**Zał. nr 1 do SWZ.**

**Opis przedmiotu zamówienia**

Zakup urządzeń oraz systemu do uruchomienia sieci bezprzewodowej WiFi dla Onkologicznego Centrum Wsparcia Badań Klinicznych w Świętokrzyskim Centrum Onkologii w Kielcach, która obejmuje:

1. Opracowanie dokumentacji projektowej w tym analizy przedwdrożeniowej i harmonogramu wdrożenia.
2. Dostawę wymaganych urządzeń i oprogramowania.
3. Montaż, instalację i konfigurację urządzeń i oprogramowania.
4. Przeprowadzenie instruktaży stanowiskowych dla administratorów.
5. Przeprowadzenie pomiarów i testów rozwiązania.
6. Opracowanie dokumentacji powykonawczej.
7. Zapewnienie obsługi gwarancyjnej, serwisu i wsparcia technicznego na okres trwania umowy.

**Wymagania szczegółowe:**

1. **Wymagania dla dostarczanych urządzeń i oprogramowania:**
2. Zamawiający wymaga, by dostarczony sprzęt był nowy oraz nieużywany (przy czym Zamawiający dopuszcza, by sprzęt był rozpakowany i uruchomiony przed jego dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania sprzętu, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem).
3. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonego przedmiotu zamówienia nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich, w szczególności Zamawiającemu nie mogą być zaoferowane sprzęt i oprogramowanie, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego.
4. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej w dniu poprzedzającym dzień składania ofert.
5. Wymagane jest, aby dostarczone urządzenia były sprzętem zakupionym w oficjalnym kanale sprzedaży producenta na terenie Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji powyższego wymogu u przedstawiciela producenta oferowanego rozwiązania.
6. Urządzenia, które Wykonawca dostarcza Zamawiającemu muszą spełniać wszelkie wymogi i normy zastrzeżone przez obowiązujące w Polsce przepisy oraz posiadać certyfikaty Wi-Fi Alliance i Bluetooth SIG.
7. Wymagane jest, aby data produkcji dostarczonych urządzeń nie była późniejsza niż 6 miesięcy.
8. **Montaż, instalacja i konfiguracja urządzeń i oprogramowania:**
9. Montaż i instalacja będzie realizowana w oparciu o istniejącą infrastrukturę LAN Zamawiającego.
10. Wykonawca zobowiązany jest w szczególności dostarczyć, zainstalować, skonfigurować i uruchomić urządzenia zgodnie z wytycznymi Zamawiającego.
11. Do czasu przetestowania urządzenia i podpisania protokołu odbioru końcowego, Wykonawca ponosi ryzyko ich niesprawności lub wystąpienia innych wad, chyba że niesprawność lub wada powstały z winy Zamawiającego.
12. Do punktów dostępowych muszą być dostarczone oficjalne, certyfikowane przez producenta punktów dostępowych, zestawy montażowe pozwalające na montaż na płaskiej powierzchni.
13. Wdrożone rozwiązanie musi być kompletne, gotowe do użytku a wszelkie niezbędne akcesoria konieczne do jego uruchomienia muszą być dostarczone przez Wykonawcę.
14. **Warunki gwarancji, serwisu i wsparcia technicznego:**
15. Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancją producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez przysłanie sprawnego urządzenia i zwrot zepsutego urządzenia do producenta. Reakcja na zgłoszenie musi nastąpić najpóźniej następnego dnia roboczego (tj. poniedziałek – piątek, godz. 07:00-15:00), a wysłanie sprawnego urządzenia musi najpóźniej następnego dnia roboczego od zarejestrowania zgłoszenia gwarancyjnego. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.
16. Wsparcie serwisowe producenta dla kontrolerów w zakresie dostępu do poprawek oprogramowania urządzenia w trybie 24x7. Całość świadczeń serwisowych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia serwisowego producenta.
17. Wsparcie serwisowe Wykonawcy dla oferowanego rozwiązania w zakresie konsultacji konfiguracji i zmian konfiguracyjnych w ilości 24 roboczogodzin.
18. Zamawiający wymaga by zapewniona była naprawa lub wymiana urządzeń lub ich części, zgodnie z metodyką i zaleceniami producenta i Zamawiającego.
19. Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta.
20. Usługi wsparcia technicznego w zakresie obsługi zgłoszeń gwarancyjnych będą świadczone przez personel Wykonawcy posiadający odpowiednie kwalifikacje i uprawnienia.
21. Wykonawca przejmuje na siebie wszelkie obowiązki związane z obsługą serwisową oferowanego sprzętu w okresie trwania umowy.
22. Serwis i wsparcie techniczne będzie świadczone w siedzibie Zamawiającego (miejscu instalacji i użytkowania urządzeń), w języku polskim (przyjmowanie zgłoszeń i realizacja świadczeń).
23. Wykonawca udostępni pojedynczy punkt przyjmowania zgłoszeń dla całości sprzętu i oprogramowania dostarczonego w ramach przedmiotu zamówienia.
24. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego tj. poniedziałek – piątek, godz. 07:00-15:00), e-mail lub WWW (przez całą dobę).
25. Zamawiający otrzyma bezpośredni dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją całości sprzętu i oprogramowania dostarczonego w ramach przedmiotu zamówienia w godzinach pracy Zamawiającego.
26. Czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego.
27. W okresie gwarancji koszty serwisu urządzeń są po stronie Wykonawcy. Wykonawca gwarantuje Zamawiającemu pełny zakres obsługi gwarancyjnej nieodpłatnie (z wyjątkiem uszkodzeń z winy użytkownika).
28. Wykonawca zobowiązuje się przenieść na Zamawiającego wszelkie uprawnienia z tytułu gwarancji na sprzedawany sprzęt wydając mu w tym celu odpowiednie dokumenty, najpóźniej w chwili podpisywania protokołu uruchomienia przedmiotu umowy, w tym instrukcje obsługi, karty gwarancyjne.
29. Zamawiający uzyska bezpośredni dostęp do stron internetowych producentów rozwiązań, umożliwiający:
30. pobieranie nowych wersji oprogramowania,
31. dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
32. dostęp do pomocy technicznej producenta.
33. **Dostawa 8 punktów dostępowych spełniających poniższe wymagania:**
34. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków.
35. Punkt dostępowy musi być wyposażony w trzy niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac/ax, 2.4GHz b/g/n/ax, 6GHz ax.
36. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej, w szczególności kontrolerem opisanym w tym dokumencie.
37. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:
    1. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https
    2. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki
    3. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.
38. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:
    1. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako kontroler a pozostałych punktów dostępowych w klastrze kontrolerów zapasowych
    2. W przypadku awarii punktu dostępowego pełniącego rolę głównego kontrolera, kolejny punkt dostępowy musi przejąć jego rolę w sposób automatyczny, przełączanie takie występuje aż do momentu awarii ostatniego punkt dostępowego pracującego w klastrze
    3. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe
    4. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję
    5. Tworzenie klastra złożonego z co najmniej 120 urządzeń.
39. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP.
40. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa.
41. W system musi być wbudowany serwer DHCP.
42. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów.
43. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
    1. EAP-TLS
    2. PEAP-MSCHAPv2
    3. PEAP-GTC
    4. TTLS-MSCHAPv2.
44. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP (w tym ActiveDirectory).
45. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID, oraz do 512 urządzeń klienckich per radio.
46. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.
47. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
    1. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania
    2. Zewnętrzny portal WWW.
48. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT.
49. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne.
50. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
    1. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe
    2. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu
    3. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma
    4. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału
    5. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz
    6. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g)
    7. Wsparcie dla 802.11d oraz 802.11h
    8. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane.
51. Minimalizacja interferencji związanych z sieciami 3G/4G LTE.
52. Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrz budynkowej oraz jako dostęp do konsoli urządzenia.
53. Obsługa roamingu klientów w warstwie 2.
54. Obsługa monitoringu przez SNMP.
55. Obsługa logowania na zewnętrznym serwerze SYSLOG.
56. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
57. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
    1. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością
    2. Wykorzystanie pasma
    3. Ilość klientów korzystających z systemu/interferujących
    4. Ilość ramek wejściowych/wyjściowych dla każdego radia
    5. Ilość odrzuconych/błędnych ramek/s dla każdego radia
    6. Szum tła dla każdego radia
    7. Wyświetlanie logów systemowych.
58. Punkt dostępowy musi wbudowane anteny dookólne do pracy w trybie 2x2: MU-MIMO. Uzysk anten nie powinien być mniejszy niż:
    1. 4,5 dBi dla 2,4 GHz
    2. 6,9 dBi dla 5 GHz
    3. 6,2 dBi dla 6 GHz.
59. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2, 802.11ax.
60. Praca w trybie MIMO 2X2:2.
61. Specyfikacja wspieranych standardów:
    1. 802.11b: DSSS
    2. 802.11a/g/n/ac: OFDM
    3. 802.11ax: OFDMA z 8 Resource units (37 dla radia 6 GHz).
62. Specyfikacja wpieranych modulacji:
    1. 802.11b: BPSK, QPSK, CCK
    2. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
    3. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
    4. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.
63. Specyfikacja wspieranych szerokości kanałów pracy:
    1. 802.11n high-throughput (HT) wspiera MT20/40
    2. 802.11ac very high-throughput (VHT) wspiera VHT20/40/80
    3. 802.11ax high efficiency (HE) wspiera HE20/40/80/160.
64. Obsługiwane częstotliwości:
    1. 2.400 ~ 2.4835 GHz (ISM)
    2. 5.150 ~ 5.250 GHz (low band)
    3. 5.250 ~ 5.350 GHz (mid band)
    4. 5.470 ~ 5.725 GHz (Europa)
    5. 5.725 ~ 5.850 GHz (high band)
    6. 5.925 ~ 6.425 GHz (U-NII-6)
    7. 6.525 ~ 6.875 GHz (U-NII-7)
    8. 6.875 ~ 7.125 GHz (U-NII-8).
65. Wspierane prędkości przesyłania danych (Mbps)
    1. 802.11b: 1,2,5.5,11
    2. 802.11a/g 6,9,12,18,24,36,48,54
    3. 802.11n: od 6.5 do 300 (MCS0 do MCS15, HT20 do HT40) 400 z 256-QAM
    4. 802.11ac: od 6.5 do 867 (MCS0 do MCS9, NSS= 1 do 2, HE20 do HE40)
    5. 802.11ax (2,4 GHz) od 3.6 do 574 (MCS0 do MCS11, NSS=1 do 2, HE20 do HE40)
    6. 802.11ax (5GHz) 3.6 do 1201 (MCS0 do MCS11, NSS = 1 do 2, HE20 do HE80)
    7. 802.11ax (6GHz) 3.6 do 2402 (MCS0 do MCS11, NSS = 1 do 2, HE20 do HE160).
66. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm
    1. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz
    2. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac
    3. Wsparcie dla:
       * MRC (Maximal ratio combining)
       * CDD/CSD (Cyclic delay/shift diversity)
       * STBC (Space-time block coding)
       * LDPC (Low-density parity check)
       * Technologia TxBF
       * TWT (Target Wait Time).
67. Punkt dostępowy musi posiadać co najmniej
    1. 2 interfejsy 100/1000/2500 Base-T
       * z funkcją PoE 802.3at/bt
       * zgodne ze standardem 802.3az Energy Effcient Ethernet EEE
    2. 1 interfejs konsoli szeregowej
    3. zasilanie PoE zgodne z 802.3at/802.3.bt
       * maksymalny pobór mocy 29.4 W PoE
    4. przycisk przywracający konfigurację fabryczną
    5. Kontrolka LED do określania statusu systemu i interfejsów radiowych
    6. slot zabezpieczający Keningston
    7. Zigbee (802.15.4)
    8. Bluetooth 5.0 Low Energy (BLE5.0)
    9. USB 2.0 (host) (Type A)
    10. Port zasilania DC 12VDC.
68. Parametry pracy urządzenia:
    1. Temperatura otoczenia: 0°C- +50°C
    2. Wilgotność 5% - 95% nie skondensowana
    3. Znak CE
    4. EN 300 019.
69. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac wave 2/ ax.
70. Wszystkie wymagane na urządzeniu funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji, o ile nie wyspecyfikowano inaczej.
71. **Dostawa 2 kontrolerów sieci bezprzewodowej spełniających poniższe wymagania:**
72. Dwa, pracujące w klastrze HA kontrolery muszą w pełni obsługiwać punkty dostępowe, opisane w tym dokumencie w punkcie IV.
73. Kontrolery muszą zarządzać siecią bezprzewodową złożoną z co najmniej 10 punktów dostępowych z możliwością rozbudowy do co najmniej 1000 punktów dostępowych. Dopuszcza się rozbudowę poprzez dodanie odpowiednich licencji i zmianę parametrów maszyn wirtualnych. Wartości łączne, dla klastra kontrolerów pracujących w HA.
74. Kontrolery muszą posiadać możliwość obsługi łącznie co najmniej 1500 użytkowników
75. Każdy z wymaganych kontrolerów musi posiadać wyspecyfikowane w tym dokumencie funkcje:
    1. Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym.
    2. Kontroler musi mieć możliwość pracy w klastrze w celu zapewnienia zwiększenia pojemności, zapewnienia nieprzerwanej pracy, balansowania obciążenia. Przełączanie użytkowników w obrębie klastra ma się odbywać niezauważalnie z poziomu klienta tzn. żadne sesje klienta nie mogą być przerwane. Dotyczy to przełączanie związanego tak z roamingiem jak i awarią kontrolera
    3. Kontroler musi posiadać mechanizm automatyzacji doboru kanałów pracy, mocy nadawania. Mechanizm musi mieć możliwość wymiany informacji pomiędzy wszystkimi kontrolerami w sieci a centralnym punktem zarządzania.
    4. Kontroler musi mieć możliwość przeprowadzenia Live update polegającego na aktualizacji klastra kontrolerów oraz punktów dostępowych bez przerwania obsługi urządzeń klienckich
    5. Kontroler ma mieć możliwość współdzielenia zasobów punktów dostępowych innemu kontrolerowi. Główny kontroler zezwala na zarzadzanie danym wirtualnym punktem dostępowym innemu kontrolerowi, na którym ten ruch jest terminowany. Kontroler ten może samodzielnie konfigurować wszystkie polityki w ramach udostępnionego wirtualnego punktu dostępowego. Funkcjonalność ta umożliwia stworzenie bezpiecznej sieci ruchu obcego np. ruch gościnny lub IoT.
    6. Kontroler musi mieć możliwość udostępniania informacji na temat stanu sieci poprzez API
    7. Kontroler musi mieć możliwość uaktualniania poszczególnych modułów np. odpowiedzialnego na dynamiczny dobór kanałów, analizę aplikacji itp. bez konieczności uaktualniana całego systemu operacyjnego
    8. Kontroler musi mieć możliwość terminowania ruchu z przełączników tego samego producenta w celu ujednolicenia polityk bezpieczeństwa dla sieci przewodowej i bez przewodowej
    9. Wspieranie wielu wersji oprogramowania. Funkcja ta umożliwia administratorowi przetestowanie nowych funkcjonalności na wybranym obszarze sieci bez konieczności aktualizowania całego środowiska
    10. Kontroler musi być wyposażony w technologię, która umożliwi optymalizację rozłożenia klientów pomiędzy dostępnymi punktami dostępowymi oraz pasmami (2,4 GHz oraz 5 GHz). Mechanizm musi zapewnić wykluczenie problemów z tzw. Sticky clients
    11. Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall)
    12. Kontroler musi być wyposażony w funkcjonalność umożliwiającą rozpoznawanie aplikacji. Liczba domyślnie rozpoznawanych aplikacji minimum 2000
    13. Kontroler musi wspierać protokoły wykorzystywane przez urządzenia Apple TV oraz Google chromcast
    14. Kontroler musi wspierać mechanizmy ochrony sieci bezprzewodowej przed atakami hackerskimi
    15. Kontroler musi mieć możliwość integracji z systemami centralnego zarządzania siecią przewodową i bezprzewodową
    16. Kontroler musi mieć możliwość wprowadzenia klasyfikacji treści przeglądanych przez użytkowników stron www (np. przemoc, hazard itp.) oraz określenia ich reputacji. (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie, dostęp do bazy treści może być oferowany w formie subskrypcji, o ile dostępna jest ona na co najmniej 10 lat bez konieczności jej odnawiania)
    17. Kontroler musi mieć możliwość automatycznej klasyfikacji i monitoringu jakości połączenia dla aplikacji komunikacyjnych takich jak:
        1. Apple FaceTime
        2. Alcatel Lucent New Office Environment (NOE)
        3. Microsoft Lync/Skype for Business
        4. Cisco Jabber
        5. Cisco Skinny Call Control Protocol (SCCP)
        6. Spectralink Voice Priority (SVP)
        7. SIP
        8. H.323
        9. Vocera
        10. Cellular Wi-Fi Calling.
76. Kontroler ma być dostępny w formie maszyny wirtualnej uruchamianej w środowisku VMware ESXi lub KVM hypervisor.
77. Kontroler musi wspierać poniższe formy uwierzytelniania:
    1. IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, EAP-POTP, EAP-GTC, EAP-TLV, EAP-AKA, EAP-Experimental, EAP-MD5)
    2. RFC 2548 Microsoft vendor-specifc RADIUS attributes
    3. RFC 2716 PPP EAP-TLS
    4. RFC 2865 RADIUS authentication
    5. RFC 3579 RADIUS support for EAP
    6. RFC 3580 IEEE 802.1X RADIUS guidelines
    7. RFC 3748 extensible authentication protocol
    8. MAC address authentication
    9. Web-based captive portal authentication.
78. Kontroler musi wspierać poniższe serwery autoryzacji:
    1. Internal database
    2. LDAP/SSL secure LDAP
    3. RADIUS
    4. TACACS+.
79. Kontroler musi wspierać następujące protokoły szyfrowania:
    1. CCMP/AES
    2. WEP 64- and 128-bit
    3. TKIP
    4. SSL and TLS:
       1. RC4 128-bit
       2. RSA 1024-bit
       3. RSA 2048-bit
    5. L2TP/IPsec (RFC 3193)
    6. XAUTH/IPsec
    7. PPTP (RFC 2637).
80. Kontroler musi wspierać Site-to-site VPN dla sposobów autentykacji X.509 PKI, IKEv2, IKE PSK, IKE aggressive mode.
81. Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne (wieczyste), nie dopuszcza się licencji czasowych, o ile nie wyspecyfikowano inaczej.
82. Wymagania dotyczące kontrolera nadrzędnego:

Jeden z ww. kontrolerów musi być kontrolerem nadrzędnym spełniającym poniższe wymagania:

* 1. Kontroler ma być dostępny w formie maszyny wirtualnej uruchamianej w środowisku VMware ESXi lub KVM hypervisor.
  2. Kontroler musi zarządzać siecią bezprzewodową złożoną z minimum 50 punktów dostępowych i kontrolerów podrzędnych, w szczególności punktów dostępowych i kontrolerów opisanych w tym dokumencie
  3. Kontroler musi umożliwiać stworzenie spójnej, centralnie zarządzanej i sterowanej struktury hierarchicznej złożonej co najmniej z 5 kontrolerów podrzędnych.
  4. Kontroler musi mieć możliwość rozbudowy do co najmniej 1000 punktów dostępowych. Dopuszcza się rozbudowę poprzez dodanie odpowiednich licencji i zmianę parametrów maszyn wirtualnych
  5. Kontroler musi obsługiwać co najmniej 5000 użytkowników
  6. Kontroler musi zapewniać redundancję, realizowaną poprzez dostarczenie licencji umożliwiającej instalację kilku maszyn wirtualnych w ramach pojedynczej licencji lub dostarczenie licencji na co najmniej dwa kontrolery lub dostarczenie licencji typu HA, pozwalającej na instalację dodatkowej maszyny wirtualnej
  7. Kontroler musi wspierać jako kontrolery podrzędne kontrolery opisane w tym dokumencie
  8. Kontroler ma umożliwić konfigurację klastrów kontrolerów podrzędnych w celu zapewnienia wysokie dostępności oraz rozkładania obciążenia
  9. Kontroler musi zapewnić centralny punkt dystrybucji licencji dla kontrolerów podrzędnych
  10. Kontroler musi umożliwiać tworzenie centralnego planu rozłożenia kanałów sieci bezprzewodowej oraz mocy jej nadawania dla całej sieci bezprzewodowej uwzględniając wszystkie kontrolery podrzędne
  11. Kontroler musi umożliwiać aktualizacje w locie klastra kontrolerów podrzędnych bez przerywana pracy sieci bezprzewodowej
  12. Kontroler musi umożliwiać tworzenie odseparowanej sieci gościnnej poprzez podłączenie osobnego kontrolera w sieci DMZ i udostępnienie zasobów punktów dostępowych zarządzanych poprzez kontroler podrzędny. (terminowanie ruchy z AP na dwóch niezależnych kontrolerach)
  13. Kontroler musi umożliwiać bezstratny roaming pomiędzy kontrolerami podrzędnymi
  14. Wszystkie dostarczone licencje i obsługiwane funkcje muszą być permanentne (wieczyste), nie dopuszcza się licencji czasowych o ile nie wyspecyfikowano inaczej.

1. **Dokumentacja projektowa i powykonawcza:**
2. Dokumentacja projektowa zawierająca:
   1. wyniki analizy przedwdrożeniowej, wizji lokalnych i uzgodnień (w tym scenariusze testów akceptacyjnych) z Zamawiającym
   2. harmonogram realizacji projektu uzgodniony i zatwierdzony przez Zamawiającego.
3. Dokumentacja powykonawcza dostarczona przez Wykonawcę na etapie odbioru końcowego zawierająca:
   1. wykaz urządzeń oraz schematy ich połączeń fizycznych wraz z oznaczeniami medium, protokołów, gniazd, urządzeń. Rzuty pionowe pomieszczeń w wersji elektronicznej udostępni Zamawiający.
   2. wykaz serwisów/usług, aplikacji oraz schematy ich połączeń logicznych wraz z oznaczeniami: adresacji numerycznej (IP), adresacji symbolicznej (DNS)
   3. nazewnictwa komponentów sprzętowych i programowych
   4. protokołów i interfejsów komunikacyjnych
   5. wykaz ustawień i parametrów konfiguracyjnych urządzeń i oprogramowania
   6. wykaz kont, loginów, uprawnień, haseł
   7. procedury diagnostyki, backupu/archiwizacji, zgłoszeń serwisowych
   8. instrukcje dla użytkownika i administratora
   9. wymagane zezwolenia, certyfikaty, licencje
   10. wyniki testów akceptacyjnych/odbiorowych.
4. Forma i ilość kopii dokumentacji:
   1. wersja elektroniczna (PDF) w języku polskim w jednym egzemplarzu.