**Technické specifikace - konektivita**

**(minimální požadované parametry)**

**Konektivita školy k veřejnému internetu**

* Šířka pásma min. 11 Mbps, full duplex
* Symetrické připojení bez agregace a omezení (FUP)
* Zakončení UTP RJ-45
* min. 2 veřejných IPv4 adres
* min. 2 veřejných IPv6 adres
* plná podpora připojení přes protokol IPv4 i IPv6 (dual-stack)
* Garance konektivity na 5 let (udržitelnost projektu)
* zapojení ISP v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX, nebo ISP splňuje technické standardy definované projektem FENIX

**1 ks Server**

|  |  |
| --- | --- |
| CPU | min. na úrovni Xeon E3-1270v5 4C 3.6GHz 8MB 2133MHz (80W) |
| CPU patic | 1 |
| RAM obsazeno | 8 GB |
| RAM slotů | 4 |
| 3,5" slot | 0 |
| 5,25" slot | 0 |
| Cache battery backup | Ne |
| Cache na řadiči | Ne |
| Ethernet | 2x 1GE |
| FDD mechanika | Ne |
| HDD formát | 2,5" |
| HDD hot plug | Ano |
| HDD technologie | SAS/SATA II |
| Max. počet HDD | 8 |
| Osazeno HDD | 4 ks 1TB 7.2K 6Gbps NL SATA 2.5in G3HS HDD |
| Optická mechanika | Ne |
| PCI-e sloty | Ano |
| PCI-X sloty | Ne |
| PCI sloty | Ne |
| Pozice pro další zdroj | Ano |
| Provedení | TOWER |
| RAID řadič | RAID 0,1,10 |
| Vzdálená správa | Ano |
| Zdroj hot plug | Ano |
| Zdroj osazený | Ano |
| Záruka | 5 let NBD |

**1 ks UPS**

* 3000VA (2700W) LCD 230V
* Montáž do datového rozvaděče, velikost 2U
* Alfanumerický LCD displej - intuitivní rozhraní poskytuje podrobné a přesné údaje a možnost lokální konfigurace.
* Zelený režim s vysokou účinností - optimální účinnost, která šetří náklady na dodávku energie a chlazení.
* Napájení v síťové kvalitě - rozšířený rozsah automatické regulace napětí (AVR),  filtrace šumu a přepěťová ochrana.
* Komunikační porty - sériový, USB a Smart-slot pro karty s příslušenstvím
* Skupina spínaných zásuvek - umožňuje opětovný start zařízení, odpojení méně důležitých zátěží pro úsporu kapacity, časové plánování zapínání a vypínání.
* Odpojení baterie - pohodlná možnost odpojit baterii při přepravě.
* Vyspělá správa baterií - nabíjení s kompenzací teploty prodlužuje životnost a vyspělé algoritmy doporučují datum výměny.
* Záruka 5 let na baterie 2 roky

Požadujeme kompletní montáž HW, aktualizaci firmware, zapojení do sítě LAN a konfiguraci UPS. Na serveru bude nainstalován OS Windows Server (min. ver. 2012 R2) včetně posledních aktualizací. Dále bude nakonfigurována služba DNS, DHCP a Active Directory pro cca 90 uživatelů. Každý uživatel bude mít vytvořen jedinečný účet. Služba Active Directory bude mít vazbu na UTM FireWall (logování dle uživatelů v AD).

**DNSSEC resolver na straně školy**

* Požadujeme konfiguraci DNSSEC na novém řadiči Microsoft ActiveDirectory 2012 R2 (2016) na kterém bude spuštěna služba DNS. Tento DNS server je primárním DNS serverem pro všechna zařízení v síti LAN.

**1 ks UTM firewall**

* 4 x Gb RJ45 port
* propustnost FW min. 500 Mbps
* propustnost IPSec VPN (UDP 512B, AES256) min. 150 Mbps
* lokální disková kapacita min. 16 GB, možnost logování na lokální disk nebo na logovací server
* možnost vysoce dostupného zapojení dvou firewallů Active-Active nebo Active-Passive
* statefull firewall
* podpora IPV6 – NAT46, 66, 64
* dynamické směrování pro IPv4 and IPv6 (RIP, OSPF, BGP a Multicast IPv4)
* policy based routing a source based routing
* funkce Load Balancing, WAN optimalizace
* monitoring a logování NAT (RFC 2663)
* logování přístupu uživatelů do Internetu min. IP adresa – čas – uživatel v stávající Microsoft Active Directory
* podpora pro rate limiting
* podpora pro antispoofing
* podpora pro ACL/xACL
* aplikační kontrola (na L7 vrstvě) s propustností min. 200 Mbps
* funkcionalita Antivir (Proxy nebo Flow), Antispyware a Antimalware
* funkcionalita Web filter - kontrola http a https provozu, kategorizace a selekce obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirová kontrola stahovaného obsahu
* integrace s Active Directory pro SSO
* funkcionalita IPS s propustností min. 200 Mbps
* SSL inspekce
* min. 5 virtuálních firewallů s oddělenou konfigurací a správou
* integrovaná 2faktorová autentizace klientů VPN či administrátorů firewallu bez nutnosti využívat další software
* správa přes min. HTTPS, SSH
* snadná konfigurace ACL/FW na základě identifikovaných útoků přes webové rozhraní
* licencování na neomezený počet uživatelů
* pravidelné automatické aktualizace signatur od výrobce
* plná záruka na UTM firewall včetně všech funkcionalit a signatur na 5 let v režimu 24x7x365
* dostupnost bezpečnostních aktualizací po celou dobu udržitelnosti projektu (5 let)
* Požadujeme novou konfiguraci, (cca 10 NAT pravidel, Antivir, WebFilter) na nově dodaný firewall.
* Součástí konfigurace bude vazba na ActiveDirectory (cca 90 uživatelů), konfigurace SSL offloading, IPS/Aplikační kontrola a vzdáleného přístupu.

**1 ks Monitoring IP datových toků**

* Vyhrazená HW sonda pro monitoring datových toků v kombinaci s integrovaným kolektorem zajistí monitoring, sběr, uchování a reporting Flow dat. Sonda bude instalována na rozhraní WAN a bude dodána včetně bezpečnostních updatů a záruky výrobce na 5 let. V rámci dodávky bude nakonfigurováno min. 5 reportů a bude zaškolena lokální administrátor sítě v rozsahu min. 0,5 den. Součástí konfigurace bude nastavení servisních protokolů NTP, SSH, HTTPS, SNMP atd.
* Sonda má 1 x 10/100/1000 monitorovací port (UTP kabeláž)
* Pasivní zapojení bez vlivu na monitorovanou síť a propustnost zařízeni (zapojení pomocí TAP sdružujícího obousměrný monitorovaný tok do jedné linky).
* Jeden plnohodnotný management port 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu
* Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.
* Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí.
* Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalickém rozhraní.
* Podpora pro SNMP
* Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru a uložení dat po dobu min. 2 měsíců
* Úložná kapacita vestavěného kolektoru min. 0,5 TB
* Výkon vestavěného kolektoru min. 50 000 toků/s
* Časová synchronizace zařízení proti centrálnímu zdroji času na síti (NTP).
* Minimální výkon 1 milion paketů za sekundu na každém portu.
* Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.
* Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232).
* Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.
* Podpora autentizace vůči LDAP (Active Directory).
* Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX.
* Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor.
* Monitorování provozu v tunelu GRE.
* Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX.
* Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu.
* Detekce aplikací dle standardu NBAR2.
* Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
* Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
* Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
* Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů.
* Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port.
* Podpora pro nastavení časů u aktivní a neaktivní expirace toků.
* Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků.
* Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX).
* Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky).
* Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port.

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

* Na novém řadiči Microsoft ActiveDirectory bude nastaveno logování přístupu do sítě umožňující dohledání vazeb IP adresa – čas – uživatel

**2 ks Centrální přepínač s podporou PoE pro WiFi**

* Do nového rozvaděče budou dodány 2ks L3 přepínačů s podporou PoE s neblokující architekturou přepínacího subsystému (wire speed) a s min. parametry uvedenými níže.
* Na přepínači bude vytvořena L2/L3 konfigurace
* Na přepínači budou nastaveny základní bezpečnostní protokoly min. NTP, SSH, HHTPS. SNMP apod.
* Velikost 1U do racku 19“
* Vrstvy L2 a L3 (pracuje na 2. a 3. vrstvě modelu OSI), plně spravovatelný
* Výkon PoE min. 370W PoE+
* Počet portů min. 24 RJ-45 100/1000 Mb/s PoE+
* Počet SFP portů min. 4
* Kapacita přepínání min. 56 Gb/s
* Datový tok min. 41,7 milionů paketů/s
* Velikost tabulky MAC adres min. 32 000 záznamů
* Vlastnosti přepínače:
  + Podpora plnohodnotné správy přes IPv4 a IPv6 rozhraní.
  + Podpora stohování
  + Podpora statického L3 směrování mezi VLANnami.
  + Podpora dynamického routingu skrze protokoly RIP, OSPFv2 a OSPFv3.
  + SNMP verze 2c a 3.
  + Quality of Service (QoS).
  + Multiple spanning tree.
  + Podpora spanning tree instance per VLAN s 802.1Q tagováním BPDU rámců.
  + Podpora protokolu MVRP pro administraci a distribuci VLAN.
  + Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty.
  + Monitoring datových toků v síti pomocí sFlow.
  + Software REST API pro automatizaci nastavení sítě.
  + Podpora technologie VxLAN
  + Podpora standardu 802.1v
  + Podpora OpenFlow
* Bezpečnost:
  + Podpora SSH/SSL
  + Podpora filtrování MAC adres
  + Podpora IEEE 802.1x
  + Podpora aktivního monitorování RADIUS serveru přednastaveným jménem a heslem.
  + Podpora RADIUS MAC autentizace, která probíhá před 802.1x autentizací pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci.
  + Podpora RADIUS Change of Authorization (RFC3576).
  + IPv6 ND snooping.
  + Private VLAN.
* Dodávka musí obsahovat veškeré potřebné licence pro využití všech funkcí nabízeného zařízení.
* Dostupnost aktualizací a podpory po celou dobu udržitelnosti projektu (5 let)

**12x bezdrátový přístupový bod (AP)**

* Bezdrátová síť bude provozována jako centralizovaná architektura s využitím funkcionality kontroleru na jednom libovolném AP. Tento řídí distribuci konfigurací, rozkládání zátěže, roaming, ladění kanálů, detekci rušení a jeho funkcionalitu může v případě HW poruch převzít libovolný jiný AP bez ztráty konfigurace a funkčnosti Wifi sítě.
* Podporou automatického rozložení zátěže klientů
* AP musí splňovat specifikaci 802.11a/b/g/n/ac, ac Wave 2
* Každé AP bude mít dvě samostatná rádia - jedno pro frekvenci 2,4GHz a druhé pro frekveci 5GHz
* MIMO konfigurace rádií minimálně 2x2 v pásmu 2,4GHz až 400 Mbps a 3x3 v pásmu 5GHz až 1300Mbps
* Podpora protokolů 802.11v, 802.11k, 802.11r, OKC
* Podpora centralizovaného automatického plánování kanálů a síly signálu
* Podpora automatického roamingu 802.1x autentizovaných klientů na další AP
* Podpora lokálního i externího guest captive portálu
* AP musí podporovat QoS a VOIP služby
* Schopnost garance poměru vysílacího času pro jednotlivé SSID
* AP musí umět pracovat v topologii Bridge a Mesh včetně algorytmu pro výběr cesty v rámci MESH stromu
* Podpora napájení přes PoE standardu 802.3af a 802.3at
* Možnost autentizace AP vůči 802.1x zabezpečenému portu metodou PEAP
* Možnost časového omezení vysílání jednotlivých SSID
* Podpora WPA2
* Podpora multi SSID
* Podpora ACL pro filtrování provozu
* Až 16 možných vysílaných BSSID na jednu radiovou část
* Možnost přenastavit režim činnosti AP do režimů: uživatelský přístup, monitor s/nebo spektrální analýza
* AP je osazeno HW spektrálními filtry zamezujícími intermodulačnímu rušení z blízkých zdrojů na podobných frekvencích (např. LTE), detekce a reakce na non-Wi-Fi rušení
* Podpora airtime fairness
* Hardware TPM modul pro uložení certifikátů zajišťujících ověření identity AP
* Jednotlivá AP musí mít plnohodnotnou WIFI-Alliance certifikaci
* Součástí dodávky AP musí být instalační sada pro pevnou instalaci na zeď
* Integrovaný čip pro spektrální analýzu + integrované bluetooth
* Plná záruka na HW v délce 60 měsíců
* Dostupnost aktualizací a podpory po celou dobu udržitelnosti projektu (5 let)
* Minimálně pasivní zapojení do federovaného systému eduroam (www.eduroam.cz).
* Součástí dodávky bude návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů, fyzická montáž AP a konfigurace WiFi systému pro cca 90 uživatelů
* Bude konfigurován min. oddělený provoz pro pedagogický sbor, studenty a návštěvy.

**1x kabeláž a příslušenství k síťovým prvkům a WIFI**

* 1 ks 19” stojanový rozvaděč - skleněné dveře 30U 600x600 včetně příslušenství

- barva šedá  
- odnímatelné boky zamykatelné  
- přední dveře prosklené  
- zadní dveře plechové  
Příslušenství:  
- sety montážní sada M6  
- 1 police  
- 2 ventilátorová jednotka  
- 4 kolečka  
- 1 sada nožiček pod stojanové rozvaděče

* odhadovaná délka LAN kabelu UTP Cat5E – 1 200 m
* lišta 40x40 – 200 m
* 10x zásuvka RJ45 na zeď, Cat5E kompletní
* Dodávka, montáž a proměření UTP kabeláže