**Příloha č. 1: Technická specifikace zařízení**

Poptávka zařízení typu Next-Generation Firewall funkčně doplňuje projekt budované Wi-Fi sítě pro objekty koleje UK, který je postupně implementován na základě **Rámcové smlouvy na dodávku LAN infrastruktury v prostorách kolejí UK a zajištění souvisejících služeb č. 725/RUK/2015** uzavřené dne 28.1.2016 na základě dříve realizované veřejné zakázky s číslem 512728. Účelem této veřejné zakázky je vybudování plně funkční Wi-Fi sítě s požadovanou úrovní pokrytí ve vybraných objektech zadavatele založené na centrální architektuře s plnou redundancí centrální Wi-Fi části.

V rámci tohoto projektu je postupně realizováno Wi-Fi pokrytí všech pokojů podle zadání Kolejí a Menz (KaM). Ubytovací kapacita KaM je přes 10.000 lůžek a při množství 3 Wi-Fi zařízení na ubytovaného plyne, že reálně může být v síti až 30 tisíc současně připojených zařízení. Budované řešení bude při plné implementaci (v případě instalace Wi-Fi ve všech zvažovaných objektech) schopné současně připojovat do WiFi sítě až 30 000 zařízení. Realizovaný projekt předpokládá, že ve Wi-Fi síti bude vysíláno SSID eduroam (WPA2/AES viz http://www.eduroam.cz). Pro hosty a návštěvníky, kteří nemají přihlašovací údaje do sítě eduroam, bude vysíláno otevřené SSID s ověřování ve web formuláři (captive portal).

Požadujeme dodání vysoce dostupného řešení firewall typu NGFW dle níže uvedené specifikace. Celá dodávka musí obsahovat všechny HW komponenty, licence, záruku a podporu výrobce na dobu 5 let v režimu NBD. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechna dodávaná zařízení/SW musí být určena pro používání v České republice a musí splňovat všechny podmínky stanovené českými normami pro takové používání. Uvedeny jsou minimální parametry.

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje ANO/NE** |
| **Základní vlastnosti** |  |  |
| Třída zařízení | HW appliance NGFW firewall (platforma postavená na HW akcelerované architektuře- tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí) umožňující konfiguraci v režimu vysoké dostupnosti |  |
| Formát zařízení | do racku 19“max 5RU, součástí dodávky je veškeré příslušenství pro montáž do racku |  |
| Počet portů 10 Gbit/s SFP+ pro zpracování komunikace | 8 |  |
| Počet portů 1/10 Gbit/s SFP/SFP+ nebo RJ45 pro management | 1 |  |
| Množství VLAN (802.1q) interface/sub interface | 100 |  |
| Redundantní napájecí zdroje 230V/50Hz s oddělenými přívody | ano |  |
| Výměna primárního i záložního zdroje za chodu zařízení | ano |  |
| Podpora režimu vysoké dostupnost (režim L2 cluster, tedy využití virtuálních MAC adres. Celý cluster se tváří z pohledu L3 jako jedno zařízení) v režimu active-passive (A/P) | Ano, po dokoupení licence |  |
| Funkce detekce aplikací na L7 (Application Control) | * detekce známých aplikací na základě signatur * signatury automaticky aktualizované výrobcem * minimálně aplikace typu P2P (bittorent) * možnost tvorby vlastních signatur * detekované aplikace je možné: povolit, monitorovat, blokovat * na základě typu aplikace je možné omezit šířku pásma pro danou aplikaci |  |
| **Výkonnostní parametry** |  |  |
| Požadovaná propustnost FW při rozpoznávání aplikací na L7 (Application Control) při současném zapnutí IPv4 NAT44, IPv6 routingu a logování NAT44 sessions přes NetFlow a do syslogu, | 15 Gbps v reálném provozu |  |
| Logování NAT44 sessions přes NetFlow a do syslogu | Ano |  |
| Propustnost při zapnutí Threat Prevention (kompletní ochrana) | 5 Gbps (měřeno na HTTP provozu) |  |
| Počet současných NAT44 session | 2 000 000 |  |
| **Servisní protokoly** |  |  |
| DNS klient | ano |  |
| NTP klient | ano |  |
|  |  |  |
| **Bezpečnost** |  |  |
| Podpora control plane policing (CoPP) nebo ekvivaletní řešení | ano |  |
| **Protokoly 3. Vrstvy** |  |  |
| IPv4 a IPv6 směrování | ano |  |
| Podpora IPv4 a IPv6 QoS | ano |  |
| Podpora ACL pro IPv4 a IPv6 pro plnou rychlost 10Gb/s full-duplex | ano |  |
| DHCP Relay pro IPv4 a IPv6 | ano |  |
| **Směrovací protokoly** |  |  |
| OSPFv2, OSPFv3 | ano |  |
| Statické směrování | ano |  |
| **Virtualizace** |  |  |
| Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). | 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) |  |
| **Management** |  |  |
| CLI rozhraní | ano |  |
| SSHv2 pro IPv4 a IPv6 | ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |  |
| Možnost definice administrátorů s různými přístupovými právy | ano |  |
| SNMP v2c a v3 | ano |  |
| Sériová nebo USB konzolová linka | ano |  |
| AAA ověřování uživatelů (autentizace, autorizace, accounting) – RADIUS | ano |  |