Warszawa, 28 listopada 2022 r.

KOMENDA GŁÓWNA
PAŃSTWOWEJ STRAŻY POŻARNEJ

BF-IV.2370.24.2022.11

do uczestników postępowania

Dot.: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji na „postępowania na dostawę urządzeń WiFi", nr sprawy: BF-IV-2370.24.2022.

Działając na podstawie art. 286 ust. 1 ustawy z dnia 11 września 2019 roku – Prawo zamówień publicznych (Dz.U. z 2022 r., poz. 1710 z późn. zm.) zwanej dalej „ustawą", Zamawiający dokonuje zmiany w treści specyfikacji warunków zamówienia (SWZ) w zakresie:

1) opisu przedmiotu zamówienia (OPZ) – załącznik nr 1 do SWZ,
– w trzecim ustępie opisu przedmiotu zamówienia wykreśla się zdanie:
„Producent sprzętu musi być sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure" i znajdować się w kwadracie liderów (Leaders), dane z raportu nie starszego niż listopad 2021."
– wykreśla się podpunkt 2.7.1. OPZ
– pkt 3.18 OPZ otrzymuje nowe brzmienie:
„Oprogramowanie musi być zgodne z następującymi parametrami ilościowymi/ wydajnościowymi:
- możliwa liczba obsługiwanych punktów dostępowych nie mniej niż 250;
- należy dostarczyć licencje na podłączenie 60 punktów dostępowych;
- obsługa minimum 2 000 VLANów;
- obsługa minimum 4000 tuneli GRE;
- równoczesna obsługa do 4000 użytkowników."

2) SWZ - Rozdziału XV. Opis kryteriów oceny ofert wraz z podaniem wag tych kryteriów i sposobu oceny ofert. Nowy zapis otrzymuje brzmienie:

„1. Przy wyborze oferty najkorzystniejszej Zamawiający będzie kierował się następującymi kryteriami, z przypisaniem im odpowiednio wag.
a) Kryteriami oceny ofert są:

Lp.	Opis kryteriów oceny	ZNACZENIE (W_{max}*)
1.	Cena brutto oferty (Pc)	50 pkt
2.	Termin dostawy (Pd)	20 pkt
3.	Producent oferowanego sprzętu jest sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure" i znajduje się w kwadracie liderów (Leaders), dane z raportu nie starszego niż listopad 2021. (Pg)	20 pkt
4.	Możliwość zapewnienia redundacji między dwoma portami w punkcie dostępowym (Pr)	10 pkt
	Razem	100 pkt

* **Wmax – waga kryterium – maksymalna liczba punktów, która może być przyznana w danym kryterium**

b) Sposób obliczania punktów dla poszczególnych kryteriów:
Kryterium nr 1 „Pc" Cena brutto - proporcjonalnie wg wzoru: 50 pkt

$$Pc = \frac{\text{najniższa cena brutto z ofert}}{\text{cena brutto oferty badanej}} \times 50 \text{ pkt}$$

Uwaga: oferta z najniższą ceną otrzyma maksymalną ilość punktów

Kryterium nr 2 „Pd" termin dostawy - 20 pkt
Za udzielony termin dostawy Zamawiający przyzna Wykonawcy następującą liczbę punktów

Lp.	Termin dostawy	WAGA
1.	od 15 do 21 dni	0 pkt
2.	do 14 dni	20 pkt

Uwaga: W przypadku kiedy Wykonawca zaoferuje termin dostawy przekraczający 21 dni, oferta Wykonawcy zostanie odrzucona.

Kryterium nr 3 „Pg" - Producent oferowanego sprzętu jest sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure" i znajduje się w kwadracie liderów (Leaders), dane z raportu nie starszego niż listopad 2021. - 20 pkt

Lp.	**Producent oferowanego sprzętu jest sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure" i znajduje się w kwadracie liderów (Leaders), dane z raportu nie starszego niż listopad 2021.**	WAGA
1.	NIE	0 pkt
2.	TAK	20 pkt

Kryterium nr 4 „Pr" - Możliwość zapewnienia redundacji między dwoma portami w punkcie dostępowym - 10 pkt

Lp.	Redundacja między dwoma portami w punkcie dostępowym	WAGA
1.	Brak takiej możliwości	0 pkt
2.	Możliwa	10 pkt

Zamawiający za najkorzystniejszą uzna ofertę, która uzyska największą liczbę punktów łącznie z określonych powyżej kryteriów. Ocenę łączną oferty stanowi suma punktów uzyskanych w ramach poszczególnych kryteriów. Zamawiający wyliczy ocenę łączą ocenianych ofert na podstawie poniższego wzoru:
P= Pc + Pd + Pg + Pr
gdzie:
P - łączna liczba punktów przyznanych badanej ofercie

Pc - liczba punktów w kryterium „*Cena brutto oferty*";
Pd - liczba punktów w kryterium „Termin dostawy";
Pg - Producent oferowanego sprzętu jest sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure" i znajduje się w kwadracie liderów (Leaders), dane z raportu nie starszego niż listopad 2021.
Pr - liczba punktów w kryterium „*Możliwość zapewnienia redundancji między dwoma portami w punkcie dostępowym*";

3) SWZ w zakresie terminu składania ofert i terminu związania ofertą. Nowe brzmienie otrzymują:

Rozdział IX Termin związania ofertą

„1. Wykonawca jest związany ofertą 30 dni od upływu terminu składania ofert tj. do dnia **4 stycznia 2022 r**. Pierwszym dniem związania ofertą jest dzień, w którym upływa termin składania ofert. „

Rozdział XII Termin składania ofert

„11. Termin składania ofert upływa w dniu **6 grudnia 2022 r. o godz. 10:00.** Decyduje data oraz dokładny czas (hh:mm:ss) generowany wg czasu lokalnego serwera synchronizowanego zegarem Głównego Urzędu Miar."

Rozdział XIII Termin otwarcia ofert

„1. Otwarcie ofert nastąpi niezwłocznie po upływie terminu składania ofert, tj. w dniu **6 grudnia 2022 godz. 10:15.** Otwarcie ofert dokonywane jest przez odszyfrowanie i otwarcie ofert."

4) W załączniku nr 3 do SWZ „Formularz Oferty" dopisuje się pkt 5) *:

„5) * Producent oferowanego sprzętu jest sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure" i znajduje się w kwadracie liderów (Leaders), dane z raportu nie starszego niż listopad 2021.

TAK **** / NIE ****

Opublikowane zmiany są wiążące i dotyczą wszystkich uczestników postępowania.

KOMENDANT GŁÓWNY
PAŃSTWOWEJ STRAŻY POŻARNEJ
z up.

nadbryg. Krzysztof Hejduk
Zastępca Komendanta Głównego

Załącznik:
- załącznik nr 1 do SWZ aktualny
- załącznik nr 3 do SWZ aktualny

Opis Przedmiotu Zamówienia (OPZ)

Przedmiotem zamówienia, jest dostawa wewnętrznych punktów dostępowych sieci WiFi wraz z uchwytami, oraz z kontrolerem wirtualnym i systemem autentykacji, autoryzacji i kontroli dostępu. Wszystkie urządzenia i systemy muszą być objęte 60 miesięcznym wsparciem producenta. Do kontrolera dostawca musi dostarczyć licencje dla 60 punktów dostępowych, a do systemu autentykacji licencje dla 300 punktów końcowych (urządzeń klienckich). Licencje muszą mieć charakter wieczysty. Wszystkie licencje, urządzenia i systemy muszą być objęte 60 miesięcznym wsparciem producenta.

Celem dostawy powyższych urządzeń do infrastruktury zamawiającego jest modernizacja środowiska WLAN KG PSP w obszarze zapewnienia bezpieczeństwa, niezawodności i dostępności usług świadczonych w sieci bezprzewodowej, jak również wyższych wydajności i przepływności, przy zachowaniu zgodności z istniejącymi elementami oraz w oparciu o kierunki i zasady budowy wydajnych i bezpiecznych sieci. Aby dotrzymać kroku zmieniającemu się otoczeniu, infrastruktura sieci teleinformatycznej musi zapewniać wysoką dostępność do usług sieciowych, płynną komunikację, wysokie wydajności, dbając jednocześnie o bezpieczeństwo danych i zasobów.

Sprzęt i systemy muszą pochodzić z autoryzowanego przez jego producenta kanału dystrybucji w UE i nie mogą być obciążone uprzednio nabytymi prawami podmiotów trzecich (niezależni brokerzy, subdystrybucja) oraz musi być przeznaczony do serwisu i oraz sprzedaży na rynku polskim.

Przedmiotem zamówienia jest w szczególności dostawa urządzeń oraz usług wymienionych poniżej:

1. Przedmioty zamówienia:

1.1. Wewnętrzny punkt dostępowy z uchwytem podsufitowym – 60 szt.
1.2. Wirtualny kontroler do zarządzania punktami dostępowymi – 1 szt.
1.3. System autentykacji, autoryzacji i kontroli dostępu – 1 szt.,
w tym:

1.4. Dostawa wraz z punktami dostępowymi i systemami licencji we wskazanej powyżej ilości wraz ze wsparciem dla nich.
1.5. Zapewnienie 60 miesięcznego okresu gwarancji i serwisu.

2. Minimalne wymagania dla urządzeń wyszczególnionych w pkt. 1.1.

CECHA	WYMAGANIA OGÓLNE
2.1. **OZNAKOWANIE**	Urządzenia muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu (nazwa, nr seryjny) jak i producenta.
2.2. **OZNAKOWANIE CE**	Wszystkie urządzenia muszą posiadać oznakowanie CE produktu albo spełniać normy równoważne.
2.3. **OPAKOWANIE**	1. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
2.4 **DOKUMENTACJA**	1. Na żądanie Zamawiającego wymagane jest dostarczenie, wraz z dostawą urządzeń, szczegółowej dokumentacji technicznej producenta oferowanych produktów potwierdzającej spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia (Zamawiający dopuszcza w tym przypadku możliwość złożenia dokumentacji w języku angielskim). Dostarczane urządzenia będą nowe i będą pochodzić z bieżącej produkcji, a jednocześnie nie będą urządzeniami, które mogły być używane w innych projektach i poddane procesowi odnowienia. Wymagane jest dostarczenie wraz ze sprzętem pisemnego potwierdzenia wydanego przez producenta lub przedstawicielstwo producenta sprzętu, poświadczającego datę produkcji sprzętu. Sprzęt musi być wyprodukowany nie wcześniej niż sześć miesięcy od daty podpisania umowy z dostawcą. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający, że oprogramowanie zawarte w dostarczonym sprzęcie jest licencjonowane na Zamawiającego. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający zarejestrowanie kontraktu serwisowego na dostarczone urządzenia i oprogramowanie.
2.5. **ZASILANIE**	1. Urządzenia muszą być zgodne ze standardem 802.3at PoE . 2. Musi być zapewniona możliwość użycia lokalnego zasilacza DC (zasilacz nie musi być dołączony).
2.6. **FUNKCJONALNOŚĆ**	1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi posiadać dwa niezależne moduły radiowe, pracujące w paśmie 2.4GHz b/g/n/ax oraz 5GHz a/n/ac wave2/ax. 2. Punkt dostępowy musi umożliwiać współpracę z centralnym kontrolerem sieci bezprzewodowej lub oprogramowaniem do zarządzania siecią bezprzewodową. Kontroler/oprogramowanie muszą pochodzić od tego samego producenta co AP w celu osiągniecia maksymalnego poziomu integracji oraz spójności. 3. AP musi móc pracować bez nadzoru kontrolera centralnego w trybie autonomicznym: a. Zmiana trybu do pracy z centralnym kontrolerem może odbywać się z poziomu GUI. Zmiana trybu pracy nie może odbywać się przez instalację na urządzeniu nowej wersji oprogramowania, b. Wszystkie zmiany/operacje konfiguracyjne muszą być możliwe do realizacji z poziomu przeglądarki, c. Urządzenie musi posiadać zarządzania przez przeglądarkę internetową oraz protokół https. 4. Zapewniona musi być opcja konfiguracji wspólnej punktów połączonych w jedną sieć LAN w warstwie drugiej:

	a. Oprogramowanie zainstalowane na urządzeniach musi umożliwiać wybór jednego punktu dostępowego jako elementu zarządzającego, b. Jeżeli awarii ulegnie punkt zarządzający kolejny AP w sieci musi przejąć jego rolę automatycznie, c. W przypadku modyfikacji konfiguracji musi się ona automatycznie propagować na pozostałe AP, d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą wersję. 5. Punkty dostępowe muszą móc pracować w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych Access Pointów. 6. W system musi być wbudowany serwer DHCP. 7. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów. 8. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach: a. PEAP-MSCHAPv2, b. TTLS-MSCHAPv2, c. EAP-TLS, d. PEAP-GTC. 9. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP. 10. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID. 11. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN. 12. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez: a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania, b. Zewnętrzny portal WWW. 13. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT. 14. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne. 15. W sieci punktów dostępowych zarządzanie pasmem radiowym odbywa się automatycznie za pomocą auto adaptacyjnych mechanizmów w tym minimum: a. Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane, b. Wsparcie dla 802.11d oraz 802.11h, c. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g), d. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz, e. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału, f. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma, g. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu, h. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe. 16. Minimalizacja interferencji związanych z sieciami 3G/4G LTE. 17. Punkt dostępowy musi mieć wbudowany moduł Zigbee (802.15.4) (co najmniej 7dBm). 18. AP posiada wbudowany moduł Bluetooth Low Energy (BLE5.0) (minimum 7dBm). 19. Obsługa roamingu klientów w warstwie 2. 20. Obsługa logowania na zewnętrznym serwerze SYSLOG.

21. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
22. W system punktów dostępowych musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów w sieci.
23. Wbudowany interfejs (zarządzania) musi umożliwiać dostarczenie następujących informacji o systemie:
    a. Wyświetlanie logów systemowych,
    b. Szum tła dla każdego radia,
    c. Ilość odrzuconych/błędnych ramek/s dla każdego radia,
    d. Ilość ramek wejściowych/wyjściowych dla każdego radia,
    e. Ilość klientów korzystających z systemu/interferujących,
    f. Wykorzystanie pasma,
    g. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością.
24. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n,802.11ac 1 Wave, 802.11ac 2 Wave, 802.11ax.
25. Access Point posiadać musi minimum 4 wbudowane anteny pracujące w trybie 4x4 MIMO, z parametrami co najmniej: 4 dBi dla 2,4GHz, 7 dBi dla 5GHz.
26. Praca w trybie SU MIMO 4X4:4 dla 5GHz.
27. Specyfikacja radia 802.11a/n/ac/ax:
    a. Obsługiwana technologia OFDM oraz OFDMA,
    b. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM,
    c. Moc transmisji konfigurowalna przez administratora możliwość zmiany co 0.5dbm,
    d. Prędkości transmisji:
        i. 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a,
        ii. MCS0-MCS23 (6,5Mbps do 450Mbps) dla 802.11n,
        iii. MCS0-MCS9, NSS = 1-4 (6.5 Mbps do 1733 Mbps) dla 802.11ac,
        iv. MCS0 do MCS11, NSS = 1-2 (3.6 Mbps do 574 Mbps) dla 802.11ax (2,4GHz),
        v. MCS0 do MCS11, NSS = 1-4 (3.6 Mbps do 4803 Mbps) dla 802.11ax (5GHz),
    e. Obsługa VHT – kanały 20/40/80/160MHz dla 802.11ac,
    f. Obsługa HT – kanały 20/40MHz dla 802.11n,
    g. Obsługa HE – kanały 20/40/80/160MHz dla 802.11ax,
    h. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz,
    i. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac,
    j. Wsparcie dla:
        i. MRC (Maximal ratio combining),
        ii. Technologia TxBF,
        iii. LDPC (Low-density parity check),
        iv. STBC (Space-time block coding),
        v. CDD/CSD (Cyclic delay/shift diversity).
28. Specyfikacja radia 802.11b/g/n/ax:
    a. Moc transmisji konfigurowalna przez administratora,
    b. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM, 256- QAM, 1024-QAM,
    c. Technologia direct sequence spread spectrum (DSSS), OFDM, OFDMA.
29. Punkt dostępowy musi posiadać co najmniej:
    a. 1 interfejs 1000/2.5G BaseT (zgodny z 802.3bz):
        i. z funkcją auto-sensing link oraz MDI/MDX,
        ii. z funkcją PoE/PoE+,
        iii. obsługą równoważenia obciążenia "load balancing",
    b. 1 interfejs 100/1000 BaseT:
        i. z funkcją auto-sensing link oraz MDI/MDX,

	ii. obsługą równoważenia obciążenia "load balancing". c. interfejs konsoli RS-232 (RJ-45) lub USB, d. interfejs USB 2.0 (Typ-A, niezależny od portu konsoli), e. przycisk przywracający konfigurację fabryczną, f. slot zabezpieczający Kensingston, g. Punkt dostępowy musi posiadać przycisk Reset umożliwiający szybie przywrócenie urządzenia do ustawień fabrycznych. 30. Punkt dostępowy powinien być wyposażone w diody informujące o stanie: a. Systemu, b. modułu radiowego.
2.7. **GWARANCJA**	1. (wykreślony) 2. Wykonawca zapewnia w okresie trwania gwarancji: – usługi serwisowe świadczone w miejscu instalacji urządzenia- zgłaszania usterek przez portal internetowy, telefonicznie lub mailowo; – dostępność wsparcia technicznego w godzinach pracy zamawiającego (8^{15} — 16^{15}). 3. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich. 4. Urządzenie powinno być objęte gwarancją typu Limited Lifetime Warranty tj. Gwarancją na sprzęt z wymianą na nowe urządzenie w przypadku awarii przez cały czas cyklu życia produktu (do 5 lat po zakończeniu przez producenta sprzedaży produktu). 5. Wymagane jest wykupienie u producenta kontraktu serwisowego z dostępem do poprawek oprogramowania urządzenia oraz wsparcia technicznego przez minimum 60 miesięcy. 6. Serwis gwarancyjny musi obejmować prawo do aktualizacji wersji oprogramowania systemowego urządzeń oraz zapewniać Zamawiającemu bezpośredni dostęp do: nowych wersji oprogramowania; narzędzi konfiguracyjnych i dokumentacji technicznej; pomocy technicznej producentów, w tym możliwość samodzielnego otwierania zgłoszeń serwisowych u producenta 7. Dostarczane urządzenia muszą być objęte serwisem gwarancyjnym na okres 60 miesięcy, opartym na bezpośrednim serwisie producenta świadczonym w trybie 8x5xNBD (8 godzin dziennie, 5 dni w tygodniu, naprawa w następnym dniu roboczym); Serwis musi umożliwiać Zamawiającemu bezpośredni dostęp do stron producenta w celu pobrania najnowszego oprogramowania lub poprawek (ang. patch) do dostarczonych urządzeń, zgłaszania problemów serwisowych oraz bezpośredni dostęp Zamawiającego do TAC (Technical Assistance Center) producenta urządzenia
2.8. **INNE WYMAGANIA**	1. Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni. 2. Parametry pracy urządzenia: – Temperatura otoczenia (zakres minimalny): 0-50 º C; – Wilgotność (zakres minimalny): 5% - 92%. 3. Obsługiwane standardy: – Ethernet IEEE 802.3 / IEEE 802.3u; – Power-over-Ethernet IEEE 802.3af; – Wireless IEEE 802.11a/b/g/n/ac/ax; – EN 300 328; – EN 301 489; – EN 301 893; – EN 60601-1-1, EN60601-1-2. 4. Wszystkie urządzenia muszą mieć możliwość rozbudowy o licencję ochrony sieciowej zapewniające poprawną współprace z kontrolerem w zakresie

	poprawnej autoryzacji w sieci wifi (dostarczenie licencji nie jest wymagane na tym etapie).

3. Wymagania dla wirtualnego kontrolera do zarządzania punktami dostępowymi – 1 szt. (pkt.1.2.)

PARAMETRY I WYMAGANIA MINIMALNE
3.1. Oprogramowanie do zarządzania siecią bezprzewodową posiadające możliwość pracy w VMware HA (jako klaster wysokiej dostępności). Oprogramowanie musi w pełni obsługiwać punkty dostępowe, opisane powyżej.
3.2. Oprogramowanie musi zarządzać siecią bezprzewodową złożoną z minimum 60 punktów dostępowych (wymagane jest dostarczenie licencji wraz z oprogramowaniem) z możliwością rozbudowy do minimum 250 punktów dostępowych.
3.3. Oprogramowanie do zarządzania siecią bezprzewodowa muszą pochodzić od tego samego producenta co punkty dostępowe opisane w pkt 2 w celu osiągniecia maksymalnego poziomu integracji oraz spójności.
3.4. Oprogramowanie musi posiadać możliwość funkcji pełnostanowej zapory sieciowej (stateful firewall). Nie jest wymagane dostarczenie licencji na tym etapie.
3.5. System musi pracować w architekturze gwarantującej centralne zarządzanie i kontrolowanie punktów dostępowych z możliwością rozbudowy i rozszerzenia funkcjonalności systemu. Całość konfiguracji odbywać się ma za pomocą oprogramowania i następnie ma być automatycznie propagowana na punkty dostępowe.
3.6. Oprogramowanie musi zapewniać centralne zarządzenia licencjami.
3.7. Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze.
3.8. Ze względu na bezpieczeństwo niedopuszczalne są żadne komponenty rozwiązania zlokalizowane w chmurze.
3.9. Oprogramowanie musi posiadać następujące funkcje: – szybkie przełączanie użytkowników między punktami dostępowymi (poniżej 5 msec), – wsparcie dla wyniesionych punktów dostępowych (podłączanych poprzez sieć Internet), – za pomocą punktów dostępowych musi zapewniać monitorowanie środowiska sieci bezprzewodowej i dynamicznie konfigurowanie parametrów punktów dostępowych (kanały i moc nadawania).
3.10. Oprogramowanie musi posiadać następujące parametry sieciowe: – możliwość wdrożenia w warstwie 2 i 3 ISO/OSI, – wsparcie dla sieci VLAN w tym również trunk 802.1q, – wbudowany serwer DHCP, – obsługa SNMPv2, SNMPv3, – OSPF.

3.11. Aplikacja do zarządzania siecią WLAN musi obsługiwać co najmniej:

- metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST , DES, 3DES, AES-CBC;
- szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze;
- SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit;
- Autoryzację dostępu użytkowników:
  - 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;
  - Funkcję wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia;
  - Wsparcie dla autoryzacji, minimum: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba NAC;
  - 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";
  - Umożliwia wykorzystanie mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES);
  - Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych oraz zewnętrznych serwerów uwierzytelniających. Oprogramowanie 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;
- Kontroler musi zapewniać obsługę XML API do uwierzytelnienia.

3.12. Oprogramowanie musi posiadać obsługę transmisji różnego typu danych w jednej sieci:

- integracja jednoczesnej transmisji danych i głosu;
- 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;
- szybkie przełączanie się klientów pomiędzy punktami dostępowymi (fast roaming);
- ograniczanie pasma dla użytkownika oraz dla roli użytkownika;
- ograniczenie pasma dla poszczególnych aplikacji;
- ograniczenie pasma dla poszczególnych SSID.

3.13. Oprogramowanie musi umożliwiać stworzenie strony dla gości (tzw. Captive Portal) a także w umożliwiać w przyszłości skorzystanie z Enhanced Open.

3.14. Oprogramowanie ma umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracowników sekretariatów).

3.15. Oprogramowanie posiada funkcję adaptacyjnego zarządzania pasmem radiowym:

- automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe;
- stałe monitorowanie pasma oraz usług;
- przełączenie punktów dostępowych w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałami;
- rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma

- automatyczne przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tym paśmie;
- zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b);
- Wykrywanie interferencji oraz miejsc bez pokrycia sygnału;
- Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w.

3.16. Oprogramowanie musi posiadać możliwość funkcjonalności wbudowanej zapory sieciowej (nie jest wymagane dostarczenie licencji na tym etapie) , posiadającej co najmniej następujące własności:

- inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia;
- kopiowanie (mirroring) sesji;
- szczegółowe logi (per pakiet) do późniejszej analizy;
- ALG (Application Layer gateway) co najmniej dla protokołów: FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera, PPTP;
- translacja źródłowa i docelowa adresów IP;
- identyfikacja i blokowanie ataków DoS;
- Obsługa protokołu GRE;
- Deep packet inspection (DPI);
- Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci wifi;

3.17. Aplikacja musi posiadać możliwość funkcji systemu WIDS/ WIPS (nie jest wymagane dostarczenie licencji na tym etapie). Moduł WIPS musi posiadać co najmniej następujące funkcje:

- detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP); automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów;
- identyfikacja i możliwość blokowania sieci Adhoc;
- identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging;
- ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler;
- identyfikacja błędów konfiguracji klientów WLAN;
- Identyfikacja podszywania się pod autoryzowane punkty dostępowe.

3.18. Oprogramowanie musi być zgodne z następującymi parametrami ilościowymi/wydajnościowymi:

- możliwa liczba obsługiwanych punktów dostępowych nie mniej niż 250;
- należy dostarczyć licencje na podłączenie 60 punktów dostępowych;
- obsługa minimum 2 000 VLANów;
- obsługa minimum 4000 tuneli GRE;
- równoczesna obsługa minimum 4000 użytkowników lub urządzeń

3.19. Gwarancja i serwis:

- oprogramowanie musi być objęte kontraktem serwisowym wykupionym u producenta na minimum 60 miesięcy;
- kontraktu serwisowy musi umożliwiać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego przez minimum 60 miesięcy;
- wymagana jest dostępność usługi w trybie 8x5xNBD w godzinach od 8:15 do 16:15. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis.
- Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

– Wszystkie licencje dostarczone wraz z oprogramowaniem muszą być dostępne przez cały okres ich użytkowania (permanentne).

4. Wymagania dla systemu autentykacji, autoryzacji i kontroli dostępu – 1 szt. (pkt.1.2.)

PARAMETRY I WYMAGANIA MINIMALNE
4.1. System kontroli dostępu musi pochodzić od tego samego producenta co punkty dostępowe i oprogramowanie do zarządzania siecią bezprzewodową w celu osiągnieciu maksymalnego poziomu integracji, spójności oraz musi umożliwić docelowe monitorowanie wszystkich danych z jednego miejsca.
4.2. System musi charakteryzować się następującymi cechami: – możliwość współpracy z urządzeniami wielu producentów (tzw. multi vendor) i posiadać przykładowe gotowe profile dla producentów sprzętu posiadanego przez zamawiającego (m.in. Cisco); – system musi odsługiwać minimum 300 urządzeń klienckich (w tym gości) z możliwością zwiększenia do 4000; – możliwość pracy w trybie HA (dostarczenie licencji HA nie jest wymagane w ramach postępowania); – praca jako maszyna wirtualna w środowisku VMware; – wbudowany serwer Radius; – wbudowany serwer TACACS+ (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie); – wsparcie dla RADIUS VSA co najmniej 100 producentów, w tym: ▪ Cisco Systems; ▪ Fortinet; ▪ Microsoft; ▪ Alcatel-lucent Enterprise; ▪ Aruba Networks; ▪ Huawei; ▪ Extreme Networks; ▪ PaloAlto; – możliwość współpracy z 2FA, MFA: ▪ SMS Link; ▪ Soft Token; ▪ Microsoft Authenticator; ▪ Hardware Token; ▪ Email Link; ▪ QR Code Authenticator; ▪ Google Authenticator; ▪ Authy Authenticator;

- OTP over SMS;
- OTP over Email;
- PUSH Notifications;

– możliwość współpracy z zewnętrznymi rozwiązaniami w chmurze oraz on-premis;
– oprogramowanie musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera;
– możliwość otrzymywania od systemu do zarządzania siecią bezprzewodową dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego;
– wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych;
– system musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych:

- Microsoft Active Directory;
- Radius;
- Kerberos;
- LDAP;
- ODBC;

– metody profilowania muszą być wbudowane w system (dopuszcza się rozbudowę poprzez dokupienie licencji, nie jest ona wymagana w ramach postepowania):

- DHCP;
- TCP;
- MAC OUI;
- SNMP;
- Cisco device sensor;

– wsparcie dla protokołów:

- Radius, Radius CoA, TACACS +, web authentication, SAML v2.0;
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD);
- TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP);
- PAP, CHAP, MSCHAPv1 i v2, EAP-MD5;
- NAC, Microsoft NAP;
- Windows machine authentication;
- MAC Auth;
- Audit (role oparte na porcie oraz skanowanie podatności);
- OCSP (Online Certificate Status Protocol);
- SNMP generic MIB, SNMP private MIB;
- CEF (Common Event Format), LEEF (Log Event Extended Format);
- TLS 1.2;

– funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami (dopuszcza się rozbudowę poprzez dokupienie licencji, która nie jest wymagana na tym etapie);
– posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji, nie jest ona wymagana na tym etapie;
– konfiguracja urządzeń musi odbywać się bez potrzeby angażowania pracowników działu IT;

- system musi wspierać obsługę następujących systemów operacyjnych:
  - Ubuntu;
  - Android;
  - Chromebook;
  - iOS;
  - Mac OS X;
  - MS Windows;
- system musi umożliwiać klientowi samorejestrację oraz bezpieczne skonfigurowanie urządzenia do pracy w sieci;
- automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej;
- użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu;
- funkcja tworzenia unikalnych certyfikatów dla urządzeń;
- wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń;
- funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID;

4.3. System musi posiadać moduł odpowiedzialny za dostęp dla gości. Obsługa użytkowników typ gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (300). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte. Obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności:
- samodzielna rejestracja klientów gościnnych w oparciu o:
  - adres e-mail;
  - numer telefonu (SMS);
- wspierać funkcję integracji z systemami trzecimi poprzez API;
- wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego;
- funkcja personalizacji strony gościnnej;

4.4. System musi posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji. System kontroli końcówek klienckich musi mieć następujące funkcjonalności:
- System musi wspierać następujące systemy operacyjne:
  - SUSE linux 10.x i nowsze;
  - Fedora Core 5 i nowsze;
  - CentOS 4 (Community Enterprise Operating System) i nowsze;
  - Red HAT Enterprise Linux 4 i nowsze;
  - Apple Mac OS X 10.7 i nowsze;
  - Microsoft Windows 10 i nowsze (może być uruchomiony jako serwis);
- wyświetlanie informacji on-line o statusie monitorowanych końcówek;
- system powinien obsługiwać agenta w formie:
  - stałej;
  - tymczasowej;
  - agenta NAP.

4.5. Gwarancja i serwis:
- oprogramowanie musi być objęte kontraktem serwisowym wykupionym u producenta na minimum 60 miesięcy;
- kontraktu serwisowy musi umożliwiać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego przez minimum 60 miesięcy;

- wymagana jest dostępność usługi w trybie 8x5xNBD w godzinach od 8:15 do 16:15. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis.
- Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.
- Wszystkie licencje dostarczone wraz z oprogramowaniem muszą być dostępne przez cały okres ich użytkowania (permanentne).

FORMULARZ OFERTY

Nazwa Wykonawcy:

Ulica : nr domu : nr lokalu :

Kod pocztowy : __-___ miejscowość :

Powiat : województwo :

NIP : ___-___-___-___ REGON : _____

Internet : http:// e-mail :

nr telefonu: nr faksu:

Bank :

nr konta do zwrotu wadium:

KRS/CEiDG:

*** Wykonawca jest: mikroprzedsiębiorstwem ☐ małym ☐ średnim przedsiębiorstwem ☐

UWAGA: W przypadku oferty składanej przez podmioty występujące wspólnie, powyższe dane należy wypełnić dla każdego podmiotu osobno (poprzez skopiowanie). Dotyczy wspólników spółki cywilnej, członków konsorcjum.

Jako Wykonawca w postępowaniu prowadzonym w trybie podstawowym bez negocjacji na dostawę urządzeń WiFi, nr sprawy BF-IV.2370.24.2022, oferujemy realizację zamówienia zgodnie z zasadami określonymi w specyfikacji warunków zamówienia (SWZ) oraz oświadczamy, że oferujemy wykonanie zamówienia publicznego za:

1)* Cenę brutto w wysokości: .....zł

(słownie.....zł);

Cenę netto w wysokości: ..... zł;

Stawka podatku VAT: .....; Wartość podatku VAT: ..... zł.

Zgodnie z załącznikiem nr 4 „Formularz cenowy", Cena brutto została obliczona wg algorytmu: Cena netto + VAT = Cena brutto.

2)* Termin dostawy: ..... (max. 21 dni).

W przypadku nieuzupełnienia przez wykonawcę terminu dostawy – zamawiający uzna, że wykonawca zaproponował maksymalny termin dostawy tj. 21 dni. Taka wartość zostanie przyjęta do obliczeń, w przedmiotowym kryterium. W przypadku wskazania terminu dostawy dłuższego niż 21 dni, oferta Wykonawcy zostanie uznana za niezgodną z warunkami zamówienia i zostanie odrzucona.

3) * Możliwość redundacji między dwoma portami w punkcie dostępowym:

TAK ** / NIE ****

W przypadku, kiedy wykonawca nie zaznaczy jednej z powyższych opcji, zamawiający przyjmie, że wykonawca nie przewiduje możliwości redundacji między dwoma portami w punkcie dostępowym i przyzna ofercie w przedmiotowym kryterium 0 pkt.

4) Warunki płatności: zgodnie z projektem umowy.

5) * Producent oferowanego sprzętu jest sklasyfikowany w raporcie Gartnera „Magic Quadrant for the Wired and Wireless LAN Access Infrastructure" i znajduje się w kwadracie liderów (Leaders), dane z raportu nie starszego niż listopad 2021.

TAK ** / NIE ****

Ponadto oświadczamy, że:

a) zapoznaliśmy się ze wszystkimi warunkami określonymi w specyfikacji warunków zamówienia (SWZ) wraz z wyjaśnieniami i modyfikacjami, projektem umowy oraz załącznikami do SWZ, akceptujemy je bez jakichkolwiek zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty;
b) uważamy się za związanych niniejszą ofertą na czas wskazany w SWZ w Rozdziale IX ust. 1;
c) w przypadku wyboru naszej oferty zobowiązujemy się do zawarcia umowy, zgodnie z zapisami projektu umowy, stanowiącego załącznik do SWZ, w terminie zaproponowanym przez Zamawiającego.

Informujemy, że:

a) ** wybór naszej oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego:

.....

zgodnie z Rozdziałem XIV ust. 5 SWZ należy podać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania obowiązku podatkowego wskazując ich wartość bez kwoty podatku (wartość netto) oraz wskazać stawkę podatku VAT, która będzie miała zastosowanie.

b) Zamówienie będzie wykonane własnymi siłami/z pomocą Podwykonawcy****

.....,

(nazwa firmy, siedziba)

który wykonywać będzie część zamówienia obejmującą *****:.....

Uwaga: brak wpisu i skreślenia powyżej rozumiany jest, iż przedmiotowe zamówienie realizowane będzie bez udziału podwykonawców.

.....

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.

* Wartości oceniane.
** jeżeli na Wykonawcy spoczywa obowiązek podatkowy związany z realizacją zamówienia, przed podpisaniem druku „Formularz oferty" należy zapis wykreślić lub wpisać nie dotyczy.
*** Wypełnić poprzez zaznaczenie krzyżykiem właściwej kratki, zgodnie z definicją:
Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.
Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.
Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR *lub* roczna suma bilansowa nie przekracza 43 milionów EUR.
**** skreślić odpowiednio.
***** wpisać właściwe