Wyposażenie w sprzęt komputerowy szkół w Gminie Dziemiany

Szczegółowa Specyfikacja Zamówienia

Część 2 zamówienia – DOSTAWA WRAZ Z INSTALACJĄ I KONFIGURACJĄ

Lp.	Nazwa urządzenia	Proponowane przez wykonawcę rozwiązanie Nazwa producenta, model urządzenia	j.m.	Ilość
1.	Router UTM		szt.	1
2.	Kontroler		szt.	1
3.	Przełącznik sieciowy		szt.	1
4.	Punkt dostępowy		szt.	4
5.	Okablowanie sieci		kpl.	1
6.	Listwy kablowe		mb	1
7.	Instalacja z konfiguracją		Kpl.	1

PODZIAŁ NA JEDNOSKTI

1. G_Sieć wifi - router/utm (narzędzia TIK)	GIM Dziemiany	1
2. G_Sieć wifi - kontroler sieci (narzędzia TIK)	GIM Dziemiany	1
3. G_Sieć wifi - instalacja i integracja sieci bezprzewodowej (narzędzia TIK)	GIM Dziemiany	1
4. G_Sieć wifi – przełącznik sieciowy (narzędzia TIK)	GIM Dziemiany	1
5. G_Sieć wifi - okablowanie pod sieć bezprzewodową (narzędzia TIK)	GIM Dziemiany	1
6. G_Sieć wifi - punkt dostępowy (narzędzia TIK)	GIM Dziemiany	4
7. G_Sieć wifi - listwa prostokątna 40x20 (narzędzia TIK)	GIM Dziemiany	1

MINIMALNE PARAMETRY TECHNICZNE

1.	**Router UTM**	**szt.**	**1**
	1. Typ urządzenia: a. Urządzenie klasy UTM (Unified Threat Management) **2. Wyposażenie:** a. Min. 4 interfejsy LAN typu 1000Base-T, z których jeden może pełnić funkcję interfejsu WAN / Internet nr 2 b. Min. 1 interfejs WAN / Internet typu 1000Base-T c. Interfejs USB do podłączenia modemu 3G/4G/LTE 3. Parametry wydajnościowe: a. Wydajność zapory ogniowej L3: min. 250 Mb/s b. Wydajność dla ochrony antywirusowej: min. 250 Mb/s c. Wydajność IDS: min. 200 Mb/s d. Wydajność urządzenia z włączonymi wszystkimi funkcjami bezpieczeństwa (NAT, VPN (Split-tunnel), filtrowanie treści, traffic shaping, anti-virus/anti-phishing, IPS): min. 200 Mb/s e. Maksymalna ilość połączeń: 100 000 f. Maksymalna ilość połączeń na sekundę: 5000 g. Przepustowość dla ruch VPN: min. 100 Mb/s h. Maksymalna liczba sesji VPN: 25 **4. Parametry fizyczne** a. Wysokość nie więcej niż 1RU b. Możliwość montażu w szafie 19”, w przypadku braku możliwości instalacji w szafie podwykonawca musi zapewnić półkę do szafy c. Praca w temperaturach 0 – 40 st.C **5. Funkcje zintegrowanego systemu zarządzania zagrożeniami UTM obejmującego:** a. Firewalling ruchu sieciowego w warstwie 3 - filtracja na podstawie: • protokołu sieciowego (TCP/UDP/dowolny); • źródłowe adresy IP • źródłowe porty • docelowe adresy IP • docelowe porty		

b. Firewalling ruchu aplikacyjnego wg. typu aplikacji w warstwie 7 – filtracja na podstawie następujących kategorii aplikacji internetowych:

- Blogging
- Email
- File Sharing
- Gaming
- News
- Online backup
- Peer-to-peer
- Social web
- Photo sharing
- Software updates
- Anti-virus updates
- Sports
- Video
- Music
- VOIP
- Video Conferencing
- Web file sharing
- Możliwość blokowania ruchu do zdefiniowanego serwera http przez podanie domeny sieciowej
- Możliwość blokowania ruchu internetowego na podstawie kryterium geograficznego (kraje)
- Możliwość blokowania ruchu poprzez podanie zakresów adresów IP i portów

c. Ograniczanie ruchu sieciowego (traffic shaping):

- Na łączach WAN niezależnie dla każdego łącza poprzez podanie z dokładnością do 1 Mb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz)
- Na łączu komórkowym 3G/4G/LTE poprzez podanie z dokładnością do 100 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz)
- Na użytkownika sieci poprzez podanie limitu z dokładnością do 100 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz)
- Dla określonego ruchu aplikacyjnego w warstwie 7 dokładnością do 10 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz):
  - Tworzenie do 8 reguł ograniczających ruch sieciowy, z których każda może się składać z dowolnej kombinacji aplikacji sieciowych
  - Możliwość priorytetyzacji ruchu (wysoki priorytet, normalny priorytet, niski priorytet) oraz oznaczania ruchu danym znacznikiem DSCP (od 0 do 7)

a. Blokowanie stron internetowych URL zgodne z CIPA (Children's Internet Protection Act) i należących do 70 różnych kategorii w tym:

- narkotyki
- treści dla dorosłych oraz treści pornograficzne
- alkohol i tytoń
- aukcje
- botnety
- potwierdzone i niepotwierdzone źródła spamu
- strony o charakterze okultystycznym
- portale randkowe
- moda i uroda
- hazard, gry
- strony wulgarne
- strony hakerskie

- rasizm oraz szerzenie nienawiści
- strony nielegalne
- wyszukiwarki zdjęć oraz filmów
- keyloggery oraz monitory stacji
- źródła malware
- wojskowość i militaria
- oprogramowanie peer to peer
- strony płatne
- blogi
- phishing
- serwisy umożliwiające omijanie proxy oraz anonimizację w sieci internet
- wyszukiwarki
- edukacja seksualna
- oprogramowanie shareware oraz freeware
- zakupy
- social networking
- spyware oraz adware
- media strumieniowe
- przemoc
- broń
- ogłoszenia sieciowe

d. Blokowanie treści dla dorosłych w wynikach działania najpopularniejszych wyszukiwarek internetowych: Google, Yahoo, Bing – funkcja działa dla wyszukiwania niezaszyfrowanego
e. Blokowanie dostępu do zaszyfrowanego wyszukiwania treści internetowych w serwisie Google.
f. Funkcja YouTube for Schools
g. Możliwość definiowana własnej listy zabronionych (czarna lista) lub dozwolonych (biała lista) stron URL
h. Wykrywanie i ochrona przed malware
i. Ochrona antywirusowa i antyphishingowa
j. Ochrona IPS i IDS

6. Monitoring i analiza ruchu sieciowego w zakresie:

a. Wykres ilości ruchu generowanego przez wszystkich użytkowników, jednego użytkownika lub grupę użytkowników w ciągu ostatniego dnia, ostatniego tygodnia i ostatniego miesiąca
b. Wykres ilości użytkowników podłączonych do sieci chronionej w ciągu ostatniego dnia, ostatniego tygodnia i ostatniego miesiąca
c. Szczegółowe informacje, jakie aplikacje sieciowe używają użytkownicy w sieci chronionej dla wszystkich użytkowników lub dla wybranego użytkownika z podaniem wolumenu przesłanego ruchu

7. Funkcje koncentratora VPN dla łączenia ze sobą placówek (site-to-site vpn przy użyciu tuneli IPSEC i 128-bitowego szyfrowania AES) oraz dla podłączenia urządzeń klienckich (Client VPN):

a. Dla połączeń site-to-site:

- obsługa trybu pracy tuneli VPN gdy cały ruch sieciowy jest tunelowany przez VPN lub trybu gdy ruch do publicznego internetu jest przesyłany bezpośrednio do internetu poza tunelem a ruch prywatny jest tunelowany
- obsługa topologii gwiazdy lub pełnej siatki połączeń
- Blokowanie ruchu sieciowego na poziomie reguł warstwy 3 wymienianego pomiędzy lokalizacjami połączonymi poprzez VPN

b. Dla połączeń Client VPN:

- obsługa protokołu L2TP dla urządzeń klienckich typu: Windows, Mac OS, IOS lub Android
- Automatyczna rejestracja do dynamicznego DNS na potrzeby dostępu VPN dla Klientów (Client VPN) z możliwością zdefiniowana nazwy dla każdego z linków WAN niezależnie

8. Funkcje routera do sieci Internet w zakresie:

a. Fizyczne podłączenie do łącza lub łączy internetowych operatora (2 x WAN w postaci interfejsów Ethernet 1 Gb/s) + interfejs USB do podłączenia modemu 3G/4G/LTE
b. NAT / PAT
c. Tryb pracy przeźroczystej (Bridge warstwy 2)
d. Serwer DHCP
e. Routing statyczny IP pomiędzy sieciami VLAN (po stronie LAN) i WAN oraz pomiędzy sieciami VLAN
f. Wykorzystanie dwóch łączy uplinkowych WAN do sieci Internet w zakresie:

- Load balancing ruchu
- Wskazanie jaki ruch sieciowy (protokół, źródłowy adres IP, źródłowy port, docelowy adres IP, docelowy port) mają zostać skierowane do którego łącza WAN
- Wykorzystanie łącza nr 2 w momencie awarii łącza nr 1

9. Zarządzanie, monitorowanie i utrzymanie urządzenia:

a. Monitoring

- Status urządzenia
- Status interfejsów WAN wraz z przypisanymi adresami IP
- Dostęp do event loga związanego z danym urządzeniem
- Status portów LAN
- Bieżący wykres ruchu internetowego (w Kb/s lub Mb/s) odświeżany na bieżąco
- Lista stacji sieciowy dzierżawiących adresy IP przez DHCP
- Możliwość restartu zdalnego urządzenia
  - Wysyłania alertów mailowych na wskazane adresy mailowe w przypadku, gdy:
  - Urządzenie jest niedostępne (offline)
  - Zmiana statusu podstawowego łącza WAN
  - Wyczerpanie puli adresów IP serwera DHCP
  - Wykrycie w sieci nielegalnego serwera DHCP

b. Konfiguracja

- Konfiguracja i uruchomienie sieci VPN site-to-site
- Konfiguracja i zmiana ustawień w zakresie:
- Tryb pracy, jako router lub bridge warstwy 3
- NAT
- Routing statyczny i konfiguracja sieci VLAN
- Serwer DHCP
- Filtry warstwy 3 i filtry aplikacyjne warstwy 7
- Filtry treści
- Polityki ograniczenia pasma sieciowego do poziomu reguł obejmujących kombinacje aplikacji sieciowych warstwy 7

	• Konfiguracja grup użytkowników wraz z możliwością zdefiniowania dla grupy użytkowników następujących parametrów: i. Godziny i dni tygodnia dostępności lub niedostępności dostępu do sieci ii. Ograniczenie pasma transmisji iii. Określenie reguł firewallingu w warstwie 3 i 7 iv. Określenie reguł ograniczania ruchu sieciowego (traffic shaping) v. Określenie reguł filtracji stron i treści internetowych vi. Określenie listy dozwolonych i niedozwolonych adresów URL vii. Uruchomienie lub wyłączenie filtrowania wyników przeszukiwania w wyszukiwarkach internetowych viii. Włączenie lub wyłączenie funkcji YouTube for Schools c. Utrzymanie: • Automatyczna aktualizacja oprogramowania jednego lub wielu urządzeń z możliwością określenia okna czasowego, kiedy taka czynność może zostać wykonana przez system zarządzający • Informowanie administratora o dostępności nowej wersji oprogramowania dla danego typu urządzenia z możliwością zablokowania automatycznego upgrade, określenia, kiedy ma być wykonany lub natychmiastowego wykonania upgrade **10. Urządzenie obsługuje SNMP v2c oraz SYSLOG** **11. Urządzenie obsługuje PPPoE dla łącza WAN** **12. Wymagania dodatkowe:** Urządzenia objęte gwarancją „lifetime warranty" oraz serwisem wymiany urządzenia next-business-day. Zarządzanie i monitorowanie urządzeniem bezpieczeństwa UTM lub grupą takich urządzeń odbywa się poprzez aplikację zarządzającą dostępną w chmurze. **13.** Wymaga się dostarczenia na urządzenie licencji 3-letniej na jego wykorzystanie w zakresie opisanych funkcjonalności oraz serwisu wymiany urządzenia next-business-day		
2.	**Kontroler – system do zarządzania**	**szt.**	**1**
	1. System centralnego zarządzania i monitoringu punktów dostępowych, przełączników, routerów oraz instancjami oprogramowania MDM (Mobile Device Management) dostępny w publicznej chmurze z dowolnego miejsca **2. Funkcje ogólne:** a. Zarządzanie przez graficzny interfejs webowy z wykorzystaniem HTTPS b. System uruchomiony w trybie wysokiej dostępności z replikacją danych w czasie rzeczywistym c. Gwarantowana dostępność systemu na poziomie 99,99% d. Certyfikacja architektury chmurowej PCI DSS Level 1 e. Centra danych architektury chmurowej o certyfikatach: ISO 27001:2013 oraz SSAE16/SAS70 typ II f. Integracja z Google Maps w celu graficznego rozmieszenia położenia urządzeń i wizualizacji ich stanu g. Wizualizacja topologii sieci • automatyczne rysowanie mapy topologii • wizualizacja stanu urządzeń • wizualizacja połączeń między urządzeniami • wizualizacja połączeń zablokowanych przez STP • po najechaniu myszką na połączenie wyświetlenie informacji o ilości przetransmitowanych danych, ilości klientów przez ostatni dzień oraz numerach portów urządzeń tworzących połączenie		

h. Podział zarządzanych urządzeń na logiczne podgrupy: np.: oddział, lokalizacja, itp.
i. Monitoring i zarządzanie siecią z podziałem na podgrupy
j. Przypisywanie tagów do różnych elementów w systemie, np.: podgrupa urządzeń, urządzenie, port urządzenia w celu łatwego wyszukiwania i konfiguracji danej grupy elementów o zadanym tagu
k. Wyświetlanie informacji w czytelnych tabelach z możliwością sortowania w kolumnach
l. Wyświetlanie informacji o znaczeniu danego parametru po zbliżeniu kursora myszki
m. Wbudowany mechanizm wyszukiwania ustawień, urządzeń, klientów po różnych parametrach
n. Porównywanie ustawień konfiguracyjnych między logicznymi podgrupami urządzeń
o. Zautomatyzowany proces dodawania nowych urządzeń do systemu zarządzania, np.: poprzez wpisane numeru seryjnego urządzenia lub numeru zamówienia
p. Centralna administracja licencjami na urządzenia
q. Otwieranie i zarządzanie zgłoszeniami dotyczącymi problemów ze sprzętem lub jego konfiguracją do wsparcia producenta bezpośrednio w systemie do zarządzania
r. Export zdarzeń do serwerów SYSLOG:
    - zarządzanie typem wysyłanych zdarzeń
    - dla routerów/UTM: log zdarzeń, alarmy IDS, URL, flow
    - dla przełączników: log zdarzeń
    - dla punktów dostępowych: log zdarzeń, URL, flow

3. Centralne zarządzanie oprogramowaniem na urządzeniach:
a. możliwość automatycznej aktualizacji w momencie gdy producent wprowadzi nowe oprogramowanie
b. możliwość wyboru daty aktualizacji
c. możliwość modyfikacji daty aktualizacji dla danego typu urządzeń

4. Narzędzia wspomagające diagnostykę problemów z urządzeniami:
a. dla punktu dostępowego: ping, traceroute, wyświetlenie tablicy ARP, test przepustowości, mruganie diodami urządzenia
b. dla przełącznika: ping, test kabla, wyświetlenie tablicy MAC, restart portu, wysłanie wiadomości Wake-on-LAN, test przepustowości, mruganie diodami urządzenia
c. dla routera/UTM: ping, traceroute, wyświetlenie przydziałów DHCP, test DNS, test przepustowości, mruganie diodami urządzenia

5. Narzędzie do przechwytywania ruchu do pliku pcap w celu szczegółowej analizy z możliwością ignorowania pakietów broadcast, multicast oraz tworzeniem wyrażeń filtrujących (np., po adresie IP, MAC, itp.)

6. Monitoring podłączonych urządzeń/klientów za zadany okres: ostatnich dwóch godzin, ostatniego dnia, tygodnia, miesiąca z następującymi informacjami:
a. sposób podłączenia do sieci: przewodowo lub bezprzewodowo
b. parametry IP: adres IPv4, IPv6, MAC, VLAN
c. parametry urządzenia: typ/model urządzenia
d. ilość przetransmitowanych danych z podziałem na aplikacje warstwy 7
e. przypisana polityka dostępowa
f. przypisana polityka firewallingu
g. dla urządzeń/klientów bezprzewodowych:
    - parametry radiowe połączenia: siła sygnału, kanał
    - wspierane standardy radiowe,
    - maksymalna przepustowość,
    - wspierana ilość strumieni przestrzennych
h. dla urządzeń/klientów przewodowych:
    - numer portu i przełącznika do którego podłączony jest klient

7. Ogólne parametry raportowania:

a. Raporty z podziałem na logiczne podgrupy
b. Raporty z podziałem na logiczne podgrupy z wybranym tagiem
c. Raporty za okres ostatniego dnia, tygodnia, miesiąca, wybranego okresu
d. Wysyłanie raportów w formacie HTML lub tekstowym na zadany adres email

8. Raporty dotyczące sieci zawierające następujące informacje za zadany okres dnia, tygodnia, miesiąca lub wybranego okresu:

a. Wykorzystanie sieci (ilość przetransmitowanych danych) w postaci wykresu
b. Całkowita wartość ruchu z podziałem na ruch upstream oraz downstream
c. Lista klientów o największej ilości przetransmitowanych danych z podaną wartością
d. Lista najbardziej wykorzystywanych aplikacji w sieci z podaną wartością transmisji
e. Lista najczęściej spotykanych systemów operacyjnych w sieci z podaną wartością transmisji
f. Lista 10 najczęściej spotykanych typów urządzeń klienckich z podaną wartością transmisji
g. Ilość klientów podłączonych do sieci z podziałem czasowym
h. Mapa rozmieszczenia urządzeń z ilością podłączonych klientów
i. Dla punktów dostępowych:
   - Lista punktów dostępowych o największej transmisji danych z podaną wartością transmisji
   - Lista SSID o największej transmisji danych z podziałem z podaną wartością transmisji
j. Dla przełączników:
   - Lista przełączników o największej transmisji danych z podaną wartością transmisji
   - Lista przełączników o największym zużyciu energii elektrycznej z podaną wartością zużycia
   - Lista typów przełączników o największej transmisji danych z podaną wartością transmisji
   - Dystrybucja portów z podziałem na prędkość podłączenia oraz stan wykorzystania i typ interfejsu (miedziany/światłowodowy)
k. Dla routerów/UTM:
   - Lista routerów o największej transmisji danych z podaną wartością transmisji
   - Lista najczęściej blokowanych stron webowych
   - Lista najczęściej blokowanych kategorii stron webowych

9. Dostęp administracyjny do systemu zarządzania:

a. Dwuskładnikowe uwierzytelnianie (np. przez nazwę i hasło oraz jednorazowy kod SMS)
b. Wymuszanie zmiany haseł (np. co 90 dni)
c. Wymaganie minimalnej długości hasła i jego złożoności
d. Blokowanie administratora po kilkukrotnych nieudanych próbach logowania
e. Uniemożliwianie ponownego wykorzystania hasła
f. Ograniczanie możliwości zalogowania się do określonego zakresu adresów IP
g. Wyznaczanie administratorów do określonych logicznych podgrup urządzeń
h. Wyznaczanie poziomu dostępu: tylko do odczytu, zarządzanie dostępem gościnnym, pełny dostęp do wprowadzania zmian
i. Wysyłanie notyfikacji email w momencie wprowadzania zmian konfiguracyjnych

j. Logowanie czasu, adresu IP oraz przybliżonej lokalizacji logującego się do systemu z możliwością weryfikacji tej informacji w logu wraz z informacją o wprowadzonych zmianach
k. Wylogowywanie administratora po określonym czasie bezczynności
l. Integracja SAML w celu uwierzytelniania administratorów do systemu za pośrednictwem zewnętrznego serwera uwierzytelniania

10. Alarmy dotyczące pracy sieci:

a. Wysyłanie alarmów do administratorów lub do określonych adresów email
b. Wysyłanie trapów SNMP
c. Wysyłanie alarmów gdy nastąpi zmiana konfiguracji
d. Alarmy dotyczące routerów/UTM:
   - Gdy urządzenie będzie nieosiągalne przez zadany okres czasu: 5, 10, 15, 30, 60 minut
   - Gdy zmieni się status głównego łącza
   - Gdy wyczerpie się pula adresów DHCP
   - Gdy pojawi się konflikt adresów IP
   - Gdy zmieni się stan połączenia przez sieć 3G/4G
   - Gdy wykryty zostanie wrogi serwer DHCP
   - Gdy nastąpi przełączenie w parze urządzeń aktywne/zapasowe
e. Alarmy dotyczące przełączników:
   - Gdy urządzenie będzie nieosiągalne przez zadany okres czasu: 5, 10, 15, 30, 60 minut
   - Gdy porty lub wybrana grupa portów będzie w stanie „down" przez zadany okres czasu: 5, 10, 15, 30, 60 minut
   - Gdy porty lub wybrana grupa portów wykryje błąd kabla
   - Gdy porty lub wybrana grupa portów zmieni prędkość pracy
   - Gdy pojawi się nowy serwer DHCP w sieci
f. Alarmy dotyczące punktów dostępowych:
   - Gdy urządzenie będzie nieosiągalne przez zadany okres czasu: 5, 10, 15, 30, 60 minut
   - Gdy punkt dostępowy straci połączenie kablowe z siecią i podłączy się drogą bezprzewodową do innego punktu dostępowego
   - Gdy punkt dostępowy wykryje wrogi punkt dostępowy

11. Mechanizmy dotyczące usług dla sieci bezprzewodowej:

a. Wgranie map pomieszczeń z możliwością rozmieszczenia AP
b. Wyświetlanie rozmieszczenia AP oraz klientów (podłączonych oraz niepodłączonych) sieci bezprzewodowej na mapie pomieszczenia z zaznaczeniem miejsc o wysokiej i niskiej gęstości
c. Zbieranie informacji o urządzeniach w zasięgu sieci radiowej z podziałem na urządzenia/klientów podłączonych do sieci, będących w jej zasięgu oraz przemieszczających się w jej zasięgu
d. Zbieranie informacji o długości czasu wizyty urządzeń/klientów w zasięgu sieci radiowej
e. Zbieranie informacji o powtarzalności wizyt urządzeń/klientów
f. Prezentacja graficzna zebranych informacji
g. Export danych analitycznych w formie pliku CSV
h. Dostępne API

   - API pozwalające na wysyłanie informacji o lokalizacji urządzeń mobilnych

	• API pozwalające na przekierowanie użytkowników na zewnętrzny portal logowania **12. Obsługa wszystkich funkcji punktu dostępowego z poziomu systemu zarządzania** **13. Obsługa wszystkich funkcji routera/UTM z poziomu systemu zarządzania** **14. Obsługa wszystkich funkcji przełącznika z poziomu systemu zarządzania** **15. Obsługa wszystkich funkcji oprogramowania MDM z poziomu systemu zarządzania**		
3.	**Przełącznik sieciowy**	**szt.**	**1**
	1. Architektura: a. Min. 8 portów 10/100/1000BaseT b. Wszystkie porty 10/100/1000 muszą pozwalać na zasilanie urządzeń klienckich zgodnie ze standardem IEEE 802.3at – dostępna moc do zasilania urządzeń min. 124W c. Automatyczne wykrywanie przeplotu na portach 10/100/1000 (AutoMDIX) d. Min. 2 porty uplink 1000BaseX, SFP – dopuszczalna zamienna praca z portami 10/100/1000 e. Porty SFP muszą umożliwiać ich obsadzanie wkładkami Gigabit Ethernet – minimum 1000BaseT, 1000Base-SX, 1000BaseLX/LH f. Nie blokująca matryca przełączająca o wydajności na poziomie min. 20Gbps **2. Parametry fizyczne:** a. Wysokość 1RU b. Możliwość montażu w szafie 19”, w przypadku braku możliwości instalacji w szafie podwykonawca musi zapewnić półkę do szafy c. Praca w temperaturach 0 – 40 °C d. Zasilanie 230V AC **3. Przełączanie w warstwie 2:** a. Obsługa min. 4000 sieci VLAN b. Obsługa min. 8.000 adresów MAC c. Obsługa ramek Jumbo do min. 9200 bajtów d. Obsługa znaczników VLAN i trunk’ów 802.1Q e. Wsparcie dla protokołów IEEE 802.1D STP (Spanning Tree Protocol) i IEEE 802.1w (Rapid Spanning Tree Protocol) f. Obsługa ruchu multicast - IGMP Snooping g. Obsługa połączeń zagregowanych zgodnie z IEEE 802.3ad (min. 8 portów w grupie) **4. Obsługa łączenia w wirtualne stosy, widziane jako pojedyncze urządzenia logiczne z poziomu zarządzania** **5. Mechanizmy zarządzania jakością ruchu w sieci:** a. Klasyfikacja ruchu do klas różnej jakości obsługi (CoS) w oparciu o znaczniki DSCP (obsługa remarkowania ruchu) poprzez wykorzystanie następujących parametrów: VLAN, źródłowy/docelowy port TCP/UDP b. Implementacja co najmniej czterech kolejek dla obsługi ruchu c. Kontrola ruchu rozgłoszeniowego (broadcast storm control)		

	6. Mechanizmy bezpieczeństwa: a. Uwierzytelnianie użytkowników w oparciu o IEEE 802.1X b. Uwierzytelnianie urządzeń na porcie w oparciu o adres MAC c. Funkcja Guest VLAN d. Obsługa list kontroli dostępu (ACL) – filtrowanie w oparciu o VLAN, źródłowe i docelowe adresy IPv4 oraz porty TCP/UDP e. Obsługa DHCP Snooping, obsługa stworzenia listy akceptowanych serwerów DHCP f. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego g. Określanie planów godzinowych aktywacji poszczególnych portów (z dokładnością do dnia tygodnia i godzin h. Analiza aplikacyjna (Deep Packet Inspection), umożliwiająca identyfikację aplikacji i klientów w warstwie 7 **7. Mechanizmy zarządzania:** a. Obsługa SNMP v2c b. Zdalne przechwytywanie ruchu (packet capture) c. Przekierowywanie ruchu z określonego portu/portów na inny (port mirroring) d. Wbudowane mechanizmy diagnostyki okablowania (długość, stan poszczególnych par) e. Obsługa protokołu LLDP f. Obsługa RADIUS, SYSLOG **8. Zarządzanie i monitorowane poprzez system zarządzania dostępny w publicznej chmurze** **9. Uproszczona instalacja urządzenia, która wymaga jedynie:** a. Podłączenia do sieci Internet b. Podania numeru seryjnego w systemie zarządzania i monitorowania siecią c. Wskazania sieci / lokalizacji, która określa konfigurację urządzenia **10. Wymaga się dostarczenia na urządzenie licencji** 3-letniej na jego wykorzystanie w zakresie opisanych funkcjonalności oraz serwisu wymiany urządzenia next-business-day		
4.	**Punkt dostępowy**	**szt.**	**4**
	1.Architektura radiowa i obsługa standardów: a. Obsługa MIMO 2x2:2 b. Moduł radiowy 802.11 b/g/n c. Moduł radiowy 802.11 a/n/ac d. Dwupasmowy moduł radiowy do zastosowań wIDS/wIPS e. Moduł BLE (Bluetooth Low Energy) f. Obsługa prędkości PHY 802.11ac do 866 Mbps g. Obsługa prędkości PHY 802.11n do 300 Mbps h. Maksymalna prędkość do 1,2 Gbps i. Obsługa kanałów 20,40,80 MHz dla 802.11ac oraz 20,40 MHz dla 802.11n j. Obsługa MRC		

k. Obsługa beamforming
l. Obsługa agregacji ramek

2.Obsługa zakresów częstotliwości:

a. 2,412 – 2,484 GHz
b. 5,150 – 5,250 GHz (UNII-1)
c. 5,250 – 5,350 GHz (UNII-2)
d. 5,470 – 5,600; 5,650 – 5,725 GHz (UNII-2e)

3.Konfigurowalna moc nadajnika:

a. Dla pasma 2,4 GHz: do 19 dBm
b. Dla pasma 5 GHz: do 20 dBm

4.Zasilanie:

a. PoE (IEEE 802.3af)
b. Adapter AC (nie wymaga się dostarczenia)
c. Power injector PoE (nie wymaga się dostarczenia)
d. Zużycie energii: max 14W

5.Parametry fizyczne i anteny:

a. Budowa niskoprofilowa (poniżej 4 cm)
b. Masa poniżej 0,8 kg
c. Zabezpieczenie Kensington
d. Temperatura pracy: 0 – 40°C
e. Dołączone elementy montażowe
f. Zintegrowane anteny dookólne o zysku 5 dBi dla 2.4 GHz oraz 5,5 dBi dla 5 GHz
g. Diodowa sygnalizacja stanu urządzenia

6.Interfejsy:

a. Min. 1 x 100/1000 Base-T

7.Mechanizmy bezpieczeństwa:

a. WEP, WPA, WPA2-PSK, WPA2-Enterprise (802.1X)
b. Szyfrowanie TKIP oraz AES
c. Szyfrowanie IPSec w celu tunelowania danych do koncentratora VPN
d. Tagowanie VLAN (IEEE 802.1q)
e. Blokowanie ruchu między klientami bezprzewodowymi
f. Wbudowany firewall warstwy 3-7
g. Firewall warstwy 7 umożliwia wykrywanie i blokowanie lub limitowanie pojedynczych aplikacji oraz grup aplikacji danego typu: blogi, email, współdzielenie plików, wiadomości, gry, p2p, portale społecznościowe i współdzielenie zdjęć, aktualizacja oprogramowania, sport, wideo i muzyka, konferencje audio i wideo

h. Firewall warstwy 7 umożliwia blokowanie określonych stron http, zakresów adresów IP/portów
i. Zintegrowany system wykrywania włamań, wrogich AP i reagowania na nie (wIPS/wIDS)

8.Funkcje modułu wIPS/wIDS:

a. Skanowanie pasma 2,4 GHz oraz 5 GHz w czasie rzeczywistym
b. Detekcja wrogich AP
c. Wykrywanie podłączenia wrogiego AP do sieci LAN
d. Klasyfikacja ataków w zależności od stopnia zagrożenia
e. Klasyfikacja ataków w oparciu o sygnatury bazujące na typie i profilu zachowania (podstawowe ataki to: spoofing, DoS, packet flood)
f. Konfiguracja polityki reagowania na ataki
g. Prowadzenie logu zdarzeń

9.Funkcje modułu BLE (Bluetooth Low Energy):

a. Praca jako beacon BLE (możliwość konfiguracji parametrów UUID, Major, Minor)
b. Skanowanie sygnałów Bluetooth

10.Mechanizmy QoS:

a. DSCP
b. 802.1p
c. Advanced Power Save (U-APSD)
d. IEEE 802.11e oraz WMM
e. Limitowanie ruchu per klient oraz per SSID
f. Rozpoznawanie aplikacji w warstwie 7
g. Limitowanie wybranego typu ruchu aplikacyjnego per klient oraz per SSID z możliwością markowania ruchu
h. Mechanizm preferowania pasma 5 GHz dla klientów dwuzakresowych
i. Mechanizm analizy widma częstotliwości z możliwością graficznej prezentacji pracujący w obu zakresach częstotliwości

2. Mechanizmy mobilności:

a. 802.11k oraz 802.11r
b. PMK oraz OKC dla szybkiego roamingu L2
c. Roaming L3

3. Mechanizmy analityczne:

a. Zbieranie informacji o urządzeniach w zasięgu sieci radiowej z podziałem na urządzenia/klientów podłączonych do sieci, będących w jej zasięgu oraz przemieszczających się w jej zasięgu
b. Zbieranie informacji o długości czasu wizyty urządzeń/klientów w zasięgu sieci radiowej
c. Zbieranie informacji o powtarzalności wizyt urządzeń/klientów
d. Prezentacja graficzna zebranych informacji
e. Export danych analitycznych w formie pliku CSV

4. Obsługa dostępu gościnnego:

a. Przekierowanie użytkowników danego SSID na portal logowania
b. Personalizacja wyglądu portalu logowania
c. Kreowanie i zarządzanie kontami gościnnymi przez interfejs webowy

	d. Uwierzytelnianie do sieci za pośrednictwem: akceptacji portalu, uwierzytelniania SMSem, serwera LDAP, serwera RADIUS, serwera Active Directory, kont z portalu Facebook e. Obsługa Walled Garden **5. Funkcje ogólne:** a. Automatyczne budowanie sieci kratowej (formowanie połączeń do innych punktów dostępowych w oparciu o radio 2,4GHz lub 5 GHz bez podłączenia do sieci kablowej) b. Konfiguracja min. 15 SSID c. Konfiguracja dostępności danego SSID w zależności od danego zakresu godzin w danym dniu tygodnia d. Zarządzanie przez interfejs webowy e. Logowanie zdarzeń systemowych f. Logowanie zmian w konfiguracji g. Obsługa SYSLOG h. Monitoring urządzenia i wyświetlanie następujących parametrów: adres MAC, numer seryjny, uruchomione sieci SSID, adres IP, DNS, transmisja danych oraz ilości klientów z ostatniego dnia i. Narzędzia wspomagające diagnostykę problemów: ping, traceroute, wyświetlenie tablicy ARP, test przepustowości, mruganie diodami urządzenia j. Narzędzie do przechwytywania ruchu do pliku pcap w celu szczegółowej analizy z możliwością ignorowania pakietów broadcast, multicast oraz tworzeniem wyrażeń filtrujących (np., po adresie IP, MAC, itp.) k. Monitoring urządzeń podłączających się do sieci w zakresie: parametrów radiowych połączenia (siła sygnału, kanał), parametrach IP (adres IPv4, IPv6, MAC, VLAN), parametrach urządzenia (typ/model urządzenia, wspierane standardy radiowe, maksymalna przepustowość, wspierana ilość strumieni przestrzennych), ilości przetransmitowanych danych z podziałem na aplikacje **6. Regulacje:** a. Zgodność z dyrektywą RoHS b. Zgodność z UL2043 **7. Zarządzanie przez kontroler/system zarządzania dostępny w publicznej chmurze o następujących funkcjach podstawowych:** a. Konfiguracja punktów dostępowych b. Zarządzanie politykami bezpieczeństwa c. Zarządzanie politykami QoS d. Automatyczny dobór mocy nadawania na punktach dostępowych e. Automatyczny dobór obsługiwanych kanałów na punktach dostępowych f. Monitorowanie pasma radiowego pod kątem wykrywania interferencji, pomiaru poziomu utylizacji i szumów w celu dynamicznej optymalizacji ustawień parametrów radiowych g. Obsługa kanałów DFS h. Zarządzanie mobilnością urządzeń i. Zarządzanie budową sieci kratowej j. Obsługa wgrania map pomieszczeń z możliwością rozmieszczenia AP k. Wyświetlanie rozmieszczenia AP oraz klientów (podłączonych oraz niepodłączonych) sieci bezprzewodowej na mapie pomieszczenia z zaznaczeniem miejsc o wysokiej i niskiej gęstości **8. Uproszczona instalacja urządzenia, która wymaga jedynie:** d. Podłączenia do sieci Internet e. Podania numeru seryjnego w systemie zarządzania i monitorowania siecią f. Wskazania sieci / lokalizacji, która określa konfigurację urządzenia **9. Wymaga się dostarczenia na urządzenie licencji** 3-letniej na jego wykorzystanie w zakresie opisanych funkcjonalności oraz serwisu wymiany urządzenia next-business-day.		
5.	**Okablowanie sieci**	**kpl.**	**1**
	• Należy doprowadzić okablowanie minimum kategorii 5 do punktów dostępowych od przełącznika sieciowego		

	• Odległość pomiędzy urządzeniami nie powinna być większa niż 100m • Okablowanie należy prowadzić w listwach kablowych		
6.	**Listwy kablowe**	**mb**	**1**
	• Należy dostarczyć i zamontować odpowiednią ilość listew kablowych w celu umieszczenia w nich przewodów pomiędzy przełącznikiem sieciowym a punktami dostępowymi		
7.	**Instalacja z konfiguracją**	**szt.**	**1**
	• Urządzenia takie jak punkty dostępowe należy zainstalować w odpowiednim miejscu do uzyskania optymalnego zasięgu w głównych punktach prowadzenia zajęć • Urządzenia takie jak Router i przełącznik sieciowy należy umieścić w szafie RACK dostępnej w szkole • Urządzenia należy skonfigurować i uruchomić		