokování přístupu pro uživatele skupinu (d) Provedení akceptačních testů.

 (e) Předání do plného provozu.

1. 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  |
| 1. Návrh a kompletní implementace serverové virtualizační platformy
2. Implementace pořízených technologií
3. Návrh vhodné struktury ActiveDirectory, její vybudování
4. Implementace automatické odstávky a najetí serveru v případě výpadku a obnovení dodávky elektrické energie
5. Návrh a provedení akceptačních testů
 |
| K2: Zabezpečení LAN a Wifi  |
| 1. Implementace pořízených technologií
2. Provedení segmentace LAN – VLAN, adresování, routování
3. Zavedení IPv6 pro přístup k internetovým zdrojům publikovaným na IPv6 adresách
4. 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 1. Návrh a implementace firewallu včetně vhodné konfigurace (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií) pro školu
2. Vybudování VPN pro vzdálený přístup uživatelů LAN
3. Respektování min. 3 různých skupinu uživatelů (učitelé, studenti, hosté) v návrzích a implementaci bezpečnostních a ostatních politik
4. 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  |

1. 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/.](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:
	1. běžných administrátorských činností pro implementované systémy
	2. 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. Harmonogram projektu

1. Zadavatel vyžaduje dodržení následujícího maximálního harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum podpisu smlouvy o dílo a protokolární předání místa plnění. Čísla značí počet kalendářních dnů.

|  |  |  |
| --- | --- | --- |
| Aktivita  | Začátek  | Termín  |
| Zahájení projektu – protokolární předání místa plnění  | D  | D  |
| Realizace předmětu plnění  | D  | D+170  |
| Školení administrátorů  | D+170  | D+175  |
| Akceptační testy  | D+175  | D+180  |
| Zahájení ostrého provozu  | D+180  | -  |

1. Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.
2. Dodavatel uvede závazný harmonogram plnění ve své nabídce a zároveň v návrhu smlouvy.

### 1.5. 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 značkové specifikace nabízených dodávek. Z popis způsobu naplnění bude možno určit, že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru.

**Povinné parametry pro Komoditu K1 - Virtualizační platforma:**

|  |  |
| --- | --- |
| **Parametr**  |  |
| **Formát serveru**  | Rackové provedení, max.. 1U. Pro přístup ke všem komponentám serveru není nutné nářadí. Barevně značené hot-plug vnitřní i vnější komponenty  |
| **CPU**  | Server musí být možno osadit min. dvěma CPU. Osazen bude min. 1x CPU, minimálně s osmi procesorovými jádry. Hodnocení výkonu nabídnutého serveru musí být publikované na webu: [https://www.cpubenchmark.net](https://www.cpubenchmark.net/) s minimálními parametry:  • Passmark CPU Mark, hodnota min: 15 000  |
| **RAM**  | 128GB v provedení min. DDR4, min. 3200 MHz rozšiřitelnou minimálně na 256GB, bez nutnosti výměny nyní nabídnutých DIMM modulů a/nebo doplnění druhého CPU a za použití identických modulů v případě rozšiřování.  |
| **Diskový subsystém**  | Server musí disponovat alespoň 8x diskovou hotswap šachtou pro disky 2,5”, přístupnou zpředu. Požadujeme osazení min. 4x SSD s kapacitou každého HDD alespoň 3.8TB a minimálně SATA 6Gbps rozhraním, a min. dvěma SSD s kapacitou alespoň 480GB s minimálně SATA 6Gbps rozhraním, min. 1DWPD  |
| **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, min. 700W *(alespoň Platinum třída podle specifikace 80 Plus)*   |
| **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**  | Záruka na 5 let 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** **NELZE použít v nabídce druhotných licencí**  | 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 36**0** zařízeních.  |
| **UPS** **1x**  | Provedení  | Provedení do racku, max. 2U, včetně montážního materiálu nebo TOWER s možností umístění ve vertikální i horizontální poloze  |
| Elektrické provedení  | Jmenovité́ 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  | RACK + ližiny  |
| Výkon  | 1xCPU min 4000bodu v CPU MARK na https://www.cpubenchmark.net  |
| Rozšiřitelnost  | 2x USB 3.2 Gen 1 1x eSATA  |
| Kapacita  | Osazeno 4x HDD 12TB 256MB, SATA 6 Gb/s, 7200ot/min, určených výrobcem pro NAS (nepřipouští se HDD určené jiným účelům (desktop, kamerové systémy apod.).  |
| Konektivita  | 4x RJ-45 1GbE LAN Port , 1x 10G NIC SFP+  |
| RAM  | min. 8G MB DDR4 SODIMM  |
| Záruka  | min. 36 měsíců NAS min 60měsíců HDD  |

**Povinné parametry pro Komoditu K2 – Zabezpečení LAN a Wifi:**

**NGF**

|  |  |  |
| --- | --- | --- |
| **Požadavky na funkcionalitu**  | **Minimální požadavky**  | **Splňuje** **ANO/NE**  |
| **Základní specifikace**  |   |    |
| Typ zařízení  | Next-generation firewall  | ANO   |
| Formát zařízení  | HW do racku 1U  | ANO     |
| Počet fyzických portů  | 2x 10 GE SFP+, 18x GE RJ45, 4x Shared Port Pairs, 8x GE SFP  | ANO     |
| Interní úložiště  | 400 GB  | ANO     |
| **Výkonová specifikace**  |    |    |
| Propustnost FW – stavový filtr (64B UDP)  | 10 Gbps  | ANO   |
| Propustnost IPSec VPN (512B rámec)  | 11,5 Gbps  | ANO     |
| Propustnost SSL VPN  | 1 Gbps  | ANO     |
| Latence firewallu (64B UDP)  | < 6 mikro sec.  | ANO     |
| Propustnost IPS (Enterprise Traffic Mix)  |  2.6 Gbps  | ANO     |
| Propustnost Threat Protection = aktivní min. IPS, Aplikační kontrola a Anti-Malware (Enterprise Traffic Mix)  | 1 Gbps  | ANO     |
| **Funkční specifikace**  |    |    |
| Integrovaný duální napájecí zdroj (Dual AC PS)  | PODPORUJE  | ANO   |
| HA zapojení, L2, Active-Active nebo Active-Passive  | PODPORUJE  | ANO     |
| Režim nasazení – L2 transparentní, nebo L3 NAT/Router  | PODPORUJE  | ANO     |
| Linková agregace 802.3ad  | PODPORUJE  | ANO     |
| Možnost vytvořit IPv4 a IPv6 vlan interface  | PODPORUJE  | ANO   |
| Podpora IPv4, IPv6  | PODPORUJE  | ANO     |
| NAT, PAT  | PODPORUJE  | ANO     |
| IPSec VPN v režimu GW to GW a GW to Client  | PODPORUJE  | ANO     |
| Podpora SSL VPN, tunelový a portálový režim  | PODPORUJE  | ANO     |
| Podpora NTP, SNMPv3, Syslog  | PODPORUJE  | ANO     |
| Logování v lokáním režimu a na centrální logovací systém  | PODPORUJE  | ANO   |
| Dynamické směrování pro IPv4 and IPv6 (RIP, OSPF, BGP a Multicast IPv4)  | PODPORUJE  | ANO     |
| Policy based routing a source based routing  | PODPORUJE  | ANO     |
| WAN optimalizace, linkový balancer  | PODPORUJE  | ANO     |
| Traffic shaping  | PODPORUJE  | ANO   |
| Explicitní Proxy, Reverzní proxy  | PODPORUJE  | ANO     |
| Více správcovských účtů s různým oprávněním  | PODPORUJE  | ANO     |
| Virtuální kontexty s oddělenou konfigurací a správou  | 10  | ANO     |
| Správa přes min. HTTPS, SSH  | PODPORUJE  | ANO   |
| Dedikovaný port pro management  | PODPORUJE  | ANO     |
| Integrovaná podpora pro dvoufaktorovou autentikaci  | PODPORUJE  | ANO     |
| Integrace s Active Directory pro SSO  | PODPORUJE  | ANO     |
| Licencování na neomezený počet uživatelů  | PODPORUJE  | ANO     |
| Intrusion Protection Systém (IPS)  | PODPORUJE  | ANO     |
| Aplikační kontrola na L7 (>3000 signatur síťových aplikací)  | PODPORUJE  | ANO   |
| Antivir (Proxy nebo Flow), Antispyware a Antimalware  | PODPORUJE  | ANO     |
| Antispam  | PODPORUJE  | ANO     |
| Web filtering, kategorizace obsahu  | PODPORUJE  | ANO     |
| Reputační databáze obsahujícící známe IP adresy a domény C&C Botnet sítí  | PODPORUJE  | ANO   |
| Pravidelné automatické aktualizace signatur od výrobce  | PODPORUJE  | ANO     |
| Databáze zranitelností pro mobilní zařízení (Mobile Malware)  | PODPORUJE  | ANO     |
| Inspekce neznámých kódů v Cloudu výrobce (SandBox)  | PODPORUJE  | ANO     |
| Funkcionalita integrovaného WiFi kontroléru  |    | ANO   |
| Počet řízených FortiSwitch switchů  | 24  | ANO     |
| Počet řízených AP v tunelovém režimu  | 64  | ANO     |
| Počet řízených AP (maximálně, bez tunelového režimu)  | 128  | ANO     |
| Plně oddělené sítě (např. pro zaměstnance a pro hosty)  | PODPORUJE  | ANO     |
| Guest (Captive) portál  | PODPORUJE  | ANO     |
| Napojení na RADIUS a LDAP  | PODPORUJE  | ANO   |
| Detekce Rogue AP a jejich potlačení  | PODPORUJE  | ANO     |
| Roaming  | PODPORUJE  | ANO     |
| Možnost vytvoření Mesh sítě  | PODPORUJE  | ANO     |
| Wireless IPS (Null SSID Probe Response, Spoofed De-authentication, Weak WEP IV Detection, Authentication Frame Flooding).  | PODPORUJE  | ANO     |
| Záruka 60měsíců  | ANO  | ANO   |
| Bezplatný nárok na nejnovější firmware  | ANO  | ANO     |
| Pravidelná aktualizace signatur popř. přístup na on-line služby výrobce  | ANO  | ANO     |
| Technický support výrobce v režimu 24x7  | ANO  | ANO     |

**1x Centrální OPTICKÝ přepínač 24x10G SFP+ - záruka 60měsíců**

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu**  | **Minimální požadavky**  | **Splňuje** **ANO/NE**  |
| **Základní vlastnosti**  |   |   |
| Třída zařízení: L3 switch  | ano  | ANO     |
| Formát zařízení do racku  | ano  | ANO   |
| Velikost zařízení: 1U  | ano  | ANO     |
| Počet 1/10 GE portů s volitelným fyzickým rozhraním:  | 24 | ANO     |
| Počet optických 10/25/50GE portů s volitelným fyzickým rozhraním:  | 4  | ANO     |
| 2x Interní AC hot-swap napájecí zdroje  | ano  | ANO     |
| Redundatní vyměnitelné ventilátory – hot swap  | ano  | ANO   |
| Celková přepínací propustnost přepínače  | 880 Gbit/s  | ANO     |
| Celkový paketový výkon přepínače  | 600 Mpps  | ANO     |
| Minimální paketový buffer: 8MB  | ano  | ANO     |
| Maximální hloubka přepínače: 39 cm  | ano  |  ANO   |
| **Vlastnosti stohování**  |  |   |
| Podporovaný počet přepínačů ve stohu: 10  | ano  | ANO     |
| Kapacita stohovacího propojení: 200 Gbps  | ano  | ANO     |
| Stoh podporuje distribuované přepínaní paketů  | ano  | ANO     |
| Redundance řídícího prvku v rámci stohu  | ano  |  ANO   |

|  |  |  |
| --- | --- | --- |
| Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)  | ano  | ANO     |
| Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)  | ano  | ANO     |
| Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF  | ano  | ANO     |
| Součástí každého přepínače je stohovací 50GE kabel s minimání délkou 1m  | ano  |  ANO   |
| **Základní funkce a protokoly**  |   |   |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte  | ano  | ANO     |
| Podpora linkové agregace IEEE 802.1AX  | ano  | ANO     |
| Konfigurovatelné rozkládání LACP zátěže podle L2,L3  | ano  | ANO     |
| Počet LACP skupin/linek ve skupině: 256/8  | ano  |  ANO   |
| Minimální počet záznamů v tabulce MAC adres: 32 000  | ano  | ANO     |
| Minimální počet záznamů v tabulce ARP: 45 000  | ano  | ANO     |
| Protokol pro definici šířených VLAN: MVRP  | ano  | ANO     |
| Podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN  | ano  |  ANO   |
| VLAN translace - swap 802.1Q tagů na trunk portu  | ano  | ANO     |
| Podpora zařazování do VLAN podle standardu 802.1v  | ano  | ANO     |
| IEEE 802.1s - Multiple Spanning Tree  | ano  | ANO     |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)  | ano  |  ANO   |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED  | ano  | ANO     |
| Detekce jednosměrnosti optické linky (např. UDLD)  | ano  | ANO     |
| DHCP server  | ano  | ANO     |
| DHCP relay pro IPv4 a IPv6  | ano  |  ANO   |
| Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace  | ano  | ANO     |
| Statické směrování IPv4 a IPv6  | ano  | ANO     |
| Minimální počet záznamů ve směrovací tabulce: 64 000  | ano  | ANO     |
| Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD  | ano  |  ANO   |
| Podpora BGP a MP-BGP včetně podpory BFD  | ano  | ANO     |
| Podpora směrovacího protokolu RIP a RIPng  | ano  | ANO     |
| Podpora Layer-3 routed port  | ano  | ANO     |
| IGMP v2 a v3  | ano  |  ANO   |
| MLD v1 a v2  | ano  | ANO     |
| Podpora protokolu ERPS  | ano  | ANO     |
| Hardware podpora IPv4 a IPv6 ACL  | ano  | ANO     |
| ACL definice na základě skupiny fyzických portů  | ano  |  ANO   |
| ACL aplikovatelný na interface, LAG, VLAN  | ano  | ANO     |
| BPDU a Root guard  | ano  | ANO     |
| DHCP snooping pro IPv4 a IPv6  | ano  | ANO     |
| HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps  | ano  |  ANO   |
| 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port  | ano  | ANO     |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)  | ano  | ANO     |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675  | ano  | ANO     |
| Podpora Critical VLAN  | ano  |  ANO   |
| Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.  | ano  |  ANO   |

|  |  |  |
| --- | --- | --- |
| Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace  | ano  |  ANO   |
| Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace  | ano  |  ANO   |
| Podpora IPv6 RA Guard  | ano  |  ANO   |
| IP source guard / dynamic IP lockdown  | ano  | ANO     |
| Podpora Dynamic ARP protection  | ano  | ANO     |
| Port security  | ano  | ANO     |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU  | ano  |  ANO   |
| Podpora IPv4 a IPv6 QoS  | ano  | ANO     |
| IEEE 802.1p - minimální počet front: 8  | ano  | ANO     |
| **SDN funkce**  |  |    |
| Podpora service insertion včetně technologie VXLAN  | ano  |  ANO   |
| Podpora BGP EVPN s využítím VXLAN  | ano  | ANO     |
| Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izololovat více koncových zařízení na jednom portu do unikátních tunelů  | ano  | ANO     |
| Přiřazení koncového zařízení do tunelu na základě výsledku autorizace  | ano  |  ANO   |
| **Analytické a automatizační nástroje**  |  |   |
| Podpora REST API pro automatizaci nastavení sítě.  | ano  | ANO     |
| Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači  | ano  | ANO     |
| Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)  | ano  | ANO     |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události  | ano  |  ANO   |
| Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů. Možnost vynášení stavu monitorovaných metrik do grafů atp.  | ano  | ANO     |
| Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.  | ano  | ANO     |
| Interní uložistě dat pro sběr provozních dat a pokročilou dignostiku zařízení  | ano  | ANO     |
| Kapacita interního úložiště dat pro analytické účely minimálně 30 GB  | ano  |  ANO   |
| **Management**  |  |    |
| USB-C konzolový port  | ano  | ANO     |
| 1xRJ45 OoB management port s podporou ethernetu  | ano  |  ANO   |
| Podpora minimálně 64 virtuálních směrovacích instancí (VRF)  | ano  |  ANO   |
| Konfigurace zařízení v člověku čitelné textové formě  | ano  | ANO     |
| Podpora automatických i manuálních snapshotů konfigurace systému  | ano | ANO     |
| USB port pro diagnostiku, přenos konfigurace a firmware  | ano  | ANO     |
| Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth  | ano  |  ANO   |
| Podpora managementu přes IPv4 i IPv6  | ano  | ANO     |
| SSHv2 a HTTPS pro IPv4 a IPv6  | ano  | ANO     |
| Podpora SNMPv2c a SNMPv3  | ano  | ANO     |
| RMON  | ano  |  ANO   |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL  | ano  | ANO     |
| Lokálně vynucené RBAC na úrovni přepínače  | ano  | ANO     |
| Dualní flash image  | ano  |  ANO   |
| Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů  | ano  |  ANO   |
| Podpora RADIUS včetně RADIUS CoA (RFC3576)  | ano  | ANO     |
| Podpora Secure RADIUS (RadSec)  |   | ANO     |
| Podpora standardního Linux Shellu (BASH) pro debugging a skriptování  | ano  | ANO     |
| Podpora TACACS+  | ano  |  ANO   |
| Analýza síťového provozu sFlow podle RFC 3176  | ano  | 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  | ANO     |
| Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN  | ano  | ANO     |
| Podpora IP SLA pro měření zpoždění provozu VoIP  | ano  |  ANO   |
| Podpora Zero Touch Provisioning (ZTP)  | ano  | ANO     |

**Ostatní podmínky:**

* + Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
	+ Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
	+ Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

**1x Centrální přepínač 24x1000Mbps - záruka 60měsíců + 38x 10G SFP+ LC SM Transceiver - záruka 36měsíců**

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu**  | **Minimální požadavky**  | **Splňuje** **ANO/NE**  |
| **Základní vlastnosti**  |   |   |
| Třída zařízení: přepínač  | ano  | ANO     |
| Formát zařízení do racku  | ano  | ANO     |
| Velikost zařízení: 1U  | ano  |  ANO   |
| Počet 1Gbit/s metalických portů  | 24x 10/100/1000Mbps RJ45  | ANO     |
| Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+)  | 4x  | ANO     |
| Interní AC zdroj  | ano  | ANO     |
| Maximální spotřeba přepínače při plném zatížení  | 66W  |  ANO   |
| Celková přepínací propustnost přepínače  | 128Gbit/s  | ANO     |
| Celkový paketový výkon přepínače  | 120Mpps  | ANO     |
| Minimální paketový buffer: 8MB  | ano  |  ANO   |
| Maximální hloubka přepínače: 33 cm  | ano  | ANO     |
| **Vlastnosti stohování**  |  | ANO     |
| Podporovaný počet přepínačů ve stohu: 8  | ano  | ANO     |
| Kapacita stohovacího propojení: 80 Gbps  | ano  |  ANO   |
| Stoh podporuje distribuované přepínaní paketů  | ano  | ANO     |
| Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 100m)  | ano  | ANO     |
| Redundance řídícího prvku v rámci stohu  | ano  |  ANO   |
| Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port)  | ano  | ANO     |
| Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)  | ano  | ANO     |
| Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)  | ano  | ANO     |
| Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF  | ano  |  ANO   |
| Součástí každého přepínače je stohovací kabel minimálně 10GE s minimální délkou 1m  | ano  | ANO     |
| **Základní funkce a protokoly**  |   | ANO     |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte  | ano  |  ANO   |
| Podpora linkové agregace IEEE 802.1AX  | ano  | ANO     |

|  |  |  |
| --- | --- | --- |
| Konfigurovatelné rozkládání LACP zátěže podle L2, L3  | ano  |  ANO   |
| Počet LACP skupin/linek ve skupině: 32/8  | ano  | ANO     |
| Minimální počet záznamů v tabulce MAC adres: 16 000  | ano  | ANO     |
| Minimální počet záznamů v tabulce ARP: 8 000  | ano  |  ANO   |
| Protokol pro definici šířených VLAN: MVRP  | ano  | ANO     |
| Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN  | ano  |  ANO   |
| Podpora zařazování do VLAN podle standardu 802.1v  | ano  | ANO     |
| IEEE 802.1s - Multiple Spanning Tree  | ano  | ANO     |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)  | ano  |  ANO   |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED  | ano  | ANO     |
| Detekce jednosměrnosti optické linky (např. UDLD)  | ano  |  ANO   |
| Podpora NTPv3  | ano  | ANO     |
| Statické směrování IPv4 a IPv6  | ano  | ANO     |
| Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000  | ano  |  ANO   |
| Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000  | ano  | ANO     |
| Dynamické směrování OSPFv2, OSPFv3, RIP, RIPng  | ano  |  ANO   |
| Podpora Layer-3 routed port  | ano  | ANO     |
| IGMP v2 a v3  | ano  | ANO     |
| IGMP snooping  | ano  |  ANO   |
| MLD v1 a v2  | ano  | ANO     |
| MLD snooping  | ano  |  ANO   |
| Hardware podpora IPv4 a IPv6 ACL  | ano  | ANO     |
| ACL definice na základě skupiny fyzických portů  | ano  | ANO     |
| ACL aplikovatelný na interface, LAG, VLAN  | ano  |  ANO   |
| BPDU a Root guard  | ano  | ANO     |
| DHCP snooping pro IPv4 a IPv6  | ano  |  ANO   |
| IPv6 RA Guard  | ano  | ANO     |
| HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps  | ano  | ANO     |
| 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port  | ano  |  ANO   |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)  | ano  | ANO     |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675  | ano  |  ANO   |
| Podpora Critical VLAN  | ano  | ANO     |
| Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.  | ano  | ANO     |
| Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace  | ano  |  ANO   |
| Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace  | ano  | ANO     |
| Podpora Dynamic ARP protection  | ano  |  ANO   |
| Port security  | ano  | ANO     |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU  | ano  | ANO     |
| Podpora IPv4 a IPv6 QoS  | ano  |  ANO   |
| IEEE 802.1p - minimální počet front: 8  | ano  | ANO     |
| **SDN funkce**  |  |  ANO   |
| Podpora technologie VXLAN  | ano  | ANO     |
| Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů  | ano  | ANO     |
| Přiřazení koncového zařízení do tunelu na základě výsledku autorizace  | ano  |  ANO   |
| **Analytické a automatizační nástroje**  |  | ANO     |
| Podpora REST API pro automatizaci nastavení sítě.  | ano  |  ANO   |
| Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači  | ano  | ANO     |
| Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)  | ano  | ANO     |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události  | ano  |  ANO   |
| Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů atp.  | ano  | ANO     |
| Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.  | ano  |  ANO   |
| Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení  | ano  | ANO     |
| Kapacita interního úložiště dat pro analytické účely minimálně 14 GB  | ano  | ANO     |
| **Management**  |  |  ANO   |
| USB-C konzolový port  | ano  | ANO     |
| 1xRJ45 OoB management port s podporou ethernetu  | ano  |  ANO   |
| Konfigurace zařízení v člověku čitelné textové formě  | ano  | ANO     |
| Podpora automatických i manuálních snapshotů konfigurace systému  | ano | ANO     |
| USB port pro diagnostiku, přenos konfigurace a firmware  | ano  |  ANO   |
| Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth  | ano  | ANO     |
| Podpora managementu přes IPv4 i IPv6  | ano  |  ANO   |
| SSHv2 a HTTPS pro IPv4 a IPv6  | ano  | ANO     |
| Podpora SNMPv2c a SNMPv3  | ano  | ANO     |
| RMON  | ano  |  ANO   |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL  | ano  | ANO     |
| Lokálně vynucené RBAC na úrovni přepínače  | ano  |  ANO   |
| Dualní flash image  | ano  | ANO     |
| Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů  | ano  | ANO     |
| Podpora RADIUS včetně RADIUS CoA (RFC3576)  | ano  |  ANO   |
| Podpora standardního Linux Shellu (BASH) pro debugging a skriptování  | ano  | ANO     |
| Podpora TACACS+  | ano  |  ANO   |
| Podpora Secure RADIUS (RadSec)  | ano  | ANO     |
| Analýza síťového provozu sFlow podle RFC 3176  | ano  | 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  |  ANO   |
| Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN  | ano  | ANO     |
| Podpora IP SLA pro měření zpoždění provozu VoIP  | ano  |  ANO   |
| Podpora Zero Touch Provisioning (ZTP)  | ano  | ANO     |
| 38x **Transceiver** 10G SFP+ LC SM Transceiver – záruka 3roky  | ano  | ANO     |

**Ostatní podmínky:**

* + Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
	+ Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
	+ Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

**19x ACCESS přepínač 48x1G PoE + 4xSFP+ - záruka 60měsíců**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Požadavek na funkcionalitu**  |  | **Minimální** |   |  | **Splňuje** |   |
| **požadavky** | **ANO/NE** |
| **Základní vlastnosti**  |   |  |   |
| Třída zařízení: L3 switch  | ano  |  |  ANO   |
| Formát zařízení do racku  | ano  |  | ANO     |
| Velikost zařízení: 1U  | ano  |  | ANO     |
| Počet 10/100/1000Mbit metalických portů  | 48×RJ45  |  |  ANO   |
| Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním  | 4×SFP+  |  | ANO     |
| 10GE interface zpětně kompatibilní s 1Gbit/s transceivery  | ano  |  |  ANO   |
| Všechny ethernet porty jsou dostupné zepředu  | ano  |  | ANO     |
| Interní napájecí zdroj  | ano  |  | ANO     |
| Podpora PoE+ dle standardu 802.3at  | ano  |  |  ANO   |
| Dostupný výkon pro PoE+ napájení  | 370W  |  | ANO     |
| Podpora Energy Efficient Ethernet (802.3az)  | ano  |  | ANO     |
| Celková propustnost přepínače  |  176 Gb/s  |  |  ANO   |
| Celkový paketový výkon přepínače  |  95 mpps  |  | ANO     |
| Minimálně 12MB paketový buffer  | ano  |  |  ANO   |
| Maximální přípustná hloubka přepínače  | max. 31cm  |   | ANO     |
| Bez ventilátoru  | ne  |  | ANO     |
| **Základní funkce a protokoly**  |   |  |   |
| Podpora "jumbo rámců" včetně velikosti 9220 Byte  | ano  |  |  ANO   |
| Podpora linkové agregace IEEE 802.3ad  | ano  |  | ANO     |
| Konfigurovatelné rozkládání LACP zátěže podle L3 a L4  | ano  |  | ANO     |
| Minimální počet LACP skupin/linek ve skupině: 8/8  | ano  |  |  ANO   |
| Protokol pro definici šířených VLAN: MVRP  | ano  |  | ANO     |
| Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN  | ano  |  |  ANO   |
| IEEE 802.1s - Multiple Spanning Tree  | ano  |  | ANO     |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)  | ano  |  | ANO     |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED  | ano  |  |  ANO   |
| Detekce jednosměrnosti optické linky (např. UDLD)  | ano  |  | ANO     |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace  | ano  |  | ANO     |
| Statické směrování IPv4 a IPv6  | ano  |  |  ANO   |
| IGMP v2 a v3  | ano  |  | ANO     |
| MLD v1 a v2  | ano  |  |  ANO   |
| Hardware podpora IPv4 a IPv6 ACL  | ano  |  | ANO     |
| ACL definice na základě skupiny fyzických portů  | ano  |  | ANO     |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN  | ano  |  |  ANO   |
| BPDU guard a Root guard  | ano  |  | ANO     |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu  | ano  |  | ANO     |
| ICMPv4 a ICMPv6 rate-limiting per port  | ano  |  |  ANO   |
| Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port  | ano  |  | ANO     |
| Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)  | ano  |  |  ANO   |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN  | ano  |  | ANO     |
| Dynamické zařazování do VLAN  | ano  |  | ANO     |
| 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)  | ano  |  |  ANO   |
| Port security - omezení počtu MAC adres na port, statické MAC  | ano  |  | ANO     |
| Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení  | ano  |  | ANO     |
| Ochrana control plane (CPU) před útoky typu DoS  | ano  |  |  ANO   |
| Podpora IPv4 a IPv6 QoS  | ano  |  | ANO     |
| Minimálně 8 front pro IEEE 802.1p  | ano  |  |  ANO   |
| **Management**  |   |  |    |
| CLI formou 1x USB-C Console Port  | ano  |  | ANO     |
| Konfigurace zařízení v člověku čitelné textové formě  | ano  |  |  ANO   |
| Podpora automatických i manuálních snapshotů konfigurace systému  | ano  |  | ANO     |
| USB port pro diagnostiku, přenos konfigurace a firmware  | ano  |  | ANO     |
| Podpora managementu přes IPv4 i IPv6  | ano  |  |  ANO   |
| SSHv2 a a SFTP  | ano  |  | ANO     |
| Podpora SNMPv2c a SNMPv3  | ano  |  |  ANO   |
| RMON  | ano  |  | ANO     |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL  | ano  |  | ANO     |
| Lokálně vynucené RBAC na úrovni přepínače  | ano  |  ANO   |
| Dualní flash image  | ano  | ANO     |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů  | ano  | ANO     |
| Podpora Syslog over TLS  | ano  |  ANO   |
| Podpora RADIUS včetně RADIUS CoA (RFC3576)  | ano  | ANO     |
| Podpora RADIUS IPSEC  | ano  |  ANO   |
| Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem  | ano  | ANO     |
| Podpora TACACS+  | ano  | ANO     |
| Analýza síťového provozu sFlow podle RFC 3176  | ano  |  ANO   |
| Port mirroring (SPAN), alespoň 4 různé obousměrné session  | ano  | ANO     |
| Podpora Zero Touch Provisioning (ZTP)  | ano  | ANO     |
| REST API pro automatizaci nastavení  | ano  |  ANO   |
| Automatická konfigurace portu podle připojeného zařízení  | ano  | ANO     |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů  | ano  |  ANO   |

**Ostatní podmínky:**

* + Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
	+ Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
	+ Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

**WiFi přístupové body (AP) INTERNI + montáž na strop - záruka 60měsíců**

**98KS**

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu**  | **Minimální požadavky**  | **Splňuje** **ANO/NE**  |
| **Základní vlastnosti**  |   |   |
| Třída zařízení: indoor přístupový bod  | ano  | ANO     |
| Uzavřená konstrukce bez ventilátorů  | ano  | ANO     |
| Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax  | ano  |  ANO   |
| Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac  | ano  | ANO     |
| Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE  | ano  |  ANO   |
| Pracovní režim AP bez kontroléru (autonomní)  | ano  | ANO     |
| Pracovní režim AP řízené kontrolérem (lightweight)  | ano  | ANO     |
| Pracovní režim AP v roli kontroléru s možností správy až 120 AP  | ano  |  ANO   |
| Minimální počet portů ethernet LAN: 1x 100/1000 Mbit/s RJ45  | ano  | ANO     |
| Podpora standardů IEEE 802.3af (PoE), IEEE 802.3at (PoE+)  | ano  | ANO     |
| Podpora standardního PoE IEEE 802.3af 15W bez nutnosti redukce výkonu libovolného rádia  | ano  |  ANO   |
| Podpora napájení z AC napájecího zdroje  | ano  | ANO     |
| Vestavěná interní anténa MIMO, omni down-tilt  | ano  |  ANO   |
| Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz  | ano  | ANO     |
| MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2  | ano  | ANO     |
| MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2  | ano  |  ANO   |
| Podpora šířky kanálu 80 MHz  | ano  | ANO     |
| HW podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO  | ano  |  ANO   |
| Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP  | ano  | ANO     |
| Možnost nastavení vysílacího výkonu s krokem 0.5 dBm  | ano  | ANO     |
| Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1200 Mbps  | ano  |  ANO   |
| Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 570 Mbps  | ano  | ANO     |
| Integrovaný TPM pro bezpečné uložení certifikátů a klíčů  | ano  | ANO     |
| Podpora 802.11ac explicitního beamformingu  | ano  |  ANO   |
| Podpora airtime fairness  | ano  | ANO     |
| Prioritizace jednotlivých SSID na základě vysílacího času  | ano  |  ANO   |
| USB port s podporou 3G/4G USB modemu jako WAN uplink  | ano  | ANO     |
| Vypínatelné indikační LED diody informující o stavu zařízení  | ano  | ANO     |
| Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno)  | ano  |  ANO   |
| Detekce Rogue AP  | ano  | ANO     |
| Minimální počet inzerovaných SSID (BSSID) na radio: 16  | ano  |  ANO   |
| Nastavitelný DTIM interval pro jednotlivé SSID  | ano  | ANO     |
| Mapování SSID do různých VLAN podle IEEE 802.1Q  | ano  | ANO     |
| VLAN Pooling  | ano  |  ANO   |
| HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu  | ano  | ANO     |
| Podpora Layer-2 izolace bezdrátových klientů  | ano  | ANO     |
| HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz  | ano  |  ANO   |
| Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)  | ano  | 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  |  ANO   |
| DHCP server, směrování a NAT pro bezdrátové klienty  | ano  | ANO     |
| AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN  | ano  | ANO     |
| Automatická identifikace připojeného zařízení a jeho operačního systému  | ano  |  ANO   |
| Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming  | ano  | ANO     |
| Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP  | ano  |  ANO   |
| Optimalizace provozu: multicast-to-unicast konverze  | ano  | ANO     |
| Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)  | ano  | ANO     |
| Filtrování přístupu na web  | ano  |  ANO   |
| Podpora RadSec (RADIUS over TLS)  | ano  | ANO     |
| 802.11w ochrana management rámců  | ano  | ANO     |
| Podpora Kensington lock  | ano  |  ANO   |
| Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP  | ano  | ANO     |
| Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN  | ano  |  ANO   |
| Volitelně možnost spravovat AP cloud management nástrojem  | ano  | ANO     |
| CLI formou serial konsole port a serial over bluetooth  | ano  | ANO     |
| SSHv2, SNMPv2c a SNMPv3  | ano  |  ANO   |
| AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem  | ano  | ANO     |
| Integrované Bluetooth 5.0 Low Energy (BLE) rádio  | ano  |  ANO   |
| Integrované Zigbee 802.15.4 rádio  | ano  | ANO     |
| Podpora režimu SLEEP s max. spotřebou energie do 4W  | ano  | ANO     |
| Součástí AP je příslušenství pro montáž na zeď nebo strop  | ano  |  ANO   |

**Ostatní podmínky:**

* + Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
	+ Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
	+ Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

**WiFi přístupové body (AP) EXTERNÍ + montáž na strop - záruka 60měsíců**

**2KS**

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu**  | **Minimální požadavek**  | **Splňuje** **ANO/NE**  |
| **Základní vlastnosti**  |   |   |
| Outdoor přístupový bod  | ano  | ANO     |
| Stupeň krytí IP67, rozsah provozních teplot -40° až +65°C  | ano  |  ANO   |
| Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax  | ano  | ANO     |
| Certifikace Wi-Fi Aliance: Wi-Fi CERTIFIED 6™ a WPA3™-Enterprise  | ano  | ANO     |
| AP podporuje přímé bridgování uživatelských data do LAN bez účasti kontroléru  | ano  |  ANO   |
| AP podporuje tunelování uživatelských data do centrálního kontroléru  | ano  | ANO     |
| Minimální počet portů ethernet LAN: 2x 100/1000 Mbit/s RJ45  | ano  |  ANO   |
| Podpora muligigabit ethernet 2.5 Gbps IEEE 802.3bz  | ano  | ANO     |
| Podpora standardů IEEE 802.3at (PoE+) a IEEE 802.3bt  | ano  | ANO     |
| Podpora standardního PoE IEEE 802.3at 30W bez nutnosti redukce výkonu libovolného rádia  | ano  |  ANO   |
| Podpora linkové agregace LACP  | ano  | ANO     |
| Podpora PoE na obou ethernet portech  | ano  |  ANO   |
| Antény: interní, MIMO, omni všesměrová  | ano  | ANO     |
| Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz  | ano  | ANO     |
| Minimální MIMO a počet spatial stream: 4x4:4 pro 5GHz  | ano  |  ANO   |
| Podpora TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax  | ano | ANO     |
| HW podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO  | ano  | ANO     |
| Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP  | ano  |  ANO   |
| Možnost nastavení vysílacího výkonu s krokem 0.5 dBm  | ano  | ANO     |
| Max data rate: 4800 Mbit/s pro 5GHz a 574 Mbit/s pro 2,4GHz  | ano  |  ANO   |
| Minimálně 16 inzerovaných BSSID na rádio  | ano  | ANO     |
| Nastavitelný DTIM interval pro jednotlivé SSID  | ano  |  ANO   |
| Integrovaný TPM pro bezpečné uložení certifikátů  | ano  | ANO     |
| Podpora WPA3-CNSA, WPA3-SAE, OWE  | ano  | ANO     |
| Podpora 802.11ac explicitního beamformingu  | ano  |  ANO   |
| Podpora airtime fairness  | ano  | ANO     |
| Prioritizace jednotlivých SSID na základě vysílacího času  | ano  |  ANO   |
| Vypínatelné indikační LED diody informující o stavu zařízení  | ano  | ANO     |
| Prioritizace 5GHz pásma – Band Steering či obdobné  | ano  | ANO     |
| Automatická detekce Rogue AP  | ano  |  ANO   |
| Mapování SSID do různých VLAN podle IEEE 802.1Q  | ano  | ANO     |
| VLAN Pooling  | ano  |  ANO   |
| Podpora WiFi MESH s protokolem pro optimální výběr cesty v rámci MESH stromu  | ano  | ANO     |
| Podpora Layer-2 izolace bezdrátových klientů  | ano  | ANO     |
| Spektrální analýza v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu)  | ano  |  ANO   |
| HW filtry pro filtraci intermodulačního rušení pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)  | ano  | 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  | ANO     |
| AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN  | ano  |  ANO   |
| Automatická identifikace připojeného zařízení a jeho operačního systému  | ano  | ANO     |
| Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming  | ano  |  ANO   |
| Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP  | ano  | ANO     |
| Optimalizace provozu: multicast-to-unicast konverze  | ano  |  ANO   |
| Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)  | ano  | ANO     |
| Podpora filtrování přístupu na web  | ano  | ANO     |
| Podpora RadSec (RADIUS over TLS)  | ano  |  ANO   |
| 802.11w ochrana management rámců  | ano  | ANO     |
| HW podpora FTM – 802.11mc  | ano  |  ANO   |
| AP se ověřuje před připojením do LAN pomocí 802.1X  | ano  | ANO     |
| Volitelně možnost spravovat AP cloud management nástrojem  | ano  | ANO     |
| CLI formou USB-C serial konsole port  | ano  |  ANO   |
| SSHv2, SNMPv2c a SNMPv3  | ano  | ANO     |
| ZTP pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem  | ano  |  ANO   |
| Integrované Bluetooth 5.0 Low Energy (BLE) rádio  | ano  | ANO     |
| Integrované Zigbee 802.15.4 rádio  | ano  | ANO     |
| Podpora režimu SLEEP s max. spotřebou energie do 4W  | ano  |  ANO   |
| Součástí AP je příslušenství pro montáž na sloup a/nebo na stěnu  | ano  | ANO     |
| Kompatibilní s kontrolerem  | ano  | ANO     |

**Ostatní podmínky:**

* + Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
	+ Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
	+ Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.

## Strukturovaná kabeláž - samostatný výkaz výměr - příloha č. 1 technické specifikace

**Povinné parametry pro Komoditu K3 – Centrální logování:**

|  |  |  |
| --- | --- | --- |
| **Číslo**  | **LOGMANGEMENT/SIEM s výkonem min. 500 událostí/s s minimálně 4TB velikostí databáze**  | **Splňuje**  |
|   | **Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat**  |  |
| 1  | Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. Doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry nabízeného systému.  | ANO     |
| 2  | Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware (viz seznam podporovaných zařízení v Příloze č. 1 zadávací dokumentace - Seznam\_podporovanych\_systemu\_Priloha\_1.xlsx).  | ANO     |
| 3  | Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.  |  ANO   |
| 4  | Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní viz bod č. 1. Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Požadujeme předložit příslušnou dokumentaci k vytváření parserů a testování jejich funkčnosti.  | ANO     |
| 5  | Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně. Předložte příslušný odkaz na dokumentaci popisující funkčnost třídění vstupních dat.  |  ANO   |
| 6  | Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta. Předložte detailní komunikační matrici s popisem všech použitých protokolů a portů pro nabízený systém a dokumentaci k nastavení sběru z databází v grafickém rozhraní systému.  | ANO     |
| 7  | Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávájí ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.  | ANO     |
| 8  | Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).  | ANO  |

|  |  |  |
| --- | --- | --- |
| 9  | Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.  | ANO     |
| 10  | Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.  | ANO     |
| 11  | Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.  |  ANO   |
| 12  | Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou - administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.  | ANO     |
| 13  | Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.  |  ANO   |
| 14  | Systém provádí konsolidaci logů na interním storage logovacího systému.  | ANO     |
| 15  | Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu. Předložte link nebo pdf popisující způsob vytváření reportů.  | ANO     |
| 16  | Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.  |  ANO   |
| 17  | Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.  | ANO     |
| 18  | Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.  |  ANO   |
| 19  | Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Mircosoft365.  | ANO     |
| 20  | V případě krátkodobého (do 10 minut) až dvounásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.  | ANO     |
| 21  | Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno,zdrojová IP, značka/tag apod.).  | ANO     |
| 22  | Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.  |  ANO   |

|  |  |  |
| --- | --- | --- |
| 23  | Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.  | ANO     |
| 24  | Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.  | ANO     |
| 25  | Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.  |  ANO   |
| 26  | Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.  | ANO     |
| 27  | Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran. Požadujeme předložit link na online dokumentaci nebo připojit pdf aktuální kompletní dokumentace k ověření jednotlivých vlastností navrhovaného systému.  |  ANO   |
| 28  | Systém nabízí kapacitní i výkonovou škálovatelnost.  | ANO     |
| 29  | Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 4TB.  | ANO     |
| 30  | Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.  |  ANO   |
| 31  | Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.  | ANO     |
| 32  | Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů. Požadujeme předložit vzorový návod na integraci s externím monitorovacím systémem.  |  ANO   |
| 33  | Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 82 / 2018 Sb. „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 Sb. „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)“.  | ANO     |
| 34  | Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní. Požadujeme předložit dokumentaci, ze které je zřejmé, jakým způsobem je realizována konfigurace v rámci jednotné konzole.  | ANO     |
| 35  | Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.  | ANO     |
| 36  | Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.  |  ANO   |
| 37  | Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.  | ANO     |
|   | **Minimální HW parametry požadovaného systému**  |  |

|  |  |  |
| --- | --- | --- |
| 38  | Jedna hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.  | ANO     |
| 39  | HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.  | ANO     |
| 40  | 1 procesor, min. 16 jader, s podporou HyperThreadingu nebo Multi-Threadingu.  |  ANO   |
| 41  | RAM Min. 64GB DDR-4.  | ANO     |
| 42  | Minimálně 4TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.  |  ANO   |
| 43  | Z výkonových důvodů požadujeme, aby v systému byly minimálně 2 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m.  | ANO     |
| 44  | Minimálně 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému a doložte příslušný odkaz na dokumentaci.  | ANO     |
| 45  | Větráky v systému musí být vyměnitelné za provozu a redundantní.  |  ANO   |
| 47  | Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.  | ANO     |
|   | **Výkonnostní a SW parametry systému**  |  ANO   |
| 48  | Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).  | ANO     |
| 49  | Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.  | ANO     |
| 50  | Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce. Popište podrobně způsob realizace downgrade.  | ANO     |
| 51  | Průměrný trvalý příjem min. 500 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.  |  ANO   |
| 52  | Špičkový příjem minimálně 2000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.  | ANO     |
| 53  | Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 4 TB a nad to musí podporovat kompresi ukládaných dat.  |  ANO   |

|  |  |  |
| --- | --- | --- |
| 54  | Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použítých komponent vizuálního programování nástroje.  | ANO     |
| 55  | Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy.  | ANO     |
| 56  | Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní. Doložte odkazem na dokumentaci, jakým způsobem lze plnit textové tabulky prostřednictvím REST-API nabízeného systému.  |  ANO   |
| 57  | Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně. Doložte odkazem na dokumentaci, ze které je zřejmé, jakým způsobem se vkládají testovací zprávy během psaní nového uživatelského parseru a jakým způsobem je prezentován výstup testu.  | ANO     |
| 58  | V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspešné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd...  | ANO     |
| 59  | Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.  | ANO     |
| 60  | Pro budoucí nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru. Doložte odkazem na dokumentaci, jakým způsobem se cluster vytváří a jakým způsobem se provádí obnovení po možném výpadku jednotlivých zúčastněných komponent.  |  ANO   |
| 61  | Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožnuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě. Popište použitou technologii zabezpečení komunikace v rámci clusteru.  | ANO     |
| 62  | V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech.  |  ANO   |
| 63  | V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.  | ANO     |

|  |  |  |
| --- | --- | --- |
| 64  | Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.  | ANO     |
| 65  | Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.  | ANO     |
| 66  | Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena. Doložte odkazem na dokumentaci, jakým způsobem se realizuje zálohování a obnova záloh.  |  ANO   |
|   | **Alerty**  |    |
| 67  | Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.  |  ANO   |
| 68  | Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.  | ANO     |
| 69  | Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.  | ANO     |
| 70  | Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby. Doložte odkazem na dokumentaci, jakým způsobem realizujete konfiguraci a testovaní alertů a korelací.  | ANO     |
| 71  | Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran. Doložte odkazem na dokumentaci, jakým způsobem se zpráva, která vyvolala spuštění alertu, odesílá na externí systém a jak se definuje formát odesílání dat.  | ANO     |
| 72  | V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku). Doložte odkazem na dokumentaci, jakým způsobem lze v jednotném grafickém rozhraní systému definovat a přiřazovat značky.  |  ANO   |
| 73  | Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci.  | ANO     |
|   | **Sběr událostí z Microsoft prostředí**  |  |
| 74  | Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému. Doložte odkaz na dokumentaci popisující požadované vlastnosti integrovaného Windows agenta.  | ANO     |
| 75  | Agent provádí instalaci a podporuje centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon a výběr z několika přednastavených konfigurací Sysmon v grafickém rozhraní centrální správcovské konzole systému. Doložte odkazem na dokumentaci, jakým způsobem se provádí centralizované řízení a konfigurace Microsoft Sysmon služby.  | ANO     |
| 76  | Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Například, zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahoď logy s EventId 7036.  |  ANO   |

|  |  |  |
| --- | --- | --- |
| 77  | Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Doložte odkazem na dokumentaci, jakým způsobem se vytváří a přiřazují filtry pro Windows agenty pro sběr logů a jakým způsobem se testuje účinnost filtru.  | ANO     |
| 78  | Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému.Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.  | ANO     |
| 79  | Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.  | ANO     |
| 80  | Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu. Doložte odkazem na dokumentaci, jakým způsobem se nastavují parametry sběru logů globálně a jakým způsobem u konkrétního agenta.  | ANO     |
| 81  | Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K bezpečnostním událostem hodným pozornosti doplňuje značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytváří SHA256 hash.  |  ANO   |
|   | **Podpora pro sběr událostí z poboček**  |  |
| 83  | Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. Doložte odkazem na dokumentaci, jakým způsobem realizujete sběr událostí z poboček.  | ANO     |
| 84  | Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.  | ANO     |
| 85  | Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.  |  ANO   |
| 86  | Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven prostup přes firewally a řešena kvalita služby (QoS) pro přenos událostí. Doložte odkazem na dokumentaci, jak vypadá komunikační matice pro připojení rešení pro sběr událostí na pobočkách.  | ANO     |
| 87  | Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.  |  ANO   |
| 88  | Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s, a to i v trvalé zátěži.  | ANO     |
| 89  | Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.  | ANO     |
| 90  | Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.  |  ANO   |
| 91  | Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).  | ANO     |
|   | **Záruka**  |   |
| 92  | Požadovaná min. 5ti letá záruka s opravou v místě instalace s garantovanou odezvou následující pracovní den od nahlášení případné závady.  | ANO     |
| 93  | Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.  | ANO     |

**Příloha č.1**

1. **Konektivita školy k veřejnému internetu (WAN)**
	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. **Povinné parametry projektu:**
		1. Šíře pásma (bandwidth) odpovídající 0,25 Mbps/žák či student[[1]](#footnote-1) nebo 0,5 Mbps/koncové uživatelské zařízení[[2]](#footnote-2)[[3]](#footnote-3) a zároveň taková šířka pásma, která neomezuje provoz zařízení a uživatelů[[4]](#footnote-4). Šíře pásma se vztahuje na počet žáků/studentů/koncových uživatelských zařízení v budově/areálu, kde se projekt realizuje.
		2. Vlastní nebo poskytovatelem přidělené veřejné IPv4 adresy.
		3. Zajištění monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu koncovému zařízení v minimální délce 3 měsíců.
		4. Síťové zařízení podporující rate limiting, antispoofing, access listy - zařízení musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality.
		5. Schopnost snadné/automatické rekonfigurace pravidel firewallu (access listů) na základě identifikovaných útoků.
		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.).
		7. Validující DNSSEC resolver na straně školy, nebo poskytovatele konektivity, nebo otevřeným DNSSEC validujícím resolverem;
		8. Software a firmware je aktualizován po dobu udržitelnosti projektu, jsou-li aktualizace k dispozici.
		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. **Doporučené parametry projektu:**

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

* + 1. Symetrické připojení (zajištění konektivity) bez agregace a omezení, doporučujeme postupně směřovat ke kapacitě konektivity 1Gbps.
		2. Plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6, včetně zajištění dostupnosti online služeb školy na IPv6 adresách.

* + 1. Poskytovatel konektivity je schopen zajistit funkci systému incident response, monitoring a aktivní notifikaci anomálií síťového provozu, zamezení podvržení zdrojových IP adres (antispoofing), 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.
		2. Antivirová kontrola internetového provozu.
1. **Vnitřní konektivita školy (LAN a WLAN)**
	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.

* 1. **Povinné parametry projektu (bez ohledu typ síťového připojení):**
		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. Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém[[5]](#footnote-5).
		3. Systémy zálohování a obnovy dat serverové infrastruktury.
		4. Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.
	2. **Povinné parametry projektu v oblasti pevné LAN:**
		1. Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex.
		2. Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex.
		3. Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3)[[6]](#footnote-6) 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.].

* + 1. Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).
		2. 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.
	1. **Minimální parametry projektu v případě řešení bezdrátových sítí (WLAN):**

* + 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. Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-

Enterprise, multi SSID, ACL pro filtrování provozu.

* + 1. Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).
		2. Podpora mechanismu izolace uživatelů.
		3. 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.
	1. **Doporučené parametry projektu (bez ohledu typ síťového připojení):**

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

* + 1. Logování provozu za účelem dohledatelnosti na úroveň koncového uživatele.
		2. Řešení dočasných přístupů (hosté, brigádníci, praktikanti, zákonní zástupci, externí subjekty) a systému blokace Wi-Fi v určitém čase.
		3. Federované služby autentizace a autorizace (včetně aktivního zapojení do národních vzdělávacích federací (např. aktvní zapojení do federovaného systému [www.eduroam.cz).](http://www.eduroam.cz/)
		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).
		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].

* + 1. Propojení aktivních prvků a důležitých systémů (např. Servery, NAS, propojení budov) rychlostí 10 Gbps, včetně uplinku.

1. **Další doporučené bezpečnostní prvky projektu**

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

* + 1. Systémy nebo zařízení pro sledování infrastruktury sítě a sledování IP provozu sítě (umožňující funkce RFC 3917 - IPFIX nebo ekvivalent).
		2. Systémy schopné detekovat nelegitimní provoz nebo síťové anomálie.
		3. Systémy vyhodnocování a správy událostí a bezpečnostních incidentů (log management, incident management).
		4. Systémy pro monitorování funkčnosti síťové a serverové infrastruktury.
		5. Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu.
		6. Systémy uživatelské podpory naplňující principy ITIL (HelpDesk, ServiceDesk aj.).
		7. Nástroje pro centrální správu a audit ICT prostředků.
		8. Podpora vzdáleného přístupu (VPN).
		9. Zavedení více-faktorové autentizace.

1. Počet žáků/studentů je definovaný celkovým počtem žáků/studentů školy. [↑](#footnote-ref-1)
2. 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.). [↑](#footnote-ref-2)
3. Metrika vhodná typicky pro školy bez mobilních popř. BYOD zařízení [↑](#footnote-ref-3)
4. Definováno jako saturace šířky pásma připojení k veřejnému internetu, která ani ve špičkách nedosáhne, a to ani krátkodobě 100 %. [↑](#footnote-ref-4)
5. 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. [↑](#footnote-ref-5)
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. [↑](#footnote-ref-6)