Příloha č. 1 – Technická specifikace

**Uchazeč zajistí, že:**

**Každý přístupový bod (AP):**

* umožní souběžné dvoupásmové (2,4Ghz – 5Ghz) připojení
* je určen pro vnitřní použití (indoor)
* má podpůrný cyklus delší než 5 let
* má střední dobu mezi poruchami (MTBF) alespoň 50 let
* má k dispozici samostatné a centralizované místo řízení u všech přístupových bodů sítě WiFi4EU (vysoce dostupné) včetně potřebných licencí min. pro 100 AP
* podporuje normu IEEE 802.1x
* vyhovuje normě IEEE 802.11ax
* podporuje normu IEEE 802.11r
* podporuje normu IEEE 802.11k
* podporuje normu IEEE 802.11v
* podporuje normu IEEE 802.3af (napájení po datovém síťovém kabelu)
* vyhovuje certifikaci Wi-Fi Aliance WPA3
* zvládá alespoň 50 souběžných uživatelů bez zhoršení výkonnosti
* má alespoň 2x2 MIMO
* vyhovuje normě Hotspot 2.0 (certifikační program Passpoint sdružení Wi-Fi Alliance)
* podporuje současné vysílání více bezdrátových sítí (SSID) – min. 16
* podporuje L2 izolaci bezdrátových klientů
* podporuje dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP

|  |  |  |  |
| --- | --- | --- | --- |
| **Umístění AP a switchů** | **Místní upřesnění** | **Počet AP** | **Počet switchů** |
| Poliklinika, Sakařova 755 | 1.PP | 1 |  |
|  | 1.NP | 4 | 1x 24p |
|  | 2.NP | 4 | 1x 24p |
|  | 3.NP | 4 |  |
| Sokolovna, Tyršova 424 | Foyer | 2 | 1x 8p |
| Městský úřad, nám. Míru 2 | 1.NP (za oknem) | 1 | 1x 8p |

**Celkem 16 ks 4 ks**

**Požadavky na switche:**

* Počet 1GE (RJ-45) portů podle typu 24x nebo 8x
* Počet nezávislých SFP portů podle typu min. 4x nebo 2x
* Podpora IEEE 802.3at PoE+
* Minimální počet aktivních VLAN 512
* Minimální počet záznamů v MAC adres tabulce 16 000
* Podpora MAC based VLAN
* IEEE 802.1s - Multiple spanning tree
* IEEE 802.1w - Rapid spanning Tree
* Podpora ověřování 802.1x
* Podpora zařazování do VLAN na základě 802.1x ověření
* Podpora mac-based ověřování
* Podpora IPv4 a IPv6 ACL per port a per VLAN
* Obsahuje sériovou nebo USB konzolovou linku
* Podporuje CLI, SSHv2, SMNP, RMON
* Podporuje dual flash image
* Podporuje RADIUS

**Požadavky na firewall:**

* Počet 1GE metalických síťových rozhraní (RJ45 10/100/1000) - min 4x
* Podpora IPv6 pro všechny funkce
* Výkonnost FW shodná pro IPv4 i IPv6
* Minimální závislost výkonu firewallu na velikosti paketů
* Propustnost FW (stavové filtrování, UDP paket) - min. 5Gbps
* Výkonnost FW na malých paketech (64B) nesmí klesnout pod 70% výkonnosti naměřené na velkých paketech
* Latence firewallu (64B UDP paket) - 4μs
* Počet naráz otevřených spojení - min 700k
* Počet nových spojení za sekundu - min. 30k
* Propustnost IPSEC VPN (512 B paket, AES256, SHA1) - min. 4Gbps
* Propustnost SSL VPN min 450Mbps
* Propustnost NGFW (IPS + App. control; traffic mix) – min. 750Mbps
* Propustnost IPS (měřeno na http komunikaci) – min 1Gbps
* Režim vysoké dostupnosti (L2 HA, tj. virtuální MAC adresy)
* Podpora L2 (transparentní) i L3 (NAT/Router) režimu
* Podpora multicast, včetně routování a firewall funkcí (tvorba multicast FW politiky)
* Podpora VPN: SSL (portálový režim, tunelový režim), IPSEC (IKE, manual key, certifikát, gateway to gateway, hub and spoke, dial up konfigurace, internet browsing konfigurace, podpora více tunelů – redundantní VPN, možnost VPN v L2 – transparentním režimu ukončená na management rozhraní, podpora IPv6, podpora dynamických routovací protokolů - OSPF), PPTP, L2TP, GRE
* Možnost nastavovat firewall politiku na základě geografických údajů
* Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace
* UTM funkce, možnost výběru mezi proxy režimem (buffer) nebo flow režimem (inspekce on-the-fly), zejména pro antivirovou/antimalware kontrolu
* Antivirová/antimalware kontrola pro vybrané protokoly, možnost volby různých databází (např. minimální, standardní a extrémní) kvůli optimalizai výkonnosti, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV engine, možnost detekce tzv. Grayware (rootkit, malware, spyware, keylogger, atd). Automatická aktualizace signatur ze strany výrobce po dobu udržitelnosti projektu.
* Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty. Aktualizace signatur ze strany výrobce po dobu udržitelnosti projektu.
* Intrusion Protection System – detekce útoků založena na signaturové kontrole a anomálním filtru. Automatická aktualizace signatur ze strany výrobce po dobu udržitelnosti projektu, možnost vytvářet vlastní signatury.
* Application control, tedy detekce aplikací bez ohledu na využívané porty. Možnost detekované aplikace monitorovat, blokovat, nebo omezit šířku pásma. Automatická aktualizace signatur ze strany výrobce po dobu udržitelnosti projektu. Možnost tvorby vlastních signatur.
* Web Filter – založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne. Automatická aktualizace signatur ze strany výrobce po dobu udržitelnosti projektu.
* SSL dekrypce/offload – možnost kontroly komunikace v SSL šifrovaných protokolech (HTTPS, IMAPS, POP3S,…)
* DoS Policy prevence proti základním útokům typu DoS, včetně syn proxy
* Ověřování uživatelů proti LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu, Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
* WAN optimalizace (optimalizace vybraných protokolů, byte caching), Web Cache, Reverzní proxy, WCCP
* Funkce Explicitní Proxy, včetně autentizace v síti MS AD protokolem Kerberos
* Podpora silné autentizace uživatelů – podpora pro generátor jednorázových hesel (OTP) – Token pro dvou faktorovou autentizaci, podpora certifikátů pro ověření uživatelů (možno jako interní součást FW nebo jako externí systém – např. RADIUS server)

**Požadavky na instalaci:**

Uchazeč zprovozní kompletní WI-FI síť tak, aby AP pokrývala WI-FI signálem dotčené prostory min. jednou sítí s názvem WiFi4EU s geografickým návěštím.

**Další požadavky po instalaci:**

Uchazeč po ukončení realizace vydá prohlášení o potvrzení na portálu WiFi4EU, že instalace bezdrátové sítě WI-FI byla dokončena v souladu s přílohou I v Grantové dohodě a síť je funkční.

Prohlášení musí u každé sítě WiFi4EU obsahovat: název sítě WiFi4EU (např.: radnice) a název domény. Kromě toho musí společnost zajišťující instalaci u každé sítě WiFi4EU poskytnout úplný seznam přístupových bodů. U každého přístupového bodu musí uvést tyto povinné údaje:

* druh umístění (např.: škola, park, metro). Portál WiFi4EU umožní výběr z předem daného seznamu.
* název umístění (např.: chodba)
* geolokalizační údaje přístupového bodu
* typ zařízení: vnitřní/venkovní
* značka zařízení
* model zařízení
* výrobní číslo zařízení
* adresa MAC (Medial Access Control)

Dále uchazeč zajišťující instalaci bezdrátové sítě WI-FI vydá Prohlášení příjemce na portálu WiFi4EU, kterým potvrdí, že instalace sítě nebo sítí WiFi4EU je v souladu s přílohou I a síť je funkční.

Veškeré požadavky jsou v souladu dle Grantové dohody, jejíž modelový vzor (Model Grant Agreement) je dostupný zde:

<https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/wifi4eu>

**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 a software min. s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
* Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.