

## OPIS PRZEDMIOTU ZAMÓWIENIA

### 1. Nazwa zamówienia

Dostawa nowych elementów oraz przebudowa systemu bezpiecznej sieci Wi-Fi wraz ze wsparciem dla całego rozwiązania (sprzętu oraz oprogramowania) na potrzeby przebudowy.

### 2. Kody CPV

32424000-1: Infrastruktura sieciowa

71356300-1: Usługi wsparcia technicznego

48000000-8: Pakiety oprogramowania i systemy informatyczne

72250000-2: Usługi w zakresie konserwacji i wsparcia systemów

### 3. Definicje

3.1. Na potrzeby niniejszego dokumentu, poniższe określenia będą miały następujące znaczenie:

3.1.1. **Aktualizacje** – uaktualnienia Oprogramowania, dostarczonego w wykonaniu Umowy, w tym wyższe wersje (update/upgrade), niższe wersje (downgrade), wydania uzupełniające, patche, zmiany, nowe wersje, poprawki oraz inne dostosowania, w tym wskazane w OPZ, zapewniające prawidłowe korzystanie z takiego oprogramowania.

3.1.2. **Awaria** – nieprawidłowe działanie Urządzeń lub Oprogramowania, w szczególności brak możliwości używania Urządzeń lub Oprogramowania w sposób zgodny z ich przeznaczeniem lub z Dokumentacją lub Dokumentacją Powykonawczą.

3.1.3. **Awaria Krytyczna** – Awaria wywołująca nieprawidłowe działanie Urządzeń lub Oprogramowania powodujące całkowity brak możliwości korzystania z Urządzeń lub Oprogramowania albo takie ograniczenie korzystania z Urządzeń lub Oprogramowania, uniemożliwiające spełnianie ich podstawowych funkcji, bez możliwości naprawy poprzez obejście proceduralne.

3.1.4. **Awaria Zwykła** – Awaria wywołująca nieprawidłowe działanie Urządzeń lub Oprogramowania niebędące Awarią Krytyczną, w szczególności działanie w sposób niezgodny z ich przeznaczeniem, z Dokumentacją lub Dokumentacją Powykonawczą.

3.1.5. **Zgłoszenie** – poinformowanie Wykonawcy przez Zamawiającego o wystąpieniu Awarii.

3.1.6. **Czas obsługi Awarii** – okres od dokonania Zgłoszenia do momentu, w jakim zostanie przywrócona pierwotna funkcjonalność i efektywność działania odpowiednio Urządzeń lub Oprogramowania.

3.1.7. **Dni Robocze** – dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.

3.1.8. **Dokumentacja** – wszelkie informacje i dokumenty, niezależnie od nośnika, dołączone przez producenta do Urządzeń lub Oprogramowania przy ich sprzedaży użytkownikom końcowym oraz dokumenty potwierdzające udzielenie gwarancji dla tych Urządzeń i Oprogramowania przez producenta. Min. wszelka dokumentacja dostarczona lub wykonana w ramach Umowy, w szczególności dokumentacja niezbędna do korzystania z Rozwiązania WIFI, w tym techniczna oraz użytkowa, w tym Dokumentacja Licencyjna.

3.1.9. **Dokumentacja Powykonawcza** – dokumentacja zawierająca szczegółowy wykaz wszystkich Urządzeń z numerami seryjnymi i modułów oraz szczegółowy opis ich instalacji wraz

z konfiguracją oraz rysunkami technicznymi.

- 3.1.10. **Dokumentacja licencyjna** – wszelka dokumentacja dostarczona lub wykonana na podstawie Umowy, w szczególności dokumentacja niezbędna do korzystania z Oprogramowania, certyfikaty licencyjne, warunki licencyjne Oprogramowania.
- 3.1.11. **Lokalizacja** – siedziba Zamawiającego na terenie miasta stołecznego Warszawy, do której ma nastąpić dostawa Rozwiązania WIFI.
- 3.1.12. **Roboczość** - Jednostka miary czasu wykonywania usługi, obejmująca pracę jednej osoby przez godzinę zegarową, do której nie wlicza się czasu dojazdu do Lokalizacji, w której usługa jest wykonywana.
- 3.1.13. **Oprogramowanie** Oprogramowanie pozwalające na korzystanie z Urządzeń, w szczególności oprogramowanie systemowe, do zarządzania systemem lub wbudowane w Urządzenie. Pojęcie to obejmuje wszystkie Aktualizacje i elementy przewidziane przez producenta Oprogramowania dla prawidłowego korzystania z Oprogramowania wraz z odpowiednimi licencjami uprawniającymi do korzystania z Oprogramowania.
- 3.1.14. **Urządzenie, Sprzęt** – urządzenie, urządzenia szczegółowo opisane w pkt. 6. OPZ, które Wykonawca zobowiązany jest sprzedać i dostarczyć Zamawiającemu wraz z wyposażeniem, komponentami, akcesoriami, elementami zapewniającymi właściwą instalację i używanie urządzeń zgodnie z ich przeznaczeniem.
- 3.1.15. **Rozwiązanie Wifi** - przedmiot zamówienia opisany w niniejszym OPZ, w tym Urządzenia i Oprogramowanie, obejmujący kompleksowe rozwiązanie informatyczne spełniające wymagania określone w OPZ.

#### **4. Przedmiot zamówienia**

- 4.1. Przedmiotem zamówienia jest przebudowa (dostarczenie nowych komponentów, wymiana starych komponentów na nowe wraz z montażem, i konfiguracją Rozwiązania WIFI) obecnie posiadanej przez Zamawiającego infrastruktury sieci Wi-Fi w siedzibie Zamawiającego na terenie miasta stołecznego Warszawy wraz z punktami dostępowymi. Dostawa musi obejmować 2 kontrolery pracujące w klastrze na potrzeby zarządzania siecią Wi-Fi w Lokalizacji, 140 Access Point-ów, system uwierzytelniania użytkowników lub urządzeń końcowych (NAC - Network Access Control) wraz z wymaganymi licencjami. Zamawiający wymaga, aby Wykonawca zamontował urządzenia, zainstalował Oprogramowanie oraz skonfigurował infrastrukturę, aby stanowiły kompletne rozwiązanie sieci Wi-Fi wraz z uwierzytelnianiem użytkowników i urządzeń końcowych.
- 4.2. W ramach zamówienia Wykonawca obejmie urządzenie 36-miesięcznym wsparciem technicznym oraz zapewni 36-miesięczną gwarancję producenta dla urządzeń oraz Oprogramowania, dostarczonych w ramach Zamówienia.
- 4.3. W ramach realizacji zamówienia Wykonawca przeprowadzi minimum 3-dniowe szkolenie certyfikowane przez producenta Rozwiązania WIFI dla 4 administratorów z konfiguracji oraz obsługi Rozwiązania.

#### **5. Wymagania Ogólne:**

- 5.1. Wykonawca, najpóźniej w dniu dostarczenia Urządzeń i Oprogramowania do Lokalizacji, jest zobowiązany do przekazania Zamawiającemu na adres e-mail wskazany przez Zamawiającego w umowie:

- 5.1.1. zestawienia w formacie .csv wszystkich dostarczonych urządzeń, zgodnie ze złożoną Ofertą, zawierającego przynajmniej informacje: producent, typ, model, numer seryjny, cenę jednostkową netto, cenę jednostkową brutto, MAC adres karty sieciowej.
- 5.1.2. Adresy poczty elektronicznej, numery telefonów oraz dane dostępowe do portalu klienckiego, umożliwiające Zamawiającemu samodzielne pobieranie Oprogramowania w ramach posiadanej licencji, korzystanie ze wsparcia technicznego w pełnym zakresie oraz z Godzin Ekspertkich.
- 5.1.3. Dokumenty licencji na Oprogramowanie, w tym certyfikaty licencyjne wystawione przez producenta, umowy/standardowe warunki licencyjne producenta Oprogramowania.
- 5.1.4. Standardowe warunki realizacji Wsparcia technicznego producenta Rozwiązania WIFI.
- 5.1.5. Dokument potwierdzający wykupienie od producenta na rzecz Zamawiającego usługi Wsparcia Technicznego.
- 5.1.6. dokument potwierdzający objęcie Rozwiązania WiFi Gwarancją producenta.
- 5.1.7. Voucher na szkolenie, o którym mowa w pkt 9 OPZ.
- 5.2. O ile inaczej nie zaznaczono, wszelkie zapisy OPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.
- 5.3. Dostarczane urządzenia muszą być kompletne, tj.: mieć okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie.
- 5.4. Wykonawca wraz z urządzeniami dokona dostawy wszystkich niezbędnych elementów koniecznych do montażu i uruchamiania urządzeń w Lokalizacjach tj. pasywnego sprzętu sieciowego i okablowania.
- 5.5. Zamawiający nie dopuszcza urządzeń refabrykowanych, wymagana jest dostawa urządzeń fabrycznie nowych, nieużywanych wraz z niezbędnym wyposażeniem producenta.
- 5.6. Urządzenia muszą być dostarczone wraz z licencjami umożliwiającymi uruchomienie na każdym z dostarczonych urządzeń pełnej funkcjonalności Oprogramowania.
- 5.7. Urządzenia zostaną dostarczone do Lokalizacji tj.  
siedziby Ministerstwa Cyfryzacji - Warszawa, Królewska 27
- 5.8. Wykonawca zobowiązuje się w ramach realizacji przedmiotu zamówienia do dostarczenia Zamawiającemu urządzeń oraz Oprogramowania, montażu oraz konfiguracji urządzeń oraz Oprogramowania opisanego w OPZ, w uzgodnionym z Zamawiającym terminie, nie dłuższym niż **60 Dni roboczych** od daty zawarcia umowy - zgodnie z uzgodnionym z Zamawiającym harmonogramem.
- 5.9. Wykonawca zobowiązany jest do dokumentowania wszystkich czynności realizowanych w ramach montażu i konfiguracji oraz przekazania tych dokumentów w ramach Dokumentacji Powykonawczej.
- 5.10. Wykonawca zobowiązany jest do przeprowadzenia końcowego testu stabilności działania wytworzonej sieci oraz pokrycia Lokalizacji siecią WiFi i do wyeliminowania ewentualnych powstałych problemów stabilności lub pokrycia, w terminie, o którym mowa w pkt. 5.8.
- 5.11. W ramach realizacji Umowy Wykonawca przeprowadzi minimum 3-dniowe szkolenia certyfikowane przez producenta urządzeń i Oprogramowania dla 4 administratorów z konfiguracji oraz obsługi urządzeń oraz Oprogramowania w terminie 40 dni od dnia podpisania Protokołu odbioru.
- 5.12. Kontrolery sieci WiFi oraz Punkty dostępowe muszą pochodzić od tego samego producenta.
- 5.13. Zamawiający wymaga, aby wszystkie komponenty dostarczone przez Wykonawcę były objęte gwarancją producenta na okres 36 miesięcy od dnia dostarczenia potwierdzonego podpisanym Protokołem odbioru końcowego.
- 5.14. Wykonawca będzie posiadał i okaże na każde żądanie Zamawiającego poświadczenie producenta

urządzeń i Oprogramowania o posiadaniu statusu partnerstwa, w przypadku gdy Wykonawcą nie jest producent, których wartościowy udział w zamówieniu jest najwyższy, z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Wykonawca posiada i będzie posiadać przez cały okres obowiązywania Umowy nie niższy niż drugi w kolejności poziom partnerstwa licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta.

## **6. Wymogi szczegółowe w zakresie Przedmiotu Zamówienia**

### **6.1. Punkt dostępowy sieci bezprzewodowej WiFi6E posiadający:**

#### **6.1.1. obsługę standardów 802.11a/b/g/n/ac/ax**

- 6.1.1.1. obsługa OFDMA (uplink/downlink), TWT, BSS Coloring
- 6.1.1.2. obsługa MU-MIMO (uplink/downlink) – min. 4x4:4 (5GHz oraz 6GHz)
- 6.1.1.3. obsługa MU-MIMO (uplink/downlink) – min. 2x2:2 (2,4GHz)
- 6.1.1.4. obsługa kanałów 20, 40, 80 MHz dla 802.11ac
- 6.1.1.5. obsługa kanałów 20, 40, 80, 160 MHz dla 6GHz oraz 20, 40, 80 MHz dla 5GHz dla 802.11ax
- 6.1.1.6. obsługa prędkości PHY do 1,7 Gbps (ac) (przy parametrach: 4x4, 80 MHz, 5GHz)
- 6.1.1.7. obsługa prędkości PHY do 7,4 Gbps (ax) (przy parametrach: 4x4 160 MHz 6GHz oraz 4x4 80 MHz 5GHz oraz 2x2 20 MHz 2,4GHz)
- 6.1.1.8. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
- 6.1.1.9. obsługa beamforming dla klientów 802.11ac/ax
- 6.1.1.10. obsługa MRC (Maximal Ratio Combining)

#### **6.1.2. konfigurowalną moc nadajnika**

- 6.1.2.1. dla zakresu 2.4GHz: do 100 mW
- 6.1.2.2. dla zakresu 5GHz: do 200 mW
- 6.1.2.3. dla zakresu 6GHz: do 200 mW

#### **6.1.3. możliwość pracy trójzakresowej w pasmach: 2,4GHz oraz 5GHz oraz 6GHz**

#### **6.1.4. zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:**

- 6.1.4.1. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
- 6.1.4.2. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
- 6.1.4.3. obsługa min. 16 BSSID
- 6.1.4.4. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
- 6.1.4.5. uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w
- 6.1.4.6. obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)
- 6.1.4.7. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników
- 6.1.4.8. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6
- 6.1.4.9. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i

- klientów WLAN)
- 6.1.4.10. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
  - 6.1.4.11. obsługa IPv6
  - 6.1.4.12. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
  - 6.1.4.13. obsługa mechanizmów QoS: ograniczanie ruchu do użytkownika, z możliwością konfiguracji, per użytkownik, obsługa WMM, TSPEC, U-APSD wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM
  - 6.1.4.14. obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting
  - 6.1.4.15. wsparcie IEEE 802.11i, WPA2, WPA3, WPA3-OWE (Enhanced Open)
  - 6.1.4.16. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)
  - 6.1.4.17. obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS
  - 6.1.4.18. obsługa blokowania ruchu Peer-to-Peer
  - 6.1.5. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)
  - 6.1.6. obsługa aWIPS (Advanced Wireless Intrusion Prevention System) polegająca na wykryciu i remediacji zagrożenia. AP będący częścią systemu WIPS pozwala na określenie m.in. następujących informacji: sygnatura ataku, rodzaj wykrytej anomalii i jej opis, czas zdarzenia:
    - 6.1.6.1. wykrywanie sygnatur DoS: Auth/Deauth Flood, Assoc/Disassoc Flood, CTS/RTS Flood, Broadcast Deauth/Dissassoc Flood, Broadcast Probe Flood, EAPOl Logoff Flood
    - 6.1.6.2. wykrywanie ataków: EAPOl-Logoff, RTS/CTS Virtual Carrier Sense
  - 6.1.7. obsługa (przy współpracy z kontrolerem) polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag)
  - 6.1.8. uruchamianie aplikacji w kontenerach bezpośrednio na AP
  - 6.1.9. obsługa VXLAN
  - 6.1.10. moduł radiowy pełniący funkcję analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz, 5GHz, 6GHz):
    - 6.1.10.1. zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych
    - 6.1.10.2. automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.)
    - 6.1.10.3. umożliwia skanowanie off-channel (funkcjonuje niezależnie od pracy modułów radiowych transmitujących do klientów) zapewniając dodatkową analizę pasma radiowego pod kątem, m.in.: wykrywania sygnałów DFS, zarządzania ustawieniami parametrów radiowych, zbierania pakietów do lokalizacji urządzeń mobilnych
  - 6.1.11. musi posiadać interfejsy minimum:
    - 6.1.11.1. interfejs MultiGigabit Ethernet (100/1000/2500)
    - 6.1.11.2. interfejs konsolowy
    - 6.1.11.3. port USB 2.0

- 6.1.12. musi mieć wbudowaną pamięć o minimalnych parametrach 2 GB RAM, 1 GB Flash
  - 6.1.13. zróżnicowane możliwości zasilania:
    - 6.1.13.1. przy zasilaniu przez 802.3bt: pełna funkcjonalność AP
    - 6.1.13.2. przy zasilaniu przez 802.3at: praca z wyłączonym portem USB
    - 6.1.13.3. przy zasilaniu przez 802.3af: możliwość uruchomienia AP w celach diagnostycznych bez pracujących modułów radiowych
  - 6.1.14. musi posiadać anteny zintegrowane o zysku:
    - 6.1.14.1. min. 3 dBi dla pasma 2,4GHz
    - 6.1.14.2. min. 5 dBi dla pasma 5GHz
    - 6.1.14.3. min. 4 dBi dla pasma 6GHz
  - 6.1.15. musi posiadać obudowę przystosowaną do pracy w zakresie temperatur 0 – 50°C
  - 6.1.16. musi posiadać certyfikację WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi6, Wi-Fi Enhanced Open, WMM, WMM-PS
  - 6.1.17. musi posiadać wbudowane radio Bluetooth Low Energy (BLE) 5.1
  - 6.1.18. musi być przeznaczony do montażu wewnątrz budynków
  - 6.1.19. musi być wyposażony w elementy umożliwiające zamontowanie go na suficie technicznym jak i nad nim.
- 6.2. **Kontroler sieci bezprzewodowej do zarządzania Punktami Dostępowymi zaproponowanymi dla punktu 6.1**
- 6.2.1. Urządzenie umożliwiające centralne zarządzanie co najmniej 250 punktami dostępowymi wraz z wymaganymi licencjami, z możliwością rozbudowy do 500 punktów.
  - 6.2.2. Kontroler musi być wyposażony w:
    - 6.2.2.1. Co najmniej 4 porty optyczne o przepływności 10/25Gbps, wyposażone we wkładki. Liczba portów i architektura kontrolerów musi zapewniać poprawne obsłużenie ruchu z obsługiwanych urządzeń bezprzewodowych niezależnie od wielkości i rodzaju przesyłanych pakietów.
    - 6.2.2.2. Port serwisowy do obsługi out-of-band management.
    - 6.2.2.3. Port konsolowy RS 232;
    - 6.2.2.4. Port USB 3.0.
    - 6.2.2.5. Dedykowany interface do połączenia dwóch kontrolerów w redundantną parę
  - 6.2.3. Obsługa łączenia interfejsów w grupę logiczną, by zabezpieczyć przed awarią pojedynczego interfejsu;
  - 6.2.4. Obsługa ruchu tunelowanego o przepustowości 10Gbps
  - 6.2.5. Obsługa 5000 klientów sieci bezprzewodowej z możliwością rozbudowy do 10 000;
  - 6.2.6. Musi poprawnie współpracować z punktami dostępowymi dostarczonymi w ramach zamówienia. W szczególności zestaw punktów dostępowych i kontroler muszą udostępniać pełną wymaganą funkcjonalność.
  - 6.2.7. Kontroler wraz ze współpracującymi Access Pointami musi umożliwiać obsługę urządzeń końcowych IPv4 i IPv6.
  - 6.2.8. Obsługa NTP (IPv4 i IPv6)
  - 6.2.9. W przypadku awarii kontrolera Access Pointy muszą posiadać możliwość automatycznego przełączenia się na kontroler zapasowy lub na inne kontrolery z wolną liczbą licencji na AP.
  - 6.2.10. Kontroler musi umożliwiać zarządzanie przez HTTPS, SNMPv2, SSH, NETCONF oraz przez port



konsoli szeregowej

- 6.2.11. Obsługa logowania SYSLOG, wsparcie dla IPSec w celu zabezpieczenie SYSLOG
- 6.2.12. Obsługa Hotspot 2.0
- 6.2.13. Obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020)
- 6.2.14. Współpraca z siecią dostępową typu SDN opartą o Network Fabric, wymiana informacji kontrolnych za pomocą protokołu LISP (Locator ID Separation Protocol)
- 6.2.15. Rozszerzona współpraca z wybranymi urządzeniami Intel i Samsung pozwalająca na widoczność informacji takich jak: typ i model urządzenia, wersja oprogramowania, system operacyjny, RSSI najbliższych AP
- 6.2.16. Obsługa Wireless IDS/IPS pozwalająca na wykrywanie ataków na sieci bezprzewodowe w oparciu o sygnatury, takie jak: Auth/De-Auth Flood, Assoc/Dis-Assoc Flood, Broadcast Probe Flood, Broadcast Dis-Assoc Flood, Broadcast De-Auth Flood, EAPOL-Logoff Attack, CTS Flood, RTS Assoc Request, De-Auth Flood by Pair, Fuzzed Beacon, Fuzzed Probe Request/Response, PS Poll Flood, EAPOL Start Flood, Re-Assoc Request Flood by Destination, Beacon Flood, Probe Response Flood by Destination, Airdrop Session, Block Ack Flood, Malformed Assoc Request, Malformed Auth, RTS/CTS Virtual Carrier Sense Attack
- 6.2.17. Możliwość przechwycenia i wysłania materiału dowodowego wywołującego alarm IDS/IPS (packet capture) do dedykowanego systemu zarządzania
- 6.2.18. Logowanie alarmów IDS/IPS za pomocą SYSLOG
- 6.2.19. Urządzenie musi umożliwiać centralną kontrolę punktów dostępu bezprzewodowego zgodnie z protokołem CAPWAP (RFC 5415):
  - 6.2.19.1. Zarządzanie politykami bezpieczeństwa;
  - 6.2.19.2. Wykrywanie zagrożeń w sieci bezprzewodowej;
  - 6.2.19.3. Zarządzanie pasmem radiowym;
  - 6.2.19.4. Zarządzanie mobilnością;
  - 6.2.19.5. Zarządzanie jakością transmisji.
- 6.2.20. Kontroler musi umożliwiać obsługę co najmniej:
  - 6.2.20.1. 4096 Vlan;
  - 6.2.20.2. 4096 Wlan.
- 6.2.21. Zarządzanie pasmem radiowym punktów dostępowych:
  - 6.2.21.1. Automatyczna adaptacja do zmian w czasie rzeczywistym;
  - 6.2.21.2. Optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia);
  - 6.2.21.3. Dynamiczne przydzielanie kanałów radiowych;
  - 6.2.21.4. Wykrywanie, eliminacja i unikanie interferencji;
  - 6.2.21.5. Równoważenie obciążenia punktów dostępowych;
  - 6.2.21.6. Tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych;
  - 6.2.21.7. Automatyczna dystrybucja klientów pomiędzy punkty dostępowe.
  - 6.2.21.8. Mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych;
  - 6.2.21.9. dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
- 6.2.22. Mapowanie SSID do segmentów VLAN w sieci przewodowej:

- 6.2.22.1. 1:1
- 6.2.22.2. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
- 6.2.22.3. Możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
- 6.2.23. Kontroler musi wspomagać następujące mechanizmy bezpieczeństwa:
  - 6.2.23.1. 802.11i, WPA3, WPA2, WPA, WEP;
  - 6.2.23.2. 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST);
  - 6.2.23.3. Obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników (min. 12.000 wpisów).
  - 6.2.23.4. Kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID.
  - 6.2.23.5. Obsługa profilowania użytkowników:
    - Przydział sieci VLAN;
    - Przydział list kontroli dostępu (ACL).
  - 6.2.23.6. Uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 (wykrywanie podszywania się punktów dostępowych użytkowników pod adresy infrastruktury) – IEEE 802.11w;
  - 6.2.23.7. Uwierzytelnianie punktów dostępowych w oparciu o certyfikaty;
  - 6.2.23.8. Obsługa list kontroli dostępu (ACL);
  - 6.2.23.9. Obsługa list kontroli dostępu opartych o nazwy domenowe;
  - 6.2.23.10. Obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X;
  - 6.2.23.11. Wykrywanie i dezaktywacja obcych punktów dostępowych;
  - 6.2.23.12. możliwość budowania reguł klasyfikacji obcych punktów dostępowych w oparciu o nazwę SSID, wybrany ciąg znaków w SSID, siłę sygnału RSSI, minimalną ilość podłączonych urządzeń;
  - 6.2.23.13. obsługa polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa z wykorzystaniem mechanizmu out-of-band, który przekazuje mapowania aktualnych adresów IP stacji;
  - 6.2.23.14. Ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP;
  - 6.2.23.15. DHCP proxy, wsparcie dla DHCP Option 82.
- 6.2.24. Obsługa mobilności (roaming-u) użytkowników (L2 i L3 – IPv4 i IPv6, w ramach i pomiędzy kontrolerami).
- 6.2.25. Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k.
- 6.2.26. Wsparcie dla IEEE 802.11u.
- 6.2.27. Obsługa mechanizmów QoS:
  - 6.2.27.1. 802.1p;
  - 6.2.27.2. WMM, TSpec, U-APSD;
  - 6.2.27.3. Ograniczanie pasma per użytkownik;
  - 6.2.27.4. Call Admission Control – ze statyczną definicją pasma i dynamiczną w oparciu o analizę profili ruchu, SIP CAC, Call snooping;
  - 6.2.27.5. Równomierna obsługa klientów sieci bezprzewodowej w oparciu o użycie czasu antenowego;



- 6.2.27.6. Kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID;
- 6.2.27.7. zbiór wbudowanych profili do automatycznej konfiguracji ustawień QoS.
- 6.2.28. Obsługa protokołu Bonjour poprzez wbudowany multicast DNS (mDNS) Gateway zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów.
- 6.2.29. Obsługa dostępu gościnnego (IPv4 i IPv6):
  - 6.2.29.1. Przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony);
  - 6.2.29.2. Obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta;
  - 6.2.29.3. Obsługa 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.
- 6.2.30. Obsługa ruchu unicast IPv4 oraz IPv6;
- 6.2.31. Zgodność z funkcjonalnościami IPv6 pod kątem RFC: 4191, 6980, 8200, 8201.
- 6.2.32. Obsługa ruchu multicast IPv4 oraz IPv6
  - 6.2.32.1. IGMP/MLD snooping
  - 6.2.32.2. Optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a AP)
  - 6.2.32.3. Obsługa konwersji ruchu multicast na unicast
- 6.2.33. Współpraca z Oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych.
- 6.2.34. Obsługa redundancji 1:1 (active/standby) zapewniającej:
  - 6.2.34.1. Utrzymanie sesji punktów dostępowych oraz urządzeń klienckich na wypadek awarii aktywnego kontrolera;
  - 6.2.34.2. Synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej.
- 6.2.35. Obsługa redundancji rozwiązania (N+1)
- 6.2.36. Analiza ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu. Współpraca z serwerami autoryzacyjnymi w celu przypisania odpowiednich polityk kontroli ruchu aplikacji per użytkownik/grupa użytkowników;
- 6.2.37. Zbieranie i eksport statystyk ruchowych za pomocą protokołu Netflow/JFlow lub odpowiednika;
- 6.2.38. Eksport dodatkowych pól w ramach statystyk Netflow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa).
- 6.2.39. Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych (np.: lista kontroli dostępu, VLAN, polityka QoS, czas sesji).
- 6.2.40. Możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania (dni tygodnia, godziny)
- 6.2.41. Obsługa EoGRE w celu tunelowania ruchu z kontrolera do dedykowanego koncentratora (np. na routerze)

### 6.3. System kontroli dostępu do sieci LAN/WLAN/VPN

System zapewnia pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu. System realizuje wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń. System może obejmować kontrolą dostęp wszystkich urządzeń podłączonych do sieci IP w tym terminali, komputerów PC, smartfonów i tabletów, telefonii IP, terminali video i innych podłączonych urządzeń.

- 6.3.1. System musi być dostarczony w postaci dwóch urządzeń wraz z odpowiednimi licencjami umożliwiającymi wykorzystanie wszystkich opisanych poniżej funkcjonalności dla co najmniej 10000 sesji.
- 6.3.2. System umożliwia instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.
- 6.3.3. System umożliwia elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych
- 6.3.4. System umożliwia wysoką skalowalność i rozbudowę w miarę wzrostu liczby urządzeń
- 6.3.5. W scenariuszu, w którym wszystkie komponenty systemu znajdują się na pojedynczym serwerze jest on w stanie obsłużyć minimalnie 10 000 jednoczesnych sesji
- 6.3.6. System umożliwia realizację wysokiej dostępności elementów funkcjonalnych, w tym:
  - 6.3.6.1. zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu
  - 6.3.6.2. zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych
- 6.3.7. System umożliwia aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS
- 6.3.8. System umożliwia zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback)
- 6.3.9. System umożliwia tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled)
- 6.3.10. System umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników
- 6.3.11. System umożliwia uwierzytelnianie administratorów za pomocą zewnętrznych repozytoriów - m.in. Active Directory, Radius i SAML 2.0
- 6.3.12. System umożliwia wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System wymusza hasło różne od trzech poprzednich haseł i jego zmianę co określonej ilości dni
- 6.3.13. System umożliwia kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
  - 6.3.13.1. dostęp do interfejsu konfiguracji usług tożsamości 802.1X
  - 6.3.13.2. dostęp do interfejsu konfiguracji urządzeń sieciowych
  - 6.3.13.3. dostęp do interfejsu konfiguracji polityk
  - 6.3.13.4. dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
  - 6.3.13.5. dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
- 6.3.14. System umożliwia kontrolę dostępu do interfejsu graficznego administratora na podstawie

adresu IP

- 6.3.15. System posiada możliwość podłączenia i identyfikacji urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520
- 6.3.16. System wspiera REST API do masowych operacji CRUD (Create, Read, Update, Delete) m.in. na użytkownikach, stacjach końcowych oraz urządzeniach sieciowych
- 6.3.17. System wspiera REST API do monitorowania w czasie rzeczywistym sesji oraz stacji końcowych
- 6.3.18. System wspiera REST API do konfiguracji i zarządzania m.in. politykami Radius, kopiami zapasowymi oraz repozytoriami plików
- 6.3.19. System umożliwia rozbudowanie funkcjonalności o m.in. profilowanie urządzeń oraz weryfikację stanu stacji końcowej – z ang. posture assessment, bez konieczności rozbudowy sprzętowej
- 6.3.20. System umożliwia rozbudowanie funkcjonalności o serwer TACACS+/Radius do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej

**System wspiera następujące protokoły uwierzytelniania i standardy:**

- 6.3.21. RADIUS, zgodnie z dokumentami:

- 6.3.21.1. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
- 6.3.21.2. RFC 2139 — RADIUS Accounting
- 6.3.21.3. RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
- 6.3.21.4. RFC 2866 — RADIUS Accounting
- 6.3.21.5. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
- 6.3.21.6. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
- 6.3.21.7. RFC 2869 — RADIUS Extensions

- 6.3.22. RADIUS Proxy dla zewnętrznego serwera RADIUS

- 6.3.23. System wspiera protokół Windows Active Directory, w tym następujące repozytoria AD:

- 6.3.23.1. Microsoft Windows Active Directory 2003 32bit
- 6.3.23.2. Microsoft Windows Active Directory 2003 R2 32bit I 64bit
- 6.3.23.3. Microsoft Windows Active Directory 2008 32bit I 64bit
- 6.3.23.4. Microsoft Windows Active Directory 2008 R2 64bit
- 6.3.23.5. Microsoft Windows Active Directory 2012
- 6.3.23.6. Microsoft Windows Active Directory 2012 R2
- 6.3.23.7. Microsoft Windows Active Directory 2016
- 6.3.23.8. Microsoft Windows Active Directory 2019

- 6.3.24. System wspiera protokół Lightweight Directory Access Protocol (LDAP)

- 6.3.25. System wspiera protokół Security Assertion Markup Language (SAML) 2.0 oraz funkcjonalność Single Sign-On (SSO)

- 6.3.26. System wspiera integrację z Azure Active Directory z użyciem technologii OAuth ROPC w celu uwierzytelnienia klientów 802.1x

- 6.3.27. System wspiera serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865

- 6.3.28. System wspiera następujące protokoły uwierzytelniania:

- 6.3.28.1. PAP/ASCII
- 6.3.28.2. CHAP
- 6.3.28.3. MS-CHAPv1
- 6.3.28.4. MS-CHAPv2

- 6.3.28.5. EAP-MD5
- 6.3.28.6. LEAP
- 6.3.28.7. EAP-TLS
- 6.3.28.8. EAP-TTLS
- 6.3.28.9. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi (EAP-MS-CHAPv2, EAP-GTC, EAP-TLS)
- 6.3.28.10. Tunnel Extensible Authentication Protocol (TEAP) z metodami wewnętrznymi (EAP-MS-CHAPv2, EAP-TLS)
- 6.3.29. System umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect
- 6.3.30. System wspiera implementację 802.1X z przynajmniej następującymi suplikantami:
  - 6.3.30.1. wbudowanym klientem 802.1X dla Windows 11
  - 6.3.30.2. wbudowanym klientem 802.1X dla Windows 10
  - 6.3.30.3. wbudowanym klientem 802.1X dla Windows 7
  - 6.3.30.4. wbudowanym klientem 802.1X dla Windows 8 i 8.1
  - 6.3.30.5. Apple Mac OS X Supplicant
  - 6.3.30.6. Google Android Supplicant
- 6.3.31. System umożliwia tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based)
- 6.3.32. System umożliwia uwierzytelnianie 802.1X maszyn i użytkowników
- 6.3.33. System umożliwia tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły
- 6.3.34. System posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)
- 6.3.35. System posiada lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC.
- 6.3.36. System wspiera uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC
- 6.3.37. System wspiera zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:
  - 6.3.37.1. tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port
  - 6.3.37.2. tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia
  - 6.3.37.3. tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden w host w domenie danych (Data VLAN) na jednym porcie fizycznym
  - 6.3.37.4. tryb uwierzytelniania 802.1X pozwalający wiele hostów na jednym porcie fizycznym
  - 6.3.37.5. mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny
  - 6.3.37.6. mechanizm umożliwiający poprawną obsługę sytuacji, w której nowy host podłącza się do portu, na którym uprzednio było uwierzytelnione urządzenie w tym w VLANie głosowym.

- 6.3.37.7. mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA.
- 6.3.37.8. mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X
- 6.3.37.9. mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X
- 6.3.37.10. obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki
- 6.3.37.11. mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych
- 6.3.37.12. mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny
- 6.3.37.13. przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
- 6.3.37.14. uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego się w VLANie głosowym
- 6.3.37.15. współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN
- 6.3.37.16. możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web
- 6.3.37.17. możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika
- 6.3.38. System wspiera uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X)
- 6.3.39. System wspiera urządzenia sieciowe umożliwiające uwierzytelnianie za pomocą protokołu RADIUS (NAD - Network Access Device) - przełączniki Ethernet, kontrolery sieci bezprzewodowej, koncentratory VPN

#### **Realizacja dostępu gościnnego**

- 6.3.40. System umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla:
  - 6.3.40.1. Microsoft Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7,
  - 6.3.40.2. Apple Mac OS X 10.x oraz 11.x
  - 6.3.40.3. Apple iOS 11.x, 12.x, 13.x i nowszych
  - 6.3.40.4. Google Android dla wersji 7.x i nowszych
  - 6.3.40.5. Linux
- 6.3.41. System umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor)
- 6.3.42. System zapewnia uwierzytelnienie sponsora, które musi odbywać się w oparciu o:
  - 6.3.42.1. wewnętrzną bazę użytkowników
  - 6.3.42.2. zewnętrzne repozytorium użytkowników

- 6.3.43. System umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do:
- 6.3.43.1. logowania się do systemu
  - 6.3.43.2. tworzenia pojedynczego konta gościnnego
  - 6.3.43.3. tworzenia wielu kont gościnnych
  - 6.3.43.4. importowania kont gościnnych z pliku CSV
  - 6.3.43.5. wysyłania wiadomości email po utworzeniu konta gościnnego
  - 6.3.43.6. wysyłania wiadomości SMS po utworzeniu konta gościnnego
  - 6.3.43.7. wyświetlenia hasła konta gościnnego
  - 6.3.43.8. wydrukowania danych konta gościnnego
  - 6.3.43.9. wyświetlenia danych stworzonych kont gościnnych
  - 6.3.43.10. zawieszenia (suspend) i reinicjacji kont gościnnych
- 6.3.44. System umożliwia personalizację wyglądu portalu sponsora i gościa, w tym:
- 6.3.44.1. zmianę logo strony logowania
  - 6.3.44.2. zmianę obrazu tła strony logowania
  - 6.3.44.3. zmianę logo banneru
  - 6.3.44.4. zmianę obrazu tła banneru
  - 6.3.44.5. zmianę koloru tła strony z treścią
- 6.3.45. System umożliwia zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS
- 6.3.46. System umożliwia zmianę adresu URL i FQDN strony sponsora
- 6.3.47. System umożliwia automatyczne kasowanie wygaśniętych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. System umożliwia wyświetlenie czasu ostatniego kasowania wygaśniętych kont gościnnych i następnego kasowania wygaśniętych kont gościnnych
- 6.3.48. System posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim,
- 6.3.49. System umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.
- 6.3.50. System umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:
- 6.3.50.1. Imienia
  - 6.3.50.2. Nazwiska
  - 6.3.50.3. Firmy
  - 6.3.50.4. adresu e-mail
  - 6.3.50.5. numeru telefonu
  - 6.3.50.6. danych opcjonalnych (nie mniej niż 5 dodatkowych pól)
- 6.3.51. System umożliwia konfigurację dla użytkowników gościnnych:
- 6.3.51.1. wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)
  - 6.3.51.2. zezwolenia gościom na zmianę hasła oraz odzyskiwanie zapomnianego hasła,
  - 6.3.51.3. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora
- 6.3.52. System umożliwia honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
- 6.3.53. System umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.



- 6.3.54. System umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje co najmniej 5 urządzeń per konto gościnne.
- 6.3.55. System umożliwia konfigurację czasu ważności hasła w dniach w przedziale zadany w dniach.
- 6.3.56. System umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny
- 6.3.57. System umożliwia konfigurację polityki złożoności haseł użytkowników gościnnych
- 6.3.58. System umożliwia konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika
- 6.3.59. System umożliwia tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.
- 6.3.60. System umożliwia przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.
- 6.3.61. System umożliwia udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP, secure SMTP i poprzez SMS,
- 6.3.62. System umożliwia wykorzystanie protokołu SAML 2.0 oraz funkcjonalności SSO dla portali gościnnych oraz sponsora.
- 6.3.63. System wspiera API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

#### **Profilowanie urządzeń**

- 6.3.64. System umożliwia dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
- 6.3.65. System umożliwia wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności zapewnia możliwość stworzenia polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc.
- 6.3.66. System umożliwia dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:
  - 6.3.66.1. DHCP
  - 6.3.66.2. DHCP SPAN
  - 6.3.66.3. HTTP
  - 6.3.66.4. RADIUS
  - 6.3.66.5. DNS
  - 6.3.66.6. SNMP
  - 6.3.66.7. Network Scan (NMAP lub inne narzędzie profilowania aktywnego)
- 6.3.67. System umożliwia wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.
- 6.3.68. System umożliwia dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
- 6.3.69. System posiada dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:
  - 6.3.69.1. Stacji roboczych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun,
  - 6.3.69.2. Urządzeń mobilnych: Android, Apple, Blackberry
  - 6.3.69.3. Telefonów IP

- 6.3.69.4. Drukarek sieciowych
  - 6.3.69.5. Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych
  - 6.3.69.6. Routerów
  - 6.3.69.7. Punktów dostępu bezprzewodowego
  - 6.3.70. System umożliwia subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:
    - 6.3.70.1. reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci
    - 6.3.70.2. reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie <http://standards.ieee.org/develop/regauth/oui/oui.txt>
  - 6.3.71. System umożliwia włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie.
  - 6.3.72. System wspiera raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.
- Wymiana informacji kontekstowych oraz automatyzacji odpowiedzi**
- 6.3.73. System umożliwia wymianę informacji kontekstowych dotyczących sesji użytkowników oraz urządzeń. Wymiana ta może występować w obu kierunkach – system NAC może zarówno udostępniać informacje jak i przyjmować je z zewnętrznych systemów producenta oraz firm trzecich.
  - 6.3.74. Wymiana informacji realizowana jest z użyciem dedykowanej szyny wymiany informacji w architekturze Consumer-Provider, opartej o technologie REST oraz Websocket. System NAC pełni rolę serwera wymiany informacji.
  - 6.3.75. Wymiana informacji może zostać skonfigurowana z systemów klasy enterprise, m.in.: next-generation firewall, network detection and response (NDR)/flow monitoring, Security Information Event Management (SIEM), IoT Security, DNS, DHCP and IP (DDI) management, skanowania/zarządzania podatnościami.
  - 6.3.76. System umożliwia zmianę autoryzacji stacji w oparciu o dyspozycje otrzymane poprzez szynę wymiany informacji. Zmiana autoryzacji może spowodować m.in. przeniesienie stacji do VLANu kwarantanny o ograniczonym dostępie do sieci lub dezaktywację portu, do którego podłączona jest stacja w celu odcięcia jej dostępu do sieci.

#### **Raportowanie**

- 6.3.77. System umożliwia generowanie m.in. następujących raportów:
  - 6.3.77.1. raportów dla protokołów AAA:
  - 6.3.77.2. diagnostyki protokołów AAA
  - 6.3.77.3. trendów uwierzytelnienia 802.1X
  - 6.3.77.4. accountingu RADIUS
  - 6.3.77.5. uwierzytelniania RADIUS
  - 6.3.77.6. raportów dozwolonych protokołów
  - 6.3.77.7. sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym: uwierzytelnień pomyślnych, uwierzytelnień nieudanych, N największych ilości uwierzytelnień Radius per protokół EAP(Top5), w tym u. pomyślnych i u.

nieudanych

- 6.3.77.8. raportów dla poszczególnych instancji serwerów systemu, w tym: uwierzytelnień RADIUS per serwer, Top „N” uwierzytelnień per serwer, monitorowania Online Certificate Status Protocol (OCSP), administratorów systemu i ich uprawnień, logowania administratorów do systemu, zmian konfiguracji serwera dokonanych przez administratorów, stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS), zmian operacyjnych serwera dokonanych przez administratorów, zmian haseł przez użytkowników
- 6.3.77.9. raportów dla stacji końcowych, w tym: uwierzytelnień typu MAC Authentication, Top „N” uwierzytelnień per adres MAC stacji, Top „N” uwierzytelnień per maszyna, Top „N” uwierzytelnień per RADIUS Calling Station ID, działań podsystemu profilera per adres MAC, czasu wymaganego na sprofilowanie stacji per adres MAC
- 6.3.77.10. raportów dla błędów, w tym: błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił, sumarycznych przyczyn nieudanych uwierzytelnień, Top „N” uwierzytelnień per rodzaj błędu
- 6.3.77.11. raportów dla urządzeń sieciowych: sumarycznych uwierzytelnień dla urządzeń sieciowych, Top „N” uwierzytelnień per urządzenie sieciowe, niedostępności serwera AAA dla urządzenia sieciowego, wiadomości logowanych przez urządzenia sieciowe, stanu portów i sesji urządzenia sieciowego widocznych przez SNMP
- 6.3.77.12. raportów użytkowników: sumarycznych uwierzytelnień użytkowników, Top „N” uwierzytelnień per użytkownik, sesji użytkowników gościnnych, aktywności użytkowników gościnnych, sumarycznych uwierzytelnień sponsorów dostępu gościnnego, uwierzytelnień per unikalny użytkownik
- 6.3.78. raportów katalogu sesji: aktywnych sesji RADIUS, historii sesji RADIUS, zaterminowanych sesji RADIUS

#### **Alarmy i diagnostyka**

- 6.3.79. System umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: wiadomości e-mail, syslog
- 6.3.80. Alarmy mogą być generowane w następujących sytuacjach:
  - 6.3.80.1. ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
  - 6.3.80.2. opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego
  - 6.3.80.3. status krytycznych procesów będzie niepożądany, w tym status: procesu wewnętrznej bazy danych systemu, serwera aplikacyjnego systemu, bazy danych sesji, kolektora i procesora wiadomości log, błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej), stan obciążenia systemu wzrośnie powyżej zadanego poziomu (obciążenia systemu, zajętości pamięci)
- 6.3.81. System posiada zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
  - 6.3.81.1. badanie łączności IP za pomocą ping, nslookup, traceroute

- 6.3.81.2. wyszukiwanie zdarzeń RADIUS z uwzględnieniem: nazwy użytkownika, adresu MAC, statusu uwierzytelnienia (udana lub nieudana), powodu, jeżeli uwierzytelnienie nieudane, zakresu czasowego, co do dnia, godziny i minuty
- 6.3.81.3. wykonanie zdalnego polecenia na urządzeniu sieciowym
- 6.3.81.4. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem: definicji serwerów AAA, protokołu RADIUS, odkrywania urządzeń, logowania, uwierzytelniania Web, konfiguracji trybu 802.1X
- 6.3.81.5. wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

#### **Wsparcie dla protokołu IPv6**

- 6.3.82. System posiada wsparcie dla SSH IPv6
- 6.3.83. System pozwala na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacji IPv6
- 6.3.84. System pozwala na konfigurację NTP IPv6
- 6.3.85. System umożliwia stworzenie reguł ograniczających dostęp administracyjny do linii poleceń lub interfejsu graficznego w oparciu o adres IPv6
- 6.3.86. System umożliwia konfigurację serwerów SNMP w oparciu o adresację IPv6
- 6.3.87. System umożliwia wysyłanie SNMP Trap do serwera SNMP IPv6
- 6.3.88. System umożliwia integrację z Active Directory w oparciu o IPv6
- 6.3.89. System umożliwia połączenie z serwerem Radius z wykorzystaniem adresu IPv6

## **7. Termin realizacji przedmiotu zamówienia**

- 7.1. Maksymalny czas dostawy Rozwiązania WIFI, o której mowa w pkt 4 – 60 dni roboczych od dnia zawarcia umowy, w tym:
  - 7.1.1. Przygotowanie oraz przekazanie Zamawiającemu planu i harmonogramu wdrożenia Rozwiązania WIFI - maksymalnie 20 dni roboczych od podpisania umowy
  - 7.1.2. Dostawa urządzeń i Oprogramowania do Lokalizacji - maksymalnie 30 dni roboczych od podpisania umowy.
  - 7.1.3. Montaż i konfiguracja Rozwiązania WiFi w Lokalizacji - maksymalnie 60 dni roboczych od podpisania umowy
  - 7.1.4. Przygotowanie oraz przekazanie Zamawiającemu Dokumentacji powykonawczej oraz Dokumentacji użytkowej - maksymalnie 60 dni roboczych od podpisania umowy.
- 7.2. Potwierdzeniem odbioru / dostawy zamówienia w Lokalizacji będzie podpisany Protokół odbioru Ilościowego.
- 7.3. Po wdrożeniu Rozwiązania WiFi zostanie podpisany Protokół Końcowy potwierdzający pełne wdrożenie Rozwiązania WiFi.
- 7.4. W ramach realizacji Umowy Wykonawca przeprowadzi minimum 3-dniowe szkolenia certyfikowane przez producenta Rozwiązania WIFI dla 4 administratorów z konfiguracji oraz obsługi Rozwiązania w terminie 40 dni od dnia podpisania Protokołu odbioru Szkolenia.
- 7.5. Objęcie Rozwiązania WIFI usługą wsparcia technicznego przez okres 36 miesięcy w zakresie określonym w pkt. 9 OPZ, od dnia podpisania Protokołu Odbioru Końcowego.

## 8. Warunki świadczenia wsparcia technicznego i gwarancji

- 8.1. Oprogramowanie i urządzenia zostaną objęte 36 - miesięcznym Wsparciem technicznym od dnia odbioru wskazanego w podpisanym przez obie Strony bez zastrzeżeń Protokole odbioru końcowego (po odbiorze realizacji zamówienia w ostatniej z trzech Lokalizacji), świadczonym przez producenta, które może być realizowany również przez autoryzowanego partnera producenta, posiadającego status partnerstwa nie niższym niż wskazany w pkt. 5.15, na poniższych zasadach.
- 8.2. W razie Awarii, Zamawiający będzie dokonywał Zgłoszeń za pośrednictwem jednego z kanałów:
  - a) e-maila;
  - b) platformy zgłoszeniowej.
- 8.3. Za chwilę dokonania zgłoszenia Awarii Strony uznają datę i godzinę jego zgłoszenia przez Zamawiającego, przez jeden z kanałów, o których mowa powyżej. W przypadku Zgłoszenia przez więcej niż jeden kanał, chwilą dokonania Zgłoszenia będzie najwcześniejsza data i godzina.
- 8.4. Wykonawca zobowiązuje się podać Zamawiającemu, najpóźniej w dniu podpisania Protokołu odbioru końcowego, a także później przy każdej zmianie tych danych, wszelkie dane niezbędne do skorzystania przez Zamawiającego ze Wsparcia Technicznego, a także dane dostępne do konta w serwisie producenta, umożliwiające samodzielne pobieranie oprogramowania w ramach posiadanej licencji.
- 8.5. Wsparcie Techniczne będzie świadczone każdorazowo w miejscu instalacji Urządzeń.
- 8.6. Wykonawca zobowiązuje się do:
  - a) przyjmowania Zgłoszeń – od 7:00 do 18:00 w Dni Robocze;
  - b) usunięcia Awarii zwykłej – **maksymalnie w następnym Dniu Roboczym** następującym po dokonaniu Zgłoszenia;
  - c) usunięcie Awarii Krytycznej – maksymalnie w ciągu 4 godzin od Zgłoszenia.
- 8.7. W przypadku braku możliwości usunięcia Awarii poprzez naprawę Urządzenia w miejscu Urządzenia, które nie może być przez Wykonawcę naprawione, Wykonawca zobowiązany jest do dostarczenia Zamawiającemu innego urządzenia, wolnego od wad, o parametrach technicznych nie gorszych od parametrów technicznych Urządzenia uszkodzonego oraz zapewniającego nie gorszy poziom bezpieczeństwa, a następnie świadczenia gwarancji i wsparcia technicznego w stosunku do tego urządzenia przez okres obowiązywania umowy.
- 8.8. Wykonawca w ramach Wsparcia Technicznego zapewnia w szczególności, lecz nie wyłącznie:
  - 9.9.1. Bieżące zarządzanie Zgłoszeniami.
  - 9.9.2. Wsparcie techniczne świadczone przez serwis producenta lub przez autoryzowanego partnera producenta – przez osoby dysponujące odpowiednimi uprawnieniami i kwalifikacjami, potwierdzonymi certyfikatami wystawionymi przez producenta, które Wykonawca okaże na każde wezwanie Zamawiającego.
  - 9.9.3. Dostęp w zakresie uaktualnień, poprawek, nowych wersji fabrycznie zainstalowanego Oprogramowania, w tym oprogramowania zainstalowanego w Urządzeniach (firmware), a także możliwość zgłoszenia zauważanych w nich błędów, tj. każdego zdarzenia w funkcjonowaniu Oprogramowania niezgodnego z dokumentacją Oprogramowania, uniemożliwiającego używanie Oprogramowania w sposób zgodny z jego przeznaczeniem.
  - 9.9.4. Autoryzowaną przez producenta naprawę lub wymianę uszkodzonego Urządzenia na Urządzenie lub części nowe i oryginalne.
  - 9.9.5. Wykonawca zobowiązuje się do informowania Zamawiającego o pojawieniu się uaktualnień,

poprawek, nowych wersji fabrycznie zainstalowanego Oprogramowania, w tym oprogramowania zainstalowanego w Urządzeniach (firmware), w terminie do 10 Dni Roboczych od dnia ich publikacji.

- 9.9.6. Wykonawca zobowiązany jest do usuwania Awarii przez wykonanie wszelkich niezbędnych czynności zmierzających do usunięcia Awarii, w sposób adekwatny do danej Awarii.
- 9.9.7. Usunięcie Awarii potwierdzone zostanie Protokołem usunięcia Awarii.
- 9.9.8. Diagnostyka i naprawa dysków twardych oraz nośników danych, które mogą przechowywać dane Zamawiającego (np. pamięci flash, dyski SSD, moduły pamięci cache) będą realizowane w miejscu ich używania, bez diagnostyki, poza tym miejscem. Uszkodzone nośniki danych (np. pamięci flash, dyski SSD, moduły pamięci cache) pozostaną u Zamawiającego.
- 9.9.9. Wykonawca dostarczy Zamawiającemu dokument potwierdzający wykupienie o producenta na rzecz Zamawiającego usługi Wsparcia Technicznego.
- 9.9.10. Wsparcie Techniczne będzie świadczone w języku polskim.
- 9.9.11. Dostarczone Urządzenia muszą być fabrycznie nowe oraz pochodzić z oficjalnego kanału sprzedaży.
- 9.9.12. Wykonawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części wymiennych i koszty transportu.
- 9.9.13. Realizacja uprawnień Zamawiającego wynikających z Gwarancji producenta będzie odbywała się za pośrednictwem Wykonawcy.

## **9. Realizacja szkoleń**

- 9.1. Wykonawca zobowiązany jest do przeprowadzenia minimum 3-dniowe szkolenie certyfikowanego przez producenta Rozwiązania WIFI dla 4 administratorów z konfiguracji oraz obsługi Rozwiązania w terminie 40 dni od dnia podpisania Protokołu odbioru końcowego.
- 9.2. Wykonawca zobowiązany jest do wyznaczenia co najmniej dwóch terminów szkolenia z co najmniej 2 tygodniowym wyprzedzeniem. Szkolenie musi być zrealizowane zdalnie w formie warsztatów, na środowisku dostarczonym przez Wykonawcę. Szkolenie uznaje się za przeprowadzone prawidłowo z chwilą podpisania przez Zamawiającego Protokołu odbioru szkolenia bez zastrzeżeń.

## **10. Pozostałe warunki realizacji zamówienia zostały opisane w Projektowanych Postanowieniach Umowy, które zawarte są w Rozdziale III SWZ.**