UNIWERSYTET JAGIELLOŃSKI
DZIAŁ ZAMÓWIEŃ PUBLICZNYCH
ul. Straszewskiego 25/3 i 4, 31-113 Kraków
tel. +48 12 663 39 03;
e-mail: www.uj.edu.pl
www.przetargi.uj.edu.pl

Kraków, dnia 24.08.2023 r.

Do wszystkich Wykonawców

Dotyczy: postępowania prowadzonego w trybie podstawowym bez możliwości negocjacji na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2021 r. poz. 1129 z późn. zm.), na wyłonienie Wykonawcy w zakresie dostawy i uruchomienia instalacji bezprzewodowego internetu wraz z urządzeniami aktywnych Access Point oraz switchami w budynku WZiKS przy ul. Łojasiewicza 4 w Krakowie

Pytania i odpowiedzi do SWZ

Szanowni Państwo,

Zamawiający przedstawia poniżej treść pytań i udzielonych odpowiedzi do treści Specyfikacji Warunków Zamówienia (SWZ), w postępowaniu na wyżej opisany zakres przedmiotowy.

Pytanie nr 1
Opisany model AP jest produktem, który już nie jest dostępny, proszę o informację czy Zamawiający dopuszcza produkty odnowione przez dostawców wskazanego modelu. Jeżeli nie to proszę o informacje z jakim kontrolerem mają współpracować oraz jaka jest wersja oprogramowania kontrolera.?

Odpowiedź nr 1
Zamawiający informuje iż, dopuszcza wyłącznie produkty fabrycznie nowe, z aktualnej oferty producenta i posiadające pełne wsparcie techniczne producenta.
Ponadto model punktu dostępowego wymieniony dokumencie pn. „Pomiary wziks" został wykorzystany wyłącznie do przygotowania pomiaru propagacji sygnału rzeczywistego i jest to tylko model przykładowy, natomiast opis modelu wymaganego zawiera Załącznik 1 do niniejszych pytań i odpowiedzi.
Ponadto Zamawiający uzupełnia opis o „Ogólne wymagania dla sieci bezprzewodowej" oraz o „wymagania dla chmurowego systemu zarządzania", które zawiera Załącznik 2 do niniejszych pytań i odpowiedzi.

Zamawiający informuje, iż powyższe pytania i odpowiedzi do SWZ stanowią jej integralną część, a przy tym z uwagi na ich zakres i charakter oraz wpłynęły na konieczność zamiany ogłoszenia o zamówieniu i tym samym doprowadziły do przedłużenia terminu składania ofert. Dlatego też, Zamawiający zawiadamia, iż terminy składania i otwarcia ofert oraz związania ofertą ulegają zmianie:

Nowy termin składania ofert 1.09.2023 r. godz. 10:00
Nowy termin otwarcia ofert 1.09.2023 r. godz. 11:00
Termin związania ofertą do dnia 30.09.2023 r. włącznie

Z poważaniem,
Jerzy Wordliczek

Załącznik 1 do pytań i odpowiedzi z dnia 24.08.2023 r. opis urządzenia Access Point

1. Punkt dostępowy przeznaczony do instalacji wewnątrz pomieszczeń
2. Punkt dostępowy musi posiadać cztery interfejsy radiowe pozwalające na obsługę:
    a. Pasma 2.4 GHz min. 2x2:2 MIMO
    b. Pasma 5 GHz min. 2x2:2 MIMO
3. Punkt dostępowy musi zapewniać możliwość pracy w trybie dual 5 GHz
4. Punkt dostępowy musi zapewniać prawidłową pracę w zakresie temperatur od 0^0C do +40^0C
5. Punkt dostępowy musi być zgodny ze standardem WiFi6 – IEEE 802.11ax.
6. Punkt dostępowy musi posiadać możliwość zabezpieczenia z wykorzystaniem systemu Kensington
7. Punkt dostępowy musi być wyposażony w akcesoryjny system montażowy pozwalający na instalację na ścianie oraz suficie (również suficie podwieszanym)
8. Punkt dostępowy musi posiadać wbudowane diody LED sygnalizujące stan pracy.
9. Punkt dostępowy musi posiadać możliwość centralnego wyłączenia diod LED sygnalizujących stan pracy oraz włączenia lokalizacji (charakterystyczna sekwencja świecenia diod LED) punktu dostępowego
10. Punkt dostępowy musi być wyposażony w minimum 1 interfejs Ethernet 10/100/1000BASE-T i musi zapewniać możliwość zasilenia punktu dostępowego przez PoE+ (IEEE 802.3at – max. 30W).
11. Punkt dostępowy musi posiadać interfejs USB.
12. Punkt dostępowy musi zapewniać obsługę min. 8 SSID na każdym radiu WiFi
13. Punkt dostępowy musi zapewniać możliwość dołączenia min. 500 klientów na każdym radiu
14. Punkt dostępowy musi zapewniać możliwość pracy z wykorzystaniem dedykowanego kontrolera sieci bezprzewodowej i z wykorzystaniem systemu chmurowego producenta punktu dostępowego.
15. Producent musi zapewniać dedykowane kontrolery zarówno w postaci sprzętowej jak i wirtualnej możliwej do instalacji w środowisku VMWare oraz HyperV.
16. Punkt dostępowy musi posiadać mechanizmy zapewniające współpracę z min. dwoma kontrolerami zapewniającymi odporność na awarie i możliwość dalszej pracy w przypadku uszkodzenia pojedynczego kontrolera.
17. Punkt dostępowy musi zapewniać możliwość monitorowania i zarządzania z chmury producenta.
18. Punkt dostępowy musi posiadać możliwość konfiguracji suplikanta IEEE 802.1X i pozwalać na uwierzytelnianie z wykorzystaniem min. PEAP oraz EAP-TLS (certyfikat zainstalowany na punkcie dostępowym)
19. Punkt dostępowy musi zapewniać możliwość terminowania połączeń bezprzewodowych bezpośrednio na punkcie dostępowym i wpuszczania ruchu do wskazanej sieci VLAN (sieć VLAN musi być konfigurowalna dla każdego SSID z osobna oraz musi być możliwość jej przekazania dla każdego klienta uwierzytelnianego z wykorzystaniem systemu RADIUS w ramach RFC 3580).
20. Punkt dostępowy musi zapewniać możliwość tunelowania ruchu klienta bezprzewodowego przez sieć LAN do kontrolera i wpuszczania ruchu do wskazanej sieci VLAN na kontrolerze (sieć VLAN musi być konfigurowalna dla każdego SSID z osobna oraz musi być możliwość jej przekazania dla każdego klienta uwierzytelnianego z wykorzystaniem systemu RADIUS w ramach RFC 3580).
21. Punkt dostępowy musi zapewniać obsługę automatycznej sygnalizacji niezbędnych sieci VLAN z wykorzystaniem IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging (PBB)
22. Punkt dostępowy musi zapewniać obsługę tunelowania ruchu poprzez VxLAN.
23. Ruch kontrolny oraz tunelowany pomiędzy punktem dostępowym a kontrolerem musi mieć możliwość zabezpieczenia z wykorzystaniem IPSec.

24. Punkt dostępowy musi zapewniać możliwość konfiguracji puli sieci VLAN dla obsługi dużej liczby klientów z zapewnieniem ich separacji w sieci LAN z wykorzystaniem wielu sieci VLAN.
25. Punkt dostępowy musi zapewniać realizację filtrowania ruchu dla dołączonych klientów bezprzewodowych. Filtracja musi być możliwa dla każdego SSID z osobna oraz musi być możliwość przekazania informacji o filtracji dla każdego klienta uwierzytelnionego z wykorzystaniem systemu RADIUS.
26. Filtracja ruchu musi się odbywać na punkcie bezprzewodowym.
27. Punkt dostępowy musi zapewniać realizację roamingu bez konieczności współpracy z kontrolerem.
28. Punkt dostępowy musi zapewniać wsparcie IEEE 802.11r, IEEE 802.11k oraz IEEE 802.11v
29. Punkt dostępowy musi umożliwiać współpracę z dedykowanym systemem IDS oraz IPS oferowanym przez producenta punktu dostępowego
30. Punkt dostępowy musi zapewniać możliwość uwierzytelniania klientów bezprzewodowych z wykorzystaniem IEEE 802.1x i protokołów min.: EAP-TLS, EAP-TTLS, PEAP
31. Punkt dostępowy musi zapewniać obsługę WPA3
32. Punkt dostępowy musi zapewniać możliwość uwierzytelniania klientów z wykorzystaniem MAC Authentication
33. Punkt dostępowy musi zapewniać współpracę z serwerami RADIUS Authentication oraz RADIUS Accounting
34. Punkt dostępowy musi zapewniać możliwość uwierzytelniania z wykorzystaniem Microsoft Active Directory
35. Punkt dostępowy musi zapewniać realizację priorytetów dla rozwiązań VoIP
36. Punkt dostępowy musi zapewniać wsparcie zabezpieczenia ramek kontrolnych zgodnie ze standardem IEEE 802.11w
37. Punkt dostępowy musi posiadać Certyfikat CE lub Deklarację zgodności
38. Punkt dostępowy musi posiadać tzw. dożywotnią gwarancję, czyli zapewnienie wymiany w przypadku awarii do min. 5 lat po zakończeniu produkcji urządzenia.

Załącznik nr 2 do pytań i odpowiedzi z dnia 24.08.2023 r.

A. Ogólne wymagania dla sieci bezprzewodowej.

1. Zamawiający wymaga, żeby dostarczone punkty dostępowe były w pełni zarządzane z chmury producenta, ale również, aby umożliwiały adopcję i zarządzanie z lokalnego kontrolera.
2. Wykonawca zobligowany jest dostarczyć wszystkie komponenty, licencje niezbędne do poprawnego funkcjonowania rozwiązania.
3. Dostarczone przez Wykonawcę urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta i posiadać pakiet usług gwarancyjnych producenta obejmujący użytkowników z obszaru Polski.
4. Zamawiający dopuszcza licencje czasowe w formie subskrypcji, ale na okres nie krótszy niż 5 lat.
5. Sieć bezprzewodowa, musi zapewnić skalowalność, czyli możliwość rozbudowy do minimum 2000 punktów dostępowych.
6. Sieć bezprzewodowa musi funkcjonować w oparciu o standard transmisji bezprzewodowej WLAN 802.11ax (WiFi 6), a także zapewniać kompatybilność z wcześniejszymi standardami 802.11ac/n a/b/g.
7. Sieć bezprzewodowa musi zapewnić możliwość zestawiania tuneli VPN bezpośrednio pomiędzy punktami dostępowymi.
8. W celu zapewnienia usługi bezpiecznego dostępu gościnnego musi być możliwość generowania wielu prywatnych haseł PSK w ramach jednego SSID. System musi zapewniać rozróżnienie poszczególnych użytkowników posiadających prywatne hasła PSK i zapewniać egzekwowanie różnych polityk Firewall oraz przydział do różnych sieci VLAN. Prywatne hasła PSK muszą mieć możliwość ograniczenia liczby korzystających z nich urządzeń. Dopuszczane jest zaproponowanie analogicznego rozwiązania usługi bezpiecznego dostępu gościnnego zapewniającego minimum:
    a. szyfrowanie WPA2/AES,
    b. osobne konta czasowe dla gości
9. System chmurowy musi posiadać możliwość dostarczenia wygenerowanych danych dostępu gościnnego poprzez email oraz SMS. Wymaga się, aby funkcjonalność ta była wbudowana w rozwiązanie chmurowe bez konieczności integracji z własną bramką internetową lub innym publicznym systemem wysyłania SMS.
10. Ze względu na rozproszoną infrastrukturę sieci, rozwiązanie sieci bezprzewodowej musi działać z pełną funkcjonalnością w przypadku utraty łączności z centralnym systemem zarządzania w chmurze.
11. Funkcję warstwy kontrolnej sieci bezprzewodowej muszą pełnić punkty dostępowe. W szczególności dotyczy to funkcjonalności jakich jak:
    a. automatyczny dobór mocy nadawania RF,
    b. automatyczny dobór kanału,
    c. Fast Secure Roaming,
    d. Pełna obsługa SSID z 802.1x,
    e. Captive Web Portal.
12. System powinien oferować zestaw narzędzi dla administratorów ułatwiających rozwiązywanie problemów klientów sieci WiFi w szczególności:
    a. monitoring komunikacji klienta podczas podłączania się do sieci,
    b. możliwość uruchomienia trybu śledzenia konkretnego urządzenia w celu analizy problemów z łącznością

c. automatyczne wykrywanie problemów z połączeniem do sieci WiFi,
d. ocenę możliwości klienta sieci bezprzewodowej: wspierane kanały, wspierana szerokość kanałów, MIMO itp.

13. Komponenty rozwiązania w postaci Access Pointów i kontrolera powinny pochodzić od jednego producenta. W celu odbioru i weryfikacji pokrycia sieci wifi, po uruchomieniu systemu Wykonawca musi przeprowadzić pomiary pokrycia i siły sygnału radiowego dla wszystkich pomieszczeń, w których dokonana zostanie instalacja punktów dostępowych i dołączyć je dokumentacji.
14. Wykonawca zobowiązany jest do sporządzenia dokumentacji powdrożeniowej rozwiązania, która obejmie co najmniej:
    a. rozmieszczenie punktów dostępowych,
    b. pomiar siły sygnału punktów dostępowych i przedstawienie go na mapach budynku,
    c. przebieg, oznaczenie i pomiary wykonanych tras kablowych naniesione na podkłady budynku,
    d. opis konfiguracji punktów dostępowych.

B. Wymagania dla chmurowego systemu zarządzania

1. W celu zapewnienia protekcji inwestycji, system zarządzania w chmurze powinien umożliwiać adopcję i prawidłowe zarządzanie urządzeniami, zarówno najnowszymi jak i starszymi. Zamawiający chce uniknąć w przyszłości potrzeby wymiany urządzeń w przypadku chęci rozbudowy systemu o nowe punkty dostępowe, które będą miały nowe funkcje oraz nowe wersje oprogramowania (ang. firmware)
2. Musi zapewnić możliwość wgrywania różnych wersji oprogramowania na punkty dostępowe w ramach systemu.
3. Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń.
4. Musi umożliwić określenie fizycznej lokalizacji punktów dostępowych na mapie oraz miejsca ich podłączenia do sieci.
5. Musi umożliwić monitorowanie całego systemu sieci bezprzewodowej.
6. Musi zapewnić kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieci bezprzewodowej.
7. Musi zapewnić wdrożenie scentralizowanych polityk WLAN, które można zastosować do wielu punktów dostępowych jednocześnie.
8. Musi zapewnić centralne wykonanie aktualizacji oprogramowania dla wszystkich urządzeń w systemie.
9. Musi zapewnić możliwość zaplanowania wykonania aktualizacji oprogramowania urządzeń w systemie.
10. Musi umożliwiać wizualizację zainstalowanych punktów dostępowych na mapach oraz planach pięter budynków. Wizualizacja musi pokazywać topologię sieciową oraz aktualny stan działania zainstalowanych punktów dostępowych.
11. Mapy pięter budynków muszą mieć, oprócz prezentacji samego rzutu piętra, możliwość obrysowania ścian i przeszkód dla sygnału radiowego, tak aby była możliwa możliwie wierna wizualizacja propagacji sygnału radiowego.
12. Musi umożliwiać wizualizację zasięgu radia punktów dostępowych (heat map), przedstawiając takie parametry jak: RSSI, kanał, prędkość transmisji.
13. Musi umożliwiać wyświetlanie na planach pięter umiejscowienia wykrytych klientów

14. Musi posiadać narzędzie do planowania radiowego w celu ustalenia miejsc montażu nowych punktów dostępowych. Planowanie musi opierać się o plany pięter budynków.
15. Musi posiadać możliwość wykonania konfiguracji dla planowanych nowych punktów dostępowych.
16. Musi zapewnić automatyczny proces rejestracji, uaktualnienia oraz konfiguracji nowych punktów dostępowych bez konieczności wykonywania działań manualnych (ang. auto provisioning).
17. System musi umożliwiać analizowanie ruchu w sieci i prezentację statystyk pod kątem używanych aplikacji oraz wolumenu danych dla każdej z aplikacji, bądź grup aplikacji.
18. Chmurowy system zarządzania musi udostępniać możliwość monitorowania, zarządzanej przez niego infrastruktury WiFi, przy użyciu dedykowanej aplikacji mobilnej, wyprodukowanej i udostępnionej przez producenta. Aplikacja powinna być możliwa do instalacji na urządzeniu mobilnym takim jak smartphone lub tablet z systemem operacyjnymi Apple iOS, Apple iPad OS, Android. Aplikacja mobilna musi być dostępna publicznie na platformach Apple AppStore oraz GooglePlay.
19. Ze względu na chmurowy charakter przetwarzania danych, system zarządzania chmurowego musi posiadać certyfikat zgodności z ISO 27001, ISO 27017 oraz ISO 27701
20. System zarządzania musi być zgodny z RODO
21. System musi umożliwiać uruchomienie podstawowej funkcjonalności WIPS (ang. Wireless Intrusion Prevention System) w zakresie:
    a. wykrywania i usuwania wrogich punktów dostępowych (ang. rogue AP detection and termination)
    b. wykrywania wrogich klientów (ang. Rogue Client Detection)
    c. wykrywania ataków w ilości minimum 30 różnych sygnatur ataku
22. System musi posiadać następujące możliwości raportowania:
    a. modyfikacja, filtrowanie i tworzenie różnych zakresów urządzeń objętych raportem.
    b. tworzenie raportów jednorazowych lub automatycznie zgodnie z zadanym harmonogramem, w formie pdf, z opcją wysyłania ich pod wskazany adres email
    c. raportowanie ilości danych w ramach każdej wykrytej aplikacji,
    d. raportowanie ilości zużytego pasma per użytkownik.
    e. dane dla potrzeb audytów
    f. generowanie wykazu produktów zainstalowanych w sieci
    g. tworzenie własnych raportów
23. System zarządzania w chmurze musi zapewniać dostęp do API pozwalający na integrację systemu bezprzewodowego rozwiązaniami firm trzecich.
24. API musi zapewniać możliwość generowania prywatnych haseł PSK tak, aby była możliwość integracji systemu rejestracji gości na recepcji z systemem obsługi gości w ramach sieci WiFi.