I. Wymagania dotyczące punktów dostępowych Wi-fi (Access-Point Wireless LAN):

1. Liczba – 10 szt.
2. Trzy tryby pracy:
   a. samodzielny (zarządzanie punktem odbywa się poprzez interfejs przeglądarki internetowej, telnet i SSH);
   b. jako kontroler sieci bezprzewodowej nadzorujący inne punkty dostępowe (do 25 AP jednocześnie);
   c. zarządzany przez zewnętrzny kontroler sieci bezprzewodowej (tzw. LWAP). Zamawiający posiada redundantny klaster kontrolerów Ruckus ZoneDirector 1200. Urządzenia muszą być zgodne z posiadanym klastrem. Zamawiający posiada odpowiednie licencje na kontrolerach. W przypadku, gdy Wykonawca oferuje urządzenia nie w pełni kompatybilne z klastrem kontrolerów Ruckus ZoneDirector 1200, Zamawiający dopuszcza zaoferowanie w ramach wynagrodzenia punktów dostępowych wraz z kontrolerami posiadającymi nie gorszą funkcjonalność niż kontrolery posiadane przez Zamawiającego.
3. Wsparcie dla trybu tunelowania ruchu klientów do kontrolera oraz lokalnego przełączania.
4. Jednoczesna praca w paśmie 2,4 GHz i 5 GHz poprzez dwa moduły radiowe.
5. Obsługa standardów IEEE 802.11a/b/g/n/ac/ac2 oraz IEEE 802.11d, 802.11h.
6. Minimum dwa moduły radiowe pracujące jednocześnie.
7. Praca w trybie MIMO o parametrach radiowych minimum 2x2:2.
8. Wymagana obsługa minimum 200 klientów (ilość asocjacji) na każdym z modułów radiowych oraz minimum łącznie 400 klientów w ramach całego urządzenia.
9. Automatyczna ochrona przed interferencjami sygnału. Jeśli funkcja ta wymaga dodatkowego oprogramowania musi być ono dostarczone wraz z systemem.
10. Monitorowanie kanałów WLAN w tle – odszukiwanie najlepszych kanałów.
11. Wbudowanie wsparcie dla analizy spektrum widma.
12. Wsparcie dla WIPS lub WIDS – urządzenie musi jednocześnie pełnić rolę Access-Point'a dla użytkowników oraz sensora bezpieczeństwa dla wykrywania ataków w ramach sieci bezprzewodowej.
13. Wsparcie dla sieci kratowych MESH.
14. Wsparcie dla sumowania sygnałów MRC odbieranych z różnych polaryzacji, pionowej i poziomej.
15. Wsparcie dla technologii beamforming 802.11ac TxBF.
16. Anteny wbudowane i zintegrowane z punktem dostępowym z wzmocnieniem minimum 3 dBi dla 2.4 GHz oraz 5 GHz.
17. Minimalna czułość odbiornika -99dBm dla dowolnej prędkości w paśmie 2.4GHz.
18. Obsługa PoE+ i PoE (IEEE 802.3af). Przy pracy na PoE (15.4W) urządzenie musi pracować z pełnymi parametrami radiowymi i systemowymi.
19. Nie mniej niż 25 jawnych BSSID z własną polityką dostępu i regułami QoS.
20. Wymagane minimum 4 kolejki QoS per stacja kliencka i wsparcie standardu 802.11e/WMM.
21. Obsługa funkcji podpowiadania klientom aby przełączali się na pasmo 5GHz z pasma 2,4GHz.
22. Obsługa roamingu w ramach całego systemu dla wszystkich podłączonych klientów.
23. Obsługa standardu Voice over Wireless LAN, obsługa nie mniej niż 25 klientów Voice jednocześnie.
24. Obsługiwane protokoły / standardy zabezpieczeń: WEP/WPAPSK/WPA-TKIP/WPA2-AES/802.11i.
25. Obsługa trybu pracy Router z funkcjonalnością NAT i serwera DHCP.
26. Obsługa autentykacji 802.1x dla portu Ethernet: tryb suplikanta i autentykatora.
27. Kanały pracy:
   a. IEEE 802.11n: 2.4 – 2.484 GHz i 5.15 – 5.85 GHz;
   b. IEEE 802.11a: 5.15 – 5.85 GHz;
   c. IEEE 802.11b: 2.4 – 2.484 GHz.
28. Obsługiwana szybkość transmisji:
   a. 802.11ac: 6.5 - 867Mbps;
   b. 802.11n: 6.5Mbps – 300Mbps;
   c. 802.11a: 54, 48, 36, 24, 18, 12, 9, 6Mbps;

d. 802.11b: 11, 5.5, 2, 1 Mbps ;
e. 802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps.

29. Charakterystyka fizyczna punktów dostępowych:
    a. Zasilanie poprzez PoE/PoE+ lub zasilacz 12V DC;
    b. Wyposażony w dwa port RJ-45, auto MDI/MDI-X, jeden z możliwością zasilania PoE, auto-sensing 10/100/1000mbps;
    c. Masa urządzenia nie większa niż 0.5kg;
    d. Praca w temperaturze 0-40^{o}C;
    e. Wyposażone w gniazdo bezpieczeństwa umożliwiające zamontowanie linki bezpieczeństwa zabezpieczającej urządzenia przed kradzieżą.
30. Zgodność ze standardem VLAN 802.1q.
31. Gwarancja Wykonawcy – minimum 12 miesięcy. Wymiana uszkodzonych elementów sprzętu on-site w reżimie 24 godzinnym od zgłoszenia. Podczas trwania gwarancji nielimitowany dostęp 24 godziny na dobę do pomocy technicznej producenta (tzw. TAC), możliwości sciągania nowego firmware i dostępu do baz wiedzy na stronie producenta.

II. Opis infrastruktury Zamawiającego

Zamawiający posiada:

– 25 szt. punktów dostępowych Wi-fi (Access-Point Wireless LAN) Ruckus r510.

– klaster kontrolerów Ruckus ZoneDirector 1200 spełniające poniższe wymagania:

1. Zamawiający posiada zestaw dwóch urządzeń pracujących w trybie High-Availability (urządzenie główne i zapasowe pracujące redundantnie).
2. Kontroler jest urządzeniem dedykowanym (appliance). Zamawiający nie dopuszczał rozwiązań na kontrolerach wirtualnych zainstalowanych na Hypervisorach wirtualizacyjnych.
3. Zestaw kontrolera Wi-Fi jest przeznaczony do montażu w szafie rack 19”, wraz z nimi są dostarczone odpowiednie mocowania (tzw. rack-mount-kit). Wielkość całego rozwiązania nie może zająć w szafie więcej niż 4U.
4. Kontroler oferuje możliwość dodania drugiego, redundantnego kontrolera realizującą funkcję klastra i redundancję 1+1 z pełną synchronizacją stanu (konfiguracja, podłączeni klienci/urządzenia, klucze, konta użytkowników i dane statystyczne). Redundancja w trybie Active/Standby. Kontroler posiada minimum 2 porty liniowe LAN typu 1Gbps Ethernet 10/100/1000 (RJ-45).
5. Kontroler zapewnia centralne zarządzanie nie mniej niż 30 punktami dostępowymi (ilość dostarczanych licencji w ramach postępowania) z możliwością rozbudowy do minimum 130 punktów dostępowych. Rozbudowa nie może wymagać zakupu dodatkowych urządzeń, musi być realizowana wyłącznie poprzez zakup nowej licencji.
6. Klaster obsługuje minimum 1950 podłączonych urządzeń Wifi (ilość asocjacji) do urządzeń AP pracujących z kontrolerami.
7. Rozbudowa licencji obsługiwanych punktów dostępowych obejmuje tylko zakup dla głównego kontrolera. Kontroler zapasowy dziedziczy licencje zakupione dla kontrolera podstawowego, aby uniknąć konieczności podwójnego kupowania licencji dla obu urządzeń.
8. Automatyczne wykrywanie punktów dostępowych przyłączonych w VLAN, którym jest kontroler. Konfiguracja umożliwia domyślną reakcję urządzenia na podłączenie nowego punktu dostępowego – dodanie go do środowiska lub poinformowanie administratorów o nowym podłączonym urządzeniu.
9. Kontrolery wspierają punkty dostępowe z radiami pracującymi w standardach IEEE 802.11a/b/g/n/ac Wave 1 oraz ac Wave 2.
10. Obsługa nie mniej niż 128 SSID jednocześnie.
11. Centralne zarządzanie aktualizacją oprogramowania punktów dostępowych z poziomu kontrolera.
12. Urządzenie jest zarządzanie poprzez WebUI (https) oraz CLI (ssh, konsola szeregowa RS232).
13. Kontrola dostępu użytkowników do zasobów sieci poprzez definiowanie list kontroli dostępu w warstwie 2 ISO/OSI (MAC adres) oraz w warstwie 3 ISO/OSI (adresy IP).

14. Kontrola dostępu bazuje na rolach użytkowników.
15. Możliwość konfiguracji izolacji klientów w warstwie 2 ISO/OSI dla tego samego SSID.
16. Centralne zarządzanie wykorzystywanymi kanałami radiowymi oraz mocą sygnału poszczególnych punktów dostępowych. Zmiana kanału radiowego na jednym punkcie dostępowym z uwagi na wykryte interferencje lub ręczna konfiguracja ze strony administratora nie wymaga zmiany kanału dla wszystkich innych punktów dostępowych podłączonych do kontrolera w ramach wspólnej konfiguracji (np. punkty dostępowe, które znajdują się w innych miejscach niż są interferencje).
17. Dobieranie optymalnych kanałów transmisyjnych za pomocą mechanizmów statystycznych bez konieczności przerywania transmisji danych.
18. Monitorowanie na bieżąco kanałów radiowych, na których pracują AP.
19. Centralne zarządzanie siecią MESH stworzoną z punktów dostępowych w celu zwiększenia zasięgu pracy systemu.
20. Automatyczne równoważenie obciążenia pomiędzy wieloma punktami dostępowymi.
21. Równoważenie obciążenia pomiędzy częstotliwością 2,4GHz a 5GHz (zachęcanie klientów do łączenia się na częstotliwości 5GHz w celu wykorzystania większej liczby kanałów dostępnych w tym paśmie, tzw. band steering).
22. Optymalizacja wydajności sieci przy podłączonych klientach WLAN obsługujących różną przepustowość (sterowanie czasem dostępu do access pointa w celu unikania spowalniania wszystkich klientów przez najwolniejsze jednostki, tzw. airtime fairness).
23. Praca w trybie Distributed Forwarding/FlexConnect, czyli w trybie gdzie ścieżka danych nie wymaga przechodzenia przez kontroler (bez konieczności tunelowania ruchu z punktu dostępowego do kontrolera, a jednocześnie z zachowaniem wszystkich funkcjonalności systemu zarządzanego kontrolerem).
24. Możliwość tunelowania ruchu z punktów dostępowych poprzez funkcję CAPWAP do kontrolera lub równoważną funkcję tunelującą. Tunelowanie musi być możliwe dla wybranych SSID przez administratora.
25. Wbudowany interfejs WWW dla uwierzytelniania użytkowników sieci bezprzewodowej (w oparciu o wewnętrzną bazę kont lub zewnętrzny serwer uwierzytelniania, tzw. captive portal).
26. Wbudowany captive portal dla gości z systemem generowania tymczasowych haseł dostępowych (specjalna rola administratora gości).
27. Obsługa funkcjonalności BYOD (Bring Your Own Device) – auto-provisioning oraz automatyczna konfiguracja klientów mobilnych, tj. automatyczne dostarczenie konfiguracji do urządzeń typu: smartfon, tablet, obsługa minimum 2000 użytkowników BYOD w ramach dostarczonej licencji. Obsługa systemów operacyjnych, nie mniej niż Apple iOS (iPhone/iPad/iPOD), Android, Windows XP/7/8/10 i Linux. Funkcja może być realizowana na zewnętrznym (redundantnym, maksymalna wielkość 2U dla dwóch appliance) komponencie programowo-sprzętowym pochodzącym od tego samego producenta, co kontroler.
28. Wbudowany serwer DHCP.
29. Integracja z Active Directory, LDAP.
30. Dynamiczne przypisanie VLAN klientom na podstawie uwierzytelniania na postawie danych z systemu AAA.
31. Dedykowany interfejs do generowana tymczasowych kont dla gości – tzw. funkcja Lobby Admin, gdzie wybrani użytkownicy w systemie mogą tworzyć konta dla gości.
32. Wsparcie dla systemów lokalizacji.
33. Wszystkie licencje dla opisanych funkcji – w szczególności WIPS/WIDS, Captive Portal, obsługa BYOD zostały dostarczone razem z urządzeniami.
34. System ochrony (WIPS/WIDS) sieci WLAN:
    a) Wykrywanie obcych/wrogich punktów dostępowych;
    b) Wykrywanie pokrywających się SSID ze skonfigurowanymi na kontrolerze (tzw. „Same SSID Attack”);

c) Wysyłanie ramek deasocjacynych przy wykryciu ataku „Same SSID";
d) Ochrona przed atakami DoS;
e) Ochrona przed próbami nieautoryzowanego dostępu przez zgadywanie haseł (password guessing);
f) Limitowanie pasma (rate limiting).

35. Obsługa następujących protokołów / standardów:
    a) WEP, WPA-TKIP, WPA2-AES, 802.11i,
    b) 802.1x,
    c) 802.1q,
    d) 802.11e,
    e) SNMP v2/v3,
    f) IPv4 i IPv6,
    g) Możliwość rozbudowy o standard 802.11u i HotSpot 2.0 lub PassPoint.
36. Obsługa wykrywania aplikacji których używają użytkownicy sieci Wifi
37. Obsługa urządzeń Access-Point z wbudowanym przełącznikiem LAN – minimum 4 portowym 10/100/1000Mb. Porty przełącznika muszą być zarządzane z kontrolera.
38. Wbudowana obsługa map wewnętrznych budynku z położeniem urządzeń Access-Point
39. Gwarancja i serwis – na dzień dzisiejszy kontrolery posiadają 38-miesięczny autoryzowany serwis producenta dla sprzętu oraz oprogramowania. Serwis zapewnia bezpośredni dostęp do ekspertów technicznych producenta poprzez centrum pomocy technicznej producenta, obejmujący pomoc ekspertów technicznych producenta przy diagnostyce problemów związanych z funkcjonowaniem urządzeń i oprogramowania. Dodatkowo w ramach serwisu jest zapewniony oficjalny dostęp do poprawek i nowych wersji oprogramowania. Serwis zapewnia wymianę lub naprawę uszkodzonego sprzętu w rygorze Następny Dzień Roboczy.