

Příloha č.: 1

Detailní popis předmětu plnění – technická specifikace

Specifická pravidla pro žadatele a příjemce integrovaných projektů ITI, příloha č. 8A „Standard konektivity Základních škol“, který je přílohou tohoto dokumentu, definuje základní technická kritéria, která musí být dodržována v rámci pětileté udržitelnosti projektu IROP, specifický cíl 2.4, kolová výzva č. 67. Dodavatel správcovských a dohledových služeb na školách, kde je Projekt realizován bude vázán smlouvou, aby dohlížel, že technická kritéria definovaná poskytovatelem dotace budou po celou dobu udržitelnosti Projektu dodržována a plněna.

Předmětem plnění veřejné zakázky je provádění následujících servisních činností nad instalovanými technologiemi:

- Oblast WAN

- internetové připojení. Komunikace s poskytovatelem připojení v případě výpadku. Asistence při řešení.
- dohled, úpravy nastavení a kontrola funkčnosti instalovaného hraničního zařízení a příslušenství - firewall Fortigate a NetFlow technologie včetně sond (Flowmon networks). V případě potřeby školy nebo v případě bezpečnostního incidentu, dohledání a vyhodnocení potřebných informací.
- dohled a kontrola logování vnějšího přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel. V případě potřeby školy nebo v případě bezpečnostního incidentu, dohledání a vyhodnocení potřebných informací.
- dohled a kontrola funkčnosti služby nad monitoringem a logování NAT. V případě potřeby školy nebo v případě bezpečnostního incidentu, dohledání a vyhodnocení potřebných informací.
- úpravy nastavení a kontrola funkčnosti filtrování http, https, DNS a emailového provozu, kategorizace a selekce obsahu a antivirovou kontrolou. Ve spolupráci se školou tvorba a vyhodnocování statistik.
- dohled, úpravy nastavení a kontrola funkčnosti validujícího DNSSEC resolveru (DNSSEC RSA a DNSSEC ECDSA).
- dohled, úpravy nastavení a kontrola funkčnosti nad protokoly IPv4 a IPv6 (dual-stack).
- dohled, úpravy nastavení a kontrola funkčnosti federovaných služeb (sítě Eduroam).
- úpravy nastavení a kontrola funkčnosti šifrovaného spojení (VPN, web stránky, email a další služby)
- kontrola nad prováděním softwarových aktualizací a aktualizací firmware

- Oblast LAN

- dohled a kontrola funkčnosti hardware serveru(ů) a LAN přepínačů. Komunikace s dodavatelem / výrobcem při případné opravě. Asistence při řešení.
- dohled, kontrola funkčnosti a aktualizace operačních systémů serverů a virtualizační platformy. Kontrola logů a náprava chybových stavů.
- dohled, úpravy nastavení a kontrola funkčnosti LAN přepínačů. Vytváření záloh konfigurací při úpravách nastavení.
- dohled, úpravy nastavení a kontrola funkčnosti instalované správy uživatelů (SAMBA AD Controller jako Linuxový Identity Management). Pravidelná kontrola funkčnosti auditovaného přístupu uživatelů k síti. Asistence (zaškolení zodpovědné osoby) při zakládání či rušení uživatelů / skupin.
- dohled a kontrola logování vnitřního přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel. V případě potřeby školy nebo v případě bezpečnostního incidentu, dohledání a vyhodnocení potřebných informací.
- kontrola funkčnosti instalovaného monitorování IP (IPv4 a IPv6) datových toků (NetFlow). V případě potřeby školy nebo v případě bezpečnostního incidentu, dohledání a vyhodnocení potřebných informací.
- dohled, úpravy nastavení a kontrola funkčnosti uživatelských účtů – služby automont, NFS exporty, SSSD, Winbind, Kerberos, CIFS, SAMBA, PAM.
- podpora monitoringu a logování NAT (RFC2663)
- podpora monitoringu a logování provozních informací (RFC 3954)

- **Oblast WIFI**

- dohled a kontrola funkčnosti instalovaných hardwarových AP. Komunikace s dodavatelem / výrobcem při případné opravě. Asistence při řešení.
- dohled, úpravy nastavení a kontrola funkčnosti centralizované správy wifi zařízení.
- dohled nad funkčností protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (SAMBA AD Controller). Řešení případných chyb a monitorování provozu. V případě potřeby školy nebo v případě bezpečnostního incidentu, dohledání a vyhodnocení potřebných informací.
- případné úpravy v nastavení wifi funkcionalit - multi SSID, ACL pro filtrování provozu
- dohled nad funkčností protokolu IEEE 802.1Q ve spojení s FreeRadius

- **Ostatní**

- součinnost se školou při zapracování zásad využívání ICT a přístupu k síti do vnitřních předpisů školy

- součinnost při případné kontrole projektu ze strany poskytovatele dotace IROP
- kontrola záloh konfigurací instalovaných aktivních prvků (switch, WIFI AP ...), monitorovacích technologií (FlowMon, Netflow atp.) a systému správy uživatelů (SAMBA4 AD server)
- udržování a vedení vytvořené dokumentace k instalovaným technologiím
- být na vyžádání k dispozici při jednáních týkající se rozvoje a rozšiřování IT infrastruktury.
- Podpora a úpravy systému pro monitoring funkčnosti IT infrastruktury
- podpora systému ITIL (Helpdesk Redmine)
- podpora úpravy dokumentačního systému (DokuWiki)

Garance reakce na servisní požadavek/doba odezvy:

- jedná se o maximální dobu, do kdy bude započato řešení servisního požadavku přímo souvisejícího s provozem instalovaných technologií
- maximální doba reakce na servisní požadavek v pracovní době/zahájení servisního zásahu: 3 hod od nahlášení
- maximální doba reakce na servisní požadavek mimo pracovní dobu: dle dispozice technika
- pracovní doba objednatele je: 7:00 – 15:30

Způsob řešení servisní požadavků:

- vzdálená správa – šifrované spojení VPN
- lokální správa – dojezd technika do sídla provozovatele v garantované době 3 hodiny od nahlášení požadavku. A to v případě havarijního požadavku, který nelze řešit vzdálenou správou
- za havarijní požadavek se považuje závada zabraňující provozu serveru(ů), LAN, WAN nebo WIFI sítě

Specifikace technologií na škole, nad kterou se budou provádět výše uvedené činnosti:

1. ZŠ U Tenisu
 - a. 2 ks fyzický server Fujitsu
 - b. NetFlow systém + sondy
 - c. 2x bare-metal hypervizor VMware, 1x Windows server, 4x Debian GNU Linux server
 - d. 3x UPS
 - e. Fortigate firewall
 - f. 11 ks switch L2/L3
 - g. 30 ks Wifi AP s centrální správou
 - h. Software VMware, Software Cisco Prime, software Nagios, software DokuWiki, software Redmine, software SAMBA, NFS a CIFS server, software FreeRadius, software rsyslog, software firewall FortiGate