

Technická specifikace pro veřejnou zakázku: SPŠ Ostrov, Standard konektivity III, Síťová a serverová infrastruktura

Investor / Zadavatel:

Střední průmyslová škola Ostrov, příspěvková organizace, Klínovecká 1197, 363 01 Ostrov

Technickou specifikaci zpracoval:

Ing. Vlastimil Šetka, setka@spsostrov.cz

Revize 13.2.2025

Předmětem zakázky je komplexní dodávka hardware (HW), software (SW), a implementačních služeb včetně záruční technické podpory po dobu udržitelnosti projektu.

Shrnutí rozsahu dodávky:

- **1: Bezpečnostní řešení typu NGFW včetně implementace**
 - 1/1: Dodávka HW a SW licencí - NGFW
 - 1/2: Dodávka služeb bezpečnostních aktualizací - NGFW
 - 1/3: Implementační služby dodavatele - NGFW
 - Záruční technická podpora dodavatele
- **2: Virtualizační infrastruktura a úložiště typu HCI včetně zálohování**
 - 2/1: Dodávka SW vč. implementačních služeb - Virtualizační systém HCI
 - 2/2: Dodávka SW vč. implementačních služeb - Zálohování HCI
 - 2/3: Dodávka SW vč. implementačních služeb - Virtuální firewall
 - 2/4: Dodávka služby bezpečnostních aktualizací - HCI
 - Záruční technická podpora dodavatele
- **3: Systém pro monitorování IT infrastruktury a archivaci logů**
 - 3/1: Dodávka SW vč. implementačních služeb - Flow monitoring
 - 3/2: Dodávka SW vč. implementačních služeb - Service monitoring
 - 3/3: Dodávka SW vč. implementačních služeb - Log management
 - Záruční technická podpora dodavatele
- **4: Konfigurace Wi-Fi sítě a integrace do infrastruktury Eduroam**
 - 4/1: Implementační služby dodavatele - Eduroam
 - Záruční technická podpora dodavatele

Přílohy:

- P1: Popis cílového stavu IT infrastruktury
- P2: Požadavky na dokumentaci skutečného provedení

Obecné požadavky

Standard konektivity

Dodavatel ve všech relevantních případech zohlední kritéria definovaná MŠMT v dokumentu „Standard konektivity škol“ (č. 16039/2022-2, vydání červenec 2022) tak, aby byly splněny všechny povinné a pokud možno i všechny zde doporučené parametry.

Implementační projekt

- Dodavatel na základě dále uvedených požadavků na všechny části této dodávky, na základě vlastností konkrétních jím nabízených zařízení a softwarových technologií a na základě svých zkušeností zpracuje Implementační projekt. Projekt bude obsahovat popis cílové architektury a konkrétního technického řešení, shrnutí všech požadavků, konkrétní technické parametry (např. IP adresní rozsahy) se zohledněním návazností na další dodávané systémy i stávající IT systémy, a dále plán funkčních zkoušek a plán přechodu ze stávajícího řešení LAN sítě na řešení nové včetně potřebné součinnosti na straně Investora.
- Konkrétnější požadavky na obsah Implementačního projektu jsou specifikovány dále pro jednotlivé části dodávky.
- Součástí Implementačního projektu bude zhodnocení navrhovaného řešení vůči parametrům definovaným ve „Standardu konektivity škol“.
- Implementační projekt bude zpracován do 30 dnů od účinnosti smlouvy.
- Investor zajistí průběžnou aktivní spolupráci osoby zodpovědné za stávající IT infrastrukturu a závěrečné schválení Projektu. Stejně tak se předpokládá aktivní spolupráce investora po celou dobu realizace zakázky.

Uvedení do provozu a předání

- Při uvádění nových systémů do provozu a zejména při nahrazování nebo migraci stávajících systémů může dojít k dočasným výpadkům IT služeb. Tyto případy je nutné koordinovat a směřovat je na časová okna kdy nenaruší běžný provoz Investora (pracovní doba, doba výuky).
- Dodavatel připraví všechny nové systémy ke zkušebnímu provozu alespoň 7 dnů před termínem dokončení díla. Po dobu zkušebního provozu zajistí Dodavatel plnou součinnost při provádění funkčních zkoušek.
- Závěrečné předání celé dodávky se uskuteční za účasti Dodavatele v místě sídla Investora.

Dokumentace skutečného provedení

- Všude, kde je tato dokumentace požadována, platí požadavky dle přílohy P2.

Záruční technická podpora dodavatele

Společnou součástí částí dodávky 1 – 4 dle specifikace dále bude Záruční technická podpora poskytovaná Dodavatelem. Cena za tuto službu bude kalkulována jako součást ceny dílčích dodávek.

Podmínky technické podpory zajištěné v rámci záruky:

- Trvání po dobu 60 měsíců od předání díla.
- Pro příjem servisních požadavků stanoví Dodavatel e-mailový a telefonický kontakt s dostupností v pracovních dnech alespoň mezi 9. – 16. hodinou. Dodavatel se zavazuje zahájit řešení servisního požadavku následující pracovní den po jeho přijetí.

Rozsah technické podpory zajištěné v rámci záruky:

- Konzultace k provozu a změnám nastavení všech dodaných systémů - v rozsahu celkem **8 hodin za 12 měsíců**, rozděleno maximálně na 4 servisní požadavky. Kapacita je alokována po období 12 měsíců a nepřevádí se do období dalšího. O čerpání kapacity bude Dodavatel průběžně informovat. Tato kapacita se nevztahuje na požadavky vzniklé reklamací vadného plnění díla.
- Celková kontrola stavu systémů a zpracování doporučení pro další provoz v rozsahu **1x za 12 měsíců**. Dodavatel zpracuje a předá technickou zprávu o této kontrole.

1: Bezpečnostní řešení typu NGFW včetně implementace

1/1: Dodávka HW a SW licencí - NGFW

Rozsah dodávky:

- Sestava 2 ks bezpečnostních síťových zařízení kategorie NGFW (Next Generation Firewall) vč. případně potřebných SW licencí.

Požadavky na obsah nabídky:

- Katalogové listy dokládající technické parametry a podmínky záruky a technické podpory výrobce, odkaz na dokumentaci na webu.

Požadované technické parametry dodaného HW a SW:

- Fyzické zařízení kategorie NGFW, montáž do 19" racku, výška 1U - 2 ks.
- Redundantní napájecí zdroj, 2x 230V AC (zdroj AC/DC může být fyzicky oddělený od zařízení, v takovém případě bude dodáno včetně příslušenství pro montáž do 19" racku).
- Podpora provozu 2 ks zařízení v režimu vysoké dostupnosti (HA, active-passive) s plně automatickou synchronizací kompletní konfigurace.
- Rozhraní Ethernet: 2x SFP+ 10Gb/s, 8x RJ45 1Gb/s, podpora LACP a VLAN.
- Propustnost v režimu Firewall 64 byte UDP: 10Gb/s, 512 byte UDP: 18Gb/s, 15Mpps, 1.5M TCP sessions, 50K new sessions/s, 5000 firewall policies.
- Propustnost v režimu IPS: 2.5Gb/s, v režimu NGFW: 1.5Gb/s.
- Konfigurace přes webové (HTTPS) i textové (SSH - CLI) rozhraní. Export kompletní konfigurace v textové formě protokolem SFTP.
- SW funkce: Stavový Firewall IPv4 a IPv6, možnost definice pravidel na základě identifikace koncového uživatele (VPN, Captive Portal, Active Directory).
- SW funkce: NAT44, NAT66, NAT64+DNS64, DNS resolver, DHCP server a relay, HTTPS Reverse Proxy.
- SW funkce: IDS/IPS (Intrusion Detection/Prevention System), AMP (Anti-Malware Protection).
- SW funkce: DNS filter, automatická aktualizace filtrů škodlivých domén (např. Botnet C&C) dostupná jako služba od výrobce zařízení.
- SW funkce: SD-WAN pro řešení Multi-WAN failover s automatickou detekcí kvality jednotlivých WAN spojení.
- SW funkce: Routing protokoly BGP, OSPF.
- SW funkce: Captive Portal autentizace uživatele pro vybrané sítě, možnost modifikace přihlašovací stránky, návaznost na LDAP databázi.
- SW funkce: IPsec VPN IKEv2, propustnost 512 byte 10Gb/s, kapacita 200 gw-gw tunnels a 2000 client-gw tunnels.
- SW funkce: SSL VPN, propustnost 1Gb/s, kapacita 200 tunnels, podpora multi-factor autentizace s využitím SAML SSO.
- SW funkce: podpora rozdělení kapacity zařízení na více (min. 8) logických instancí (virtual partitions, domains) s nezávislou konfigurací.
- Možnost souběžné konfigurace všech funkcí dle požadavků v části 1/3.

- Součástí dodávky je systém pro ukládání a analýzu provozních záznamů (logů) z NGFW. Kapacita 5GB/den, licence platná bez časového omezení. Funkce pro automatickou detekce kompromitace a napadení sítě na základě služby aktualizace signatur dostupné od výrobce zařízení. Provoz systému bude řešen jako virtuální server na dodané HCI infrastruktuře.
- Všechny SW funkce jsou bez omezení počtu připojených zařízení v LAN síti.
- Všechny SW funkce jsou dostupné bez časového omezení i po skončení záruky, resp. technické podpory (mimo bezpečnostní aktualizace a aktualizace signatur).
- Všechny SW funkce jsou s plnou podporou protokolů IPv4 a IPv6.
- Záruka dodavatele a výrobce: 60 měsíců od dodání (může být podmíněno objednáním služby bezpečnostních aktualizací a technické podpory).

1/2: Dodávka služeb bezpečnostních aktualizací - NGFW

Rozsah dodávky:

- Předplacené záruční služby výrobce zařízení NGFW.

Požadovaný rozsah služeb:

- Po dobu 60 měsíců od dodání zařízení NGFW.
- Technická podpora výrobce, případně autorizovaného servisního partnera, pro zařízení NGFW, dostupná na e-mailu a telefonu v režimu NBD (reakce následující pracovní den po nahlášení závady).
- Přístup k bezpečnostním aktualizacím software pro zařízení NGFW.
- Přístup k aktualizacím signatur pro zařízení NGFW: IPS (Intrusion Prevention System), AMP (Anti-Malware Protection), DNS filter, Log analýza - Detekce kompromitace a napadení sítě.

1/3: Implementační služby dodavatele - NGFW

Rozsah dodávky:

- Odborné implementační služby poskytované Dodavatelem.

Požadovaný rozsah služeb:

- Úvodní konzultace a diskuse celkového návrhu LAN sítě ve vztahu k vlastnostem dodaných zařízení a doporučení jejich výrobce.
- Zpracování Implementačního projektu - shrnutí všech požadavků a konkrétních parametrů v návaznosti na další dodávané systémy i stávající systémy, plán přechodu ze stávajícího řešení LAN sítě na řešení nové. Celkový potřebný rozsah lze odvodit od popisu cílového stavu LAN sítě - viz příloha P1.
- Investor zajistí montáž a zapojení dodaných zařízení dle Implementačního projektu a zapojení do oddělené management sítě a její zpřístupnění Dodavateli pomocí VPN přes Internet.
- Kompletní konfigurace zařízení - viz dále.
- Předání - základní školení obsluhy a údržby, předvedení funkce, funkční zkoušky - test firewall pravidel, test propustnosti, test chování ve failover stavech.
- Zpracování technické dokumentace skutečného provedení.

Požadovaný rozsah konfigurace zařízení NGFW:

- Primární WAN IPv4 (routed prefix /29), IPv6 (routed prefix /56)
 - Routing části rozsahů IPv4 i IPv6 do vnitřní sítě (IT laboratoř)
 - NAT pro IPv4 s využitím více veřejných IP adres pro různý provoz
 - Příprava na dual-path připojení s protokolem BGP (default route)
- Záložní WAN IPv4 (1x IP). Přístup k vybraným službám z internetu zároveň přes obě WAN připojení. Automatické přepnutí výchozí cesty do internetu při výpadku primární WAN.
- Přímé připojené VLAN (cca 20), Firewall zóny a politiky - Bude navrženo v rámci Implementačního projektu.
- Jednoduchá možnost zablokování určité IP adresy nebo rozsahu jak na straně LAN tak WAN.
- Identity-based policy na základě integrace s VPN a servery RADIUS a Active Directory.
- Kompletní flow monitoring (se zpracováním všech paketů procházejících zařízením) s výstupem protokolem IPFIX, včetně dat o NAT adresách.
- Pro vybrané VLAN DHCPv4 server s definicí IP pool a rezervací IP adres na základě MAC adres.
- Captive Portal pro autentizaci uživatelů v rámci určených Guest VLAN (WiFi a Ethernet) - návaznost na LDAP databázi uživatelů (bude upřesněno v rámci Implementačního projektu).
- VPN pro scénář "BYOD Workstation": SSL VPN s klientskou aplikací pro Windows 10/11 a Mac OS, autentizace SAML SSO MFA (Microsoft Entra ID), split-routing.
- VPN pro scénář "Managed Workstation": IKEv2 VPN pro zařízení s Windows 11 centrálně spravované v Active Directory s využitím integrovaného klienta, autentizace certifikátem zařízení, režim "always on", split-routing, split-DNS; součástí dodávky je dokumentace referenční konfigurace klienta.
- VPN pro scénář "Remote Admin": IKEv2 VPN, autentizace certifikátem a jménem/heslem z lokální databáze, split-routing.
- Všechny funkcionality budou pokud možno v režimu IPv4+IPv6, detailněji bude stanoveno v rámci Implementačního projektu.

2: Virtualizační infrastruktura a úložiště typu HCI včetně zálohování

2/1: Dodávka SW vč. implementačních služeb - Virtualizační systém HCI

Rozsah dodávky:

- Softwarové licence pro provoz virtuálních serverů včetně softwarově-definovaného úložiště s využitím stávajícího HW Investora a odborné implementační služby poskytované Dodavatelem.

Požadavky na obsah nabídky:

- Katalogové listy dokládající klíčové technické vlastnosti nabízeného řešení, odkaz na dokumentaci na webu.

Požadované technické parametry virtualizačního software:

- Trvalá licence bez časového omezení i po skončení záruky resp. technické podpory (nevztahuje se na bezpečnostní aktualizace).
- Možnost instalace na 3x fyzický server Fujitsu PY RX1440 M2 dle specifikace níže.
- Síťové připojení každého serveru bude 4x 25Gb/s do 2 ks core switchů (2x MC-LAG) + oddělená síť pro management 1x 1Gb/s.
- Podpora Guest-OS typu Linux, Windows Server 2019 a 2022. Podpora importu virtuálních serverů z prostředí Proxmox VE. Požadavky jsou dány stávající technologií provozovanou Investorem.
- Síťová integrace virtuálních serverů s využitím VLAN v režimu L2 bridge.
- Softwarově definované úložiště pro disky virtuálních serverů a pro souborový systém exportovaný přes protokol NFS a SMB/CIFS s integrací do Active Directory; využití NVMe disků přímo připojených do serverů, 3-násobná redundance ukládání dat, podpora automatického vytváření snímků (snapshots).
- Provoz virtualizace a softwarově-definovaného datového úložiště v režimu vysoké dostupnosti (HA) s automatickým přesunem služeb na jiný server při selhání jednoho z fyzických serverů.
- Správa celého systému a jednotlivých VM přes webové rozhraní s podporou uživatelských rolí a oprávnění na jednotlivé virtuální servery.
- Výkon při čtení dat ze softwarově definovaného úložiště přes protokol SMB/CIFS min. 40Gb/s na síťové vrstvě při 60 klientech (sekvenční čtení souborů o velikosti min. 100MB).

Požadovaný rozsah implementačních služeb:

- Zpracování Implementačního projektu - shrnutí všech požadavků a konkrétních parametrů v návaznosti na další dodávané systémy i stávající systémy.
- Investor zajistí zapojení serverů dle Implementačního projektu a zapojení do oddělené management sítě a její zpřístupnění Dodavateli pomocí VPN přes Internet.
- Provedení instalace a kompletní konfigurace softwarového systému HCI v rozsahu dle požadovaných technických parametrů.

- Předání - základní školení obsluhy a údržby, předvedení funkce, funkční zkoušky - test importu a spuštění virtuálních serverů, test chování ve failover stavech, test propustnosti SMB/CIFS úložiště.
- Zpracování technické dokumentace skutečného provedení.

Poznámky:

- V případě, že by pro provoz dodavatelem nabízeného řešení bylo nutné doplnit hardwarové vybavení serverů, musí být takové komponenty součástí dodávky v rámci celkové nabízené ceny.

2/2: Dodávka SW vč. implementačních služeb - Zálohování HCI

Rozsah dodávky:

- Softwarové licence pro zálohovací systém virtuálních serverů s využitím stávajícího HW Investora a odborné implementační služby poskytované Dodavatelem.

Požadavky na obsah nabídky:

- Katalogové listy dokládající klíčové technické vlastnosti nabízeného řešení, odkaz na dokumentaci na webu.

Požadované technické parametry zálohovacího software

- Trvalá licence bez časového omezení i po skončení záruky, resp. technické podpory (nevztahuje se na bezpečnostní aktualizace)
- Možnost instalace na 1x fyzický server Dell R540 dle specifikace níže
- Součástí řešení je virtualizační systém instalovaný na fyzický server, tato virtualizace bude oddělena od hlavního HCI clusteru, ale případně umožní obnovu a nouzové spuštění záloh z lokálního úložiště.
- Zálohovací systém umožní inkrementální zálohování virtuálních serverů a souborového úložiště z hlavního HCI clusteru, s podporou komprese a deduplikace.
- Správa a monitorování systému přes webové rozhraní s podporou uživatelských rolí a oprávnění
- Možnost částečné obnovy zálohy, webové a command-line rozhraní pro procházení historie a obsahu záloh
- Individuální nastavení doby uchování jednotlivých záloh (např. posledních 7 dnů, 4 týdny a 12 měsíců)
- Možnost Inkrementální synchronizace zvolených záloh na vzdálené úložiště, šifrování.

Požadovaný rozsah implementačních služeb:

- Zpracování Implementačního projektu - shrnutí všech požadavků a konkrétních parametrů v návaznosti na další dodávané systémy i stávající systémy.
- Investor zajistí zapojení serveru dle Implementačního projektu a zapojení do oddělené management sítě a její zpřístupnění Dodavateli pomocí VPN přes Internet.
- Provedení instalace a kompletní konfigurace zálohovacího systému HCI v rozsahu dle požadovaných technických parametrů.

- Předání - základní školení obsluhy a údržby, předvedení funkce, funkční zkoušky - záloha všech VM a souborového úložiště, obnova celého VM, obnova jednotlivých souborů.
- Zpracování technické dokumentace skutečného provedení.

Poznámky:

- V případě, že by pro provoz dodavatelem nabízeného řešení bylo nutné doplnit hardwarové vybavení serverů, musí být takové komponenty součástí dodávky v rámci celkové nabízené ceny.

2/3: Dodávka SW vč. implementačních služeb - Virtuální firewall

Rozsah dodávky:

- Softwarové licence pro systém virtuálního firewallu a odborné implementační služby poskytované Dodavatelem.

Požadavky na obsah nabídky:

- Katalogové listy dokládající klíčové technické vlastnosti nabízeného software, odkaz na dokumentaci na webu.

Požadované technické parametry dodaného software:

- Řešení virtuálního firewallu a routeru s vysokou propustností pro izolaci interních VLAN (2nd level firewall - viz příloha 1).
- Virtualizovaný provoz na dodané HCI infrastruktuře se zajištěním vysoké dostupnosti v případě selhání jednoho fyzického serveru.
- Trvalá licence bez časového omezení i po skončení záruky resp. technické podpory; připouští se i použití řešení s licencí typu OSS (Open Source) pro kterou zajistí plnou technickou podporu Dodavatel.
- Konfigurace přes i textové (SSH - CLI) rozhraní; export kompletní konfigurace v textové formě protokolem SFTP.
- SW funkce: Statický routing IPv4 a IPv6.
- SW funkce: DHCP relay agent IPv4 + IPv6, podpora RFC 6939.
- SW funkce: Stavový Firewall IPv4 a IPv6, konfigurace pravidel s využitím zón a skupin adres (address list, address group).
- Propustnost minimálně 40 Gb/s (512 byte UDP/TCP).

Požadovaný rozsah implementačních služeb:

- Zpracování Implementačního projektu - shrnutí všech požadavků a konkrétních parametrů v návaznosti na další dodávané systémy i stávající systémy, plán přechodu ze stávajícího řešení LAN sítě na řešení nové; celkový potřebný rozsah lze odvodit od popisu cílového stavu LAN sítě - viz příloha 1.
- Instalace na Virtualizační infrastrukturu HCI.
- Provedení kompletní SW konfigurace dle Implementačního projektu.
- Předání - základní školení obsluhy a údržby, předvedení funkce, funkční zkoušky - test firewall pravidel, test propustnosti, test chování ve failover stavech.
- Zpracování technické dokumentace skutečného provedení.

2/4: Dodávka služeb bezpečnostních aktualizací - HCI

Rozsah dodávky:

- Předplacené záruční služby výrobce virtualizačního software.

Požadovaný rozsah služeb:

- Po dobu 60 měsíců od instalace systému HCI.
- Přístup k bezpečnostním aktualizacím software pro Virtualizační infrastrukturu HCI a Zálohování HCI v rozsahu 3x server + 1x server.

2/X: Specifikace hardware pro HCI

Pro konfiguraci nové virtualizační infrastruktury budou dodavateli plně k dispozici 3 ks nových serverů v konfiguraci:

- **Fujitsu PY RX1440 M2** 10x 2.5" NVMe chassis
- 1x AMD EPYC 9224 24C 2.5 GHz
- 6x 64GB DDR5-4800 R ECC
- 4x SSD NVMe PCIe5 3.84TB Read-Int. Hotplug
- 2x SSD SSD PCIe4 480GB M.2 N; osazeno v kartě PDUAL CP300 LP; OS drive
- 1x PLAN CP N41T 4X 1000BASE-T OCPV3 IL
- 2x PLAN EP E810-XXVDA2 2X 25G SFP28 PCIe LP
- 1x volný slot PCIe x8 LP, 1x volný slot OCP 3.0
- iRMC advanced pack, iRMCS6 eLCM License

Pro zálohování virtualizační infrastruktury bude k dispozici 1 ks stávajícího serveru:

- **Dell R540** 12x 3.5" SAS/SATA chassis
- 1x Intel Xeon Silver 4108 8C 1.8GHz
- 96 GB DDR4-2667 (PC4-21300R) RDIMM
- PERC H730P RAID Controller, 2GB NV Cache
- 4x HDD 16TB SAS 7.2K RPM (Toshiba MG08SCA16TE)
- 1x LAN Intel X520 2X 10G
- iDRAC9, Enterprise License

Propojení serverů a ostatních částí síťové infrastruktury bude zajištěno 2 ks přepínačů:

- **HPE Aruba 8100** 24x SFP+, 4x QSFP28 (R9W86A)
- Přepínače budou nastaveny v redundantní konfiguraci VSX. Všechny vnější propoje budou v režimu MC-LAG (multichassis link aggregation).
- Pro připojení VM serverů rychlostí 25Gb/s budou použity Split-DAC kabely 4x25G.
- Konfiguraci zajistí investor. Bude k dispozici při zahájení projektu. Dodavatel může provést její revizi a případně doporučit vhodné úpravy.

3: Systém pro monitorování IT infrastruktury a archivaci logů

3/1: Dodávka SW vč. implementačních služeb - Flow monitoring

Rozsah dodávky:

- Softwarové řešení pro systém monitoringu síťových toků vč. odborné implementační služby poskytované Dodavatelem.

Požadavky na obsah nabídky:

- Katalogové listy dokládající klíčové technické vlastnosti nabízeného software, odkaz na dokumentaci na webu.

Požadované technické parametry dodaného software:

- Monitorovací systém pro sledování a analýzu síťových toků s vizualizací formou webového rozhraní.
- Licence včetně technické podpory a aktualizací po dobu 60 měsíců od dodání.
- Licencovaná kapacita úložiště 1TB, výkonová kapacita 75000 flow/sec.
- Provoz jako jeden nebo více virtuálních serverů na dodané HCI infrastruktuře.
- Podpora vstupních dat protokoly NetFlow a IPFIX (funkce collector); kompatibilita s formátem dat z dodaných systémů NGFW a Virtuální firewall; deduplikace shodných toků z více sond.
- Uživatelsky konfigurovatelný webový dashboard, předdefinované pohledy a reporty, vyhledávání podle časového období, zdrojových/cílových adres, protokolů, identity uživatele.

Požadovaný rozsah implementačních služeb:

- Zpracování Implementačního projektu.
- Instalace na Virtualizační infrastrukturu HCI a konfigurace:
 - NetFlow (IPFIX) zdroje: NGFW, Virtuální firewall HCI
 - Identity zdroje: Eduroam Radius, Active Directory, NGFW
- Předání - základní školení obsluhy a údržby, předvedení funkce, funkční zkoušky.
- Zpracování technické dokumentace skutečného provedení.

3/2: Dodávka SW vč. implementačních služeb - Service monitoring

Rozsah dodávky:

- Softwarové řešení pro systém monitoringu stavu síťových zařízení a služeb vč. odborné implementační služby poskytované Dodavatelem.

Požadavky na obsah nabídky:

- Katalogové listy dokládající klíčové technické vlastnosti nabízeného software, odkaz na dokumentaci na webu.

Požadované technické parametry dodaného software:

- Monitorovací systém, který na jednom místě s vizualizací formou webového rozhraní umožní sledování funkčního stavu celé IT infrastruktury.
- Trvalá licence bez časového omezení i po skončení záruky resp. technické podpory; připouští se i použití řešení s licencí typu OSS (Open Source) pro kterou zajistí plnou technickou podporu po dobu záruky Dodavatel.
- Provoz jako jeden nebo více virtuálních serverů na dodané HCI infrastruktuře.
- Sledování dostupnosti serverů, vč. základních provozních parametrů operačního systému - vytížení operační paměti a procesoru, zaplnění diskového prostoru (Linux, Windows Server 2019 a 2022).
- Sledování dostupnosti síťových služeb - HTTPS, LDAP, Active Directory, MS SQL Server, HTTP/HTTPS, obecný TCP port.
- Sledování základních provozních a síťových parametrů dodané HCI infrastruktury.
- Sledování provozu síťových prvků - Ethernet switche - provoz a chybovost na portech, MAC adresy na portech, zatížení CPU, teploty (HPE Aruba 6100, 8100).
- Sledování provozu síťových prvků - Wi-Fi AP (HPE Aruba AP-505 Virtual Controller).
- Obecná podpora sledování hodnot z jiných zařízení přes protokol SNMP.
- Ukládání historie všech sledovaných parametrů po zvolené období, minimálně 1 rok.
- Notifikace významných událostí přes e-mail a mobilní aplikaci.
- Konfigurace založená na šablonách zařízení, správa konfigurace v systému pro správu verzí, export konfigurace do textového formátu.
- V případě licencování vázaného na množství sledovaných hodnot navrhne Dodavatel vhodné řešení dle dále uvedeného rozsahu implementace, případně si vyžádá upřesnění zadání na základě licenční politiky konkrétního uvažovaného produktu.

Požadovaný rozsah implementačních služeb:

- Zpracování Implementačního projektu.
- Instalace na Virtualizační infrastrukturu HCI a komplexní konfigurace monitoringu v rozsahu:
 - dodaný firewall NGFW (dostupnost, stav HA uzlů, vytížení),
 - dodaná HCI infrastruktura vč. management rozhraní fyzických serverů,
 - 6x Windows Server (2x AD DC, 1x MS SQL, 1x IIS, 1x Firebird SQL, 1x RDP), 10x Linux Server (Ubuntu, Debian),
 - 12x Ethernet switch Aruba 6100 48P, 2x Ethernet switch Aruba 8100
 - 40x Wi-Fi AP Aruba AP-505
- Předání - základní školení obsluhy a údržby, předvedení funkce, funkční zkoušky.
- Zpracování technické dokumentace skutečného provedení.

3/3: Dodávka SW vč. implementačních služeb - Log management

Rozsah dodávky:

- Softwarové řešení pro systém centrálního sběru a ukládání provozních záznamů (logů) vč. odborné implementační služby poskytované Dodavatelem.

Požadavky na obsah nabídky:

- Katalogové listy dokládající klíčové technické vlastnosti nabízeného software, odkaz na dokumentaci na webu.

Požadované technické parametry dodaného software:

- Integrovaný systém pro sběr, archivaci a prohledávání logů s webovým rozhraním.
- Sběr logů ze zdrojových systémů protokolem Syslog a Windows Event.
- Archivace logů v databázi po nastavitelnou dobu.
- Webové rozhraní pro vyhledávání na základě časového rozsahu, zdrojového systému, úrovně závažnosti, fulltext obsahu a dalších extrahovaných parametrů.
- Trvalá licence bez časového omezení i po skončení záruky resp. technické podpory; připouští se i použití řešení s licencí typu OSS (Open Source) pro kterou zajistí plnou technickou podporu po dobu záruky Dodavatel.
- Provoz jako jeden nebo více virtuálních serverů na dodané HCI infrastruktuře.
- V případě licencování vázaného na množství událostí, velikost úložiště apod. navrhne Dodavatel vhodné řešení dle dále uvedeného rozsahu implementace s uvažovanou retencí logů 6 měsíců, případně si vyžádá upřesnění zadání na základě licenční politiky konkrétního uvažovaného produktu.

Požadovaný rozsah implementačních služeb:

- Zpracování Implementačního projektu.
- Instalace na Virtualizační infrastrukturu HCI a konfigurace zdrojů logů:
 - dodaný firewall NGFW,
 - dodaná HCI infrastruktura,
 - 6x Windows Server (2019, 2022), 10x Linux Server (Ubuntu, Debian),
 - 12x Ethernet switch Aruba 6100, 2x Ethernet switch Aruba 8100
 - Wi-Fi AP Aruba AP-505 Instant Virtual Controller
- Předání - základní školení obsluhy a údržby, předvedení funkce, funkční zkoušky.
- Zpracování technické dokumentace skutečného provedení.

4: Konfigurace Wi-Fi sítě a integrace do infrastruktury Eduroam

Pozn.: Síť Eduroam se myslí mezinárodní roaming federace, v ČR zajišťovaná akademickým sdružením CESNET z. s. p. o., viz <https://www.eduroam.cz/cs/start>.
Uživatel má jediný účet (ve své domovské síti) a tento účet jej opravňuje k použití bezdrátové sítě kteréhokoliv člena projektu Eduroam.

4/1: Implementační služby dodavatele - Eduroam

Rozsah dodávky:

- Odborné implementační služby poskytované Dodavatelem.

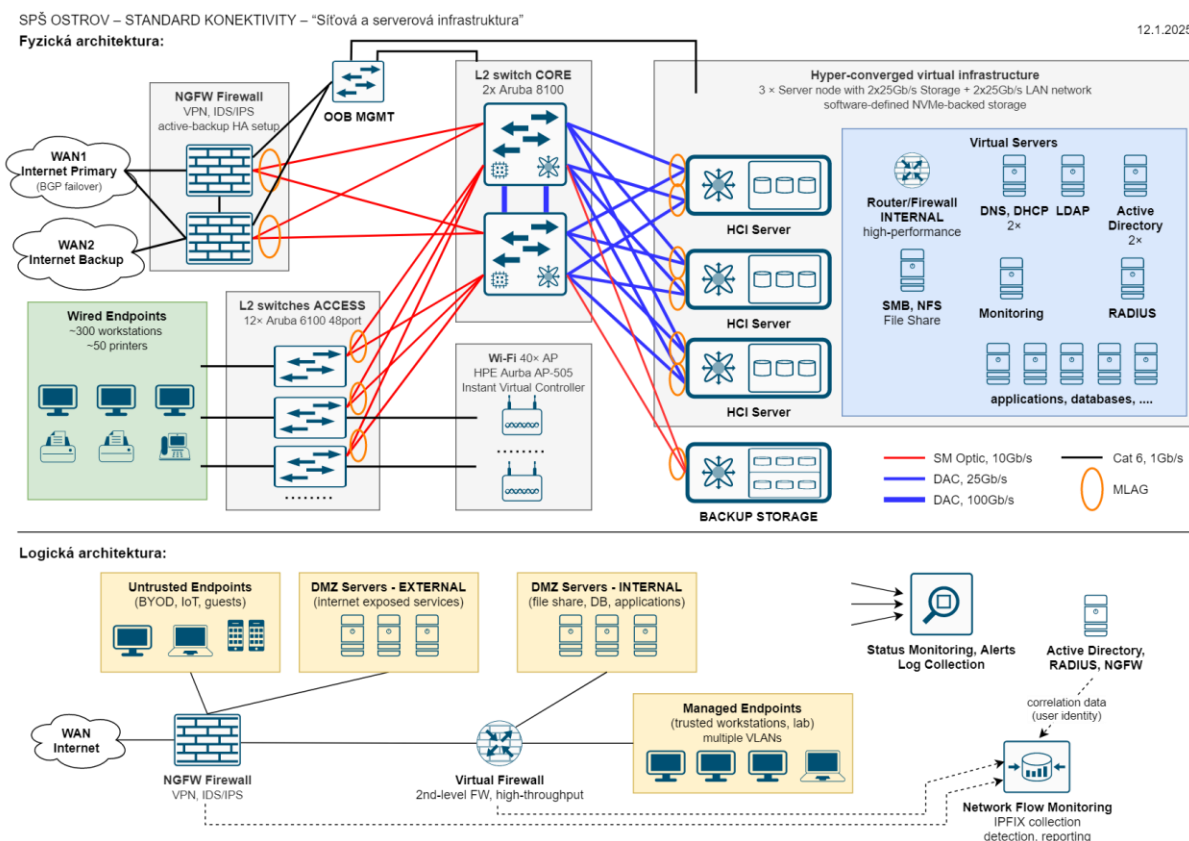
Požadovaný rozsah implementačních služeb:

- Instalace a konfigurace serverové služby RADIUS a zajištění její integrace do sítě Eduroam pro ověřování WiFi připojení.
- Serverový software a jeho nastavení bude splňovat všechny požadavky pro kompatibilitu se sítí Eduroam, tj. předpokládá se řešení FreeRADIUS.
- Pro provoz serveru bude využita Virtualizační infrastruktura HCI dle tohoto projektu.
- Autentizace uživatelů ve vlastní doméně bude řešena proti stávající databázi LDAP.
- Logování událostí (připojení a odpojení uživatele, přiřazené IP adresy) bude možné do databáze SQL a do centrálního systému pro sběr logů.
- Řešení umožní přenos identit pro firewall politiky systému NGFW.
- Konfigurace WiFi systému HPE Aruba AP-505 (v režimu Instant Virtual Controller) pro síť Eduroam s využitím lokální RADIUS služby.
- Předání - základní školení obsluhy a údržby, předvedení funkce, funkční zkoušky.
- Zpracování technické dokumentace skutečného provedení.

Příloha P1: Popis cílového stavu IT infrastruktury

V rámci projektové dokumentace „SPŠ Ostrov – Standard konektivity (2023)“ (V. Šetka, 9.10.2023), podle výzvy „Konektivita škol“ OP „Spravedlivá transformace“ a v souladu s dokumentem „Standard konektivity škol“ (MŠMT, č. 16039/2022-2, vydání červenec 2022) byl zpracován návrh cílového stavu IT infrastruktury SPŠ Ostrov. Projekt uvažuje vybudování zcela nové síťové a serverové infrastruktury, částečně s využitím stávajícího vybavení. Zachovány zůstanou stávající hlavní infrastrukturní prvky (Active Directory, LDAP IDM) a stávající aplikační servery (vše VM na platformě Proxmox VE).

Cílový stav infrastruktury nejlépe ilustruje následující schéma:



Předpokládaný postup přechodu provozu na cílový stav lze shrnout v bodech:

Zajistí investor:

- Nasazení nových Ethernet switchů CORE, propojení se stávající infrastrukturou.
- Nasazení nových Ethernet switchů ACCESS, přepojení koncových zařízení.
- Nasazení nových Wi-Fi AP. Zatím nebudou používána, stávající Wi-Fi zůstává.

Zajistí dodavatel:

- Nasazení NGFW - nahrazení stávajícího hraničního firewallu, přepojení WAN.
- Nasazení HCI - provoz souběžně se stávajícím řešením.
- Nasazení Eduroam Wi-Fi na HW Aruba.
- Funkční zkoušky, předvedení funkce a obsluhy systémů.

Zajistí investor v úzké součinnosti s dodavatelem:

- Po otestování postupná migrace stávajících VM na novou HCI infrastrukturu.
- Po otestování migrace stávajících koncových VLAN pod nový Virtuální firewall.

Příloha P2: Požadavky na dokumentaci skutečného provedení

- Dokumentace se předává elektronicky formou PDF souborů. Dokumenty vytvořené dodavatelem, vztahující se ke konkrétnímu dodanému systému jsou předány i ve zdrojové (editovatelné) podobě. Preferuje se použití formátů Microsoft Office, nebo lépe textových formátů (např. AsciiDoc) doplněných nástroji pro převod do PDF.
- Součástí je Seznam dokumentace, který odkazuje na všechny další dílčí dokumenty s jejich jednoznačnou identifikací, označením verze a data poslední úpravy.
- Provozní dokumentace k jednotlivým dodaným HW s SW částem je označena jako “Dokumentace Systému”. Rozdělení realizovaného rozsahu na dílčí Systémy a jejich označení schvaluje Investor, aby byla zajištěna jasná identifikace a konzistence vůči všem stávajícím Systémům.
- Hlavním cílem provozní dokumentace je, aby osoba s dostatečnou kvalifikací a znalostí byla schopna se v konkrétní instalaci systému rychle zorientovat pro případ řešení abnormálních stavů a pro možnost případného převzetí správy systému bez úplné závislosti na znalostech jiných osob. Dalším cílem je zajištění schopnosti efektivního obnovení provozu systémů v případě fatálního selhání části infrastruktury nebo při řešení následků bezpečnostních incidentů.
- Obsahem “Dokumentace Systému” je zejména:
 - Identifikace systému - Kód a název přiřazený Investorem
 - Označení verze, data a autora poslední změny dokumentu
 - Základní informace o systému - Stručný popis funkce / účelu
 - Identifikace všech HW a SW produktů, které jsou součástí systému (výrobce, typové označení, objednávací kódy, specifická konfigurace, odkaz na webovou prezentaci výrobce, výrobní / licenční čísla apod.)
 - Popis licenčních podmínek a omezení softwarových produktů
 - Popis záručních podmínek, kontakty pro uplatnění záruky
 - Popis architektury, zapojení, návaznosti na jiné systémy
 - Identifikace aktuálních verzí software a firmware
 - Informace o uživatelských účtech, způsobu řízení přístupu a zabezpečení
 - Postupy instalace a konfigurace, způsob zálohování a obnovy konfigurace
 - Postupy pro běžnou kontrolu provozu, správu a údržbu, aktualizace
 - Postupy pro zálohování a obnovu dat
 - Postupy pro automatizovaný monitoring provozního stavu
 - Odkazy na uživatelskou a servisní dokumentaci výrobce;
pozn.: detaily provozních postupů mohou být řešeny odkazem na konkrétní místa dokumentace výrobce
 - Identifikaci účtů v online systémech výrobce, pokud jsou potřebné pro přístup k servisním informacím, aktualizacím apod.
 - Evidence historie změn v dokumentaci