

**Zapytanie ofertowe: 5/DOSTOSOWANIE OFERTY KSZTAŁCENIA/2025**

**na opracowanie i zaimplementowanie środowiska dydaktycznego do potrzeb kształcenia praktycznego
w zakresie sieci bezprzewodowych na studiach II stopnia na kierunku informatyka umożliwiającego
realizację kształcenia w systemie zdalnym**

w ramach projektu

**„Dostosowanie oferty kształcenia na kierunku informatyka prowadzonym przez Warszawską Wyższą
Szkółę Informatyki do rynku pracy oraz potrzeb zielonej i cyfrowej transformacji”**

(FERS.01.05-IP.08-0269/23-00)

Opis konfiguracji sprzętowej pracowni/laboratorium sieci bezprzewodowych w WWSI:

L.p.	Element wyposażenia pracowni	Ilość	Właściwości urządzeń
A.1	Punkt dostępu bezprzewodowego WiFi7	4 szt.	<ol style="list-style-type: none"> Obsługa standardów 802.11a/b/g/n/ac/ax/be <ol style="list-style-type: none"> Obsługa OFDMA (uplink/downlink), TWT, BSS Coloring Obsługa MU-MIMO (uplink/downlink) – min. 4x4:4 (2,4GHz, 5GHz, 6GHz) Obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac Obsługa kanałów 20, 40, 80, 160 MHz w paśmie 5GHz oraz 6GHz dla 802.11ax Obsługa kanałów 20, 40, 80, 160, 320 MHz w paśmie 6GHz dla 802.11be Obsługa prędkości PHY do 3,4 Gbps (ac) (przy parametrach: 4x4 160MHz gdy dwa moduły pracują w 5GHz) Obsługa prędkości PHY do 14,4 Gbps (ax) (przy parametrach: 4x4 160 MHz 6GHz oraz dwóch modułów 5GHz pracujących w trybie 4x4 160MHz) Obsługa prędkości PHY do 23 Gbps (be) (przy parametrach: 4x4 320 MHz 6GHz oraz dwóch modułów 5GHz pracujących w trybie 4x4 160MHz) Obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) Obsługa beamforming dla klientów 802.11ac/ax Obsługa MRC (Maximal Ratio Combining) Obsługa MLO (Multi Link Operation) Obsługa modulacji 4096 QAM Obsługa preamble puncturing Konfigurowalna moc nadajnika: <ol style="list-style-type: none"> dla zakresu 2.4GHz: do 100 mW dla zakresu 5GHz: do 200 mW dla zakresu 6GHz: do 200 mW



			<p>3. Możliwość zmiany trybu pracy modułów radiowych (elastyczna praca pierwszego modułu):</p> <ol style="list-style-type: none"> praca trójzakresowa w pasmach: 2,4GHz oraz 5GHz oraz 6GHz dwa moduły pracujące w paśmie 5GHz (praca w trybie podwójnego 5GHz) oraz trzeci moduł pracujący w paśmie 6GHz <p>4. Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:</p> <ol style="list-style-type: none"> automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) obsługa min. 16 BSSID definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID uwierzelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w obsługa trybów pracy tunelowania ruchu klientów do kontrolera i centralnego terminowania ruchu do sieci LAN oraz lokalnego przełączania ruchu do sieci LAN możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6 jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN) obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h obsługa IPv6 obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r obsługa mechanizmów QoS: <ol style="list-style-type: none"> 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 obsługa modyfikacji autoryzacji w wyniku uwierzelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting wsparcie IEEE 802.11i, WPA2, WPA3, OWE (Enhanced Open), 802.1x, 802.1x-SHA256, CCMP256, GCMP256
--	--	--	--



			<ul style="list-style-type: none"> q. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) r. obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS s. obsługa blokowania ruchu Peer-to-Peer t. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie) <p>5. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:</p> <ul style="list-style-type: none"> a. sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia b. bezpieczna sekwencja uruchamiania c. sprawdzenie autentyczności urządzenia <p>6. Wbudowany moduł radiowy pełniący funkcję analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz, 5GHz, 6GHz):</p> <ul style="list-style-type: none"> a. zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych b. automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.) c. 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 <p>7. Wbudowany moduł UWB (Ultra Wide Band) wraz z wbudowanymi antenami dookólnymi o zysku 7dBi</p> <p>8. Wbudowany moduł BLE (Bluetooth Low Energy) 5.3</p> <p>9. Wbudowany moduł GNSS (Global Navigation Satellite System)</p> <p>10. Interfejs MultiGigabit Ethernet (100/1000/2500/5000/10000)</p> <p>11. Interfejs konsoli RJ45</p> <p>12. Port USB 2.0 (9W)</p> <p>13. 4 GB RAM, 16 GB Flash</p> <p>14. Zróżnicowane możliwości zasilania:</p> <ul style="list-style-type: none"> a. przy zasilaniu przez 802.3bt (Class 6) 60W: pełna funkcjonalność AP b. przy zasilaniu przez 802.3at 30W: praca z wyłączonym portem USB, radio 2,4GHz pracujące w trybie 2x2 oraz interfejs przewodowy z maksymalną prędkością 2,5Gbps c. przy zasilaniu przez 802.3af: możliwość uruchomienia AP w celach diagnostycznych bez pracujących modułów radiowych <p>15. Anteny zintegrowane dookólne o zysku:</p> <ul style="list-style-type: none"> a. min. 5 dBi dla pasma 2,4GHz b. min. 5 dBi dla pasma 5GHz c. min. 6 dBi dla pasma 6GHz
--	--	--	---



			16. Obudowa przystosowana do pracy w zakresie temperatur 0 – 50oC
A.2	Przełącznik sieciowy 24 portowy 1GbE z obsługą PoE+	1 szt.	<ol style="list-style-type: none"> Typ i liczba portów: <ol style="list-style-type: none"> 24 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x1G SFP Moc dostępna dla PoE: <ol style="list-style-type: none"> 370W (z jednym zasilaczem o mocy 600W), 370W (z dwoma zasilaczami o mocy 600W pracującymi w układzie redundantnym), 740W (z dwoma zasilaczami o mocy 600W pracującymi w układzie współdzielenia mocy), Porty SFP możliwe do obsadzenia następującymi rodzajami wkładek: <ol style="list-style-type: none"> Gigabit Ethernet 1000Base-T, Gigabit Ethernet 1000Base-SX, Gigabit Ethernet 1000Base-LX/LH, Gigabit Ethernet 1000Base-EX, Gigabit Ethernet 1000Base-ZX, Gigabit Ethernet 1000Base-BX-D/U Możliwość stackowania przełączników poprzez rozbudowę przyszłości z zapewnieniem następujących funkcjonalności: <ol style="list-style-type: none"> Przepustowość w ramach stosu - 80Gb/s, 8 urządzeń w stosie, Zarządzanie poprzez jeden adres IP, Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, Zasilanie i chłodzenie: <ol style="list-style-type: none"> Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia, W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika), Redundantne wentylatory, Parametry wydajnościowe: <ol style="list-style-type: none"> Przepustowość przełącznika (switching capacity): 56 Gb/s (bez podłączenia do stosu), 136 Gb/s (z podłączeniem do stosu) Prędkość przesyłania (forwarding rate): 41.66 Mpps Bufor pakietów – 6MB Pamięć DRAM – 2GB Pamięć flash – 4GB Obsługa: <ul style="list-style-type: none"> 500 aktywnych sieci VLAN 16000 adresów MAC



			<ul style="list-style-type: none"> ▪ 3000 tras IPv4 ▪ 1500 tras IPv6 ▪ Ilość wpisów w listach kontroli dostępu Security ACL – 1000 ▪ ilość wpisów w listach kontroli dostępu QoS ACL – 1000 ▪ 512 interfejsów SVI L3 ▪ Jumbo frame 9198B ▪ 48 połączeń zagregowanych typu „port channel” ▪ 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP <p>7. Obsługa protokołu NTP</p> <p>8. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping</p> <p>9. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:</p> <ol style="list-style-type: none"> a. IEEE 802.1w Rapid Spanning Tree b. Per-VLAN Rapid Spanning Tree (PVRST+) c. IEEE 802.1s Multi-Instance Spanning Tree d. Obsługa 64 instancji protokołu STP e. Wsparcie dla protokołu REP (Resilient Ethernet Protocol) f. Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego <p>10. Obsługa protokołu LLDP i LLDP-MED</p> <p>11. Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ)</p> <p>12. Funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC</p> <p>13. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego</p> <p>14. Możliwość uruchomienia funkcji serwera DHCP</p> <p>15. Mechanizmy związane z bezpieczeństwem sieci:</p> <ol style="list-style-type: none"> a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level), b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, d. Obsługa funkcji Guest VLAN umożliwiającą uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
--	--	--	--



			<ul style="list-style-type: none"> e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, g. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, i. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), j. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, k. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), l. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, m. Obsługa list kontroli dostępu (ACL) następujących typów: <ul style="list-style-type: none"> ▪ Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, ▪ VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samej sieci VLAN w obrębie przełącznika, ▪ Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, ▪ Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); ▪ Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA), ▪ Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), ▪ Funkcja Private VLAN z obsługą dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS, ▪ Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci, <p>16. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:</p>
--	--	--	---



			<ul style="list-style-type: none"> a. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, b. bezpieczna sekwencja uruchamiania, c. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia. <p>17. Mechanizmy związane z zapewnieniem jakości usług w sieci:</p> <ul style="list-style-type: none"> a. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), f. Kontrola sztormów dla ruchu broadcast/multicast/unicast, g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP; <p>18. Obsługa protokołów i mechanizmów routingu:</p> <ul style="list-style-type: none"> a. Routing statyczny dla IPv4 i IPv6, b. Routing dynamiczny – RIP, OSPF do 1000 routes PIM Stub do 1000 routes c. Policy-based routing (PBR), d. Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup, e. Obsługa 10 tuneli GRE (Generic Routing Encapsulation); <p>19. Przetątnik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,</p> <p>20. Przetątnik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,</p> <p>21. Przetątnik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),</p> <p>22. Funkcjonalność sondy IP SLA Responder,</p> <p>23. Zarządzanie:</p> <ul style="list-style-type: none"> a. Port konsoli, b. Dedykowany port Ethernet do zarządzania out-of-band, c. Możliwość realizacji dostępu do konsoli znakowej lub
--	--	--	--



			<p>wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,</p> <p>d. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,</p> <p>e. Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,</p> <p>f. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,</p> <p>g. Wsparcie dla protokołu RESTCONF,</p> <p>h. Wsparcie dla protokołu gNMI,</p> <p>i. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,</p> <p>j. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,</p> <p>k. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,</p> <p>l. Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,</p> <p>24. Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:</p> <p>a. Monitoring pracy przełącznika w zakresie:</p> <ul style="list-style-type: none"> ▪ Użycie CPU, użycie pamięci, temperatura pracy, ▪ Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny, ▪ Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, ▪ Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzenia sąsiada np. przełącznik, router) ▪ Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o
--	--	--	---



			<p>dacie ostatniego restartu liczników, liczniki ruchu broadcast oraz multicast,</p> <ul style="list-style-type: none"> ▪ Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu broadcast oraz multicast, ▪ Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik, ▪ Protokół REP (Resilient Ethernet Protocol), ▪ Protokół STP (Spanning Tree Protocol), ▪ Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy), <p>b. Konfigurację przełącznika w zakresie:</p> <ul style="list-style-type: none"> ▪ Konfiguracja interfejsów: <p>Fizycznych:</p> <ul style="list-style-type: none"> - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP), - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x, - przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów broadcastowych, multicastowych i unicastowych) <p>Logicznych typu „port channel”:</p> <ul style="list-style-type: none"> - opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, - przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów broadcastowych, multicastowych i unicastowych) <p>Wirtualnych typu SVI:</p> <ul style="list-style-type: none"> - opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do” oraz „z”, parametry protokołu DHCP Relay (adres IP serwera DHCP) <p>b. Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,</p>
--	--	--	--



			<ul style="list-style-type: none"> c. Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), d. Konfiguracja mechanizmów SPAN i RSPAN, e. Konfiguracja protokołu STP, f. Konfiguracja protokołu REP, g. Konfiguracja routingu statycznego i dynamicznego, h. Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów, i. Tworzenie i przypisanie list kontroli dostępu ACL, j. Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, k. Konfiguracja i uruchomienie NetFlow, l. Konfiguracja polityk QoS, m. Administracja przełącznika w zakresie: <ul style="list-style-type: none"> ▪ Zdalne uruchamianie komend linii poleceń, ▪ Nazwa przełącznika, ▪ Tryb pracy L2/L3, ▪ Adres IP przełącznika do celów zarządzania zdalnego, ▪ Konfiguracja serwera DHCP, ▪ Konfiguracja DNS, ▪ Czas systemowy w tym protokół NTP, ▪ Konta administracyjne, ▪ Upgrade oprogramowania, ▪ Backup konfiguracji, ▪ Zdalny restart urządzenia, ▪ Konfiguracja i dostęp przez SNMP, n. Diagnostyka urządzenia: <ul style="list-style-type: none"> ▪ Narzędzie PING i TRACEROUTE, ▪ Przeglądanie logów systemowych, ▪ Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego, <p>25. Parametry fizyczne:</p> <ul style="list-style-type: none"> a. Możliwość montażu w szafie rack 19”, b. Wysokość urządzenia 1 RU, c. Głębokość chassis urządzenia bez wentylatorów i zasilaczy mniejsza niż 30 cm d. Głębokość chassis urządzenia z wentylatorami i zasilaczami mniejsza niż 33 cm e. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow), <p>26. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji</p>
--	--	--	---



			<p>zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,</p> <p>27. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,</p> <p>28. Wyposażenie urządzenia Przełącznik wyposażony w pojedynczy zasilacz. Urządzenie wyposażone jest w licencję subskrypcyjną na wskazane funkcjonalności.</p>
A.3	Firewall sprzętowy z licencją na oprogramowanie klienta	1 szt.	<ol style="list-style-type: none"> 1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia 2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall) 3. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band 4. Urządzenie jest zasilane prądem przemiennym 230V 5. Możliwość montażu w szafie rack 19” (dołączone niezbędne elementy montażowe) 6. Urządzenie wyposażone w 8 wbudowanych portów GbE RJ45 w tym 2 porty PoE+ 7. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – 60 interfejsów VLAN 8. Interfejsy fizyczne mogą pracować jak interfejsy przełącznika sieciowego ze sprzętowym wsparciem dla funkcjonalności L2 9. Urządzenie wyposażone w port USB 3.0 10. Wysokość urządzenia 1RU 11. Przepustowość urządzenia dla uruchomionych modułów firewall’a oraz kontroli aplikacji (AVC) na poziomie 650 Mbps dla pakietów wielkości 1024B 12. Urządzenie osiąga powyższe parametry wydajnościowe również wraz z uruchomionym silnikiem IPS. 13. 100 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 6 000 nowych połączeń na sekundę 14. Możliwość połączeń VPN do 75 urządzeń z maksymalną sumaryczną przepustowością 300 Mbps dla pakietów 1024B TCP 15. Przepustowość dekrypcji ruchu szyfrowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048B) wynosi przynajmniej 150 Mbps 16. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej 17. Możliwość uruchomienia urządzenia w trybie firewall’a L2 oraz L3 18. Urządzenie obsługuje routing statyczny oraz dynamiczny: RIP, OSPF, OSPFv3, BGP 19. Możliwość monitorowania dostępności „next hop” w trasach statycznych i automatycznego wyłączania trasy, gdy jest niedostępny.



			<p>20. Urządzenie obsługuje ruch multicastowy oraz protokoły IGMP, PIM-SM oraz bidirectional PIM</p> <p>21. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory</p> <p>22. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT)</p> <p>23. Urządzenie może pracować jako serwer DHCP lub DHCP relay oraz zapewnia usługę DDNS</p> <p>24. Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby</p> <p>25. Urządzenie zapewnia możliwość obsługi użytkowników zdalnych VPN (RA VPN)</p> <p>26. Urządzenie zapewnia możliwość konfiguracji połączeń VPN typu Site-to-Site w następujących topologiach:</p> <ol style="list-style-type: none"> Point to Point Hub and Spoke Full Mesh <p>27. Urządzenie zapewnia możliwość ograniczenia pasma w konkretnym kierunku – upload i download dla:</p> <ol style="list-style-type: none"> Źródłowych i docelowych stref NGFW Źródłowych i docelowych adresów IP oraz portów Aplikacji Użytkowników URLi zdefiniowanych przez administratora <p>28. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System może stworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:</p> <ol style="list-style-type: none"> Wiedza o użytkownikach – uwierzytelnienie Wiedza o urządzeniach – pasywne skanowanie ruchu Wiedza o urządzeniach mobilnych, load balancerach, urządzeniach NAT Wiedza o aplikacjach wykorzystywanych po stronie klienta <p>29. System posiada otwarte API dla współpracy z systemami zewnętrznymi</p> <p>30. Rozwiązanie współpracuje z systemami SIEM</p> <p>31. System posiada wbudowany moduł wykrywania aplikacji AVC, który zapewnia:</p> <ol style="list-style-type: none"> możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji możliwość tworzenia profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na
--	--	--	--



			<p>wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach</p> <p>32. Rozwiązanie umożliwia integrację z chmurową konsolą korelacji informacji o zagrożeniach z różnych rozwiązań bezpieczeństwa tego samego producenta.</p> <p>33. Urządzenie może być zarządzane lokalnie lub przez scentralizowaną konsolę zarządzającą</p> <p>34. System umożliwia zdefiniowanie różnych wartości czasu wygaśnięcia sesji dla takich protokołów jak: ARP, SIP, H.323, H225, ICMP, UDP oraz dla sesji translacji PAT i sesji pół-otwartych.</p> <p>35. System umożliwia zdefiniowanie następujących podstawowych zabezpieczeń dla połączeń:</p> <ol style="list-style-type: none"> Randomizacja TCP sequence number Ograniczenie ilości wszystkich połączeń globalnie oraz do jednego hosta Ograniczenie ilości połączeń pół-otwartych globalnie oraz do jednego hosta Detekcja wygasłych połączeń, poprzez sprawdzanie czy dwie strony sesji są nadal aktywne <p>36. Urządzenie umożliwia wybór następujących metod kompilacji reguł polityki dostępu w przypadku użycia obiektów (np. grupy adresów IP, portów):</p> <ol style="list-style-type: none"> Rozłożenie jednej skonfigurowanej reguły na reguły szczegółowe będące wszystkimi możliwymi kombinacjami wszystkich elementów zawartych w obiektach w celu monitorowania każdej z tych reguł z osobna (np. ilość dopasowani połączeń hit-counts) kosztem większego wykorzystania pamięci Dopasowanie ruchu do głównej reguły na podstawie zdefiniowanych obiektów bez tworzenia wszystkich możliwych kombinacji obiektów w celu zmniejszenia wykorzystania pamięci przez szczegółowe reguły. <p>37. Urządzenie zapewnia możliwość przypisania do reguł czasu jej aktywności. Istnieje możliwość zdefiniowania czasu całkowitego oraz zaplanowania interwałów czasowych.</p>
A.4	Kontroler sieci bezprzewodowej	1 szt.	<p>1. Urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:</p> <ol style="list-style-type: none"> zarządzanie politykami bezpieczeństwa wykrywanie zagrożeń w sieci bezprzewodowej zarządzanie pasmem radiowym zarządzanie mobilnością zarządzanie jakością transmisji zgodnie z protokołem CAPWAP (RFC 5415) obsługę 1000 punktów dostępowych <p>2. Wspierane tryby uruchomienia:</p> <ol style="list-style-type: none"> na platformach wirtualizacyjnych (chmura prywatna): ESXi, KVM, Hyper-V



			<ul style="list-style-type: none"> b. w chmurze publicznej: AWS (Amazon Web Services), GCP (Google Cloud Platform) <ol style="list-style-type: none"> 3. ·Wydajność centralnego przełączania ruchu 1,5 Gbps (dotyczy platform ESXi, KVM, HyperV), przy zastosowaniu SR-IOV wydajność do 5Gbps (dotyczy platform ESXi, KVM) 4. W przypadku uruchomienia na AWS i GCP: wsparcie dla lokalnego przełączania ruchu do sieci przewodowej na AP (bez obsługi tunelowania ruchu do kontrolera oraz obsługi usług wymagających ruchu do kontrolera) 5. Obsługa 4000 klientów sieci bezprzewodowej 6. ·Zarządzanie pasmem radiowym punktów dostępowych: <ul style="list-style-type: none"> a. automatyczna adaptacja do zmian w czasie rzeczywistym b. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia) c. dynamiczne przydzielanie kanałów radiowych d. wykrywanie, eliminacja i unikanie interferencji e. równoważenie obciążenia punktów dostępowych f. tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych g. automatyczna dystrybucja klientów pomiędzy punkty dostępowe h. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych i. dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe 7. Mapowanie SSID do segmentów VLAN w sieci przewodowej <ul style="list-style-type: none"> a. 1:1 b. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty) c. możliwość tunelowania ruchu klientów do kontrolera (dotyczy platform ESXi, KVM, HyperV) oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID) 8. Obsługa sieci kratowych (dotyczy platform ESXi, KVM, HyperV) <ul style="list-style-type: none"> a. komunikacja między punktami dostępowymi bez medium kablowego b. separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi) c. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja
--	--	--	--



			<p>interferencji z możliwością awaryjnego przełączenia na inne pasmo)</p> <p>d. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)</p> <p>e. autoryzacja punktów dostępowych w oparciu o certyfikaty, adresy MAC</p> <p>9. Obsługa mechanizmów bezpieczeństwa:</p> <p>a. 802.11i, WPA3, WPA2, WPA</p> <p>b. 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)</p> <p>c. obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników</p> <p>d. kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID</p> <p>e. obsługa profilowania użytkowników:</p> <p>a. § przydział sieci VLAN</p> <p>b. § przydział list kontroli dostępu (ACL)</p> <p>f. uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w</p> <p>g. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty</p> <p>h. obsługa list kontroli dostępu (ACL)</p> <p>i. obsługa list kontroli dostępu opartych o nazwy domenowe (DNS ACL)</p> <p>j. obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X</p> <p>k. wykrywanie i dezaktywacja obcych punktów dostępowych</p> <p>l. możliwość budowania reguł klasyfikacji obcych punktów dostępowych w oparciu o nazwę SSID, wybrany ciąg znaków w SSID, siłę sygnału RSSI, minimalną ilość podłączonych urządzeń</p> <p>m. ochrona kryptograficzna (DTLS) ruchu użytkowników (dotyczy platform ESXi, KVM, HyperV) oraz ruchu kontrolnego CAPWAP</p> <p>n. DHCP proxy, wsparcie dla DHCP Option 82</p> <p>o. 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 i znacznika (dotyczy platform ESXi, KVM, HyperV)</p> <p>10. Zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową:</p> <p>a. kryptograficzne podpisywanie obrazów oprogramowania</p>
--	--	--	---



			<p>b. bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych</p> <p>11. Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak: VLAN, polityka QoS, lista kontroli dostępu, czas trwania sesji</p> <p>12. ·Obsługa ruchu unicast IPv4 i IPv6</p> <p>13. ·Zgodność z funkcjonalnościami IPv6 pod kątem RFC: 4191, 6980, 8200, 8201 (dotyczy platform ESXi, KVM, HyperV)</p> <p>14. ·Obsługa ruchu multicast IPv4 i IPv6 (dotyczy platform ESXi, KVM, HyperV)</p> <p>a. IGMP / MLD snooping</p> <p>b. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)</p> <p>c. obsługa konwersji ruchu multicast do unicast</p> <p>15. ·Obsługa mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami (dotyczy platform ESXi, KVM, HyperV))</p> <p>16. ·Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k</p> <p>17. ·Obsługa mechanizmów QoS</p> <p>a. 802.1p</p> <p>b. WMM, TSpec, U-APSD</p> <p>c. Ograniczanie pasma per użytkownik</p> <p>d. Call Admission Control, SIP CAC, Call Snooping</p> <p>e. równomierna obsługa klientów sieci bezprzewodowej w oparciu o użycie czasu antenowego</p> <p>f. kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID</p> <p>g. zbiór wbudowanych profili do automatycznej konfiguracji ustawień QoS</p> <p>18. ·Analiza ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu; rozpoznawanie ponad 1000 aplikacji; współpraca z serwerami autoryzacyjnymi w celu przypisania odpowiednich polityk kontroli ruchu aplikacji per użytkownik/grupa użytkowników (dotyczy platform ESXi, KVM, HyperV)</p> <p>19. ·Obsługa protokołu Bonjour poprzez wbudowany mDNS (multicast DNS) Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów (dotyczy platform ESXi, KVM, HyperV)</p>
--	--	--	---



			<p>20. ·Obsługa dostępu gościnnego (IPv4 i IPv6)</p> <ol style="list-style-type: none"> przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony) przekierowanie użytkowników do strony logowania na zewnętrznym serwerze obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta obsługa konfiguracji jako dedykowany kontroler do obsługi ruchu gości – całość ruchu z SSID dostępu gościnnego zebranego na pozostałych kontrolerach musi być przesyłana do tego kontrolera w sposób zapewniający logiczną separację od ruchu wewnętrznego (dotyczy platform ESXi, KVM, HyperV) <p>21. ·Obsługa NTP (IPv4 oraz IPv6), możliwość ustawienia różnych serwerów NTP dla wybranych grup AP</p> <p>22. ·Możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania (dni tygodnia, godziny)</p> <p>23. ·Obsługa EoGRE w celu tunelowania ruchu z kontrolera do dedykowanego koncentratora (np. na routerze) (dotyczy platform ESXi, KVM, HyperV)</p> <p>24. ·Wsparcie dla IEEE 802.11u</p> <p>25. ·Obsługa Hotspot 2.0 (dotyczy platform ESXi, KVM, HyperV)</p> <p>26. ·Obsługa redundancji rozwiązania (N+1)</p> <p>27. Obsługa redundancji 1:1 (Active/Standby) zapewniającej (dotyczy platform ESXi, KVM, HyperV):</p> <ol style="list-style-type: none"> utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej <p>27. ·Zarządzanie przez HTTPS, SNMP, SSH, NETCONF, wirtualny port konsoli</p> <p>28. ·Obsługa logowania Syslog, wsparcie dla IPSec w celu zabezpieczenia Syslog (dotyczy platform ESXi, KVM, HyperV)</p> <p>29. ·Obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020)</p> <p>30. ·Wbudowana baza najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem</p> <p>31. ·Zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow, w tym również informacji zawartych w pakiecie od warstw 2 do 7 (w szczególności informacji o aplikacjach) (dotyczy platform ESXi, KVM, HyperV)</p>
--	--	--	---



A.5	Komputer jednopłytkowy	4 szt.	<ol style="list-style-type: none"> 1. Typ urządzenia: Komputer jednopłytkowy (SBC – Single Board Computer) 2. Procesor: Czterordzeniowy procesor ARM o architekturze 64-bit Częstotliwość taktowania min. 2,4 GHz 3. Pamięć operacyjna: Min. 8 GB RAM typu LPDDR4X 4. Układ graficzny: Zintegrowany układ graficzny Obsługa rozdzielczości min. 2× 4K 5. Wyjścia wideo: Min. 2 × wyjście microHDMI Obsługa jednoczesnej pracy dwóch monitorów 6. Interfejsy sieciowe: 1 × Ethernet 1 Gb/s Wi-Fi min. 802.11ac Bluetooth min. 5.0 7. Porty USB: Min. 2 × USB 3.0 Min. 2 × USB 2.0 8. Złącza rozszerzeń: Złącze PCIe (minimum 1 linia) 9. Magazyn danych: Gniazdo na kartę microSD 10. Zasilanie: Zasilanie napięciem 5V DC Pobór mocy: do ok. 15–20 W Złącze USB-C 11. System operacyjny: Urządzenie musi umożliwiać instalację i uruchomienie systemów Linux (np. Debian/Ubuntu) oraz dedykowanych systemów embedded.
A.6	Trójkresowy adapter Wi-Fi w formie USB	4 szt.	<ol style="list-style-type: none"> 1. Standardy sieciowe: IEEE 802.11a / b / g / n / ac / ax / be (Wi-Fi 7) 2. Pasmo częstotliwości: 2,4 GHz, 5 GHz, 6 GHz 3. Interfejs fizyczny: min 1 × USB 2.0 4. Szyfrowanie / Bezpieczeństwo: AES; WPA / WPA2 / WPA3 Personal 5. Anteny: min 2 × anteny wewnętrzne 6. Wymiary urządzenia: max: 19 mm × 31,5 mm × 8,5 mm 7. Waga: max 6 g 8. Systemy operacyjne: Wsparcie dla Windows 11