# 4. Splnění technických požadavků zadavatele

| Technické požadavky | Nabídka - splnění požadavku |
|---|---|
| **WI-FI Controller - 2ks** | **2ks [redacted] Cisco Catalyst [redacted] Wireless Controller_Fiber Uplink** |
| Kontroler bezdrátové sítě - primární a/nebo redundantní zařízení pro doplnění Mobility domény stávajících kontrolerů provozovaných Zadavatelem | Ano |
| Požadovaný formát zařízení | Ano |
| Minimální počet Ethernet portů per kontroler. | Ano |
| Aktivní 10m Twinax kabely pro všechny porty součástí dodávky | Ano |
| Minimální propustnost pro data Gb/s | Ano |
| Licence dle počtu nově pořizovaných AP, možnost upgradu až na minimálně 250 registrovaných AP | Ano |
| Podpora stávajících AP řady 1700/2700/18xx/2800, které má Zadavatel nasazeny ve své infrastruktuře, a nově pořizovaných AP | Ano |
| Minimální počet současně připojených klientů | Ano |
| Redundance na úrovni kontrolerů a jejich portů, výpadek aktivního kontroleru v redundantním páru nemá žádný dopad na provoz již připojených klientů (tj. bez potřeby reautentizace) | Ano |
| Lokální síť - možnost tunelování uživatelských dat z AP až na kontroler, možnost šifrování těchto uživatelských dat bez výrazného vlivu na propustnost | Ano |
| Mesh síť - podpora mesh sítí, současné připojení normálních a mesh AP k jednomu kontroleru | Ano |
| Vzdálené lokality - možnost lokálního bridgování uživatelských dat per SSID přímo na příslušném AP | Ano |
| Šifrovaná řídící komunikace AP-kontroler | Ano |
| Současná funkčnost AP pro přenos dat, analýzu spektra a detekci bezpečnostních incidentů | Ano |
| Bezpečnost a Guest Access | Ano |
| Podpora 802.11i, respektive jeho implementace WPA2 včetně enterprise variant autentizace/šifrování | Ano |
| Podpora WPA3 – WPA3 Enterprise, WPA3 SAE, WPA3 OWE | Ano |
| PSK autentizace vč. možnosti různých PSK klíčů pro různé klienty v rámci jednoho SSID | Ano |
| Podpora standardu „802.11w" pro ochranu řídících rámců na AP a klientovi | Ano |
| Podpora standardu „802.11u" pro výběr SSID a autentizaci klienta | Ano |
| Integrované řešení návštěvnického přístupu s možností webové autentizace (včetně nativních IPv6 klientů), bezpečné oddělení od zaměstnaneckého provozu, funkční i v módu lokálního bridgování uživatelských dat přímo na AP | Ano |
| Podpora řešení návštěvnického přístupu pro klienty bezdrátové i drátové sítě | Ano |

| | |
|---|---|
| Možnost omezit počet klientů per SSID | Ano |
| Lokální profilování zařízení – per uživatel a per zařízení | Ano |
| Podpora IPv6 | Ano |
| Podpora IPv6 – management kontroleru (vč. Syslog, radius) | Ano |
| Podpora IPv6 – komunikace AP-kontroler | Ano |
| Podpora IPv6 – Guest Access i pro nativní klienty vč. webové autentizace pro IPv6 klienty | Ano |
| Podpora IPv6 – IPv6 multicast, MLD snooping | Ano |
| Podpora IPv6 – bezpečnost (RA Guard, IPv6 Source Guard, DHCPv6 Server Guard, ACL) | Ano |
| Podpora IPv6 – ND cache na kontroleru, optimalizace přenosu ND zpráv, rate-limiting pro RA | Ano |
| Dohled a správa kontroleru, zabezpečení HW/SW | Ano |
| Centrální administrace správců s granularitou přístupových práv | Ano |
| Podpora správy přes serial CLI nebo přes IP pomocí SSH/telnet a https web GUI, SNMP | Ano |
| RJ45 konzolový port a/nebo USB konzolový port, dedikovaný ethernetový RJ45 management port | Ano |
| Podpora API rozhraní pro plnou konfiguraci kontroleru pomocí NETCONF, RESTCONF za použití YANG data modelů. Podpora exportu provozních dat z kontroleru. | Ano |
| Důvěryhodný HW/SW – kontroler používá bezpečný zavaděč OS, ověřování podpisu SW komponent, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům | Ano |
| Servisní podpora na 60 měsíců. | Ano |
| Výměna vadného dílu nebo zařízení do následujícího pracovního dne od ohlášení závady (8x5xNBD), včetně dopravy a dalších logistických služeb | Ano |
| Pomoc dodavatele při řešení konfiguračních a provozních problémů (8x5xNBD) nebo závad dodaného software, v případě potřeby s využitím služby technické podpory výrobce | Ano |
| Nárok na nové verze programového vybavení v rámci zakoupené licence | Ano |
| Plná podpora AP na poptávaném kontroleru | Ano |
| Zařízení musí pocházet z autorizovaného prodejního kanálu výrobce | Ano |
| Začlenení zařízení do současné infrastruktury nesmí kolidovat se současným řešením. | Ano |
| **Wi-Fi AP - 10 ks** | **Cisco Catalyst** [redacted] |
| WiFi-AP - 802.11 a,b,g,n,ac vzdálené napájení PoE možnost centrálního ovládání. | Ano |
| Access Point určený pro instalaci na strop/podhled | Ano |
| Typ antén | Ano |
| Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí | Ano |
| Podpora standardů 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax) | Ano |
| Podpora minimálně 2x2 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 80 MHz kanál pro 802.11ax | Ano |

| | |
|---|---|
| Minimální počet inzerovaných SSID (BSSID) per radio | Ano |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming) | Ano |
| Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma | Ano |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | Ano |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | Ano |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | Ano |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH | Ano |
| Podpora rozpoznání zdroje rušivého signálu podle signatur | Ano |
| Access Point obsahuje radio podporující BLE 5.0, ZigBee | Ano |
| 1 x 100/1000 Mbit/s RJ45 ethernet rozhraní | Ano |
| Možnost 802.3af/at PoE napájení AP z přepínače nebo injectoru – plná funkce AP při použití 802.3at | Ano |
| AP uzavřené konstrukce bez větracích otvorů a ventilátoru | Ano |
| Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu | Ano |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem. | Ano |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům | Ano |
| Servisní podpora na 60 měsíců. | Ano |
| Výměna vadného dílu nebo zařízení do následujícího pracovního dne od ohlášení závady (8x5xNBD), včetně dopravy a dalších logistických služeb | Ano |
| Pomoc dodavatele při řešení konfiguračních a provozních problémů (8x5xNBD) nebo závad dodaného software, v případě potřeby s využitím služby technické podpory výrobce | Ano |
| Nárok na nové verze programového vybavení v rámci zakoupené licence | Ano |
| Plná podpora AP na poptávaném kontroleru | Ano |
| Zařízení musí pocházet z autorizovaného prodejního kanálu výrobce | Ano |
| **Centrální switch - 1ks** | **[redacted]Cisco Catalyst[redacted] 24x1G/10G/25G SFP28 ports and 2 power supply slots; 4x40G/100G up link** |
| Typ přepínače L2/L3 přepínač | Ano |
| Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP28 24 | Ano |
| Uplink porty 4x100GE QSFP28 | Ano |
| Interní redundantní napájecí zdroj ANO | Ano |

| | |
|---|---|
| Min. velikost sdíleného systémového bufferu 36MB | Ano |
| Velikost MAC address tabulky 80000 | Ano |
| Min. počet IPv4 routes 200000 | Ano |
| Min. počet IPv6 routes 200000 | Ano |
| Min. počet konfigurovatelných security ACL 27000 | Ano |
| Flexibilní alokace SRAM a TCAM zdrojů | Ano |
| IEEE 802.3ad (Link Aggregation - LAG) | Ano |
| Minimální počet aktivních VLAN | Ano |
| IEEE 802.1w - Rapid Spanning Tree Protocol | Ano |
| Podpora instance spanning-tree protokolu per VLAN 4000 | Ano |
| Podpora jumbo rámců (min. 9216 bytes) | Ano |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | Ano |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | Ano |
| OSPFv2, OSPFv3 | Ano |
| ISIS | Ano |
| BGPv4 | Ano |
| IP Multicast (PIM SSM, PIM SM) | Ano |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | Ano |
| Min. počet oddělených (nezávislých) směrovacích tabulek 10 | Ano |
| MPLS VPN | Ano |
| MPLS VPN - 6VPE | Ano |
| First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6 | Ano |
| Reverse path check (uRPF) | Ano |
| Minimální počet HW QoS front 8 | Ano |
| QoS - Strict Priority Queue | Ano |
| QoS classification – ACL, DSCP, CoS based | Ano |
| QoS marking - DSCP, CoS | Ano |
| QoS Policing | Ano |
| QoS-Hierarchical QoS | Ano |
| IPv6 First Hop Security (RA guard, DHCPv6 guard, IPv6 source guard) | Ano |
| Port ACL, VLAN ACL | Ano |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | Ano |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | Ano |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | Ano |
| Podpora SUDI (IEEE 802.1AR) autentizace | Ano |
| IPv6 Port ACL, VLAN ACL | Ano |
| IEEE 802.1AE na všech portech | Ano |
| IEEE 802.1ae (AES-GCM-256) na všech portech | Ano |
| Source-Group Tag Exchange Protocol nebo ekvivalentní | Ano |

| | |
|---|---|
| IGMPv2/v3 snooping | Ano |
| MLD snooping | Ano |
| Multicast DNS (mDNS) gateway | Ano |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | Ano |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type | Ano |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Ano |
| SSHv2 | Ano |
| CLI rozhraní | Ano |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | Ano |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | Ano |
| Python scripting | Ano |
| Linux shell | Ano |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | Ano |
| Application hosting | Ano |
| Streaming telemetrie prostřednictvím NETCONF/XML | Ano |
| SNMPv2/v3 | Ano |
| Inventarizovatelnost komponent integrovanou RFID identifikací | Ano |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | Ano |
| Vzdálený port mirroring (ERSPAN) | Ano |
| NTPv3 server | Ano |
| Servisní podpora na 60 měsíců. | Ano |
| Výměna vadného dílu nebo zařízení do následujícího pracovního dne od ohlášení závady (8x5xNBD), včetně dopravy a dalších logistických služeb | Ano |
| Pomoc dodavatele při řešení konfiguračních a provozních problémů (8x5xNBD) nebo závad dodaného software, v případě potřeby s využitím služby technické podpory výrobce | Ano |
| Nárok na nové verze programového vybavení v rámci zakoupené licence | Ano |
| Plná podpora AP na poptávaném kontroleru | Ano |
| Zařízení musí pocházet z autorizovaného prodejního kanálu výrobce | Ano |
| **Materiál nezbytný pro instalaci** | |
| Materiál nezbytný pro úplné zprovoznění ( ochrana sváru, Pigtail, patch cord atd.) | Ano |
| optický kabel 8 vl, singlemode (SM)E9 /125 (cca 500m) | Ano |
| kabeláž ukončená RJ45 stíněná alespon AWG24 cat6A (3000m) | Ano |

| **Firewall** | **Fortinet FG400E 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 16 x GE SFP slots, SPU NP6 and CP9 hardware accelerated, Licence, Enterprise Protection + FortiCare Premium 3YR** |
|---|---|
| Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, akcelerace IPsec VPN, porovnávání se signaturovou databází, ...) | Ano |
| Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 3 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány. | Ano |
| Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1RU | Ano |
| Řešení bude dodáno v režimu vysoké dostupnosti (HA), včetně všech případných potřebných licencích. | Ano |
| Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu | Ano |
| Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem. | Ano |
| Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality | Ano |
| **HW parametry** | |
| Počet síťových rozhraní copper, RJ45 10/100/1000 - min 16x | Ano |
| Počet síťových rozhraní optických, GE SFP – min 16x | Ano |
| Dedikovaný port pro management – min 1x | Ano |
| Dedikovaný konzolový port – min 1x | Ano |
| Dedikovaný port pro heartbeat při zapojení do režimu cluster – min 1x | Ano |
| Možnost rozšíření o záložní napájecí zdroj pro redundantní zapojení, vyměnitelný za chodu bez nutnosti vypnutí systému (hot swappable) | Ano |
| USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min 2x | Ano |
| **Výkonnostní parametry** | |
| Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B – min. 31 Gbps, 31 Gbps, 19 Gbps | Ano |
| Latence firewallu (64 B UDP paket) – max 4.78 mikro sec | Ano |

| | |
|---|---|
| Počet naráz otevřených spojení – min. 3 000 000 | Ano |
| Počet nových spojení za sekundu – min. 280 000 | Ano |
| Propustnost IPSEC VPN (512 B paket) - min. 13 Gbps | Ano |
| Propustnost SSL VPN min 2 Gbps | Ano |
| Propustnost SSL inspekce – min. 3,7 Gbps | Ano |
| Propustnost IPS (enterprise mix včetně logování) - min 4,8 Gbps | Ano |
| Propustnost AV – min 2,8 Gbps | Ano |
| Podpora virtuallizace (min 10 virtuálních kontextů) | Ano |
| Podpora funkce bezdrátový kontrolér s až min. 256 AP | Ano |
| Podpora přímé integrace hw switchů – min. 64 | Ano |
| **Networking a Vysoká dostupnost (HA)** | |
| Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru | Ano |
| HA musí podporovat až 4 nódy v HA režimu | Ano |
| Režim fungování L2 – transparentní režim, L3 – NAT/Router | Ano |
| Podpora VLAN | Ano |
| Podopora multicast, vytváření politiky pro multicast routování | Ano |
| Podpora 802.3ad link aggregation | Ano |
| Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading | Ano |
| Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace | Ano |
| Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP | Ano |
| Policy-based routing | Ano |
| Podpora uplatňování základních pravidel pro kontrolu na přístupové vrstvě (NAC pravidla, politiky) | Ano |
| Zařízení musí podporovat možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky (SD-WAN). | Ano |
| Funkce SD-WAN nesmí být licenčně omezeno. V rámci nabízeného řešení musí být dodáno v podobě, jenž umožňuje neomezené využívání i v případě, že dojde k nárůstu počtů zařízeních komunikující skrze SW-WAN do internetu, tak i v případě, že dojde k navýšení počtu konektivit a jejich rychlosti. | Ano |
| Integrované SD-WAN řešení musí podporovat podle dokumentace výrobce min. 500 členů virtuálního rozhraní, které sdružuje konektivitu a jsou na něj uplatněna pravidla provozu a routingu. | Ano |
| **Funkce SSL VPN** | |
| Nabízené řešení musí podporovat možnost připojení klientů do VPN pomocí proprietární SSL VPN. Aplikace pro do VPN musí být podporována nejběžnějšími operačními systémy, jako například: Windows, macOS, Linux, Android nebo iOS. | Ano |

| | |
|---|---|
| Podpora bez klientského připojení do VPN na úrovni webového portálu, pomocí standardního internetového prohlížeče. | Ano |
| Možnost zabezpečení připojení do VPN vynucením dvou faktorového ověření. Například pomocí emailu, SMS, hardwarovou klíčenkou, nebo proprietární aplikace dostupné pro Android i iOS. | Ano |
| Zařízení musí umožňovat rozšíření až na 4800 možných licencí pro využití dostupného dvou faktorového ověření | Ano |
| Zařízení musí být dodáno s min. 2 licencemi pro případné vyzkoušení dvou faktorového ověření | Ano |
| Vynucení ověření klientského certifikátu pro zvýšení zabezpečení. | Ano |
| Minimální počet současně navázaných SSL VPN tunelů: 1000 | Ano |
| Minimální propustnost SSL VPN: 2Gbps | Ano |
| **Funkce IPsec VPN** | |
| podpora site-to-site VPN | Ano |
| podpora klientských VPN | Ano |
| dostupnost VPN klienta pro koncové stanice (Windows, MacOS) z veřejně dostupných webových stránek | Ano |
| funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence. | Ano |
| Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1 800 | Ano |
| Minimální počet klientských IPSEC VPN tunelů: 16 000 | Ano |
| propustnost IPSec VPN min. 13 Gbps (měřeno při AES256-SHA256) | Ano |
| podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování | Ano |
| podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování | Ano |
| podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace | Ano |
| Podpora VXLAN | Ano |
| Podpora L2TP, PPTP, GRE | Ano |
| podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec | Ano |
| **UTM funkce** | |
| **Funkce detekce aplikací na L7 (Application Control)** | |
| detekce známých aplikací na základě signatur | Ano |
| signaturové database automaticky aktualizované výrobcem | Ano |
| alespoň 4 000 podporovaných aplikací | Ano |
| pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci) | Ano |
| možnost tvorby vlastních signatur | Ano |
| detekované aplikace je možné: povolit, monitorovat, blokovat | Ano |

| | |
|---|---|
| na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci | Ano |
| funkce detekce aplikací se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše. | Ano |
| **Funkce detekce a potlačení narušení (IPS/IDS)** | |
| signatury automaticky aktualizované výrobcem | Ano |
| alespoň 11 000 rozpoznávaných hrozeb (signatur) definovaných výrobcem | Ano |
| možnost tvorby vlastních signatur | Ano |
| funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům | Ano |
| funkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu | Ano |
| **Funkce antivirové kontroly** | |
| ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem | Ano |
| signatury automaticky aktualizované výrobcem | Ano |
| požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky) | Ano |
| možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce | Ano |
| deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 900 Mbps | Ano |
| funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. | Ano |
| Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů | Ano |
| Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací. | Ano |
| **Funkce kategorizace webových stránek** | |
| založená na centrálně spravované databázi výrobce | Ano |
| minimálně 50 filtračních kategorií | Ano |
| možnost definice vlastních kategorií | Ano |
| možnost definice vlastních seznamů zakázaných URL | Ano |
| kategorizace musí zahrnovat I české a slovenské internetové stránky | Ano |
| **Funkce DNS filtru** | |
| Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu) | Ano |
| Možnost definovat vlastní tzv. deny-list domén | Ano |
| Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL | Ano |
| Možnost importu seznamu blokovaných domén do DNS filtru | Ano |

| | |
|---|---|
| Detekce a blokování komunikace do botnet sítí | Ano |
| **Funkce ochrany před únikem citlivých informací (DLP)** | |
| možností analýzy běžných typů dokumentů a protokolů | Ano |
| možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum | Ano |
| **Funkce blokace stahování konkrétních typů souborů** | |
| možnosti zablokovat stahování souborů s konkrétními typy, jako napři. MSI, EXE... | Ano |
| funkce blokace stahování konkrétních typů souborů se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. | Ano |
| **Emailový antispamový modul** | |
| jednoduchá antispamová a antivirová inspekce elektronické pošty | Ano |
| **Podpora SSL dekrypce** | |
| podpora SSL dekrypce a inspekce pro ochranu jak koncových zařízeních, nebo serverů | Ano |
| funkce SSL dekrypce se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. | Ano |
| zařízení musí u SSL inspekce dosáhnout min. propustnost 3,6 Gbps | Ano |
| **Podpora pravidel pro obranu proti útokům typu DoS** | |
| zařízení musí umožnit uplatnit pravidla proti DoS útokům na základě politik, které se aplikují na konkrétní interface zařízení. | Ano |
| podpora detekce anomálií na 3. a 4. vrstvě | Ano |
| podpora např. TCP SYN FLOOD, ICMP FLOOD, SCTP SRC SESSION | Ano |
| funkce musí umožňovat provoz nejen blokovat, ale i sledovat pro možnost orientace na síti | Ano |
| **Explicitní proxy** | |
| podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP) | Ano |
| podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos | Ano |
| funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta | Ano |
| Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru | Ano |
| **Integrovaný bezpečnostní asistent** | |
| Dodávané řešení musí být dodáno s licencemi umožňujícími využití služby bezpečnostního asistenta, jenž umí monitorovat nastavení firewallu a doporučovat vhodné akce k nápravě a posílení bezpečnosti | Ano |
| Bezpečnostní asistent musí být dostupný výhradně z GUI firewallu | Ano |
| Kromě doporučované akce musí být bezpečnostní asistent schopen akce k nápravě aplikovat sám na základně jednoduchého příkazu z GUI | Ano |

| **Podpora ochrany industriálních zařízení** | |
|---|---|
| Zařízení musí být dodáno s licencemi umožňujícími využít pro ochranu na síti bezpečnostní signatury industriálních zařízeních | Ano |
| Musí být podporovány protokoly min. ICS a SCADA | Ano |
| **Detekce IoT zařízení** | |
| Zařízení musí být dodáno s licencemi umožňujícími pokročilou detekci IoT zařízení | Ano |
| Na základě politik musí být definována automatizace přiřazení zařízení do dostupných VLAN skrze integrovaný switch výrobce | Ano |
| **Funkce migrace firewallu** | |
| Zařízení musí být dodáno s licencemi umožňujícími využití chytré migrační služby, jenž pomůže při migraci ze starší platformy výrobce | Ano |
| Kromě podpory platformy výrobce nástroj musí nástroj podporovat také výrobce třetích stran | Ano |
| **Firewall** | |
| Možnost nastavovat firewall politiku na základě geografických údajů | Ano |
| Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem | Ano |
| Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud | Ano |
| Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru | Ano |
| Viditelnost do provozu na aplikační úrovni | Ano |
| Možnost dynamického stahování externích seznamů IP adres a jejich následné použití ve firewall policy | Ano |
| Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo). | Ano |
| Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu | Ano |
| Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. | Ano |
| Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii | Ano |
| Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu | Ano |
| Podpora funkce reverzní proxy | Ano |
| Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů | Ano |
| Administrátorské účty mohou být volitelně zabezpečený pomocí dvou faktorového ověření | Ano |
| **Integrovaný kontroler bezdrátových sítí (WiFi)** | |

| | |
|---|---|
| Wifi kontroler integrovaný do NGFW platformy | Ano |
| Bezdrátová síť (SSID) může být reprezentována virtuálním síťovým rozhraním – provoz tunelován z AP do kontroleru | Ano |
| podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi kontroleru | Ano |
| podpora SSL dekrypce uživatelského provozu přímo na wifi kontroleru | Ano |
| Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení | Ano |
| Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor, WiFi 6) | Ano |
| Podpora BSS Coloring | Ano |
| On-wire rogue AP detekce a mitigace | Ano |
| Podpora fast-roamingu (802.11 k,v,r) | Ano |
| podpora více PSK u jednoho SSID | Ano |
| podpora IPSEC tunelu pro šifrování data plane (uživatelských dat) | Ano |
| Podpora WPA3 protokolu | Ano |
| **Integrovaný switch kontroler** | |
| Zařízení musí podporovat switch kontroler jenž umožní spravovat switche výrobce z jednoduchého GUI | Ano |
| Možnost správy VLAN | Ano |
| Spolu s NAC politikami musí nabídnout možnost automatické přiřazení VLAN pro konkrétní zařízení či skupinu zařízeních | Ano |
| Z integrovaného switch kontroleru musí být obsluha schopna pomocí GUI jednoduše definovat VLAN na konkrétní port | Ano |
| V případě správy switche s funkcí PoE musí být v GUI možnost resetování PoE pro vzdálený restart zařízení | Ano |
| **Multi-tenance (virtualizace)** | |
| Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů atp. | Ano |
| Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) | Ano |
| Každý virtuální kontext je zároveň samostatným wifi kontrolerem | Ano |
| Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů) | Ano |
| **Management** | |
| FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici | Ano |
| Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě | Ano |

| | |
|---|---|
| Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury) | Ano |
| **Další požadavky** | |
| Požadavky – komplexní služby spojené s instalací - tj. dodávka "na klíč" | Ano |
| Součástí dodávky bude instalace a nastavení v místě zákazníka včetně začlenění do stávající infrastruktury. | Ano |
| Ověření a otestování veškerých funkcí | Ano |
| Provedení testu HA (zkušební výpadek) | Ano |
| Provozní dohled po dobu minimálně 14 dní od převedení nové infrastruktury do ostrého provozu | Ano |
| Zaškolení obsluhy min. 8 hod. | Ano |
| Zajištění klientské podpory - není - li výše stanoveno jinak - po dobu 60ti měsíců v režimu 24/7 prosgřednictvím telefonu, emailu a dálkové podpory s reakční dobou 2 hodiny a s povinností odstranit kritickou závadu nejpozději do 4 hodin od nahlášení (za kritickou závadu se považuje závada bránící provozu datové sítě nebo takový provopz přímo ohrožující), v ostatních případech v limitu NBD. | Ano |

**OBLASTNÍ NEMOCNICE PŘÍBRAM, a. s.**

Příloha č. 2
Kupní smlouvy

*Dodavatel vyplní všechny údaje kromě výrobního čísla a přiloží ve své nabídce k návrhu smlouvy. Kompletně vyplněný formulář bude dodavatelem předložen při předání předmětu plnění, přejímatel potvrdí správnost údajů. Po převzetí je formulář postoupen Odboru zdravotnické techniky.*

**Dodáno na základě Kupní smlouvy č.....** **Příloha č. ...**

**Za přejímatele:** Datum převzetí: Inventární úsek: Nákladové středisko:

| Název přístroje | Výrobce | Typ | Výrobní číslo | Třída zdr. prostředku[1] | Perioda PBTK/ revize/ validace[2] | Protokol platné PBTK/ revize/ validace[3] | Návod v ČJ[4] | Prohlášení o shodě[5] | Instruktáž[6] |
|---|---|---|---|---|---|---|---|---|---|
| [redacted] Cisco Catalyst 9[redacted] Wireless Controller_Fiber Uplink | CISCO | [redacted] | | Ne | Ne | NE | ANO | ANO | ANO |
| Access point Cisco Catalyst [redacted] | CISCO | | | Ne | Ne | NE | ANO | ANO | ANO |
| [redacted] Cisco Catalyst [redacted] 24x1G/10G/25G SFP28 ports and 2 power supply slots; 4x40G/100G up link | CISCO | | | Ne | Ne | NE | ANO | ANO | ANO |
| Fortinet [redacted], icence, Enterprise Protection + FortiCare Premium 3YR | Fortinet | | | Ne | Ne | NE | ANO | ANO | ANO |

Za dodavatele (datum, jméno, podpis, razítko): Za přejímatele (jméno, podpis, razítko pracoviště):

[1] Dle Nařízení vlády č. 54/2015 Sb.

[2] Pravidelná bezpečnostně technická kontrola (PBTK) – tzn. revize/kalibrace/validace/ZDS dle předpisu výrobce a dle §65, §67 a §68 zákona č. 268/2014 Sb., o zdravotnických prostředcích v platném znění. Není-li předepsána, prosíme tuto skutečnost uvést.

[3] Vyplňujte pouze u zdravotnických prostředků, které byly již někdy použity i u jiného poskytovatele zdravotních služeb, např. výpůjčka, dodávka demoverze, dar apod. Vyplňte prosím ANO/NE.

[4] Vyplňte prosím ANO/NE.

[5] Vyplňte prosím ANO/NE.

[6] Instruktáž (u aktivních zdravotnických prostředků třídy IIb a III, AIZP a tam, kde to stanovuje výrobce) dle §61 zákona č. 268/2014 Sb., o zdravotnických prostředcích

**Povinnosti při připojování zařízení do LAN sítě Oblastní nemocnice Příbram,a.s. (dále jen „ONP“)**

1. Připojení každého zařízení do LAN sítě „ONP“ musí být předem konzultováno s Úsekem Informatiky ICT. Info na telefonu [redacted]
2. Instalace a provozování jakéhokoli software v síti ONP musí být předem konzultováno s Úsekem Informatiky „ONPB““. Info na telefonu [redacted]
3. Je zakázáno svévolně zapojovat zařízení do LAN sítě a jakkoli měnit LAN síť „ONP““.
4. Je zakázáno měnit, instalovat a nahrávat jakýkoli softwarový obsah na zařízení „ONP““.
5. Je zakázáno jakýmkoli způsobem měnit a zasahovat do hardware vybavení „ONP““.
6. Je zakázáno využívat pro vzdálený přístup na připojovaná zařízení jiných než Úsekem Informatiky „ONP“ schválených metod - viz níže.
7. Při umisťování IT zařízení (server, PC) do sítě „ONP“ je vlastník IT zařízení povinen na své náklady, pokud není ve smlouvě uvedeno jinak, udržovat toto zařízení v aktuálním (aktualizace operačního systému, aktualizace antivirového programu) a bezpečném (nemožnost jednoduše zneužít, používání silných přístupových hesel...) stavu. Úsek Informatiky provádí náhodné testy zneužitelnosti zařízení. Vlastník IT zařízení je povinen na své náklady, pokud není ve smlouvě uvedeno jinak, případné zjištěné hrozby a nedostatky neprodleně odstranit.
8. Vlastník IT zařízení je povinen, na vyžádání Úseku Informatiky, předložit ke kontrole konfiguraci IT zařízení.V situaci, kdy připojené zařízení způsobuje vážné bezpečnostní a nebo technické problémy v síti „ONP““, má „ONP“ možnost takovéto zařízení bez předchozího upozornění odpojit od sítě „ONP“.