Załącznik nr 1 do Formularza ofertowego

**WYKAZ OFEROWANYCH PARAMETRÓW/FUNKCJONALNOŚCI ZGODNIE Z OPISEM PRZEDMIOTU ZAMÓWIENIA**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp. z OPZ** | | **Opis wymagania z OPZ** | **Oświadczenie Wykonawcy:**  **Spełnia/Nie spełnia** | **Opis oferowanych parametrów  lub sposobu spełnienia wymagania** | **Wskazanie nazwy dokumentacji urządzenia/oprogramowania np. zrzut konfiguracji, karta katalogowa, specyfikacja techniczna, dokumentacja licencyjna, inna dokumentacja urządzenia/oprogramowania lub oświadczenie producenta urządzenia/oprogramowania oraz miejsca, w którym znajduje się potwierdzenie spełnienie danego wymagania (numer strony dokumentu) lub adresu strony WWW pod którym dokument jest opublikowany, a także publicznie i powszechnie dostępny bez konieczności logowania.**  **W przypadku jeśli wskazanie opisanego wyżej dokumentu, strony WWW nie jest możliwe lub nie jest wystarczające, Wykonawca powinien opisać sposób spełnienia danego wymagania dołączając równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane dostawy spełniają określone przez zamawiającego wymagania, cechy lub kryteria.** |
| **Producent:**  **Model:** | | | | | |
| 1.1. | | **Punkt dostępowy sieci bezprzewodowej WiFi6E posiadający:** | | | |
| 1.1.1. | | Obsługę standardów 802.11a/b/g/n/ac/ax | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.1. | | Obsługa OFDMA (uplink/downlink), TWT, BSS Coloring | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.2. | | Obsługa MU-MIMO (uplink/downlink) – min. 4x4:4 (5GHz oraz 6GHz) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.3. | | Obsługa MU-MIMO (uplink/downlink) – min. 2x2:2 (2,4GHz) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.4. | | Obsługa kanałów 20, 40, 80 MHz dla 802.11ac | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.5. | | Obsługa kanałów 20, 40, 80, 160 MHz dla 6GHz oraz 20, 40, 80 MHz dla 5GHz dla 802.11ax | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.6. | | Obsługa prędkości PHY do 1,7 Gbps (ac) (przy parametrach: 4x4, 80 MHz, 5GHz) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.7. | | Obsługa prędkośći PHY do 7,4 Gbps (ax) (przy parametrach: 4x4 160 MHz 6GHz oraz 4x4 80 MHz 5GHz oraz 2x2 20 MHz 2,4GHz) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.8. | | Obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.9. | | Obsługa beamforming dla klientów 802.11ac/ax | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.1.10. | | Obsługa MRC (Maximal Ratio Combining) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.2. | | Konfigurowalną moc nadajnika | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.2.1. | | Dla zakresu 2.4GHz: do 100 mW | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.2.2. | | Dla zakresu 5GHz: do 200 mW | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.2.3. | | Dla zakresu 6GHz: do 200 mW | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.3. | | Możliwość pracy trójzakresowej w pasmach: 2,4GHz oraz 5GHz oraz 6GHz | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4. | | Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami: | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.1. | | Automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.2. | | Optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.3. | | Obsługa min. 16 BSSID | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.4. | | Definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.5. | | Uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.6. | | 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) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.7. | | Możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.8. | | Obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.9. | | Jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.10. | | Obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.11. | | Obsługa IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.12. | | Obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.13. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.14. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.15. | | Wsparcie IEEE 802.11i, WPA2, WPA3, WPA3-OWE (Enhanced Open) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.16. | | Wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.17. | | Obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.4.18. | | Obsługa blokowania ruchu Peer-to-Peer | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.5. | | Analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.6. | | 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: | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.6.1. | | Wykrywanie sygnatur DoS: Auth/Deauth Flood, Assoc/Disassoc Flood, CTS/RTS Flood, Broadcast Deauth/Dissassoc Flood, Broadcast Probe Flood, EAPOL Logoff Flood | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.6.2. | | Wykrywanie ataków: EAPOL-Logoff, RTS/CTS Virtual Carrier Sense | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.7. | | Obsługa (przy współpracy z kontrolerem) polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.8. | | Uruchamianie aplikacji w kontenerach bezpośrednio na AP | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.9. | | Obsługa VXLAN | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.10. | | Moduł radiowy pełniący funkcję analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz, 5GHz, 6GHz): | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.10.1. | | Zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.10.2. | | Automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.10.3. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.11. | | Musi posiadać interfejsy minimum: | | | |
| 1.1.11.1. | | Interfejs MultiGigabit Ethernet (100/1000/2500) | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.11.2. | | Interfejs konsolowy | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.11.3. | | Port USB 2.0 | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.12. | | Musi mieć wbudowaną pamięć o minimalnych parametrach 2 GB RAM, 1 GB Flash | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.13. | | Zróżnicowane możliwości zasilania: | | | |
| 1.1.13.1. | | Przy zasilaniu przez 802.3bt: pełna funkcjonalność AP | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.13.2. | | Przy zasilaniu przez 802.3at: praca z wyłączonym portem USB | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.13.3. | | Przy zasilaniu przez 802.3af: możliwość uruchomienia AP w celach diagnostycznych bez pracujących modułów radiowych | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.14. | | Musi posiadać anteny zintegrowane o zysku: | | | |
| 1.1.14.1. | | Min. 3 dBi dla pasma 2,4GHz | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.14.2. | | Min. 5 dBi dla pasma 5GHz | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.14.3. | | Min. 4 dBi dla pasma 6GHz | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.15. | | Musi posiadać obudowę przystosowaną do pracy w zakresie temperatur 0 – 50oC | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.16. | | Musi posiadać certyfikację WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi6, Wi-Fi Enhanced Open, WMM, WMM-PS | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.17. | | Musi posiadać wbudowane radio Bluetooth Low Energy (BLE) 5.1 | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.18. | | Musi być przeznaczony do montażu wewnątrz budynków | **Spełnia**  **Nie spełnia** |  |  |
| 1.1.19. | | Musi być wyposażony w elementy umożliwiające zamontowanie go na suficie technicznym jak i nad nim. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2. | | **Kontroler sieci bezprzewodowej do zarządzania Punktami Dostępowymi zaproponowanymi dla punktu 1.1** | | | |
| 1.2.1. | | Urządzenie umożliwiające centralne zarządzanie co najmniej 250 punktami dostępowymi wraz z wymaganymi licencjami, z możliwością rozbudowy do 500 punktów. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.2. | | Kontroler musi być wyposażony w: | | | |
| 1.2.2.1. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.2.2. | | Port serwisowy do obsługi out-of-band management; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.2.3. | | Port konsolowy RS 232; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.2.4. | | Port USB 3.0. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.2.5. | | Dedykowany interface do połączenia dwóch kontrolerów w redundantną parę | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.3. | | Obsługa łączenia interfejsów w grupę logiczną, by zabezpieczyć przed awarią pojedynczego interfejsu; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.4. | | Obsługa ruchu tunelowanego o przepustowości 10Gbps | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.5. | | Obsługa 5000 klientów sieci bezprzewodowej z możliwością rozbudowy do 10 000; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.6. | | Musi poprawnie współpracować z punktami dostępowymi dostarczonymi w ramach zamówienia. W szczególności zestaw punktów dostępowych i kontroler muszą udostępniać pełną wymaganą funkcjonalność. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.7. | | Kontroler wraz ze współpracującymi Access Pointami musi umożliwiać obsługę urządzeń końcowych IPv4 i IPv6. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.8. | | Obsługa NTP (IPv4 i IPv6) | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.9. | | W przypadku awarii kontrolera Access Pointy muszą posiadać możliwość automatycznego przełączenie się na kontroler zapasowy lub na inne kontrolery z wolną liczbą licencji na AP. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.10. | | Kontroler musi umożliwiać zarządzanie przez HTTPS, SNMPv2, SSH, NETCONF oraz przez port konsoli szeregowej | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.11. | | Obsługa logowania SYSLOG, wsparcie dla IPSec w celu zabezpieczenie SYSLOG | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.12. | | Obsługa Hotspot 2.0 | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.13. | | Obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020) |  |  |  |
| 1.2.14. | | Współpraca z siecią dostępową typu SDN opartą o Network Fabric, wymiana informacji kontrolnych za pomocą protokołu LISP (Locator ID Separation Protocol) | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.15. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.16. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.17. | | Możliwość przechwycenia i wysłania materiału dowodowego wywołującego alarm IDS/IPS (packet capture) do dedykowanego systemu zarządzania | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.18. | | Logowanie alarmów IDS/IPS za pomocą SYSLOG | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.19. | | Urządzenie musi umożliwiać centralną kontrolę punktów dostępu bezprzewodowego zgodnie z protokołem CAPWAP (RFC 5415): | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.19.1. | | Zarządzanie politykami bezpieczeństwa; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.19.2. | | Wykrywanie zagrożeń w sieci bezprzewodowej; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.19.3. | | Zarządzanie pasmem radiowym; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.19.4. | | Zarządzanie mobilnością; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.19.5. | | Zarządzanie jakością transmisji. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.20. | | Kontroler musi umożliwiać obsługę co najmniej: | | | |
| 1.2.20.1. | | 4096 Vlan; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.20.2. | | 4096 Wlan. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21. | | Zarządzanie pasmem radiowym punktów dostępowych: | | | |
| 1.2.21.1. | | Automatyczna adaptacja do zmian w czasie rzeczywistym; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21.2. | | Optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia); | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21.3. | | Dynamiczne przydzielanie kanałów radiowych; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21.4. | | Wykrywanie, eliminacja i unikanie interferencji; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21.5. | | Równoważenie obciążenia punktów dostępowych; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21.6. | | Tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21.7. | | Automatyczna dystrybucja klientów pomiędzy punkty dostępowe. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21.8. | | Mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.21.9. | | Dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.22. | | Mapowanie SSID do segmentów VLAN w sieci przewodowej: | | | |
| 1.2.22.1. | | 1:1 | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.22.2. | | 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty) | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.22.3. | | Możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID) | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23. | | Kontroler musi wspomagać następujące mechanizmy bezpieczeństwa: | | | |
| 1.2.23.1. | | 802.11i, WPA3, WPA2, WPA, WEP; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.2. | | 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST); | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.3. | | Obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników (min. 12.000 wpisów). | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.4. | | Kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.5. | | Obsługa profilowania użytkowników:  - Przydział sieci VLAN;  - Przydział list kontroli dostępu (ACL). | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.6. | | Uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 (wykrywanie podszywania się punktów dostępowych użytkowników pod adresy infrastruktury) – IEEE 802.11w; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.7. | | Uwierzytelnianie punktów dostępowych w oparciu o certyfikaty; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.8. | | Obsługa list kontroli dostępu (ACL); | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.9. | | Obsługa list kontroli dostępu opartych o nazwy domenowe; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.10. | | Obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.11. | | Wykrywanie i dezaktywacja obcych punktów dostępowych; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.12. | | Możliwość budowania reguł klasyfikacji obcych punktów dostępowych w oparciu o nazwę SSID, wybrany ciąg znaków w SSID, siłę sygnału RSSI, minimalną ilość podłączonych urządzeń; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.13. | | 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 ; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.14. | | Ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.23.15. | | DHCP proxy, wsparcie dla DHCP Option 82. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.24. | | Obsługa mobilności (roaming-u) użytkowników (L2 i L3 – IPv4 i IPv6, w ramach i pomiędzy kontrolerami). | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.25. | | Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.26. | | Wsparcie dla IEEE 802.11u. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.27. | | Obsługa mechanizmów QoS: | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.27.1. | | 802.1p; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.27.2. | | WMM, TSpec, U-APSD; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.27.3. | | Ograniczanie pasma per użytkownik; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.27.4. | | Call Admission Control – ze statyczną definicją pasma i dynamiczną w oparciu o analizę profili ruchu, SIP CAC, Call snooping; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.27.5. | | Równomierna obsługa klientów sieci bezprzewodowej w oparciu o utylizację czasu antenowego; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.27.6. | | Kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.27.7. | | Zbiór wbudowanych profili do automatycznej konfiguracji ustawień QoS. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.28. | | Obsługa protokołu Bonjour poprzez wbudowany multicast DNS (mDNS) Gateway zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.29. | | Obsługa dostępu gościnnego (IPv4 i IPv6): | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.29.1. | | Przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony); | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.29.2. | | Obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.29.3. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.30. | | Obsługa ruchu unicast IPv4 oraz IPv6; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.31. | | Zgodność z funkcjonalnościami IPv6 pod kątem RFC: 4191, 6980, 8200, 8201. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.32. | | Obsługa ruchu multicast IPv4 oraz IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.32.1. | | IGMP/MLD snooping | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.32.2. | | Optymalizacja dystrybucji ruchu multicast w sieci przewodowej(między kontrolerem a AP) | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.32.3. | | Obsługa konwersji ruchu multicast na unicast | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.33. | | Współpraca z Oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.34. | | Obsługa redundancji 1:1 (active/standby) zapewniającej: | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.34.1. | | Utrzymanie sesji punktów dostępowych oraz urządzeń klienckich na wypadek awarii aktywnego kontrolera; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.34.2. | | Synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej. | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.35. | | Obsługa redundancji rozwiązania (N+1) | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.36. | | 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; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.37. | | Zbieranie i eksport statystyk ruchowych za pomocą protokołu Netflow/JFlow lub odpowiednika; | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.38. | | Eksport dodatkowych pól w ramkach statystyk Netflow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa). | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.39. | | 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). | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.40. | | Możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania (dni tygodnia, godziny) | **Spełnia**  **Nie spełnia** |  |  |
| 1.2.41. | | Obsługa EoGRE w celu tunelowania ruchu z kontrolera do dedykowanego koncentratora (np. na routerze) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3. | | **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. | | | |
| 1.3.1. | | System musi być dostarczony w postaci dwóch urządzeń wraz z odpowiednimi licencjami umożliwiającymi wykorzystanie wszystkich opisanych poniżej funkcjonalności dla co najmniej 10000 sesji. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.2. | | System umożliwia instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.3. | | System umożliwia elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.4. | | System umożliwia wysoką skalowalność i rozbudowę w miarę wzrostu liczby urządzeń | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.5. | | W scenariuszu, w którym wszystkie komponenty systemu znajdują się na pojedynczym serwerze jest on w stanie obsłużyć minimalnie 10 000 jednoczesnych sesji | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.6. | | System umożliwia realizację wysokiej dostępności elementów funkcjonalnych, w tym: | | | |
| 1.3.6.1. | | Zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.6.2. | | Zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.7. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.8. | | System umożliwia zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.9. | | System umożliwia tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.10. | | System umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.11. | | System umożliwia uwierzytelnianie administratorów za pomocą zewnętrznych repozytoriów - m.in. Active Directory, Radius i SAML 2.0 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.12. | | 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 określoną ilość dni | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.13. | | System umożliwia kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora: | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.13.1. | | Dostęp do interfejsu konfiguracji usług tożsamości 802.1X | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.13.2. | | Dostęp do interfejsu konfiguracji urządzeń sieciowych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.13.3. | | Dostęp do interfejsu konfiguracji polityk | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.13.4. | | Dostęp do interfejsu konfiguracji kontroli dostępu gościnnego | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.13.5. | | Dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.14. | | System umożliwia kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.15. | | System posiada możliwość podłączenia i identyfikacji urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.16. | | System wspiera REST API do masowych operacji CRUD (Create, Read, Update, Delete) m.in. na użytkownikach, stacjach końcowych oraz urządzeniach sieciowych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.17. | | System wspiera REST API do monitorowania w czasie rzeczywistym sesji oraz stacji końcowych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.18. | | System wspiera REST API do konfiguracji i zarządzania m.in. politykami Radius, kopiami zapasowymi oraz repozytoriami plików | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.19. | | System umożliwia rozbudowanie funkcjonalności o m.in. profilowanie urządzeń oraz weryfikację stanu stacji końcowej– z ang. posture assessment, bez konieczności rozbudowy sprzętowej | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.20. | | System umożliwia rozbudowanie funkcjonalności o serwer TACACS+/Radius do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej | **Spełnia**  **Nie spełnia** |  |  |
| **System wspiera następujące protokoły uwierzytelniania i standardy:** | | | | | |
| 1.3.21. | | RADIUS, zgodnie z dokumentami: | | | |
| 1.3.21.1. | | RFC 2138 — Remote Authentication Dial In User Service (RADIUS) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.21.2. | | RFC 2139 — RADIUS Accounting | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.21.3. | | RFC 2865 — Remote Authentication Dial In User Service (RADIUS) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.21.4. | | RFC 2866 — RADIUS Accounting | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.21.5. | | RFC 2867 — RADIUS Accounting for Tunnel Protocol Support | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.21.6. | | RFC 2868 — RADIUS Attributes for Tunnel Protocol Support | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.21.7. | | RFC 2869 — RADIUS Extensions | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.22. | | RADIUS Proxy dla zewnętrznego serwera RADIUS | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.23. | | System wspiera protokół Windows Active Directory, w tym następujące repozytoria AD: | | | |
| 1.3.23.1. | | Microsoft Windows Active Directory 2003 32bit | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.23.2. | | Microsoft Windows Active Directory 2003 R2 32bit I 64bit | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.23.3. | | Microsoft Windows Active Directory 2008 32bit I 64bit | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.23.4. | | Microsoft Windows Active Directory 2008 R264bit | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.23.5. | | Microsoft Windows Active Directory 2012 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.23.6. | | Microsoft Windows Active Directory 2012 R2 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.23.7. | | Microsoft Windows Active Directory 2016 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.23.8. | | Microsoft Windows Active Directory 2019 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.24. | | System wspiera protokół Lightweight Directory Access Protocol (LDAP) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.25. | | System wspiera protokół Security Assertion Markup Language (SAML) 2.0 oraz funkcjonalność Single Sign-On (SSO) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.26. | | System wspiera integrację z Azure Active Directory z użyciem technologii Oauth ROPC w celu uwierzytelnienia klientów 802.1x | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.27. | | System wspiera serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28. | | System wspiera następujące protokoły uwierzytelniania: | | | |
| 1.3.28.1. | | PAP/ASCII | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.2. | | CHAP | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.3. | | MS-CHAPv1 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.4. | | MS-CHAPv2 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.5. | | EAP-MD5 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.6. | | LEAP | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.7. | | EAP-TLS | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.8. | | EAP-TTLS | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.9. | | Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi (EAP-MS-CHAPv2, EAP-GTC, EAP-TLS) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.28.10. | | Tunnel Extensible Authentication Protocol (TEAP) z metodami wewnętrznymi (EAP-MS-CHAPv2, EAP-TLS) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.29. | | System umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.30. | | System wspiera implementację 802.1X z przynajmniej następującymi suplikantami: | | | |
| 1.3.30.1. | | wbudowanym klientem 802.1X dla Windows 11 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.30.2. | | wbudowanym klientem 802.1X dla Windows 10 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.30.3. | | wbudowanym klientem 802.1X dla Windows 7 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.30.4. | | wbudowanym klientem 802.1X dla Windows 8 i 8.1 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.30.5. | | Apple Mac OS X Supplicant | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.30.6. | | Google Android Supplicant | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.31. | | System umożliwia tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.32. | | System umożliwia uwierzytelnianie 802.1X maszyn i użytkowników | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.33. | | System umożliwia tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.34. | | System posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik  lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.35. | | System posiada lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.36. | | System wspiera uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37. | | System wspiera zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym: | | | |
| 1.3.37.1. | | tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.2. | | tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.3. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.4. | | tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.5. | | mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.6. | | mechanizm umożliwiający poprawną obsługę sytuacji, w której nowy host podłącza się do portu, na którym uprzednio było uwierzytelnione urządzenie w tym w VLANie głosowym. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.7. | | mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.8. | | mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.9. | | mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.10. | | obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.11. | | mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.12. | | mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.13. | | przypisanie przez serwer AAA dla użytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.14. | | uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego sie w VLANie głosowym | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.15. | | współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.16. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.37.17. | | możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.38. | | 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) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.39. | | System wspiera urządzenia sieciowe umożliwiające uwierzytelnianie za pomocą protokołu RADIUS (NAD - Network Access Device)- przełączniki Ethernet, kontrolery sieci bezprzewodowej, koncentratory VPN | **Spełnia**  **Nie spełnia** |  |  |
| **Realizacja dostępu gościnnego** | | | | | |
| 1.3.40. | | System umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla: | | | |
| 1.3.40.1. | | Microsoft Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7, | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.40.2. | | Apple Mac OS X 10.x oraz 11.x | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.40.3. | | Apple iOS 11.x, 12.x, 13.x i nowszych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.40.4. | | Google Android dla wersji 7.x i nowszych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.40.5. | | Linux | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.41. | | System umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.42. | | System zapewnia uwierzytelnienie sponsora, które musi odbywać się w oparciu o: | | | |
| 1.3.42.1. | | wewnętrzną bazę użytkowników | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.42.2. | | zewnętrzne repozytorium użytkowników | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43. | | System umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do: | | | |
| 1.3.43.1. | | logowania się do systemu | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.2. | | tworzenia pojedynczego konta gościnnego | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.3. | | tworzenia wielu kont gościnnych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.4. | | importowania kont gościnnych z pliku CSV | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.5. | | wysyłania wiadomości email po utworzeniu konta gościnnego | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.6. | | wysyłania wiadomości SMS po utworzeniu konta gościnnego | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.7. | | wyświetlenia hasła konta gościnnego | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.8. | | wydrukowania danych konta gościnnego | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.9. | | wyświetlenia danych stworzonych kont gościnnych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.43.10. | | zawieszenia (suspend) i reinicjacji kont gościnnych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.44. | | System umożliwia personalizację wyglądu portalu sponsora i gościa, w tym: | | | |
| 1.3.44.1. | | zmianę logo strony logowania | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.44.2. | | zmianę obrazu tła strony logowania | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.44.3. | | zmianę logo bannera | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.44.4. | | zmianę obrazu tła bannera | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.44.5. | | zmianę koloru tła strony z treścią | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.45. | | System umożliwia zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.46. | | System umożliwia zmianę adresu URL i FQDN strony sponsora | **Spełnia**  **Nie spełnia** |  |  |
| 1.4.47. | | System umożliwia automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. System umożliwia wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych | **Spełnia**  **Nie spełnia** |  |  |
| 1.4.48. | | System posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.49. | | System umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.50. | | System umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora: | | | |
| 1.3.50.1. | | Imienia | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.50.2. | | Nazwiska | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.50.3. | | Firmy | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.50.4. | | adresu e-mail | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.50.5. | | numeru telefonu | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.50.6. | | danych opcjonalnych (nie mniej niż 5 dodatkowych pól) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.51. | | System umożliwia konfigurację dla użytkowników gościnnych: | | | |
| 1.3.51.1. | | wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.51.2. | | zezwolenia gościom na zmianę hasła oraz odzyskiwanie zapomnianego hasła, | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.51.3. | | samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.52. | | System umożliwia honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.53. | | System umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.54. | | System umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje co najmniej 5 urządzeń per konto gościnne. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.55. | | System umożliwia konfigurację czasu ważności hasła w dniach w przedziale zadanym w dniach. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.56. | | System umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.57. | | System umożliwia konfigurację polityki złożoności haseł użytkowników gościnnych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.58. | | System umożliwia konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.59. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.60. | | System umożliwia przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.61. | | System umożliwia udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP, secure SMTP i poprzez SMS, | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.62. | | System umożliwia wykorzystanie protokołu SAML 2.0 oraz funkcjonalności SSO dla portali gościnnych oraz sponsora. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.63. | | System wspiera API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych. | **Spełnia**  **Nie spełnia** |  |  |
| **Profilowanie urządzeń** | | | | | |
| 1.3.64. | | System umożliwia dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.65. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.66. | | System umożliwia dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł: | | | |
| 1.3.66.1. | | DHCP | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.66.2. | | DHCP SPAN | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.66.3. | | HTTP | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.66.4. | | RADIUS | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.66.5. | | DNS | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.66.6. | | SNMP | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.66.7. | | Network Scan (NMAP lub inne narzędzie profilowania aktywnego) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.67. | | System umożliwia wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.68. | | System umożliwia dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.69. | | System posiada dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla: | | | |
| 1.3.69.1. | | Stacji robocznych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun, | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.69.2. | | Urządzeń mobilnych: Android, Apple, Blackberry | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.69.3. | | Telefonów IP | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.69.4. | | Drukarek sieciowych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.69.5. | | Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.69.6. | | Routerów | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.69.7. | | Punktów dostępu bezprzewodowego | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.70. | | System umożliwia subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji: | | | |
| 1.3.70.1. | | reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.70.2. | | reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.71. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.72. | | System wspiera raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta. | **Spełnia**  **Nie spełnia** |  |  |
| **Wymiana informacji kontekstowych oraz automatyzacji odpowiedzi** | | | | | |
| 1.3.73. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.74. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.75. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.76. | | 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. | **Spełnia**  **Nie spełnia** |  |  |
| **Raportowanie** | | | | | |
| 1.3.77. | | System umożliwia generowanie m.in. następujących raportów: | | | |
| 1.3.77.1. | | raportów dla protokołów AAA: | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.2. | | diagnostyki protokołów AAA | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.3. | | trendów uwierzytelnienia 802.1X | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.4. | | accountingu RADIUS | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.5. | | uwierzytelniania RADIUS | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.6. | | raportów dozwolonych protokołów | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.7. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.8. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.9. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.10. | | raportów dla błędów, w tym: błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił, sumarycznych przyczyn nieudanych uwierzytelnień, Top „N” uwierzytelnień per rodzaj błędu | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.11. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.77.12. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.78. | | raportów katalogu sesji: aktywnych sesji RADIUS, historii sesji RADIUS, zaterminowanych sesji RADIUS | **Spełnia**  **Nie spełnia** |  |  |
| **Alarmy i diagnostyka** | | | | | |
| 1.3.79. | | System umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: wiadomości e-mail, syslog | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.80. | | Alarmy mogą być generowane w następujących sytuacjach: | | | |
| 1.3.80.1. | | ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.80.2. | | opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.80.3. | | 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) | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.81. | | System posiada zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: | | | |
| 1.3.81.1. | | badanie łączności IP za pomocą ping, nslookup, traceroute | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.81.2. | | 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 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.81.3. | | wykonanie zdalnego polecenia na urządzeniu sieciowym | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.81.4. | | ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem: definicji serwerów AAA, protokołu RADIUS, odkrywania urządzeń, logowania, uwierzytelniania Web, konfiguracji trybu 802.1X | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.81.5. | | wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu | **Spełnia**  **Nie spełnia** |  |  |
| **Wsparcie dla protokołu IPv6** | | | | | |
| 1.3.82. | | System posiada wsparcie dla SSH IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.83. | | System pozwala na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacji IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.84. | | System pozwala na konfigurację NTP IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.85. | | System umożliwia stworzenie reguł ograniczających dostęp administracyjny do linii poleceń lub interfejsu graficznego w oparciu o adres IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.86. | | System umożliwia konfigurację serwerów SNMP w oparciu o adresację IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.87. | | System umożliwia wysyłanie SNMP Trap do serwera SNMP IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.88. | | System umożliwia integrację z Active Directory w oparciu o IPv6 | **Spełnia**  **Nie spełnia** |  |  |
| 1.3.89. | | System umożliwia połączenie z serwerem Radius z wykorzystaniem adresu IPv6 | **Spełnia**  **Nie spełnia** |  |  |
|  | | | | |  |
|  | | | | |  |

Do Wykazu Wykonawca zobowiązany jest załączyć **dokumentację urządzenia/oprogramowania, w której znajduje się potwierdzenie spełnienie danego wymagania.**

**Dokumentacją urządzenia/oprogramowania, o której mowa powyżej może być m.in. zrzut konfiguracji, karta katalogowa, specyfikacja techniczna, dokumentacja licencyjna, inna dokumentacja urządzenia/oprogramowania lub oświadczenie producenta urządzenia/oprogramowania, z którego wynika sposób spełnienia danego wymagania lub adres strony WWW pod którym dokument jest opublikowany, a także publicznie i powszechnie dostępny bez konieczności logowania.**

**Uwaga!**

**Plik sporządza się w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym przez osobę uprawnioną do reprezentacji.**