**Technická zpráva**

Realizace datových rozvodů a řešení WiFi bezdrátové komunikace a Firewallu

ZŠ Mánesova, Mánesova 908, 765 02 Otrokovice

Při budování kabelových tras pro přístupové body bude využito i stávajících tras kabelových rozvodů a instalovaných datových rozvaděčů. U nových tras je požadována instalace lišt větších rozměrů pro vybudování tras s dostatečnou rezervou, stejně jako dostatečně velké průrazy pro případné další využití.

Pro instalaci metalických rozvodů je počítáno s kabelem minimálně kategorie 6. Napájení přístupových bodů bude realizováno přes PoE switche, které musí mít dostatečnou rezervu napájecího výkonu pro připojení dalších zařízení.

Všechna instalovaná zařízení, rozvody i jejich jednotlivé části musí splňovat platné normy a předpisy a všechny požadavky na aktuální legislativu ČR.

**1. Obecné technické požadavky na řešení:**

1. **Strukturovaná kabeláž**

V objektu ZŠ Mánesova (SO01 Hlavní budova a SO01 Přístavba) v Otrokovicích bude provedena instalace strukturované kabeláže pro WiFi (AccessPointy). Celý systém jako celek bude proveden v souladu s normami ČSN 50173 a ČSN 50174.

Jednotlivé koncové datové zásuvky (1xRJ 45) instalované na povrch z vytipovaných pozic pro WiFi (AccessPointy) pak budou "hvězdicovitě" připojeny do datového rozváděče objektu SO01 hlavní budova a SO02 přístavba. Při realizaci je nutno dodržet maximální délku segmentu 90m. Přesné rozmístění zásuvek pro WiFi (AccessPointy) je určeno na základě měření signálu. WiFi (AccessPointy) budou připojeny do zásuvek patch cordem UTP cat.6.

Celá instalace bude provedena twistovaným kabelem UTP Cat.6. Kabeláž bude vedena v chodbách pomocí stávajícího drátěného kabelového žlabu na povrchu a pomocí nově instalovaných elektroinstalačních vkládacích lišt na povrchu, v jednotlivých místnostech budou kabely vedeny v elektroinstalačních vkládacích lištách na povrchu.

Datové kabely budou ukončeny na jedné straně v datových zásuvkách 1x RJ45 Cat.6., na straně druhé budou datové kabely ukončeny v datovém rozváděči na PATCH panelech 24xRJ45 Cat.6, UTP. Jednotlivé porty v RACK rozváděči a na datových zásuvkách budou označeny pomocí popisných štítků a značení portů v datovém rozváděči musí přesně odpovídat označení na datových zásuvkách. Pro organizaci kabeláže v RACK rozváděči budou instalovány vyvazovací panely.

Po dokončení celé instalace bude provedeno měření metalické i optické kabeláže včetně vyhotovení měřících protokolů.

Měřící protokoly každého metalického kabelu budou obsahovat:

• Wire map - mapa zapojení

• Lenght [m] – délka

• Propagation Delay[ns] - zpoždění šíření signálu

• Delay Skew [ns] - diferenciální zpoždění na párech

• Rezistance [Ω] – reálný odpor jednotlivých párů

• Insertion Lost [dB] - ztráta na vstupu

• NEXT (Near-End Crosstalk [dB]) - přeslech na blízkém konci mezi jednotlivými páry

• PSNEXT (Power Sum Near-End Crosstalk [dB]) - přeslech na blízkém konci, tři páry vůči jednomu - je vypočítán z kombinace NEXT hodnot.

• ACR (Attenuation to Crosstalk Ratio [dB]) – odstup signál-šum mezi jednotlivými páry na obou stranách páru

• PSACR (Power Sum Attenuation to Crosstalk Ratio [dB]) – odstup signál šum, tři páry vůči jednomu na obou stranách páru

• RL (Return Loss [dB]) – zpětný odraz

Měřící protokoly každého optického vlákna budou obsahovat:

• Celkový útlum trasy a délka trasy dle ISO 11801

Prostupy rozvodů:

Součástí předávky dokumentace skutečného provedení bude kompletní kniha požárních ucpávek. Podle čl. 6.2.1 ČSN 73 0810 prostupy rozvodů a instalací požárně dělícími konstrukcemi musí být požárně utěsněny v souladu s ČSN 73 0810 kapitola 6.2 a musí splňovat podmínky požární odolnosti klasifikace podle ČSN EN 13501-2 a požadavků podle ČSN EN 1366-3. Prostupy elektrických rozvodů (kabelů, vodičů) mají být navrženy tak, aby co nejméně prostupovaly požárně dělícími konstrukcemi. Konstrukce, ve kterých se vyskytují tyto prostupy, musí být dotaženy až k vnějším povrchům prostupujících zařízení a to ve stejné skladbě a se stejnou požární odolností jakou má požárně dělící konstrukce. Požárně dělící konstrukce může být případně i zaměněna (nebo upravena) v dotahované části k vnějším povrchům prostupů za předpokladu, že nedojde ke snížení požární odolnosti a ani ke změně druhu konstrukce. Pokud však skladba požárně dělící konstrukce nezaručuje požární utěsnění prostupujících rozvodů a instalací, musí být bez ohledu na použitý materiál prostupujících zařízení a jejich rozměry (např. průřezovou plochu) zajištěno utěsnění podle ČSN EN 13501-2 (obdobně jako podle 6.2.2 ČSN 73 0810 – viz. dále). Podle čl. 6.2.2 ČSN 73 0810 u dále uvedených prostupů požárně dělícími konstrukcemi se kromě úpravy podle čl. 6.2.1 ČSN 73 0810 zabraňuje šíření požáru hmotou (výrobkem) nebo jiného prostupujícího zařízení. Toto těsnění prostupů se zajišťuje pomocí manžet, tmelů a jiných výrobků (dále jen manžet), jejichž požární odolnost EI je určena požadovanou odolností požárně dělící konstrukce, za postačující se považuje odolnost do 90 minut; těsnění prostupů se hodnotí podle ČSN EN 13501-2, a to v případě kabelových a jiných elektrických rozvodů tvořených svazkem vodičů (prostupující jedním otvorem) s izolací šířící požár o celkové hmotnosti větší než 1kg/m. Prostupy realizované podle čl. 6.2.2 ČSN 73 0810 musí být zřetelně označeny štítkem s informacemi o požární odolnosti, druhu nebo typu ucpávky, datu provedení, firmě, adrese a jméně zhotovitele, označení výrobce systému (podle vyhlášky MV ČR č.23/2008 §9 odstavec 6). Stávající prostupy musí být opraveny. Nové prostupy mezi požárními úseky musí být utěsněny.

|  |  |  |
| --- | --- | --- |
| Popis položky | Počet | MJ |
| zapojení konektoru UTP | 68 | ks |
| instalace lišt ,kabeláže,průrazy, | 1 | ks |
| instalace AP | 34 | ks |
| vyvázání rozvaděče | 3 | ks |
| instalace Patch panelu | 3 | ks |
| spojovací a spotřební materiál | 1 | ks |
| proměření zapojení CAT6 + protokoly | 34 | ks |
| přeprava mater. a osob | 1 | ks |
| zásuvka na omítku 1xRJ45 CAT 6 | 34 | ks |
| instalace zásuvky | 34 | m |
| patch panel 24port RJ45 CAT 6 prázdný | 3 | ks |
| patch cord organizer | 3 | ks |
| UTP kabel CAT 6 | 2500 | ks |
| elektroinstalační lišta 20/20 | 70 | m |
| elektroinstalační lišta 40/40 | 150 | m |
| elektroinstalační lišta 70/40 | 30 | m |
| keystone CAT6 samořezný | 68 | ks |
| proměření optiky + protokoly | 4 | ks |
| požární ucpávka /90min | 3 | ks |
| rozvodný panel s přepět. ochr. 230V/5x | 2 | ks |
| patch kabel CAT6 2m | 38 | ks |
| patch kabel CAT6 0,5m | 34 | ks |
| provozní vlivy a vedlejší náklady | 1 | ks |

1. **Bezdrátová síť**

• Bezdrátová síť bude sloužit pro připojení žáků, zaměstnanců a externích hostů, konektivita bude zajištěna v pásmech 2,4 a 5GHz současně.

• Je požadovaná vysoká dostupnost a škálovatelnost, řešení musí umožňovat současné připojení bezdrátových zařízení v řádu stovek až tisíců, systém musí být možno rozšiřovat bez nutnosti výměny centrálních řídících prvků.

• Jsou požadovány vnitřní přístupové body s podporou standardu IEEE 802.11ax/ Wi-Fi 6, každý přístupový bod umožňuje obsloužit minimálně 50 aktivních klientů stahujících data.

• Inteligentní provoz v prostředí s vysokou hustotou klientů, tzn. dynamické vyvažování zátěže klientů mezi Acces Pointu (AP) a pásmy 2,4 a 5GHz.

• Současný provoz více SSID včetně odlišných autentizačních a QoS politik. Podpora VLAN Pooling pro distribuci Wi-Fi provozu do LAN a využívání VLAN pro oddělení jednotlivých bezpečnostních zón.

• Současný provoz více SSID s různým nastavením ověřením (AAA) a zabezpečení provozu. Vyžadována je podpora WPA2-Enterprise, PSK, Open a Web (Captive portál) autentizace, Možnost filtrování na základě seznamu MAC adres.

• Schopnost rozpoznávat aplikace na základě DPI a možnost omezit přenosové pásmo na uživatele a zvolenou aplikaci. Možnost definice odlišných a unikátním filtrovacích pravidel na každého uživatele v rámci jednoho SSID. Oddělení bezdrátového provozu s možností filtrovat komunikaci jak dle IP, tak podle aplikací.

• Dalším požadavkem je podpora plynulého roamingu a zohlednění možnosti budoucího využití Wi-Fi pro hlasový provoz VoWiFi, tzn. klasifikace VoIP provozu a možnost aplikace rozdílných QoS profilů na jednotlivé třídy provozu.

• Z důvodu vyšší propustnosti je požadována možnost využití SingleSSID, kdy je do prostředí vysíláno minimálního množství SSID a tím i minimální množství servisních rámců. Systém musí umožňovat aplikovat na každého bezdrátového klienta nejen rozdílnou VLANu, ale i aplikační pravidla a QoS (např. pro omezení rychlosti).

• Podpora spektrální analýzy pro detekci RF rušení nepocházející z 802.11b/g/n/ac sítí.

• Požadavek na web content filtering (dle URL, podle IP, podle web obsahu, podle typu provozu).

• Centrální monitoring a management nástroj s možností uchování dlouhodobých statistik např. pro účely řešení bezpečnostních incidentů.

1. **AAA platforma**

• AAA platforma bude primárně sloužit k řízení přístupu uživatelů do dodávané bezdrátové sítě a dále pak pro řízení přístupu do lokální drátové sítě.

• Systém musí být plně kompatibilní s dodávanými

• Systém bude dodán jako řešení s vysokou dostupností (High Availability - HA řešení - redundantní cluster), který může být instalován do virtuálního prostředí zadavatele (VMware).

**Pokročilé AP – Specifikace požadavků v počtu 1 ks včetně podpory a potřebného SW na 5 let**

|  |  |
| --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** |
| **Základní vlastnosti** |  |
| Třída zařízení: indoor přístupový bod | ano |
| Uzavřená konstrukce bez ventilátorů | ano |
| Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax | ano |
| Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac | ano |
| Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE | ano |
| Pracovní režim AP bez kontroléru (autonomní) | ano |
| Pracovní režim AP řízené kontrolérem (lightweight) | ano |
| Pracovní režim AP v roli kontroléru s možností správy až 120 AP | ano |
| Minimální počet portů ethernet LAN: 2x 100/1000 Mbit/s RJ45 | ano |
| Podpora muligigabit ethernet 2.5 Gbps IEEE 802.3bz | ano |
| Podpora standardů IEEE 802.3af (PoE), IEEE 802.3at (PoE+) a IEEE 802.3bt | ano |
| Podpora linkové agregace LACP | ano |
| Podpora standardního PoE+ IEEE 802.3at 30W bez nutnosti redukce výkonu libovolného rádia | ano |
| Podpora napájení z AC napájecího zdroje | ano |
| Vestavěná interní anténa MIMO, omni down-tilt | ano |
| Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz | ano |
| MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2 | ano |
| MIMO a počet nezávislých streamů na 5GHz rádio: 4x4:4 | ano |
| Podpora šířky kanálu 160 MHz | ano |
| Podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO | ano |
| Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP | ano |
| Možnost nastavení vysílacího výkonu s krokem 0.5 dBm | ano |
| Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 4800 Mbps | ano |
| Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 574 Mbps | ano |
| Integrovaný TPM pro bezpečné uložení certifikátů a klíčů | ano |
| Podpora 802.11ac explicitního beamformingu | ano |
| Podpora airtime fairness | ano |
| Prioritizace jednotlivých SSID na základě vysílacího času | ano |
| USB port s podporou 3G/4G USB modemu jako WAN uplink | ano |
| Vypínatelné indikační LED diody informující o stavu zařízení | ano |
| Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno) | ano |
| Detekce Rogue AP | ano |
| Minimální počet inzerovaných SSID (BSSID) na radio: 16 | ano |
| Nastavitelný DTIM interval pro jednotlivé SSID | ano |
| Mapování SSID do různých VLAN podle IEEE 802.1Q | ano |
| VLAN Pooling | ano |
| HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu | ano |
| Podpora Layer-2 izolace bezdrátových klientů | ano |
| HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz | ano |
| Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné) | ano |
| Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček | ano |
| DHCP server, směrování a NAT pro bezdrátové klienty | ano |
| AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN | ano |
| Automatická identifikace připojeného zařízení a jeho operačního systému | ano |
| Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming | ano |
| Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP | ano |
| Optimalizace provozu: multicast-to-unicast konverze | ano |
| Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace) | ano |
| Filtrování přístupu na web | ano |
| Podpora RadSec (RADIUS over TLS) | ano |
| 802.11w ochrana management rámců | ano |
| Podpora Kensington lock | ano |
| Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP | ano |
| Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN | ano |
| Volitelně možnost spravovat AP cloud management nástrojem | ano |
| CLI formou serial konsole port a serial over bluetooth | ano |
| SSHv2, SNMPv2c a SNMPv3 | ano |
| AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem | ano |
| Integrované Bluetooth 5.0 Low Energy (BLE) rádio | ano |
| Integrované Zigbee 802.15.4 rádio | ano |
| Podpora režimu SLEEP s max. spotřebou energie do 6W | ano |
| Součástí AP je příslušenství pro montáž na zeď nebo strop | ano |

**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 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.

**Základní AP – Specifikace požadavků** **v počtu 33 ks včetně podpory a potřebného SW na 5 let**

|  |  |
| --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** |
| **Základní vlastnosti** |  |
| Třída zařízení: indoor přístupový bod | ano |
| Uzavřená konstrukce bez ventilátorů | ano |
| Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax | ano |
| Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac | ano |
| Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE | ano |
| Pracovní režim AP bez kontroléru (autonomní) | ano |
| Pracovní režim AP řízené kontrolérem (lightweight) | ano |
| Pracovní režim AP v roli kontroléru s možností správy až 120 AP | ano |
| Minimální počet portů ethernet LAN: 1x 100/1000 Mbit/s RJ45 | ano |
| Podpora standardů IEEE 802.3af (PoE) a IEEE 802.3at (PoE+) | ano |
| Podpora standardního PoE 15,4W bez nutnosti redukce výkonu 5GHz rádia | ano |
| Podpora napájení z AC napájecího zdroje | ano |
| Vestavěná interní anténa MIMO, omni down-tilt | ano |
| Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz | ano |
| MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2 | ano |
| MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2 | ano |
| Podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO | ano |
| Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP | ano |
| Možnost nastavení vysílacího výkonu s krokem 0.5 dBm | ano |
| Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1200 Mbps | ano |
| Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 300 Mbps | ano |
| Integrovaný TPM pro bezpečné uložení certifikátů a klíčů | ano |
| Podpora 802.11ac explicitního beamformingu | ano |
| Podpora airtime fairness | ano |
| Prioritizace jednotlivých SSID na základě vysílacího času | ano |
| USB port s podporou 3G/4G USB modemu jako WAN uplink | ano |
| Vypínatelné indikační LED diody informující o stavu zařízení | ano |
| Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno) | ano |
| Detekce Rogue AP | ano |
| Minimální počet inzerovaných SSID (BSSID) na radio: 16 | ano |
| Nastavitelný DTIM interval pro jednotlivé SSID | ano |
| Mapování SSID do různých VLAN podle IEEE 802.1Q | ano |
| VLAN Pooling | ano |
| HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu | ano |
| Podpora Layer-2 izolace bezdrátových klientů | ano |
| HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz | ano |
| Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné) | ano |
| Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček | ano |
| DHCP server, směrování a NAT pro bezdrátové klienty | ano |
| AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN | ano |
| Automatická identifikace připojeného zařízení a jeho operačního systému | ano |
| Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming | ano |
| Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP | ano |
| Optimalizace provozu: multicast-to-unicast konverze | ano |
| Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace) | ano |
| Filtrování přístupu na web | ano |
| Podpora RadSec (RADIUS over TLS) | ano |
| 802.11w ochrana management rámců | ano |
| Podpora Kensington lock | ano |
| Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP | ano |
| Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN | ano |
| Volitelně možnost spravovat AP cloud management nástrojem | ano |
| CLI formou serial konsole port a serial over bluetooth | ano |
| SSHv2, SNMPv2c a SNMPv3 | ano |
| AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem | ano |
| Integrované Bluetooth 5.0 Low Energy (BLE) rádio | ano |
| Integrované Zigbee 802.15.4 rádio | ano |
| Podpora režimu SLEEP s max. spotřebou energie do 6W | ano |
| Součástí AP je příslušenství pro montáž na zeď nebo strop | ano |

**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 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.

**Management – Specifikace požadavků** **v počtu 37 ks včetně podpory a potřebného SW na 5 let**

|  |  |
| --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** |
| **Základní vlastnosti** |  |
| Management nástroj pro správu WiFi sítě s podporou správy produktů výrobce a kompatibilní s nabízenými AP a switchem. | ano |
| Virtuální appliance (OVA formát) bez nutnosti pořizovat další licence např. pro OS nebo databáze. | ano |
| Správa prvků: přístupových bodů, WiFi kontrolerů a přepínačů | ano |
| Licence pro správu všech prvků, možnost flexibilního rozšiřování až do 4000 zařízení. | ano |
| Manuální a automatické discovery síťových zařízení pomocí SNMP, HTTP a CDP skenování. | ano |
| Monitorovací nebo plný-managed režim pro nově objevená zařízení jako ochrana před nechtěným přepsáním konfigurace. | ano |
| Role pro jednotlivé síťové operátory na úrovni síťových zařízení a jejich funkcí. | ano |
| Webové uživatelské rozhraní s podporou HTTPS | ano |
| Real-time monitoring každého uživatele v síti včetně charakteristik jako jsou: kvalita RF signálu, utilizace pásma (in/out), autentizační status a čas, historie roamingu, délka trvání připojení, typ klientského zařízení, asociace s SSID, objem a seznam používaných L7 aplikací a navštívených webových kategorií. | ano |
| Vyhledávání koncových uživatelů na základě MAC adresy, IP adresy, uživatelského jména a LAN hostname. | ano |
| Konfigurace formu politik aplikovatených na všechna zařízení, jejich skupinu nebo jednotlivé zařízení. | ano |
| Tvorba konfiguračních šablon: jak nových tak z běžících zařízení | ano |
| Podpora konfigurační změn a upgrade firmware pomocí jednorázových nebo opakujících se pracovních úloh (scheduled-job). | ano |
| Archivace konfigurací | ano |
| Audit konfigurace, porovnávní rozdílů proti přednastaveným politikám individuálně pro jednotlivá a hromadně proti skupině zařízení. V případě nesouladu definice a runtime stavu konfigurační rollback. | ano |
| Konfigurační management: zálohy a obnova konfigurace, srovnávání rozdílů, auditování podle přednastavených i vlastních pravidel. | ano |
| Podpora alarmování s možností nastavitelných prahů pro jednotlivé událostí. Podporované události: odchylka od baseline konfigurace, RF metrika, nově objevené zařízení, Radius autentizace, Rogue AP, nadměrné utilizace AP (bandwidth), počet připojených klientů, nadměrná utilizace klientem (bandwidth), Up/Down zařízení, Up/Down Radio, IDS událost. | ano |
| Možnost monitorování stability a odezvy ostatních síťových služeb pro jednotlivé klienty jako je průměrný čas odpovědi DHCP, DNS či čas zpracování RADIUS autentizace. | ano |
| Vytváření reportů v PDF formátů reportujících různé přehledové statistiky o využití sítě a jejím stavu. Automatizované pravidelné zasílání reportů mailem. | ano |
| Monitoring a detekce síťových anomálií jako je např. nadměrné a neobvyklé navýšení objemu provozu a upozorňování na tyto stavy pomocí alarmů. | ano |
| Vizualizace umístění prvků sítě ve fyzických mapách. Zobrazení bezdrátových klientů na mapě a jejich signálu a využívaných L7 aplikací. | ano |
| Podpora plánování WiFi a lokalizace uživatelů | ano |
|  |  |

Rozšířená záruka s servisní podpora na 5 let garantovaná přímo výrobcem zařízení v režimu 24x7. Možnost otevírat servisní požadavky přímo u výrobce.

**NAC (network access control) – Specifikace požadavků v počtu 1 ks včetně podpory a potřebného SW na 5 let**

|  |  |
| --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** |
| Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení | ano |
| Forma dodání: virtuální appliance pro VMware | ano |
| Minimální celková kapacita řešení pro autentizaci unikátních koncových zařízení | 700 v redundantním clusteru |
| Řešení musí poskytovat vysokou dostupnost tak aby v případě výpadku primárního AAA serveru převzal jeho roli sekundární server. | ano |
| Možnost vytváření clusteru více virtuálních appliance. | ano |
| Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance. | ano |
| Podpora minimálně 20ti předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě) | ano |
| Požadované metody autentizace uživatelů a zařízení | PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace |
| Podpora RADIUS CoA | ano – dle RFC3576 |
| Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD | ano |
| Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období | ano |
| Možnost licenčního rozšíření o TACACS+ autentizaci správců síťových zařízení | ano |
| Další požadované autentizační a autorizační zdroje a metody. | LDAP, MS AD, Token, MAC, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta) |
| Možnost integrace s MDM (Mobile Device Management) platformami třetích stran | minimálně AirWatch, Citrix, MobileIron, JAMF, InTune |
| Podpora REST API pro většinu základních úkonů AAA platformy | ano |
| Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.) | ano |
| Možnost licenčního rozšíření o zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení. | ano |
| Možnost licenčního rozšíření o sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě. | ano |
| LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter, Google+. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě s SMS, email ověřením nebo na elektronickou notifikaci a schválení pověřených pracovníků. | ano |
| Možnost licenčního rozšíření o bezpečnou registraci soukromých zařízení do interní sítě na základě uživatelských údajů z AD či LDAP. Uživatel musí být schopen jednoduchým uživatelským wizardem instalovat osobní certifikát a síťový profil na své soukromé zařízení (BYOD systém). | ano |
| Možnost licenčního rozšíření o certifikační autoritu pro vydávání certifikátů na soukromá zařízení musí být součástí AAA platformy. | ano |
| Možnost licenčního rozšíření o samoobslužný portál pro hosty či interní uživatele s možností správy svých vlastních registrací. | ano |
| Možnost licenčního rozšíření o systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení. | ano |
| Možnost licenčního rozšíření o kontrolu stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku. | ano |
| Možnost licenčního rozšíření o podporu jednorázového i permanentního klienta pro kontroly na koncových zařízeních. Podpora klienta pro kontrolu koncových zařízení na OS Windows, MAC OS a Linux | ano |
| Možnost licenčního rozšíření o integraci tohoto koncového klienta s VPN klientem | ano |
| Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je AAA systém. | ano |

Rozšířená záruka a servisní podpora na 5 let garantovaná přímo výrobcem zařízení v režimu 24x7. Možnost otevírat servisní požadavky přímo u výrobce.

**Switch 24 – Specifikace požadavků** **v počtu 3 ks včetně podpory a potřebného SW na 5 let**

|  |  |
| --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** |
| **Základní vlastnosti** |  |
| Třída zařízení | L3 switch |
| Formát zařízení | do racku |
| Velikost zařízení: 1U | ano |
| Počet 1Gbit/s metalických portů | 24x10/100/1000Mbit RJ45 |
| Počet 10Gbit/s optických portů s volitelným fyzickým rozhraním | 4x10Gbit SFP+ nezávislé |
| 10GE interface zpětně kompatibilní s 1Gbit/s a 100Mbit/s transceivery | ano |
| Všechny ethernet porty jsou dostupné zepředu | ano |
| Primární napájecí zdroj | 1x interní AC |
| Podpora PoE+ dle standardu 802.3at | ano |
| Dostupný výkon pro PoE+ napájení | 370W |
| Podpora Energy Efficient Ethernet (802.3az) | ano |
| Celková propustnost přepínače | 128 Gb/s |
| Celkový paketový výkon přepínače | 95 Mpps |
| Pamětový buffer | 12MB |
| **Vlastnosti stohování** |  |
| Podporovaný počet přepínačů ve stohu | 8 |
| Stohování přes standardizované síťové rozhraní | ano |
| Stoh podporuje distribuované přepínaní paketů | ano |
| Kterýkoli prvek ve stohu může být řídícím prvkem (1:N redundance) | ano |
| Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor) | ano |
| Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG) | ano |
| Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF | ano |
| Stohování mezi vzdálenými lokalitami až 10 km | ano |
| **Základní funkce a protokoly** |  |
| Podpora "jumbo rámců" včetně velikosti 9220 Byte | ano |
| Podpora linkové agregace IEEE 802.1AX | ano |
| Konfigurovatelné rozkládání LACP zátěže podle L2,L3 a L4 | ano |
| Počet LACP skupin/linek ve skupině | 60/8 |
| Počet záznamů v tabulce MAC adres | 32 000 |
| Protokol pro definici šířených VLAN | MVRP |
| Podpora VLAN podle IEEE 802.1Q | 2000 aktivních VLAN |
| Protokol-based VLAN (zařazovní do VLAN podle protokolu) | ano |
| Podpora MAC based VLAN | ano |
| Podpora Private VLAN | ano |
| IEEE 802.1s - Multiple Spanning Tree | ano |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) | ano |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED | ano |
| Detekce jednosměrnosti optické linky (např. UDLD) | ano |
| Tunelování 802.1Q v 802.1Q | ano |
| DHCP server | ano |
| DHCP relay pro IPv4 a IPv6 včetně option 82 a 79 | ano |
| NTP pro IPv4 a IPv6 včetně MD5 autentizace | ano |
| Statické směrování IPv4 a IPv6 | ano |
| Počet záznamů ve směrovací tabulce | 10 000 |
| Dynamické směrování RIPv2 a RIPng | ano |
| Dynamické směrování OSPFv2 a OSPFv3 | ano |
| IGMP v2 a v3 | ano |
| MLD v1 a v2 | ano |
| Hardware podpora IPv4 a IPv6 ACL | ano |
| ACL definice na základě skupiny fyzických portů | ano |
| ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN | ano |
| BPDU guard | ano |
| Root guard | ano |
| DHCP snooping pro IPv4 a IPv6 | ano |
| HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na % rychlosti portu a množství paketů za vteřinu | ano |
| ICMPv4 a ICMPv6 rate-limiting per port | ano |
| Podpora ověřování 802.1X včetně více uživatelů per-port | 32 uživatelů na port |
| RADIUS MAC autentizace, probíhající před 802.1x pro případy, že koncové zařízení není softwarově vybaveno pro 802.1x autentizaci | ano |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 | ano |
| Podpora 802.1X Guest VLAN | ano |
| Podpora IPv6 RA Guard | ano |
| IP source guard / dynamic IP lockdown | ano |
| Podpora Dynamic ARP protection | ano |
| Port security | ano |
| Ochrana control plane (CPU) před útoky typu DoS | ano |
| Podpora IPv4 a IPv6 QoS | ano |
| IEEE 802.1p - minimální počet front | 8 |
| **Management** |  |
| CLI formou RJ45 serial konsole port | ano |
| USB konzolový port | ano |
| Konfigurace zařízení v člověku čitelné textové formě | ano |
| Podpora managementu přes IPv4 i IPv6 | ano |
| SSHv2 a a SFTP | ano |
| Podpora SNMPv2c a SNMPv3 | ano |
| RMON | ano |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |
| Lokálně vynucené RBAC na úrovni přepínače | ano |
| Dualní flash image | ano |
| Podpora oddělených čítačů paketů pro IPv4 a IPv6 provoz | ano |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) | ano |
| Aktivní monitorování dostupnosti RADIUS serveru přednastaveným jménem a heslem | ano |
| Podpora TACACS+ | ano |
| Podpora konfiguračních změn pomocí naplánovaných pracovních úloh (Job scheduler) | ano |
| Analýza síťového provozu sFlow podle RFC 3176 | ano |
| Port mirroring, alespoň 4 různé obousměrné session | SPAN, RSPAN |
| Zrcadlení provozu na základě filtrů: Mac-adressa, VLAN, ACL (traffic mirroring) | ano |
| Podpora IP SLA pro měření zpoždění provozu VoIP | ano |
| Podpora OpenFlow verze 1.3 | ano |
| Podpora Zero Touch Provisioning (ZTP) | ano |
| Podpora REST API pro automatizaci nastavení sítě. | ano |
| Podpora Chromecast Gateway | ano |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subenty. (Apple Bonjour Gateway) | ano |
| Podpora service insertion včetně technologie VXLAN | ano |
| Automatická konfigurace portu podle připojeného zařízení | ano |
| Podpora Cloud based management | ano |

**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 s výměnou NBD v délce 84 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
* Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.
* Je požadovaná technická podpora výrobce po dobu 60 měsíců.
* Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

1. **Centrální síťový prvek - router a firewall**

Komplexní řešení pro zabezpečení interní sítě před útoky z internetu. Zařízení, které integruje bezpečnostní prvky do jediného systému. Chrání a kontroluje data, protokoly, počítače, uživatele jednoduše celou privátní síť. Samozřejmostí je nejen firewall, ochrana přenášených dat, ochrana DNS, bezpečný přístup na internet, ale také rozsáhlé možnosti autentizace uživatelů nebo šifrovaný VPN přístup umožňující bezpečné připojení vzdálených klientů. Součástí bezpečnostního řešení je důkladná analýza HTTP a HTTPS protokolů umožňující detailní kontrolu a vynucení pravidel bezpečnostní politiky. Uživatelé i cenné zdroje jsou bezpečně chráněni autentizací, identifikací skutečného typu souboru. Přístup uživatelů na web musí být efektivně řízen webovým filtrem který v praxi dosahuje min 90% úspěšnost. Potřeba je také zajistit, aby se interní síť a uživatelé nestali oběťmi stále rostoucího počtu útoků na doménová jména a jejich překlad. Komunikace s DNS servery musí procházet výhradně přes DNS proxy, která kontroluje správný překlad dotazovaného jména. Zařízení se musí vyznačovat vysokou mírou flexibility při nastavení bezpečnostních politik od jednoduchých pravidel stavové inspekce až po sofistikované řízení na úrovni aplikačních protokolů. Pravidla bezpečnostních politik tak mohou být vázaná na konkrétního uživatele, skupinu, tým včetně autentizace uživatelů na terminálových serverech. Požadujeme bezpečnostní aktivní síťový prvek, který efektivně chrání síťovou infrastrukturu před kybernetickými útoky, které jsou v danou chvíli skutečnou aktivní hrozbou. Využívá k tomu unikátní databázi hrozeb, obsahující charakteristiky útoků, díky níž dokáže na aktuální bezpečnostní situaci rychle reagovat a útoky automaticky blokuje

Zařízení musí podporovat autentizační mechanizmy, jako jsou Active Directory, Kerberos, LDAP, RADIUS, případně konfiguraci na stávající autentizační infrastrukturu. Pravidla vázaná na konkrétního uživatele či skupinu umožňují uplatnění bezpečnostních politik pro různé pracovní týmy včetně autentizace uživatelů na terminálových serverech

|  |  |  |
| --- | --- | --- |
| **Název a specifikace části** | **kusů** | **Minimální požadavky** |
| **Centrální síťový prvek - router a firewall** | **1** |
| HW appliance – all-in-one box od jednoho výrobce, provedení rackmount 19" |  | ANO |
| Záruka na HW 5 let v režimu NBD | ANO |
| Možnost provozu v konfiguraci cluster active-active v případě zakoupení druhého node | ANO |
| Rozhraní minimálně 12x 1 Gbps Ethertnet,2 x SFP+, 1 x remote console, podpora agregace a redundance interface | ANO |
| Redundantní zdroj napajení in box | ANO |
| Mininimální velikost interního úložiště 480GB | ANO |
| FW řešení podporující technologii stavového paketového filteru i aplikačních proxy bran firewallu | ANO |
| Dedikovaný management port | ANO |
| Podpora NAT / PAT | ANO |
| Možnost řízení komunikace volitelně na sítových vrstvách L3 až L7 | ANO |
| Možnost řízení komunikace na úrovni jednotlivých aplikačních příkazů (aplikační proxy) alespoň pro protokoly: HTTP, SMTP, POP3, IMAP4, DNS, FTP, SIP, H.323, SQLNet | ANO |
| Možnost HTTPS Inspekce (kontrola HTTPS, rozlamování TLS) | ANO |
| Podpora VLAN | ANO |
| Podpora IPV4 a IPv6, dual stack | ANO |
| Podpora SNMP | ANO |
| QoS – řízení šířky pásma podle uživatele, portu i typu souboru | ANO |
| Podpora autentizace (Kerberos, NTLM, LDAP, RADIUS, SAML2) | ANO |
| Zasílání NETFLOW v9 nebo IPFIX včetně informace o překladech IP adres se vzorkem max. 1:10 na min. jeden cíl | ANO |
| Možnost doplnění VPN s dvou faktorovou SMS autentizaci pro uživatele | ANO |
| Neomezený počet VPN licencí, podpora IPSec, Open VPN |  |
| Podpora Integrace s Microsoft Active Directory včetně řízení dle skupin uživatelů a podpory SSO tj. transparentní autentizace bez nutnosti ověřování mezi klientem a firewallem. | ANO |
| HONEYPOT s automatickým blokováním zdrojové adresy potenciálního útočníka na definované servery z lokální sítě včetně časového omezení |  |
| Možnost ukončení TLS / SSL komunikace na FW s prováděním všech kontrol v šifrovaném provozu a to jak v provozu na server i klienta včetně rozšifrování a zašifrování spojení. | ANO |
| Reverzní web proxy pro účely publikace webových serverů: Terminace SSL/TLS, Autentizace uživatele, Publikace více webových serverů na jedné IP adrese a stejném portu | ANO |
| Aktivní ochrana před aktuálními kybernetickými útoky prostřednictvím automaticky aktualizované databáze hrozeb z prostředí českého internetu (CSIRT.cz a jiné) | ANO |
| Autentizace uživatelů oproti MS Active directory, LDAP nebo lokální databáze uživatelů (protokol Kerberos nebo NTLM) bez nutnosti instalace klientského SW na stanici | ANO |
| Podpora paralerní instalace více verzí firmware s možností okamžitého návratu k poslední verzi a libovolné přepínání | ANO |
| Logování s podporou více úrovní a možností úplného záznamu komunikace na úroveň dump IP komunikace | ANO |
| Možnost nastavit dobu pro uchování logovaných provozních záznamů | ANO |
| Doba pro uchování logů po dobu min. 1 roku na interním úložišti | ANO |
| Záznamy provozu pro následný forezní audit dle české jurisdikce | ANO |
| Dostupnost bezpečnostních aktualizací minimálně po dobu 5 let | ANO |
| Kompletní instalace, konfigurace | ANO |
| Česká databáze webových serverů | ANO |
| Zaškolení obsluhy minimálně v rozsahu 1MD | ANO |
| Statistiky přístupu uživatelů k internetovým serverům | ANO |
| Zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu | ANO |
| Podpora automatické detekce proxy pomocí WPAD | ANO |
| Řízení přístupu na web dle kategorií obsahu | ANO |
| Možnost definovat vlastní kategorií serverů | ANO |
| Minimálně 90% úspěšnost kategorizace webového provozu při nasazení | ANO |
| Dostupná informace o úspěšnosti kategorizace pro webový provoz přes zařízení | ANO |
| Aktualizace databáze webfiltru o neznámé navštívené domény do druhého pracovního dne | ANO |
| Možnost snadné reklamace chybného záznamu pomocí webového formuláře | ANO |
| Snadná reklamace chybného záznamu uživatelem | ANO |
| Zpětná vazba o vyřízení reklamace | ANO |
| Vyřízení reklamace do dvou hodin v pracovní době | ANO |
| Politika přístupu definovaná dle času, kategorií, cílové URL, cílové IP adresy, uživatele, skupiny uživatel | ANO |
| Definovatelné black/white listy pro jednotlivé uživatele nebo zdrojové IP adresy | ANO |
| Kontrola obsahu HTTPS komunikace – HTTPS inspekce | ANO |
| Možnost definovat důvěryhodné CA | ANO |
| Výjimky z HTTPS inspekce na vybrané zdrojové IP adresy, servery nebo kategorie | ANO |
| Upozornění a blokování rizikových kategorií | ANO |
| Funkce pro upozornění a podmíněné zpřístupnění obsahu uživateli na předdefinovanou dobu | ANO |
| Blokování streamovaného obsahu (audio, video) | ANO |
| Blokování rizikového tunelování (skype, teamwiever, tor, atd.) | ANO |
| Podpora automatické detekce proxy pomocí WPAD | ANO |
| Dokumentace pro údržbu a užívání | ANO |