***Załącznik nr 3 do SWZ***

**Szczegółowy opis przedmiotu zamówienia**

# Wprowadzenie

Przedmiotem niniejszego postępowania jest rozbudowa infrastruktury sieci bezprzewodowej Politechniki Wrocławskiej opartej o rozwiązania Aruba na które składają się:

* dwa kontrolery sieci bezprzewodowej Aruba 7220 (RW) Controller wraz z licencjami Aruba AirWave;
* punkty dostępowe serii Aruba 300, Aruba 500, Aruba 600;

Zamawiający informuje na potrzeby niniejszego postępowania, że **Politechnika Wrocławska** (Wrocławskie Centrum Sieciowo - Superkomputerowe - WCSS) jest **Operatorem** WASK.

**Wymagania ogólne dla wszystkich zadań**

1. Niniejszy opis przedmiotu zamówienia (OPZ) nie podlega interpretacji. Jeśli zapisy specyfikacji są zdaniem Wykonawcy niejasne, niepełne, nieprecyzyjne lub błędne, to Wykonawca ma obowiązek zadać pytanie przed złożeniem oferty.
2. Oferowany sprzęt musi spełniać poniższe wymagania minimalne:

* Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanych kanałów sprzedaży producentów.
* Całość dostarczanego rozwiązania, tzn. każde z dostarczonych urządzeń, musi być nowe (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), wcześniej nieużywane. Przy dostawie Wykonawca na każdorazowe żądania Zamawiającego musi dostarczyć oświadczenie o spełnieniu tego wymogu.
* Wszystkie oferowane urządzenia muszą być wyprodukowane przez producenta, który posiada wdrożony i certyfikowany system zarządzania jakością zgodny z normą jakości ISO 9001 lub równoważną.
* Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, jak i producenta.
* Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
* Do każdego urządzenia musi być dostarczony niezbędny osprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) przewidziany do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Dostarczony osprzęt eksploatacyjny musi zapewniać minimalnie wymagania redundancji. Osprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
* Wszystkie urządzenia muszą posiadać oznakowanie CE.
* Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
* Wszystkie dostarczone urządzenia musza się zintegrować z oprogramowaniem do zarządzania w ramach jednego rozwiązania dla wszystkich dostarczonych komponentów.

# Przedmiot zamówienia.

# Kontroler sieci bezprzewodowej (w tym urządzeń sieciowych oraz z funkcjonalnością router/firewall stanowy) wraz z oprogramowaniem układowym – 2 szt.

Tabela 1. Wymagania techniczne kontrolera sieci bezprzewodowej (w tym urządzeń sieciowych oraz z funkcjonalnością router/firewall stanowy) wraz z oprogramowaniem układowym

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Wymaganie | Wymagana wielkość parametru | Oferowany parametr |
| Wypełnia wykonawca  - należy podać poszczególne parametry, zgodnie z kolumną „c”  - należy podać „Producent, Model, Numer katalogowy” w miejscach wskazanych przez Zamawiającego  - należy podać wymagane dane, zgodnie ze wskazaniem przez Zamawiającego: numerów katalogowych produktów i wszystkich jego dodatkowych składników (licencje, zasilacze, wkładki SFP, etc.) umożliwiających ich jednoznaczną identyfikację u producenta sprzętu |
| a | b | c | d |
| Kontroler sieci bezprzewodowej (w tym urządzeń sieciowych oraz z funkcjonalnością router/firewall stanowy) wraz z oprogramowaniem układowym | | | **Producent:………………………**  **Model:……………………….**  **Numer katalogowy:………………………..** |
| 1 | **Wymagania funkcjonalne** | 1. Kontroler musi zarządzać siecią bezprzewodową złożoną docelowo z 1000 punktów dostępowych 2. Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall) 3. Musi posiadać funkcje VPN Gateway 4. Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym. 5. Kontroler musi umożliwiać pracę w klastrze HA z drugim identycznym urządzeniem 6. Komunikacja pomiędzy kontrolerami musi wykorzystywać protokoły sieciowe niewymagające instalacji dodatkowych urządzeń sieciowych. 7. Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania 8. Kontroler musi zapewniać centralne zarządzenia licencjami, tzn. w architekturze sieci, w której występuję więcej niż jedne kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom. 9. Kontroler musi posiadać następujące parametry sieciowe:    1. możliwość wdrożenia w warstwie 2 i 3 ISO/OSI,    2. wsparcie dla sieci VLAN w tym również trunk 802.1q    3. wbudowany serwer DHCP    4. obsługa SNMPv2, SNMPv3    5. routing dynamiczny OSPF 10. Kontroler sieci WLAN musi obsługiwać co najmniej:     1. Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST , DES, 3DES, AES-CBC     2. Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze     3. Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit     4. Autoryzację dostępu użytkowników:        1. Typy uwierzytelnienia: IEEE 802.1X (EAP,LEAP,PEAP,EAP-TLS,EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal”, 802.1X i MAC        2. Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia        3. Wsparcie dla autoryzacji, minumum: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba NAC        4. Musi umożliwiać utworzenie nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal”        5. Musi umożliwiać wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES)        6. Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym        7. Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius.     5. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających.     6. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu     7. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia 11. Kontroler musi posiadać obsługę transmisji różnego typu danych w jednej sieci:     1. Integracja jednoczesnej transmisji danych i głosu     2. Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejkowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p     3. Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming)     4. Ograniczanie pasma dla użytkownika oraz dla roli użytkownika     5. Ograniczenie pasma dla poszczególnych aplikacji     6. Ograniczenie pasma dla poszczególnych SSID 12. Kontroler musi umożliwiać integrację ze środowiskiem Microsoft Lync poprzez SDN API. 13. Kontroler musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal) 14. Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni) 15. Kontroler musi posiadać funkcję adaptacyjnego zarządzania pasmem radiowym:     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     3. Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi     4. Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma     5. Przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie     6. Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b)     7. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału     8. Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w     9. Integracja z systemami RFID - wymagane jest wbudowane stosowne API 16. Kontroler musi posiadać funkcję wbudowanej zapory sieciowej, posiadającej co najmniej następujące własności:     1. Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia     2. Kopiowanie (mirroring) sesji     3. Szczegółowe logi (per pakiet) do późniejszej analizy     4. ALG (Application Layer gateway) co najmniej dla protokołów: FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera     5. Translacja źródłowa, docelowa adresów IP     6. Identyfikacja i blokowanie ataków DoS     7. Obsługa protokołu GRE     8. Deep packet inspection (DPI)     9. Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci WiFi 17. Kontroler musi posiadać funkcję systemu WIDS/ WIPS. Moduł WIPS musi posiadać co najmniej następujące funkcje:     1. Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.     2. Identyfikacja i możliwość blokowania sieci Adhoc     3. Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging     4. Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler     5. Identyfikacja błędów konfiguracji klientów WLAN     6. Identyfikacja podszywania się pod autoryzowane punkty dostępowe 18. Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w zamawianych dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników. 19. 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) 20. Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli. 21. Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA 22. Kontroler musi być zgodny z następującymi parametrami ilościowymi/wydajnościowymi:     1. Możliwa liczba obsługiwanych punktów dostępowych nie mniej niż 1000     2. Liczba aktywnych sesji zapory sieciowej nie mniej niż 2000000,     3. Przepustowość nie mniej niż 30Gbps     4. Liczba jednoczesnych sesji IPSEC nie mniej niż 24000     5. Minimum 4 porty 1/10/25GBaseX ze stykiem definiowanym przez SFP28 – kontroler musi być wyposażony w 4 moduły optyczne tego samego producenta 10 GB LR umożliwiające transmisję opartą na światłowdzie jednomodowym.     6. Wykonawca dodatkowo dostarczy 4 szt. kabli DAC 10Gb SFP+ o długości 1m tego samego producenta.     7. 1 interfejs konsoli (USB-C/RJ-45)     8. Port Ethernet dedykowany do zarządzania poza pasmowego (out-of-band management)     9. Minimum 2 porty USB 3.0     10. Zużycie energii nie większe niż 200W     11. Pełna obsługa standardu 802.1Q – 4094 tagów sieci VLAN     12. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.     13. Minimum 2 redundantne, modularne wentylatory (minimum dwa, niezależne, moduły wentylatorów) 23. Dla kontrolera wymagana zgodność z normami CE 24. Wszystkie dostępne na urządzeniu funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), o ile nie wyspecyfikowano inaczej, nie dopuszcza się licencji czasowych i subskrypcji. 25. Zamawiający wymaga, aby dostarczony kontroler w pełni integrował się z obecnie posiadanym systemem Centralnego Arbitra (Aruba Mobility Conductor) na, którym przechowywane są między innymi licencje ilościowe i funkcjonalne dla punktów dostępowych posiadanych przez Zamawiającego. 26. Zamawiający nie wymaga w ramach przedmiotu zamówienia dostawy licencji ilościowych i funkcjonalnych niezbędnych do podłączenia punktów dostępowych do oferowanego kontrolera. 27. Minimum 5 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy urządzenia (również zasilacze i wentylatory) zapewniająca dostawę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 8x5 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. 28. Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim. 29. Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych. 30. Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy. 31. Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Przedmiot dostawy** | **Ilość** | **Cena jednostkowa netto** | **Wartość netto** (cena jednostkowa x ilość) |
| *1* | *2* | *3* | *4* | *5* |
| **1.** | Kontroler sieci bezprzewodowej (w tym urządzeń sieciowych oraz z funkcjonalnością router/firewall stanowy) wraz z oprogramowaniem układowym | 2 | zł | zł |
| Wartość VAT (23%) | | | | zł |
| **Cena ogółem brutto** (wartość netto + wartość vat): | | | | zł *(cena ofertowa – kwotę należy wpisać*  *do formularza ofertowego)* |

**Oferta powinna być sporządzona w języku polskim, z zachowaniem postaci elektronicznej i podpisana kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym**