Fundusze Europejskie Polska Cyfrowa

NASK PAŃSTWOWY INSTYTUT BADAWCZY

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Warszawa, 27 marca 2018 roku

**Do wszystkich Wykonawców**

Dotyczy: ***„Zakup urządzeń w ramach projektu Budowa szkolnych sieci dostępowych Ogólnopolskiej Sieci Edukacyjnej", Część nr 1 - Urządzenia brzegowe, CPE; Część nr 2 - Przełączniki sieci lokalnej, SW; Część nr 3 - Punkty dostępowe WLAN, AP"***

znak postępowania: **ZZ.2131.94.2018.TKI [OSE-D]**

## WYJAŚNIENIE TREŚCI ZAPYTANIA OFERTOWEGO oraz ZMIANA TREŚCI ZAPYTANIA OFERTOWEGO

Szanowni Państwo,

I. **Zgodnie z rozdz. VIII. pkt 7 Zapytania ofertowego, Zamawiający przekazuje poniżej pytania Wykonawcy dot. treści Zapytania ofertowego wraz z wyjaśnieniami Zamawiającego:**

**Pytanie nr 1:**
Dotyczy: SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA Część nr 2 Tabela 3. Wymagania obligatoryjne na SW punkt 4.11
Czy Zmawiający zgodzi się na dostarczenie przełącznika, który umożliwia za pomocą protokołu SNMP jedynie zdalny monitoring pod warunkiem, że posiada dodatkowo możliwość zdalnej konfiguracji za pomocą API i/lub poprzez urządzenie brzegowe CPE pochodzące od tego samego producenta?
**Odpowiedź nr 1:**
Zamawiający nie dopuszcza realizacji funkcji przez urządzenia zewnętrzne. Zamawiający nie przewiduje możliwości zapewnienia obecności urządzeń brzegowych jednego producenta we wszystkich lokalizacjach, w których będą instalowane przełączniki sieci lokalnej.

**Pytanie nr 2:**
Dotyczy: SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA Część nr 3 Tabela 5. Wymagania obligatoryjne na AP WiFi punkt 3.1
Regulacje i standard nie przewidują pracy w paśmie 2,4 GHz w standardzie 802.11ac. Prosimy o potwierdzenie czy w związku z tym Zamawiający zgodzi się na dostarczenie urządzenia, które wspiera standard 802.11ac jedynie w paśmie 5GHz?
**Odpowiedź nr 2:**
Ponieważ standard 802.11ac opisuje działanie sieci bezprzewodowej wyłącznie w paśmie 5GHz, to Zamawiający dopuszcza urządzenia, które wspierają ww. standard wyłącznie dla pasma 5GHz. W celu uniknięcia wszelkich nieporozumień Zamawiający wyjaśnia, że Urządzenia AP WLAN zgodnie z punkt 3.1

ul. Kolska 12, 01-045 Warszawa, tel.: +48 22 380 82 00, fax: +48 22 380 82 01
nask@nask.pl, www.nask.pl
NIP: 521-04-17-157, Regon: 010464542, KRS: 0000012938
Bank: Raiffeisen Bank Polska S.A., Numer konta: 28 1750 0009 0000 0000 0094 9997

wymagań powinny zapewniać pracę równoczesną w pasmach 2,4 GHz i 5 GHz zgodnie z odpowiednimi standardami.

**Pytanie nr 3**

Dotyczy: SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA Część nr 3 Tabela 5. Wymagania obligatoryjne na AP WiFi punkt 5.2, 5.3, 5.6

Czy dopuszczalne jest aby wymagania z punktów 5.2, 5.3, 5.6 były realizowane przez centralne urządzenie pełniące funkcję kontrolera lub Zamawiający zgodzi się na przeniesienie tych punktów do wymagań fakultatywnych?

**Odpowiedź nr 3:**

Zamawiający nie dopuszcza realizowania wymagań, opisanych w p. 5.2, 5.3, 5.6 Części 3, Tabeli 5 Wymagań obligatoryjnych na AP WiFi, przez centralne urządzenie pełniące funkcję kontrolera. Zamawiający nie zgadza się także na przeniesienie wymagań, opisanych w zdaniu poprzednim, do wymagań fakultatywnych.

II. **Zgodnie z rozdz. VIII. pkt 9 Zapytania ofertowego, Zamawiający dokonuje następujących zmian treści Zapytania ofertowego:**

1. **Zapytanie ofertowe** – wyrażenie ***„szkolenie"*** zastępuje się słowem ***„instruktaż"***. Zmiana dotyczy wszystkich miejsc w Zapytaniu ofertowym w których wystąpiło przedmiotowe słowo.

2. **Zapytanie ofertowe – w rozdziale IV. pkt 4 po ppkt 1 dodaje się pkt 2) oraz pkt 3) w następującym brzmieniu:**

   *2) Dokumenty składane przez podmioty zagraniczne:*

   *a) Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu, o którym mowa w pkt 4 ppkt 1 niniejszego rozdziału składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające, że: nie otwarto jego likwidacji ani nie ogłoszono upadłości, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.*

   *b) Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentu, o których mowa w ppkt 2a powyżej zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy. Dokument powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.*

   *3) Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów, o których mowa powyżej, jeżeli Zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 poz. 570 z późn. zm.).*

   *Jeżeli Wykonawca nie złoży wraz z Ofertą oświadczeń lub dokumentów, o których mowa powyżej zobowiązany jest wskazać w pkt. 10 Oferty jaki dokument Zamawiający może uzyskać oraz wskazać odpowiednią bazę danych.*

3. **Zapytanie ofertowe – w rozdziale VII. po pkt 6 dodaje się pkt 7 w następującym brzmieniu:**

7. *Wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę pod warunkiem, że nastąpi to przed wyznaczonym przez Zamawiającego terminem składania ofert. Powyższa zmiana oferty lub złożenie oświadczenia o wycofaniu oferty wymaga formy pisemnej. Zmiana oferty oraz oświadczenie o wycofaniu oferty powinno być opakowane i zaadresowane w ten sam sposób co oferta. Koperta będzie dodatkowo oznaczona określeniem „ZMIANA" lub „WYCOFANIE". Do oświadczenia o zmianie lub wycofaniu oferty Wykonawca dołączy stosowne dokumenty, potwierdzające, że oświadczenie o zmianie lub wycofaniu zostało podpisane przez osobę uprawnioną do reprezentowania Wykonawcy.*

4. **Zapytanie ofertowe – w Załączniku nr 4 do Zapytania po pkt 9 dodaje się pkt 10 w następującym brzmieniu:**

   10. ***OŚWIADCZAMY*** *o dostępności poniżej wskazanych oświadczeń lub dokumentów w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych**:*

| *Nazwa oświadczenia lub dokumentu (lub odpowiednie odesłanie do dokumentu wymaganego w Zapytaniu ofertowym)* | *Adres strony internetowej ogólnodostępnej i bezpłatnej bazy danych* |
|---|---|
| | |

*** wypełnić jeśli dotyczy*

5. **Zapytanie ofertowe – w Załączniku nr 1 do Zapytania – SOPZ , A – Część ogólna, pkt. 1 dodaje się zapis w następującym brzmieniu:**
   *Urządzenia muszą pochodzić z legalnych kanałów sprzedaży i posiadać wymagane certyfikaty i licencje pozwalające na pracę na terenie Polski (jako samodzielne urządzenia).*

6. **Zapytanie ofertowe – Załącznik nr 1 do Zapytania - SOPZ , B - Część szczegółowa, Część nr 1, Tabela 1. Wymagania obligatoryjne na CPE:**
   **Było:**

**Część nr 1**

Tabela 1. Wymagania obligatoryjne na CPE

| L.p. | Wymaganie – opis | min/max | wartość | jednostka |
|---|---|---|---|---|
| **1** | **Wymagania na interfejsy sieciowe** | | | |
| 1.1 | Interfejs w kierunku sieci zewnętrznej 1Gb/s - typ zależny od realizacji przyłącza (elektryczny RJ45 lub optyczny z użyciem modułu SFP). | min | 1 | szt. |
| 1.2 | Interfejs w kierunku sieci wewnętrznej RJ45 100/1000 Mb/s | min | 6 | szt. |
| **2** | **Funkcje** | | | |
| 2.1 | Funkcja routera brzegowego dla sieci wewnętrznej w szkole z obsługą routingu statycznego IPv4 i IPv6 | nd | nd | nd |
| 2.2 | Na wszystkich interfejsach znakowanie ramek Ethernet zgodnie z normą IEEE 802.1q (co najmniej dziesięciu VLAN'ów, z wartościami numerów VLAN z pełnego zakresu protokołu IEEE 802.1q) | nd | nd | nd |

| L.p. | Wymaganie – opis | min/max | wartość | jednostka |
|---|---|---|---|---|
| 2.3 | Funkcja firewall'a pełnostanowego (stateful inspection firewall) z filtrowaniem ruchu TCP/IP zarówno dla protokołu IPv4 jak i dla IPv6 | nd | nd | nd |
| 2.4 | Obsługa translacji adresów dla protokołu IPv4: statycznej 1:1, dynamicznej 1:n oraz przekierowywania portów | nd | nd | nd |
| 2.6 | Usługi dla sieci wewnętrznej: DHCP | nd | nd | nd |
| 2.7 | Klasyfikacja pakietów IP z użyciem DSCP | nd | nd | nd |
| 2.8 | Synchronizacja czasu do serwera NTP | nd | nd | nd |
| 2.9 | Możliwość uwierzytelniania użytkowników sieci przy pomocy serwerów: LDAP, RADIUS, Active Directory wraz z możliwością użycia lub współpracą z systemem zapewniającym mechanizm Single Sign On (SSO z AD i/lub z serwerem RADIUS) | nd | nd | nd |
| 2.10 | Możliwość uwierzytelniania użytkowników bez konieczności tworzenia lokalnej informacji o każdym użytkowniku na lokalnych urządzeniach wraz ze sprawdzeniem przynależności do uprawnionej grupy na podstawie atrybutów otrzymanych z zewnętrznych serwerów | nd | nd | nd |
| 2.11 | Możliwość tworzenia polityk filtrowania ruchu dla każdego uwierzytelnionego użytkownika/grupy użytkowników | nd | nd | nd |
| 2.12 | Funkcjonalność typu "captive portal" na interfejsach logicznych i fizycznych | nd | nd | nd |
| 2.13 | Urządzenie nie może wprowadzać licencyjnych ograniczeń na liczbę użytkowników i adresację IP albo posiadać takie licencje w wersji "bez ograniczeń" | nd | nd | nd |
| **3** | **Wydajność** | | | |
| 3.1 | Przepustowość z włączoną funkcją pełnostanowego firewall'a dla ruchu IMIX (suma ruchu przechodzącego przez urządzenie) przy dwudziestu regułach filtrowania (pojedyncze źródło, cel, serwis TCP/UDP/ICMP) : | min | 1,1 | Gb/s |
| 3.2 | Liczba równoczesnych sesji | min | 100 000 | szt. |
| 3.3 | Liczba nowych połączeń | min | 10 000 | sesji/s |
| 3.4 | ilość reguł bezpieczeństwa firewall'a | min | 500 | szt. |
| **4** | **Wymagania na zarządzanie** | | | |
| 4.1 | Współpraca z serwerem RADIUS w celu uwierzytelnienia administratora, możliwość tworzenia poziomów dostępu do urządzenia (minimum 2 - full access i read-only) oraz możliwość uwierzytelniania administratora poprzez klucz SSH. | nd | nd | nd |
| 4.2 | Kolekcjonowanie lokalne logów do celów analizy naruszeń bezpieczeństwa - w tym możliwość kierowania logów do zewnętrznego serwera | nd | nd | nd |
| 4.3 | Możliwość monitorowania ilości bieżącego ruchu na interfejsach fizycznych i logicznych | nd | nd | nd |
| 4.4 | Możliwość monitorowania i logowania stanu sesji tablicy translacji NAT | nd | nd | nd |
| 4.5 | Możliwość monitorowania i logowania przydziałów adresów przez DHCP | nd | nd | nd |
| 4.7 | Wsparcie dla zdalnego nadzoru (SNMP, SNMP-TRAP, syslog) | nd | nd | nd |

| L.p. | Wymaganie – opis | min/max | wartość | jednostka |
|---|---|---|---|---|
| 4.8 | Cała konfiguracja musi mieścić się w pojedynczym, czytelnym pliku tekstowym, plik musi być eksportowalny i importowalny.<br>Alternatywnie dopuszczalna jest możliwość konfiguracji opartej na interfejsach programistycznych API (typu REST/JSON lub równoważne) umożliwiającym bezpośrednio (lub z zewnętrznym, dostarczonym systemem zarządzania) podstawowe funkcje zarządzania konfiguracją takie jak: backup konfiguracji, wgranie konfiguracji, konfigurację urządzeń opartą na szablonach, wersjonowanie, odnotowanie autora zmiany itp. | nd | nd | nd |
| 4.9 | Szyfrowany kanał zarządzania urządzeniem w modelu klasycznym (SSH/HTTPS) lub poprzez chmurę | nd | nd | nd |
| 4.10 | Możliwość zdalnej aktualizacji oprogramowania; | nd | nd | nd |
| 4.11 | Możliwość podsłuchiwania na urządzeniu nagłówków i zawartości pakietów przechodzących przez urządzenie | nd | nd | nd |
| 4.12 | Wsparcie dla systemów zarządzania umożliwiających konfigurację polityk bezpieczeństwa, translacji adresów, przetrzymywanie obiektów sieciowych | nd | nd | nd |
| 4.13 | Wsparcie dla systemów zarządzania umożliwiających utworzenie konfiguracji z szablonu | nd | nd | nd |
| 4.14 | Monitorowanie zmiennych środowiskowych (temperatura CPU) | nd | nd | nd |
| 4.15 | Monitorowanie stanu zajętości pamięci RAM, pamięci nieulotnej i obciążenia CPU | nd | nd | nd |
| **5** | **Warunki fizyczne pracy** | | | |
| 5.1 | Napięcie zasilania | | 230 | V AC |
| 5.2 | Najwyższa temperatura pracy | min | 35 | °C |
| 5.3 | Najniższa temperatura pracy | maks. | 5 | °C |
| 5.4 | Najwyższa wilgotność pracy | min | 60 | % |
| 5.5 | Najniższa wilgotność pracy | maks. | 20 | % |

**Po zmianie jest:**

**Część nr 1**

Tabela 1. Wymagania obligatoryjne na CPE

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | uwagi |
|---|---|---|---|---|---|
| **1** | **Wymagania na interfejsy sieciowe** | | | | |
| 1.1 | Interfejs w kierunku sieci zewnętrznej 1Gb/s - typ zależny od realizacji przyłącza (elektryczny RJ45 lub optyczny z użyciem modułu SFP). | min | 1 | szt. | |
| 1.2 | Interfejs w kierunku sieci wewnętrznej RJ45 100/1000 Mb/s | min | 6 | szt. | |
| **2** | **Funkcje** | | | | |
| 2.1 | Funkcja routera brzegowego dla sieci wewnętrznej w szkole z obsługą routingu statycznego IPv4 i IPv6 | nd | nd | nd | |
| 2.2 | Na wszystkich interfejsach znakowanie ramek Ethernet zgodnie z normą IEEE 802.1q (co najmniej dziesięciu VLAN'ów, z wartościami numerów VLAN z pełnego zakresu protokołu IEEE 802.1q) | nd | nd | nd | |
| 2.3 | Funkcja firewall'a pełnostanowego (stateful inspection firewall) z filtrowaniem ruchu TCP/IP zarówno dla protokołu IPv4 jak i dla IPv6 | nd | nd | nd | |

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | uwagi |
|---|---|---|---|---|---|
| 2.4 | Obsługa translacji adresów dla protokołu IPv4: statycznej 1:1, dynamicznej 1:n oraz przekierowywania portów | nd | nd | nd | |
| **2.5** | **Translacja pomiędzy protokołami IPv4 i IPv6 (NAT46, NAT64)** | **nd** | **nd** | **nd** | |
| 2.6 | Usługi dla sieci wewnętrznej: DHCP | nd | nd | nd | |
| 2.7 | Klasyfikacja pakietów IP z użyciem DSCP | nd | nd | nd | |
| 2.8 | Synchronizacja czasu do serwera NTP | nd | nd | nd | |
| 2.9 | Możliwość uwierzytelniania użytkowników sieci przy pomocy serwerów: LDAP, RADIUS, Active Directory wraz z możliwością użycia lub współpracą z systemem zapewniającym mechanizm Single Sign On (SSO z AD i/lub z serwerem RADIUS) | nd | nd | nd | |
| 2.10 | Możliwość uwierzytelniania użytkowników bez konieczności tworzenia lokalnej informacji o każdym użytkowniku na lokalnych urządzeniach wraz ze sprawdzeniem przynależności do uprawnionej grupy na podstawie atrybutów otrzymanych z zewnętrznych serwerów | nd | nd | nd | |
| 2.11 | Możliwość tworzenia polityk filtrowania ruchu dla każdego uwierzytelnionego użytkownika/grupy użytkowników | nd | nd | nd | |
| 2.12 | Funkcjonalność typu "captive portal" na interfejsach logicznych i fizycznych | nd | nd | nd | |
| 2.13 | Urządzenie nie może wprowadzać licencyjnych ograniczeń na liczbę użytkowników i adresację IP albo posiadać takie licencje w wersji "bez ograniczeń" | nd | nd | nd | |
| **3** | **Wydajność** | | | | |
| 3.1 | Przepustowość z włączoną funkcją pełnostanowego firewall'a dla ruchu IMIX (suma ruchu przechodzącego przez urządzenie) przy dwudziestu regułach filtrowania (pojedyncze źródło, cel, serwis TCP/UDP/ICMP) : | min | 1,1 | Gb/s | |
| 3.2 | Liczba równoczesnych sesji | min | 100 000 | szt. | |
| 3.3 | Liczba nowych połączeń | min | 10 000 | **szt./s** | |
| 3.4 | ilość reguł bezpieczeństwa firewall'a | min | 500 | szt. | |
| **4** | **Wymagania na zarządzanie** | | | | |
| 4.1 | Współpraca z serwerem RADIUS w celu uwierzytelnienia administratora, możliwość tworzenia poziomów dostępu do urządzenia (minimum 2 - full access i read-only) oraz możliwość uwierzytelniania administratora poprzez klucz SSH. | nd | nd | nd | |
| 4.2 | Kolekcjonowanie lokalne logów do celów analizy naruszeń bezpieczeństwa - w tym możliwość kierowania logów do zewnętrznego serwera | nd | nd | nd | |
| 4.3 | Możliwość monitorowania ilości bieżącego ruchu na interfejsach fizycznych i logicznych | nd | nd | nd | |
| 4.4 | Możliwość monitorowania i logowania stanu sesji tablicy translacji NAT | nd | nd | nd | |
| 4.5 | Możliwość monitorowania i logowania przydziałów adresów przez DHCP | nd | nd | nd | |
| 4.7 | Wsparcie dla zdalnego nadzoru (SNMP, SNMP-TRAP, syslog) | nd | nd | nd | |

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | uwagi |
|---|---|---|---|---|---|
| 4.8 | Cała konfiguracja musi mieścić się w pojedynczym, czytelnym pliku tekstowym, plik musi być eksportowalny i importowalny.<br>Alternatywnie dopuszczalna jest możliwość konfiguracji opartej na interfejsach programistycznych API (typu REST/JSON lub równoważne) umożliwiającym bezpośrednio (lub z zewnętrznym, dostarczonym systemem zarządzania) podstawowe funkcje zarządzania konfiguracją takie jak: backup konfiguracji, wgranie konfiguracji, konfigurację urządzeń opartą na szablonach, wersjonowanie, odnotowanie autora zmiany itp. | nd | nd | nd | |
| 4.9 | Szyfrowany kanał zarządzania urządzeniem w modelu klasycznym (SSH/HTTPS) lub poprzez chmurę | nd | nd | nd | |
| 4.10 | Możliwość zdalnego **upgradu** oprogramowania; | nd | nd | nd | |
| 4.11 | Możliwość podsłuchiwania na urządzeniu nagłówków i zawartości pakietów przechodzących przez urządzenie | nd | nd | nd | |
| 4.12 | Wsparcie dla systemów zarządzania umożliwiających konfigurację polityk bezpieczeństwa, translacji adresów, przetrzymywanie obiektów sieciowych | nd | nd | nd | |
| 4.13 | Wsparcie dla systemów zarządzania umożliwiających utworzenie konfiguracji z szablonu | nd | nd | nd | |
| 4.14 | Monitorowanie zmiennych środowiskowych (temperatura CPU) | nd | nd | nd | |
| 4.15 | Monitorowanie stanu zajętości pamięci RAM, pamięci nieulotnej i obciążenia CPU | nd | nd | nd | |
| **5** | **Warunki fizyczne pracy** | | | | |
| 5.1 | Napięcie zasilania | | 230 | V | **AC** |
| 5.2 | Najwyższa temperatura pracy | min | 35 | °C | |
| 5.3 | Najniższa temperatura pracy | maks. | 5 | °C | |
| 5.4 | Najwyższa wilgotność pracy | min | 60 | % | **bez kondensacji pary wodnej** |
| 5.5 | Najniższa wilgotność pracy | maks. | 20 | % | |

7. **Zapytanie ofertowe – Załącznik nr 1 do Zapytania SOPZ , B - Część szczegółowa, Część nr 3, Tabela 5. Wymagania obligatoryjne na CPE**

**Było:**

**Część nr 3**

Tabela 5. Wymagania obligatoryjne na AP WiFi .

| L.p. | Wymaganie – opis | min/max | wartość | jednostka |
|---|---|---|---|---|
| 1. | **Wymagania na interfejsy sieciowe** | | | |
| 1.1 | Interfejs w kierunku sieci zewnętrznej TCP/IP - Ethernet RJ45 1 Gb/s | min | 1 | szt. |
| 2. | **Funkcje** | | | |
| 2.1 | Separacja ruchu dla poszczególnych SSID | nd | nd | nd |
| 2.2 | Obsługa VLAN IEEE 802.1q | nd | nd | nd |
| 2.3 | Mostkowanie SSID do VLAN | nd | nd | nd |
| 2.4 | Separacja klientów radiowych (uniemożliwienie ruchu pomiędzy różnymi klientami radiowymi w ramach jednego SSID) | nd | nd | nd |
| 2.5 | Możliwość użycia WPA2 Enterprice i Personal (z użyciem szyfrowania AES), uwierzytelnianie IEEE 802.1x (EAP) | nd | nd | nd |

| L.p. | Wymaganie – opis | min/max | wartość | jednostka |
|---|---|---|---|---|
| 2.6 | Zarządzanie pasmem, w szczególności ograniczenie max. użycia pasma per pojedynczy użytkownik | nd | nd | nd |
| 3. | **Wymagania radiowe** | | | |
| 3.1 | Praca równoczesna w paśmie 2,4 GHz i 5 GHz zgodnie ze standardem IEEE 802.11a/b/g/n/ac | nd | nd | nd |
| 3.2 | Liczba możliwych do jednoczesnego rozgłoszenia SSID | min | 4 | szt. |
| 3.3 | Min. 2x2 MIMO | nd | nd | nd |
| 3.4 | Maksymalna moc nadawania EIRP w paśmie 2,4 GHz | maks. | 20 | dBm |
| **3.5** | **Maksymalna moc nadawania EIRP w paśmie 5 GHz – zakres 5,150 – 5,350 GHz** | **maks.** | **23** | **dBm** |
| **3.6** | **Maksymalna moc nadawania EIRP w paśmie 5 GHz – zakres 5,470 – 5,725 GHz** | **maks.** | **30** | **dBm** |
| 3.7 | Możliwość konfiguracji użytkowanych kanałów radiowych w obu wymaganych pasmach | nd | nd | nd |
| 4 | **Wymagania wydajnościowe** | | | |
| 4.1 | Obsługiwana liczba jednoczesnych użytkowników | min | 20 | szt. |
| 4.2 | Przepustowość sieciowa | min | 800 | Mb/s |
| 5 | **Wymagania na zarządzanie** | | | |
| 5.1 | Dostęp do zarządzania z użyciem SSH lub HTTPS | nd | nd | nd |
| 5.2 | Współpraca z serwerem RADIUS w celu uwierzytelnienia administratora oraz możliwość uwierzytelniania administratora poprzez klucz SSH | nd | nd | nd |
| 5.3 | Wsparcie dla zdalnego nadzoru (SNMP, SNMP-TRAP, syslog) | nd | nd | nd |
| 5.4 | Cała konfiguracja musi mieścić się w pojedynczym pliku tekstowym, plik musi być eksportowalny i importowalny.<br>Alternatywnie dopuszczalna jest możliwość konfiguracji opartej na interfejsach programistycznych API (typu REST/JSON lub równoważne) umożliwiającym bezpośrednio (lub z zewnętrznym, dostarczonym systemem zarządzania) podstawowe funkcje zarządzania konfiguracją takie jak: backup konfiguracji, wgranie konfiguracji, konfigurację urządzeń opartą na szablonach, wersjonowanie, odnotowanie autora zmiany itp. | nd | nd | nd |
| 5.5 | Szyfrowany kanał zarządzania urządzeniem w modelu klasycznym (SSH / HTTPS) lub poprzez chmurę | nd | nd | nd |
| 5.6 | Możliwość zdalnej aktualizacji oprogramowania; | nd | nd | nd |
| **6** | **Warunki fizyczne pracy** | | | |
| 6.1 | Zasilanie przez PoE w standardzie IEEE 802.3at lub IEEE 802.3af z zasilaczem (injector) na napięcie 230V AC | nd | nd | nd |
| 6.2 | Najwyższa temperatura pracy | min | 35 | °C |
| 6.3 | Najniższa temperatura pracy | maks. | 5 | °C |
| 6.4 | Najwyższa wilgotność pracy | min | 60 % | bez kondensacji pary wodnej |
| 6.5 | Najniższa wilgotność pracy | max | 20 | % |

**Po zmianie jest:**

**Część nr 3**

Tabela 5. Wymagania obligatoryjne na AP WiFi .

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | **uwagi** |
|---|---|---|---|---|---|
| 1. | **Wymagania na interfejsy sieciowe** | | | | |
| 1.1 | Interfejs w kierunku sieci zewnętrznej TCP/IP - Ethernet RJ45 1 Gb/s | min | 1 | szt. | |
| 2. | **Funkcje** | | | | |

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | uwagi |
|---|---|---|---|---|---|
| 2.1 | Separacja ruchu dla poszczególnych SSID | nd | nd | nd | |
| 2.2 | Obsługa VLAN IEEE 802.1q | nd | nd | nd | |
| 2.3 | Mostkowanie **(bridge)** SSID do VLAN | nd | nd | nd | |
| 2.4 | Separacja klientów radiowych (uniemożliwienie ruchu pomiędzy różnymi klientami radiowymi w ramach jednego SSID) | nd | nd | nd | |
| 2.5 | Możliwość użycia WPA2 Enterprice i Personal (z użyciem szyfrowania AES), uwierzytelnianie IEEE 802.1x (EAP) | nd | nd | nd | |
| 2.6 | Zarządzanie pasmem, w szczególności ograniczenie max. użycia pasma per pojedynczy użytkownik | nd | nd | nd | |
| 3. | **Wymagania radiowe** | | | | |
| 3.1 | Praca równoczesna w paśmie 2,4 GHz i 5 GHz zgodnie ze standardem IEEE 802.11a/b/g/n/ac | nd | nd | nd | |
| 3.2 | Liczba możliwych do jednoczesnego rozgłoszenia SSID | min | 4 | szt. | |
| 3.3 | Min. 2x2 MIMO | nd | nd | nd | |
| 3.4 | Maksymalna moc nadawania EIRP w paśmie 2,4 GHz | maks. | 20 | dBm | |
| 3.5 | Możliwość konfiguracji użytkowanych kanałów radiowych w obu wymaganych pasmach | nd | nd | nd | |
| 4 | **Wymagania wydajnościowe** | | | | |
| 4.1 | Obsługiwana liczba jednoczesnych użytkowników | min | 20 | szt. | |
| 4.2 | Przepustowość sieciowa | min | 800 | Mb/s | |
| 5 | **Wymagania na zarządzanie** | | | | |
| 5.1 | Dostęp do zarządzania z użyciem SSH lub HTTPS | nd | nd | nd | |
| 5.2 | Współpraca z serwerem RADIUS w celu uwierzytelnienia administratora oraz możliwość uwierzytelniania administratora poprzez klucz SSH | nd | nd | nd | |
| 5.3 | Wsparcie dla zdalnego nadzoru (SNMP, SNMP-TRAP, syslog) | nd | nd | nd | |
| 5.4 | Cała konfiguracja musi mieścić się w pojedynczym pliku tekstowym, plik musi być eksportowalny i importowalny. Alternatywnie dopuszczalna jest możliwość konfiguracji opartej na interfejsach programistycznych API (typu REST/JSON lub równoważne) umożliwiającym bezpośrednio (lub z zewnętrznym, dostarczonym systemem zarządzania) podstawowe funkcje zarządzania konfiguracją takie jak: backup konfiguracji, wgranie konfiguracji, konfigurację urządzeń opartą na szablonach, wersjonowanie, odnotowanie autora zmiany itp. | nd | nd | nd | |
| 5.5 | Szyfrowany kanał zarządzania urządzeniem w modelu klasycznym (SSH / HTTPS) lub poprzez chmurę | nd | nd | nd | |
| 5.6 | Możliwość **zdalnego updatu** oprogramowania; | nd | nd | nd | |
| **6** | **Warunki fizyczne pracy** | | | | |
| 6.1 | Zasilanie przez PoE w standardzie IEEE 802.3at lub IEEE 802.3af z zasilaczem (injector) na napięcie 230V AC | nd | nd | nd | |
| 6.2 | Najwyższa temperatura pracy | min | 35 | °C | |
| 6.3 | Najniższa temperatura pracy | maks. | 5 | °C | |
| 6.4 | Najwyższa wilgotność pracy | min | 60 | % | **bez kondensacji pary wodnej** |
| 6.5 | Najniższa wilgotność pracy | max | 20 | % | |

8. **Zapytanie ofertowe –Załącznik nr 6 do Zapytania - Opis techniczny oferowanych urządzeń, Część nr 1 - Urządzenia brzegowe, CPE, Tabela 1. Wymagania obligatoryjne na urządzenia brzegowe, CPE**

**Było:**

**Część nr 1 – Urządzenia brzegowe, CPE**

Tabela 1. Wymagania obligatoryjne na urządzenia brzegowe, CPE.

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | Zgodność z wymaganiem [tak / nie] |
|---|---|---|---|---|---|
| **1** | **Wymagania na interfejsy sieciowe** | | | | |
| 1.1 | Interfejs w kierunku sieci zewnętrznej 1Gb/s - typ zależny od realizacji przyłącza (elektryczny RJ45 lub optyczny z użyciem modułu SFP) | min | 1 | szt. | |
| 1.2 | Interfejs w kierunku sieci wewnętrznej RJ45 100/1000 Mb/s | min. | 6 | szt. | |
| **2** | **Funkcje** | | | | |
| 2.1 | Funkcja routera brzegowego dla sieci wewnętrznej w szkole z obsługą routingu statycznego IPv4 i IPv6 | | | | |
| 2.2 | Na wszystkich interfejsach znakowanie ramek Ethernet zgodnie z normą IEEE 802.1q (co najmniej dziesięciu VLAN'ów, z wartościami numerów VLAN z pełnego zakresu protokołu IEEE 802.1q) | | | | |
| 2.3 | Funkcja firewall'a pełnostanowego (stateful inspection firewall) z filtrowaniem ruchu TCP/IP zarówno dla protokołu IPv4 jak i dla IPv6 | | | | |
| 2.4 | Obsługa translacji adresów dla protokołu IPv4: statycznej 1:1, dynamicznej 1:n oraz przekierowywania portów | | | | |
| 2.6 | Usługi dla sieci wewnętrznej: DHCP | | | | |
| 2.7 | Klasyfikacja pakietów IP z użyciem DSCP | | | | |
| 2.8 | Synchronizacja czasu do serwera NTP | | | | |
| 2.9 | Możliwość uwierzytelniania użytkowników sieci przy pomocy serwerów: LDAP, RADIUS, Active Directory wraz z możliwością użycia lub współpracą z systemem zapewniającym mechanizm Single Sign On (SSO z AD i/lub z serwerem RADIUS) | | | | |
| 2.10 | Możliwość uwierzytelniania użytkowników bez konieczności tworzenia lokalnej informacji o każdym użytkowniku na lokalnych urządzeniach wraz ze sprawdzeniem przynależności do uprawnionej grupy na podstawie atrybutów otrzymanych z zewnętrznych serwerów | | | | |
| 2.11 | Możliwość tworzenia polityk filtrowania ruchu dla każdego uwierzytelnionego użytkownika/grupy użytkowników | | | | |
| 2.12 | Funkcjonalność typu "captive portal" na interfejsach logicznych i fizycznych | | | | |
| 2.13 | Urządzenie nie może wprowadzać licencyjnych ograniczeń na liczbę użytkowników i adresację IP albo posiadać takie licencje w wersji "bez ograniczeń" | | | | |
| **3** | **Wydajność** | | | | |
| 3.1 | Przepustowość z włączoną funkcją pełnostanowego firewall'a dla ruchu IMIX (suma ruchu przechodzącego przez urządzenie) przy dwudziestu regułach filtrowania (pojedyncze źródło, cel, serwis TCP/UDP/ICMP) : | min | 1,1 | Gb/s | |
| 3.2 | Liczba równoczesnych sesji | min | 100 000 | szt. | |
| 3.3 | Liczba nowych połączeń | min | 10 000 | sesji/s | |
| 3.4 | ilość reguł bezpieczeństwa firewall'a | min | 500 | | |
| **4** | **Wymagania na zarządzanie** | | | | |
| 4.1 | Współpraca z serwerem RADIUS w celu uwierzytelnienia administratora, możliwość tworzenia poziomów dostępu do urządzenia (minimum 2 - full access i read-only) oraz możliwość uwierzytelniania administratora poprzez klucz SSH | | | | |
| 4.2 | Kolekcjonowanie lokalne logów do celów analizy naruszeń bezpieczeństwa - w tym możliwość kierowania logów do zewnętrznego serwera | | | | |
| 4.3 | Możliwość monitorowania ilości bieżącego ruchu na interfejsach fizycznych i logicznych | | | | |
| 4.4 | Możliwość monitorowania i logowania stanu sesji tablicy translacji NAT | | | | |
| 4.5 | Możliwość monitorowania i logowania przydziałów adresów przez DHCP | | | | |
| 4.7 | Wsparcie dla zdalnego nadzoru (SNMP, SNMP-TRAP, syslog) | | | | |
| 4.8 | Cała konfiguracja musi mieścić się w pojedynczym, czytelnym pliku tekstowym, plik musi być eksportowalny i importowalny.<br>Alternatywnie dopuszczalna jest możliwość konfiguracji opartej na interfejsach programistycznych | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | API (typu REST/JSON lub równoważne) umożliwiającym bezpośrednio (lub z zewnętrznym, dostarczonym systemem zarządzania) podstawowe funkcje zarządzania konfiguracją takie jak: backup konfiguracji, wgranie konfiguracji, konfigurację urządzeń opartą na szablonach, wersjonowanie, odnotowanie autora zmiany itp. | | | | |
| 4.9 | Szyfrowany kanał zarządzania urządzeniem w modelu klasycznym (SSH/HTTPS) lub poprzez chmurę | | | | |
| 4.10 | Możliwość zdalnej aktualizacji oprogramowania; | | | | |
| 4.11 | Możliwość podsłuchiwania na urządzeniu nagłówków i zawartości pakietów przechodzących przez urządzenie | | | | |
| 4.12 | Wsparcie dla systemów zarządzania umożliwiających konfigurację polityk bezpieczeństwa, translacji adresów, przetrzymywanie obiektów sieciowych | | | | |
| 4.13 | Wsparcie dla systemów zarządzania umożliwiających utworzenie konfiguracji z szablonu | | | | |
| 4.14 | Monitorowanie zmiennych środowiskowych (temperatura CPU) | | | | |
| 4.15 | Monitorowanie stanu zajętości pamięci RAM, pamięci nieulotnej i obciążenia CPU | | | | |
| **5** | **Warunki fizyczne pracy** | | | | |
| 5.1 | Napięcie zasilania | | 230 | V AC | |
| 5.2 | Najwyższa temperatura pracy | min | 35 | °C | |
| 5.3 | Najniższa temperatura pracy | maks. | 5 | °C | |
| 5.4 | Najwyższa wilgotność pracy | min | 60 | % | |
| 5.5 | Najniższa wilgotność pracy | maks. | 20 | % | |
| **6.** | **Wymagania formalne** | | | | |
| 6.1 | Urządzenia nie znajdują się na liście End-of-Sale i/lub End-of-Life producenta | | | | |
| 6.2 | Urządzenia posiadają niezbędne certyfikaty i licencje dopuszczające je do eksploatacji na terenie Polski w zakładanych warunkach instalacji | | | | |

**Po zmianie jest:**

## Część nr 1 – Urządzenia brzegowe, CPE

Tabela 1. Wymagania obligatoryjne na urządzenia brzegowe, CPE.

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | Zgodność z wymaganiem [tak / nie] |
|---|---|---|---|---|---|
| **1** | **Wymagania na interfejsy sieciowe** | | | | |
| 1.1 | Interfejs w kierunku sieci zewnętrznej 1Gb/s - typ zależny od realizacji przyłącza (elektryczny RJ45 lub optyczny z użyciem modułu SFP) | min | 1 | szt. | |
| 1.2 | Interfejs w kierunku sieci wewnętrznej RJ45 100/1000 Mb/s | min. | 6 | szt. | |
| **2** | **Funkcje** | | | | |
| 2.1 | Funkcja routera brzegowego dla sieci wewnętrznej w szkole z obsługą routingu statycznego IPv4 i IPv6 | | | | |
| 2.2 | Na wszystkich interfejsach znakowanie ramek Ethernet zgodnie z normą IEEE 802.1q (co najmniej dziesięciu VLAN'ów, z wartościami numerów VLAN z pełnego zakresu protokołu IEEE 802.1q) | | | | |
| 2.3 | Funkcja firewall'a pełnostanowego (stateful inspection firewall) z filtrowaniem ruchu TCP/IP zarówno dla protokołu IPv4 jak i dla IPv6 | | | | |
| 2.4 | Obsługa translacji adresów dla protokołu IPv4: statycznej 1:1, dynamicznej 1:n oraz przekierowywania portów | | | | |
| **2.5** | **Translacja pomiędzy protokołami IPv4 i IPv6 (NAT46, NAT64)** | | | | |
| 2.6 | Usługi dla sieci wewnętrznej: DHCP | | | | |
| 2.7 | Klasyfikacja pakietów IP z użyciem DSCP | | | | |
| 2.8 | Synchronizacja czasu do serwera NTP | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 2.9 | Możliwość uwierzytelniania użytkowników sieci przy pomocy serwerów: LDAP, RADIUS, Active Directory wraz z możliwością użycia lub współpracą z systemem zapewniającym mechanizm Single Sign On (SSO z AD i/lub z serwerem RADIUS) | | | | |
| 2.10 | Możliwość uwierzytelniania użytkowników bez konieczności tworzenia lokalnej informacji o każdym użytkowniku na lokalnych urządzeniach wraz ze sprawdzeniem przynależności do uprawnionej grupy na podstawie atrybutów otrzymanych z zewnętrznych serwerów | | | | |
| 2.11 | Możliwość tworzenia polityk filtrowania ruchu dla każdego uwierzytelnionego użytkownika/grupy użytkowników | | | | |
| 2.12 | Funkcjonalność typu "captive portal" na interfejsach logicznych i fizycznych | | | | |
| 2.13 | Urządzenie nie może wprowadzać licencyjnych ograniczeń na liczbę użytkowników i adresację IP albo posiadać takie licencje w wersji "bez ograniczeń" | | | | |
| **3** | **Wydajność** | | | | |
| 3.1 | Przepustowość z włączoną funkcją pełnostanowego firewall'a dla ruchu IMIX (suma ruchu przechodzącego przez urządzenie) przy dwudziestu regułach filtrowania (pojedyncze źródło, cel, serwis TCP/UDP/ICMP) : | min | 1,1 | Gb/s | |
| 3.2 | Liczba równoczesnych sesji | min | 100 000 | szt. | |
| 3.3 | Liczba nowych połączeń | min | 10 000 | **szt./s** | |
| 3.4 | ilość reguł bezpieczeństwa firewall'a | min | 500 | szt. | |
| **4** | **Wymagania na zarządzanie** | | | | |
| 4.1 | Współpraca z serwerem RADIUS w celu uwierzytelnienia administratora, możliwość tworzenia poziomów dostępu do urządzenia (minimum 2 - full access i read-only) oraz możliwość uwierzytelniania administratora poprzez klucz SSH | | | | |
| 4.2 | Kolekcjonowanie lokalne logów do celów analizy naruszeń bezpieczeństwa - w tym możliwość kierowania logów do zewnętrznego serwera | | | | |
| 4.3 | Możliwość monitorowania ilości bieżącego ruchu na interfejsach fizycznych i logicznych | | | | |
| 4.4 | Możliwość monitorowania i logowania stanu sesji tablicy translacji NAT | | | | |
| 4.5 | Możliwość monitorowania i logowania przydziałów adresów przez DHCP | | | | |
| 4.7 | Wsparcie dla zdalnego nadzoru (SNMP, SNMP-TRAP, syslog) | | | | |
| 4.8 | Cała konfiguracja musi mieścić się w pojedynczym, czytelnym pliku tekstowym, plik musi być eksportowalny i importowalny.<br>Alternatywnie dopuszczalna jest możliwość konfiguracji opartej na interfejsach programistycznych API (typu REST/JSON lub równoważne) umożliwiającym bezpośrednio (lub z zewnętrznym, dostarczonym systemem zarządzania) podstawowe funkcje zarządzania konfiguracją takie jak: backup konfiguracji, wgranie konfiguracji, konfigurację urządzeń opartą na szablonach, wersjonowanie, odnotowanie autora zmiany itp. | | | | |
| 4.9 | Szyfrowany kanał zarządzania urządzeniem w modelu klasycznym (SSH/HTTPS) lub poprzez chmurę | | | | |
| 4.10 | Możliwość zdalnej aktualizacji oprogramowania; | | | | |
| 4.11 | Możliwość podsłuchiwania na urządzeniu nagłówków i zawartości pakietów przechodzących przez urządzenie | | | | |
| 4.12 | Wsparcie dla systemów zarządzania umożliwiających konfigurację polityk bezpieczeństwa, translacji adresów, przetrzymywanie obiektów sieciowych | | | | |
| 4.13 | Wsparcie dla systemów zarządzania umożliwiających utworzenie konfiguracji z szablonu | | | | |
| 4.14 | Monitorowanie zmiennych środowiskowych (temperatura CPU) | | | | |
| 4.15 | Monitorowanie stanu zajętości pamięci RAM, pamięci nieulotnej i obciążenia CPU | | | | |
| **5** | **Warunki fizyczne pracy** | | | | |
| 5.1 | Napięcie zasilania | | 230 | V AC | |
| 5.2 | Najwyższa temperatura pracy | min | 35 | °C | |
| 5.3 | Najniższa temperatura pracy | maks. | 5 | °C | |
| 5.4 | Najwyższa wilgotność pracy | min | 60 | % | |
| 5.5 | Najniższa wilgotność pracy | maks. | 20 | % **bez kondensacji pary** | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | **wodnej** | |
| **6.** | **Wymagania formalne** | | | | |
| 6.1 | Urządzenia nie znajdują się na liście End-of-Sale i/lub End-of-Life producenta | | | | |
| 6.2 | Urządzenia posiadają niezbędne certyfikaty i licencje dopuszczające je do eksploatacji na terenie Polski w zakładanych warunkach instalacji | | | | |

9. **Zapytanie ofertowe – Załącznik nr 6 do Zapytania - Opis techniczny oferowanych urządzeń, Część nr 3 – Punkt dostępowy WLAN, AP, Tabela 1. Wymagania obligatoryjne na AP:**

**Było:**

**Część nr 3 – Punkt dostępowy WLAN, AP**

Tabela 1. Wymagania obligatoryjne na AP

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | **Zgodność z wymaganiem [tak / nie]** |
|---|---|---|---|---|---|
| 1. | **Wymagania na interfejsy sieciowe** | | | | |
| 1.1 | Interfejs w kierunku sieci zewnętrznej TCP/IP - Ethernet RJ45 1 Gb/s | min | 1 | szt. | |
| 2. | **Funkcje** | | | | |
| 2.1 | Separacja ruchu dla poszczególnych SSID | | | | |
| 2.2 | Obsługa VLAN IEEE 802.1q | | | | |
| 2.3 | Mostkowanie SSID do VLAN | | | | |
| 2.4 | Separacja klientów radiowych (uniemożliwienie ruchu pomiędzy różnymi klientami radiowymi w ramach jednego SSID) | | | | |
| 2.5 | Możliwość użycia WPA2 Enterprise i Personal (z użyciem szyfrowania AES), uwierzytelnianie IEEE 802.1x (EAP) | | | | |
| 2.6 | Zarządzanie pasmem, w szczególności ograniczenie max. użycia pasma per pojedynczy użytkownik | | | | |
| 3. | **Wymagania radiowe** | | | | |
| 3.1 | Praca równoczesna w paśmie 2,4 GHz i 5 GHz zgodnie ze standardem IEEE 802.11a/b/g/n/ac | | | | |
| 3.2 | Liczba możliwych do jednoczesnego rozgłoszenia SSID | min | 4 | szt. | |
| 3.3 | Min. 2x2 MIMO | | | | |
| 3.4 | Maksymalna moc nadawania EIRP w paśmie 2,4 GHz | maks. | 20 | dBm | |
| **3.5** | **Maksymalna moc nadawania EIRP w paśmie 5 GHz – zakres 5,150 – 5,350 GHz** | **maks.** | **23** | **dBm** | |
| **3.6** | **Maksymalna moc nadawania EIRP w paśmie 5 GHz – zakres 5,470 – 5,725 GHz** | **maks.** | **30** | **dBm** | |
| 3.7 | Możliwość konfiguracji użytkowanych kanałów radiowych w obu wymaganych pasmach | | | | |
| 4 | **Wymagania wydajnościowe** | | | | |
| 4.1 | Obsługiwana liczba jednoczesnych użytkowników | min | 20 | szt. | |
| 4.2 | Przepustowość sieciowa | min | 800 | Mb/s | |
| 5 | **Wymagania na zarządzanie** | | | | |

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | Zgodność z wymaganiem [tak / nie] |
|---|---|---|---|---|---|
| 5.1 | Dostęp do zarządzania z użyciem SSH lub HTTPS | | | | |
| 5.2 | Współpraca z serwerem RADIUS w celu uwierzytelnienia administratora oraz możliwość uwierzytelniania administratora poprzez klucz SSH | | | | |
| 5.3 | Wsparcie dla zdalnego nadzoru (SNMP, SNMP-TRAP, syslog) | | | | |
| 5.4 | Cała konfiguracja musi mieścić się w pojedynczym pliku tekstowym, plik musi być eksportowalny i importowalny.<br>Alternatywnie dopuszczalna jest możliwość konfiguracji opartej na interfejsach programistycznych API (typu REST/JSON lub równoważne) umożliwiającym bezpośrednio (lub z zewnętrznym, dostarczonym systemem zarządzania) podstawowe funkcje zarządzania konfiguracją takie jak: backup konfiguracji, wgranie konfiguracji, konfigurację urządzeń opartą na szablonach, wersjonowanie, odnotowanie autora zmiany, itp. | | | | |
| 5.5 | Szyfrowany kanał zarządzania urządzeniem w modelu klasycznym (SSH / HTTPS) lub poprzez chmurę | | | | |
| 5.6 | Możliwość zdalnej aktualizacji oprogramowania; | | | | |
| **6** | **Warunki fizyczne pracy** | | | | |
| 6.1 | Zasilanie przez PoE w standardzie IEEE 802.3at lub IEEE 802.3af z zasilaczem (injector) na napięcie 230V AC | | | | |
| 6.2 | Najwyższa temperatura pracy | min | 35 | °C | |
| 6.3 | Najniższa temperatura pracy | maks. | 5 | °C | |
| 6.4 | Najwyższa wilgotność pracy | min | 60 % | bez kondensacji pary wodnej | |
| 6.5 | Najniższa wilgotność pracy | max | 20 | % | |
| **7.** | **Wymagania formalne** | | | | |
| 7.1 | Urządzenia nie znajdują się na liście End-of-Sale i/lub End-of-Life producenta | | | | |
| 7.2 | Urządzenia posiadają niezbędne certyfikaty i licencje dopuszczające je do eksploatacji na terenie Polski w zakładanych warunkach instalacji. | | | | |

**Po zmianie jest:**

## Część nr 3 – Punkt dostępowy WLAN, AP

Tabela 1. Wymagania obligatoryjne na AP

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | Zgodność z wymaganiem [tak / nie] |
|---|---|---|---|---|---|
| 1. | **Wymagania na interfejsy sieciowe** | | | | |
| 1.1 | Interfejs w kierunku sieci zewnętrznej TCP/IP - Ethernet RJ45 1 Gb/s | min | 1 | szt. | |
| 2. | **Funkcje** | | | | |
| 2.1 | Separacja ruchu dla poszczególnych SSID | | | | |
| 2.2 | Obsługa VLAN IEEE 802.1q | | | | |
| 2.3 | Mostkowanie **(bridge)** SSID do VLAN | | | | |
| 2.4 | Separacja klientów radiowych (uniemożliwienie ruchu pomiędzy różnymi klientami radiowymi w ramach jednego SSID) | | | | |
| 2.5 | Możliwość użycia WPA2 Enterprise i Personal (z użyciem szyfrowania AES), uwierzytelnianie IEEE 802.1x (EAP) | | | | |
| 2.6 | Zarządzanie pasmem, w szczególności ograniczenie max. użycia pasma per pojedynczy użytkownik | | | | |
| 3. | **Wymagania radiowe** | | | | |

| L.p. | Wymaganie – opis | min/max | wartość | jednostka | **Zgodność z wymaganiem [tak / nie]** |
|---|---|---|---|---|---|
| 3.1 | Praca równoczesna w paśmie 2,4 GHz i 5 GHz zgodnie ze standardem IEEE 802.11a/b/g/n/ac | | | | |
| 3.2 | Liczba możliwych do jednoczesnego rozgłoszenia SSID | min | 4 | szt. | |
| 3.3 | Min. 2x2 MIMO | | | | |
| 3.4 | Maksymalna moc nadawania EIRP w paśmie 2,4 GHz | maks. | 20 | dBm | |
| 3.5 | Możliwość konfiguracji użytkowanych kanałów radiowych w obu wymaganych pasmach | | | | |
| 4 | **Wymagania wydajnościowe** | | | | |
| 4.1 | Obsługiwana liczba jednoczesnych użytkowników | min | 20 | szt. | |
| 4.2 | Przepustowość sieciowa | min | 800 | Mb/s | |
| 5 | **Wymagania na zarządzanie** | | | | |
| 5.1 | Dostęp do zarządzania z użyciem SSH lub HTTPS | | | | |
| 5.2 | Współpraca z serwerem RADIUS w celu uwierzytelnienia administratora oraz możliwość uwierzytelniania administratora poprzez klucz SSH | | | | |
| 5.3 | Wsparcie dla zdalnego nadzoru (SNMP, SNMP-TRAP, syslog) | | | | |
| 5.4 | Cała konfiguracja musi mieścić się w pojedynczym pliku tekstowym, plik musi być eksportowalny i importowalny.<br>Alternatywnie dopuszczalna jest możliwość konfiguracji opartej na interfejsach programistycznych API (typu REST/JSON lub równoważne) umożliwiającym bezpośrednio (lub z zewnętrznym, dostarczonym systemem zarządzania) podstawowe funkcje zarządzania konfiguracją takie jak: backup konfiguracji, wgranie konfiguracji, konfigurację urządzeń opartą na szablonach, wersjonowanie, odnotowanie autora zmiany, itp. | | | | |
| 5.5 | Szyfrowany kanał zarządzania urządzeniem w modelu klasycznym (SSH / HTTPS) lub poprzez chmurę | | | | |
| 5.6 | Możliwość zdalnego **updatu** oprogramowania; | | | | |
| **6** | **Warunki fizyczne pracy** | | | | |
| 6.1 | Zasilanie przez PoE w standardzie IEEE 802.3at lub IEEE 802.3af z zasilaczem (injector) na napięcie 230V AC | | | | |
| 6.2 | Najwyższa temperatura pracy | min | 35 | °C | |
| 6.3 | Najniższa temperatura pracy | maks. | 5 | °C | |
| 6.4 | Najwyższa wilgotność pracy | min | 60 % | bez kondensacji pary wodnej | |
| 6.5 | Najniższa wilgotność pracy | max | 20 | % | |
| **7.** | **Wymagania formalne** | | | | |
| 7.1 | Urządzenia nie znajdują się na liście End-of-Sale i/lub End-of-Life producenta | | | | |
| 7.2 | Urządzenia posiadają niezbędne certyfikaty i licencje dopuszczające je do eksploatacji na terenie Polski w zakładanych warunkach instalacji. | | | | |

**III. Zamawiający informuje, iż termin składania ofert pozostaje bez zmian tj. ofertę należy złożyć do dnia 12 kwietnia 2018 r. do godz. 12:00**

**Powyższe informacje należy traktować jako integralną część Zapytania ofertowego.**

DYREKTOR FINANSOWY
Naukowej i Akademickiej Sieci Komputerowej

*Tomasz Chabior*

---

*podpis Zamawiającego*