ŠPECIFIKÁCIE AKTÍVNYCH PRVKOV SIETE

1.1. BEZDRÔTOVÝ PRÍSTUPOVÝ BOD (WIRELESS ACCESS POINT)

Integrované dual-band všesmerové antény
Zisk antén min. 3,5dBi pre 2,4GHz a 3,5dBi pre 5GHz
Min. 1x10/100/1000BASE-T RJ45 rozhrania pre pripojenie do infraštruktúry
Napájanie bezdrôtového prístupového bodu pomocou štandardu 802.3af (Power over Ethenet) alebo pomocou DC adaptéra
Certifikovaný bezdrôtový prístupový bod pre nasadenie v Európe
Min. 2x2 MIMO s 2 spatial streams
Podpora min. 80 MHz šírky kanálov v 5GHz pásme pre štandard 802.11ac Wave 2
Podpora technológie zabezpečujúcej sústavné monitorovanie bezdrôtového spektra, za účelom detekcie rôznych interferencií bez toho aby boli afektovaný bezdrôtový klienti pripojený na bezdrôtový prístupový bod
Podpora agregácie paketov
Podpora prevádzkových teplôt v min. rozsahu: 0 až 35˚C
Integrované BLE (Bluetooth Low Energy) rádio
Podpora 256 QAM (Quadrative Amplitude Modulation)
Podpora limitovania rýchlosti per SSID
Podpora limitovania rýchlosti per bezdrôtový klient
Podpora limitovania rýchlosti jednotlivých aplikácií na základe aplikačných signatúr
Prideľovanie IP adries bezdrôtovým klientom z bezdrôtového prístupového bodu
Podpora technológie prekladania IP adries NAT (Network Address Translation)
Automatická aktualizácia firmvéru a aplikačných signatúr v administrátorom preddefinovanom čase a dni v týždni

Centralizovaná správa:
Centralizované riadenie bezdrôtového prístupového bodu poskytované ako služba
Administratívny dashboard v cloude dostupný cez internet odkiaľkoľvek, so zabudovanou autmatickou aktualizáciou funkcionalít počas trvania subskripcie na prevádzku
Dashboard s prehľadnými informáciami o aktivitách užívateľov v sieti, návštevnosti stránok, štatistikách užívateľov
Dashboard ako zdieľaná platforma na unifikovanú správu pre cloudom riadené AP, voliteľne aj prepínače, bezpečnostné firewally, IP kamery, resp. IP telefóny s jednotným uzívateľským rozhranim a unifikovanou správou
Musí byť zabezpečené kompatibilita medzi centralizovaným riadiacim systémom pre bezdrôtovú sieť a bezdrôtovým prístupovým bodom

Požadovaná podpora týchto štandardov:
IEEE 802.11a/b/g, 802.11n, 802.11ac Wave 1 a 802.11ac Wave 2
IEEE 802.11h
Wi-Fi Protected Access 2 (WPA2)
802.1x
Advanced Encryption Standards (AES)
Wi-Fi Multimedia (WMM)
EAP-Transport Layer Security (TLS)
EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MCSHAPv2)
Protected EAP (PEAP) v0 or EAP-MSCHAPv2

EAP-Subscriber Identity Module (SIM)

Zariadenie musí podporovať úplnú správu a monitorovanie prostredníctvom Centrálneho systému riadenia a monitorovania siete.

Subskripcia na prevádzku zariadenia na 1 rok zahŕňajúca podporu od výrobcu vrátane aktualizácii softvéru, výmeny hardvéru v prípade poruchy.

1.2. SIEŤOVÝ PREPÍNAČ - POTREBNÝ POČET PORTOV PODĽA UŽÍVATEĽOV V JEDNOTLIVÝCH OBJEKTOCH NAVRHNE UCHÁDZAČ

Zariadenie musí mať minimálne 8x RJ-45 10/100/1000Base-T rozhraní.
Zariadenie misí mať minimálne 2x 1 GE SFP rozhraní pre uplink/downlink.
RJ-45 rozhrania na zariadení musia podporovať funkciu auto-MDIX.
Zariadenie musí podporovať PoE (IEEE 802.3af-2003) na aspoň polovici RJ45 rozhraní.
Zariadenie musí podporovať PoE+ (IEEE 802.3at-2009) na aspoň štvrtine RJ45 rozhraní.
Zariadenie musí podporovať jumbo frame 9578 bajtov.
Zariadenie musí podporovať L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
Zariadenie musí podporovať minimálne 16000 MAC adries.
Zariadenie musí podporovať minimálne 4094 virtuálnych sietí LAN (802.1Q).
Zariadenie musí podporovať 802.1x na všetkých rozhraniach.
Zariadenie musí podporovať autentifikáciu pomocou MAC adries prostredníctvom protokolu RADIUS.

Priepustnosť musí byť najmenej 20 Gb/s.
Zariadenie musí podporovať princípy QoS podľa 802.1p a DSCP a umožniť klasifikáciu paketov podle zdrojových a cieľových TCP/UDP portov (podľa 4. vrstvy ISO/OSI).
Zariadenie musí podporovať zachytávanie klientskej prevádzky per port s možnosťou odoslania do ethernetového analyzátora (napr. Wireshark) pre vzdialené riešenie problémov pripojených klientov.
Zariadenie musí podporovať funkciu testovania pripojených UTP/STP káblov – zistenie stavu jednotlivých párov a celkovej dĺžky kábla.

Zariadenie musí podporovať funkciu rozpoznávania klientských aplikácií (podľa 7. vrstvy ISO/OSI) a identifikáciu operačných systémov a hostname klientských zariadení.
Zariadenie musí podporovať filtrovanie prechádzajúcich užívateľských dát podľa zdrojových a cieľových IP adries a UDP/TCP portov.

Zariadenie musí byť schopné odosielať správy na vzdialený SYSLOG server.
Zariadenie musí obsahovať licencie pre zabezpečenie požadovanej funkcionality na obdobie minimálne 12 mesiacov.

Súčasťou dodávky musí byť platná podpora od výrobcu po dobu minimálne 12 mesiacov a to vrátane výmeny vadného hardware, aktualizácií softwaru a firmwaru, bezpečnostných aktualizácií a prístupu k technickej podpore výrobcu.
Zariadenie musí podporovať správu a monitorovanie prostredníctvom Centrálneho systému riadenia a monitorovania siete.

1.3. INTEGROVANÁ BEZPEČNOSTNÁ BRÁNA

Zariadenie musí mať minimálne 5x1GE rozhraní 1000BASE-T
Priepustnosť firewallu musí byť aspoň 200 Mbps.
Zariadenie musí podporovať minimálne 500.000 súčasných pripojení.
Zariadenie musí podporovať minimálne 12.000 nových spojení za sekundu.
Zariadenie musí kombinovať tieto možnosti zabezpečenia v jednom zariadení: FW, anti-virus, anti-phishing, IPS, antispoofing, filtrovanie http a https na základe kategorizácie webových stránok (aj podľa skupiny uživateľov).
Kombinovaný výkon (súčasný beh FW, IPS, AV) musí byť minimálne 650 Mbps.
Zariadenie musí podporovať stavový firewall.
Zariadenie musí podporovať IPSec VPN pre pripojenie vzdialených lokalít.
Zariadenie musí podporovať VPN pripojenie vzdialených klientov.
Zariadenie musí podporovať statické smerovanie.
Zariadenie musí podporovať 802.1Q VLAN.
Zariadenie musí podporovať 1:1 a 1:N NAT na preklad IP adries.
Zariadenie musí podporovať funkci DHCP servera.
Zariadenie musí podporovať funkcie pre bezpečné vyhľadávanie.
Zariadenie musí podporovať funkciu kontroly súborov pomocou reputačnej databázy a sandboxingu ako ochranu voči malwaru.
Zariadenie musí podporovať funkciu rozpoznávania klientských aplikácií (podľa 7. vrstvy ISO/OSI) a identifikáciu operačných systémov a hostname klientských zariadení.
Zariadenie musí umožniť zakázať komunikáciu vybraných klientov a to aj jednotlivo podľa rozpoznaných tried aplikácií (podľa 7. vrstvy ISO/OSI).
Zariadenie musí umožnit obmedziť celkovú priepustnosť na uplinku a to aj jednotlivo podľa rozpoznaných tried aplikácií (podľa 7. vrstvy ISO/OSI).
Zariadenie musí umožniť QoS klasifikáciu paketov pomocou DSCP tagu a to aj jednotlivo podľa rozpoznaných tried aplikácií (podľa 7. vrstvy ISO/OSI).
Zariadenie musí podporovať redundantné WAN rozhranie s možnosťou dynamickej voľby výstupného rozhrania per aplikácia na základe stratovosti, oneskorenia a časového rozptylu na príslušnej WAN linke.
Zariadenie musí umožniť monitorovanie IP (IPv4 a IPv6) dátových tokov formou exportu prevádzkových informácií o prenesených dátach v členení minimálne zdrojová/cieľová IP adresa, zdrojový/cieľový TCP/UDP port (alebo ICMP typ) vo formáte NetFlow v9.
Zariadenie musí byť schopné odosielať správy na vzdialený SYSLOG server.
Zariadenie musí voliteľne podporovať režim vysokej dostupnosti (možnosť voliteľne zapojiť pár zariadení) s automatickou obnovou konektivity v prípade HW chyby primárneho zariadenia.
Zariadenie musí zahrnovať všetky licence s požadovanou funkcionalitou na obdobie pokryté príslušnou subskripciou.
Súčasťou dodávky musí byť platná podpora od výrobcu počas doby platnosti adekvátnej subskripcie a to vrátane výmeny hardware v prípade poruchy, aktualizácií softwaru a firmwaru, bezpečnostných aktualizácií a prístupu k technickej podpore výrobcu.
Zariadenie musí podporovať úplnú správu a monitorovanie prostredníctvom Centrálneho systému riadenia a monitorovania siete.