Specyfikacja techniczna – załącznik nr 2 do SWZ
Zadanie nr 3: Kontroler sieci bezprzewodowej 1 szt.

Zamawiający posiada obecnie sieć WiFi zbudowaną i w pełni zarządzaną przez dwa kontrolery **Cisco AIR-CT5508**, a także AccessPointy **AIR-CAP3502I-E-K9** i **AIR-CAP3502E-E-K9** .
Zamawiający wymaga dostarczenia urządzenia producent/model: **Cisco AIR-CT5508-250-K9** lub urządzenia równoważnego spełniającego poniższe wymagania, które jest w pełni kompatybilne i współpracuje ze sprzętem posiadanym przez Zamawiającego, tj. kontrolerami **Cisco AIR-CT5508** oraz AccessPointami **AIR-CAP3502I-E-K9** i **AIR-CAP3502E-E-K9**.

Wymagane parametry urządzenia równoważnego:

1. Urządzenie w pełni kompatybilne i współpracuje ze sprzętem posiadanym przez Zamawiającego, tj. kontrolerami **Cisco AIR-CT5508** oraz AccessPointami **AIR-CAP3502I-E-K9** i **AIR-CAP3502E-E-K9**.
2. Urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego, a w szczególności:
   a. zarządzanie politykami bezpieczeństwa;
   b. wykrywanie intruzji nieuprawnionych dostępów;
   c. zarządzanie pasmem radiowym;
   d. zarządzanie mobilnością;
   e. zarządzanie jakością transmisji;
3. Urządzenie powinno działać zgodnie z protokołem CAPWAP (RFC 5415) lub równoważnym;
4. Urządzenie powinno zapewniać obsługę co najmniej 250 punktów dostępowych z możliwością rozszerzenia do min. 500 (kratowe lub klasyczne);
5. Jeżeli do powyższego wymagane są licencje to należy dostarczyć je z urządzeniem;
6. Urządzenie powinno posiadać min. 8 interfejsów GE 1000BaseX, umożliwiających obsadzenie wkładkami SFP;
7. Urządzenie powinno zapewniać co najmniej zarządzanie pasmem radiowym punktów dostępowych a w tym:
   a. automatyczna adaptacja do zmian w czasie rzeczywistym;
   b. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia);
   c. dynamiczne przydzielanie kanałów radiowych;
   d. wykrywanie, eliminacja i unikanie interferencji;
   e. równoważenie obciążenia punktów dostępowych;
   f. tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych;
   g. automatyczna dystrybucja klientów pomiędzy punkty dostępowe;
   h. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych;

8. Urządzenie powinno zapewniać mapowanie SSID do segmentów VLAN w sieci przewodowej:
   a. 1:1;
   b. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty);
   c. możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID);
9. Urządzenie powinno zapewniać obsługę sieci kratowych, a w tym obsługiwana powinna/o być:
   a. komunikacja między punktami dostępowymi bez medium kablowego;
   b. separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi z możliwością tworzenia wyjątków);
   c. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo);
   d. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji);
   e. autoryzacja punktów dostępowych w oparciu o certyfikaty X.509, adresy MAC;
10. urządzenie powinno obsługiwać co najmniej poniższe mechanizmy bezpieczeństwa:
    a. 802.11i, WPA2, WPA, WEP;
    b. 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST);
    c. obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, LDAP, wbudowana lokalna baza użytkowników (min. 2.000 wpisów);
    d. możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID;
    e. możliwość profilowania użytkowników: przydział sieci VLAN, przydział list kontroli dostępu (ACL);
    f. uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 (wykrywanie podszywania się punktów dostępowych użytkowników pod adresy infrastruktury) – 802.11w lub podobny;
    g. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty X.509;
    h. obsługa list kontroli dostępu (ACL);
    i. wykrywanie i dezaktywacja obcych punktów dostępowych;
    j. wbudowany system IDS wykrywający typowe ataki na sieci bezprzewodowe (fake AP, netstumbler, deathentication flood itp.);
    k. współpraca z systemami IDS/IPS;
    l. ochrona kryptograficzna (DTLS lub równoważny) ruchu kontrolnego i ruchu użytkowników CAPWAP;
    m. DHCP proxy;
11. urządzenie powinno obsługiwać ruch unicast IPv4 i IPv6

12. urządzenie powinno obsługiwać ruch multicast IPv4 i IPv6 a w tym:
    a. IGMP / MLD snooping;
    b. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym);
    c. obsługa konwersji ruchu multicast do unicast;
13. urządzenie powinno obsługiwać mobilność (roaming) użytkowników (L2 i L3 – IPv4 i IPv6, w ramach i pomiędzy kontrolerami)
14. urządzenie powinno obsługiwać co najmniej poniższe mechanizmy QoS:
    a. 802.1p;
    b. WMM, TSpec;
    c. ograniczanie pasma per użytkownik;
    d. Call Admission Control – ze statyczną definicją pasma i dynamiczna w oparciu o analizę profili ruchu;
    e. U-APSD;
15. urządzenie powinno zapewniać obsługę dostępu gościnnego (IPv4 i IPv6):
    a. przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony);
    b. możliwość kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta;
    c. możliwość konfiguracji jako dedykowanego kontrolera do obsługi ruchu gości – całość ruchu z SSID dostępu gościnnego zebranego na pozostałych kontrolerach musi być przesyłana do tego kontrolera (umieszczonego w publicznej części sieci) w sposób zapewniający logiczną separację od ruchu wewnętrznego;
16. urządzenie powinno współpracować z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne i zapewniać obsługę tagów telemetrycznych
17. urządzenie powinno zapewniać możliwość pracy redundantnej (N+1) oraz zastosowanie redundancji 1:1 (active/standby) zapewniającej:
    a. utrzymanie sesji punktów dostępowych oraz urządzeń klienckich na wypadek awarii aktywnego kontrolera;
    b. synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej;
18. urządzenie powinno zapewniać co najmniej możliwość analizy ruchu przechodzącego przez kontroler pozwalającą na identyfikację oraz klasyfikację na poziomie aplikacji oraz możliwość markowania lub odrzucania ruchu
19. urządzenie powinno wspierać możliwość zbierania i eksportu statystyk ruchowych za pomocą co najmniej protokołu Netflow/JFlow lub odpowiednika
20. urządzenie powinno zapewniać możliwość profilowania urządzeń podłączających się do sieci bezprzewodowej oraz przydzielanie na podstawie typu urządzenia odpowiednich uprawnień i parametrów dostępowych
21. urządzenie powinno obsługiwać mechanizmy pozwalające na dezaktywację modułów radiowych w określonych godzinach w celu redukcji poboru energii przez system

22. urządzenie powinno posiadać zarządzanie co najmniej przez HTTPS, SNMPv3, SSH oraz port konsoli szeregowej
23. urządzenie powinno być wyposażone w dodatkowy redundantny zasilacz instalowany w obudowie urządzenia
24. Wyposażenie urządzenia: urządzenie musi być wyposażone w zestaw do montażu w szafie rak - szyny montażowe długie (do montażu z przodu i z tyłu szafy rack);