**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Tabela 1. Dostawa kontrolerów WiFi (z udzieleniem licencji) wraz z ich montażem i konfiguracją oraz z konfiguracją punktów dostępowych WiFi oraz dostawą wsparcia Producenta.**

(wypełnić wykropkowanie)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Przedmiot** | | **Cena jednostkowa netto [zł]** | **Ilość [szt.]** | **Cena całkowita netto [zł]** | **Kwota [zł]**  **VAT całkowity**  **(23%)** | **Cena całkowita brutto [zł]** | **Producent, model**  (w tabeli uzupełnić tylko miejsca wykropkowane) |
| A | | B | C | D | E | F | G |
| **Dostawa kontrolerów WiFi (z udzieleniem licencji) wraz z ich montażem i konfiguracją oraz z konfiguracją punktów dostępowych WiFi oraz dostawą wsparcia Producenta** (wypełnić wykropkowanie) | | ……….………….. | **2** | ……………... | …………. | …………………… | **Producent**  …………………….………………..…………….….  **Dokładny model**  …………..……………………...………………….…  …………………….…………………………………  **Kod producenta** (jeśli producent podaje)  …………………….…………………………………  **(przez pojęcie „dokładny model” – Zamawiający rozumie opis pozwalający Zamawiającemu na jednoznaczną identyfikację oferowanego urządzenia na stronach www producenta urządzenia – celem weryfikacji spełnia stawianych w opisie wymagań)** |
| **Lp.** | **Parametr wymagany** | | | | | | **Podzespół/Parametr oferowany**  (*w tabeli uzupełnić tylko miejsca wykropkowane*) |
| 1 | Kontrolery WiFi:   * 1. Dwa kontrolery fizyczne (Zamawiający nie dopuszcza rozwiązań wirtualnych/programowych) sieci WiFi zastępujące klaster dwóch kontrolerów HPE Aruba 7220 będące własnością Zamawiającego, pracujące w trybie HA (High Availability – wysoka dostępność);   2. **Parametr oceniany:** Liczba dostępnych dla Zamawiającego punktów dostępowych WiFi (access point) obsługiwanych przez system zaoferowanych kontrolerów pracujących w trybie HA - nie mniejsza niż 2000 (dwa tysiące), które będzie obsługiwał kontroler – jeżeli spełnienie tego warunku wymaga dostarczenia licencji do obsługi zaoferowanej ilości punktów dostępowych WiFi – wymaga się, aby wszystkie niezbędne licencje zostały dostarczone przez Wykonawcę w ramach tego zamówienia;   3. Poprawna i w pełni funkcjonalna obsługa wszystkich punktów dostępowych systemu HPE Aruba będących własnością Zamawiającego w szczególności:   - AP 207,  - AP 505,  - AP 365;  (przez pojęcie „poprawna i w pełni funkcjonalna obsługa” Zamawiający rozumie, że zaoferowane kontrolery nadzorują oraz realizują w pełni prawidłowo wszystkie funkcje przewidziane/zaprojektowane przez producenta punktów dostępowych WiFi będących własnością Zamawiającego a wymiana danych i komunikacja pomiędzy nimi (pomiędzy kontrolerem – punktem dostępowym) odbywa się poprawianie i bezbłędnie);   * 1. Każdy kontroler musi:      1. posiadać funkcję pełno-stanowej zapory sieciowej (stateful firewall);      2. obsługiwać funkcję VPN Gateway;      3. zapewniać współpracę z kontrolerami rożnej wielkości (pojemności) obsługi punktów dostępowych WiFi, pracując w systemie hierarchicznym, w tym z będącymi własnością Zamawiającego kontrolerami Aruba 7220;      4. umożliwiać komunikację pomiędzy kontrolerami z wykorzystaniem protokołów sieciowych niewymagających instalacji dodatkowych urządzeń sieciowych;      5. zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania;      6. zapewniać centralne zarządzenia licencjami, tzn. w architekturze sieci, w której występuje więcej niż jeden kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom;      7. posiadać następujące parametry sieciowe:         1. możliwość wdrożenia w warstwie 2. i 3. w modelu ISO/OSI;         2. wsparcie dla sieci VLAN w tym również trunk 802.1q;         3. wbudowany serwer DHCP;         4. obsługa SNMPv2, SNMPv3;         5. obsługa routingu dynamicznego OSPF;      8. 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, 802.1X i MAC;            2. funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia;            3. wsparcie dla autoryzacji, minimum: 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.            8. 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;      9. 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;      10. umożliwiać integrację ze środowiskiem Microsoft Lync poprzez SDN API;      11. umożliwiać stworzenie strony dla gości (tzw. Captive Portal);      12. umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób niepracujących w jednostce organizacyjnej Zamawiającego (np. dla osób odwiedzających Zamawiającego);      13. 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. rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma;          4. przełączania użytkowników zdolnych pracować w paśmie 5 GHz do pracy w tym paśmie;          5. zapewnienie sprawiedliwego dostępu do medium w środowisku, w którym znajdują się użytkownicy pracujący zgodnie ze standardami (802.11ac, 802.11n, 802.11g, 802.11a, 802.11b);          6. wykrywanie interferencji oraz miejsc bez pokrycia sygnału;          7. wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w;          8. integracja z systemami RFID-wymagane jest wbudowane stosowne API;      14. 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. obsługa Deep Packet Inspection (DPI);          9. możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach, których używają klienci WiFi;      15. mieć wbudowany serwer VPN, charakteryzujący się następującymi parametrami, nie mniej niż:          1. site-to-site oraz client-site VPN;          2. terminacja ruchu L2TP/IPSEC VPN, XAUTH/IPSEC, PPTP;          3. obsługa tokenów;          4. wsparcie dla serwerów Radius i LDAP w celu uwierzytelnienia sesji VPN przy użyciu: PAP CHAP, MS-CHAP, MS-CHAP2;          5. wsparcie dla algorytmów kryptograficznych: DES, 3DES, AES przy wykorzystaniu dedykowanych układów scalonych kontrolera;      16. zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody:          1. interfejs przeglądarki Web (https);          2. linia komend przez SSH i dedykowany port konsoli;      17. zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA;      18. być zgodny z następującymi parametrami ilościowymi/wydajnościowymi:          1. liczba aktywnych sesji zapory sieciowej nie mniej niż 2000000;          2. przepustowość nie mniej niż 40 Gb/s;          3. liczba jednoczesnych sesji IPSEC nie mniej niż 32000;          4. minimum 4 porty 1/10/25GBaseX ze stykiem definiowanym przez SFP28;          5. 1 interfejs konsoli (USB-C/RJ-45);          6. port Ethernet dedykowany do zarządzania poza pasmowego (out-of-band management);          7. minimum 2 porty USB3.0;          8. zużycie energii nie większe niż 200W;          9. pełna obsługa standardu 802.1Q–4094 tagów sieci VLAN;          10. dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia;          11. minimum 2 redundantne, modularne wentylatory (minimum dwa, niezależne, moduły wentylatorów);      19. spełniać wymagania zgodność z normami CE;      20. jeżeli do działania którejkolwiek z wymaganych funkcji potrzebna jest licencja, należy ją dostarczyć;   2. Wszystkie wymagane w kontrolerach funkcjonalności muszą być dostępne przez cały okres użytkowania (brak ograniczeń czasowych), nie dopuszcza się licencji czasowych i subskrypcji o ile nie wyspecyfikowano inaczej.   3. Wykonawca przenalizuje bieżącą konfigurację kontrolerów u Zamawiającego i dokona wymiany i rekonfiguracji środowiska sieci komputerowej Zamawiającego;   4. Kontrolery powinny być podłączone przez Wykonawcę do przełączników rdzeniowych będących własnością Zamawiającego (HPE FlexNetwork 10504) z zachowaniem wysokiej dostępności infrastruktury;   5. Awaria lub wyłączenie jednego kontrola WiFi, jak i awaria lub wyłączenie jednego przełącznika rdzeniowego nie powoduje zatrzymania pracy (dostępności) sieci WiFi;   6. Wszystkie niezbędne prace oraz elementy sprzętowe niezbędne do przeprowadzenia takiej operacji są elementem dostawy przez Wykonawcę;   7. Maksymalny czas niedostępności całej infrastruktury WiFi nie może być dłuższy niż 1h. Maksymalna niedostępności usługi dla pojedynczego, mniejszego obszaru/segmentu sieci (piętro budynku) nie może być dłuższy niż 4h. Czas i obszar niedostępności usługi WiFi musi odbywać się według ustalonego wcześniej z Zamawiającym harmonogramu;   8. Wykonawca zapewni poprawne działanie wszystkich aktualnie działających obszarów sieci WiFi Zamawiającego w szczególności:      1. usługa dostępu do sieci WiFi;      2. telefonia bezprzewodowa w oparciu o telefony Ascom współpracujący w ramach funkcjonującej u Zamawiającego łączności telefonicznej LG-Eriksson (systemy będące własnością Zamawiającego);      3. sieć bezprzewodowa WiFi dla gości w oparciu o oprogramowanie HPE Clearpass (użytkowane przez Zamawiającego);   9. Wykonawca zintegruje dostarczona infrastrukturę z oprogramowaniem HPE AirWave;   10. Wykonawca w ramach przedmiotowego zamówienia (w cenie oferty) dostarczy jednorazowo produkt w postaci wsparcia (support) producenta sprzętu dla dostarczanej infrastruktury (w tym sprzętu) na okres 5 lat. Przedmiotowe wsparcie producenta sprzętu ma spełniać następujące wymagania: Wsparcie na okres 5 lat; Działające w trybie 24/7/365 ~~z czasem reakcji nie dłuższym niż 6h~~ w siedzibie Zamawiającego, przy czym wsparcie serwisowe producenta ma zapewniać dostawę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (w trybie tzw. NBD AHR - Next Business Day Advanced Hardware Replacement); Wsparcie musi obejmować zarówno sprzęt (również zasilacze i wentylatory), jak i oprogramowanie; Wsparcie musi być realizowane przez producenta sprzętu co Wykonawca potwierdzi Zamawiającemu przedstawiając dokumenty świadczące o wykupieniu u producenta sprzętu wsparcia (support’u/kontraktów serwisowych) – dokumenty te należy przedstawić Zamawiającemu do odbioru wykonania przedmiotu zamówienia tj. do protokołu odbioru;   11. Zamawiający wymaga od Wykonawcy udzielenia 5-letniej gwarancji dla poprawnego/bezproblemowego działania dostarczanej infrastruktury (wraz ze sprzętem). Wykonawca w ramach udzielonej gwarancji zobowiązany będzie rozwiązywać istotne usterki sieci oraz wykonywać aktualizacje oprogramowanie kontrolerów nie rzadziej niż raz w roku;   12. W przypadku ogłoszenia przez producenta sprzętu podatności krytycznych Wykonawca będzie zobowiązany niezwłocznie powiadomić o tym Zamawiającego i wykonać niezbędne aktualizacje zalecane przez producenta sprzętu;   13. Wykonawca dokona wymiany 25 punktów dostępowych HPE MSM (będących własnością Zamawiającego) w lokalizacji ul. Kopernika 50 w Krakowie w oparciu o punkty dostępowe AP 505 i licencje będące własnością Zamawiającego. Wykonawca dokona aktualizacji map w oprogramowaniu AirWave dla nowej lokalizacji;   14. Wykonawca dostarczy dokumentację powdrożeniową obejmującą opis wykonanych prac w zakresie sprzętu oraz oprogramowania;   15. Zamawiający nie dopuszcza produktów/urządzeń, dla których producent sprzętu ogłosił koniec wsparcia lub koniec sprzedaży, który jest krótszy niż 7 lat licząc od daty otwarcia ofert;   16. Zamawiający nie dopuszcza stosowanie elementów, w szczególności wkładek, które nie są wspierane i zalecane przez producenta sprzętu. W szczególności nie dopuszcza się stosowanie tzw. zamienników.   17. Wykonawca dysponuje odpowiednimi środkami technicznymi, wiedzą oraz wykwalifikowanym personelem techniczny – wykwalifikowany zawodowo inżynier lub zespół inżynierów, który będzie realizował usługę poprze fizyczną obecność w siedzibie Zamawiającego – minimum 1 specjalista certyfikowany przez producenta zaoferowanego sprzętu (kontrolerów WiFi) na poziomie co najmniej Professional, który będzie uczestniczył w realizacji zamówienia, w szczególności będzie odpowiedzialny za świadczenie usługi konfiguracyjno-instalacyjnej u Zamawiającego. | | | | | | **PARAMETR OCENIANY**  **Podać ilość obsługiwanych punktów dostępowych WiFi**  **Dotyczy Lp. 1.2, Tabela 1**  **szt.**  **………………………………..……………..**  (podać wartość liczbową)  **Jeśli licencja jest niezbędna do obsługi - podać nazwę/kod producenta licencji oferowanej do obsługi zaoferowanej ilości punktów dostępowych WiFi**  **Dotyczy Lp. 1.2, Tabela 1**    **…………………..…………………………………..**  **…………………..…………………………………..**  (podać nazwę/kod producenta licencji)  **Parametr wymagany**  (nie wypełniać)  **Parametr wymagany**  (nie wypełniać)  **Parametr wymagany**  (nie wypełniać)  **Parametr wymagany**  (nie wypełniać)  **Parametr wymagany**  (nie wypełniać) |