Miejscowość: \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Załącznik nr 1**

**FORMULARZ OFERTOWY**

**ZAPYTANIE OFERTOWE nr 25/ Sieć komputerowa**

Nazwa Wykonawcy:

Adres:

NIP:

Nr telefonu:

Adres e-mail:

Dane osoby do kontaktu:

W odpowiedzi na zapytanie ofertowe pn. *ZAPYTANIE OFERTOWE nr 25/ Sieć komputerowa* oferuję wykonanie przedmiotu zamówienia, zgodnie z wymogami i zakresem określonym w zapytaniu ofertowym, za:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Przedmiot zamówienia** | **Waluta oferty**  **(PLN / EUR)** | **Ogółem wartość NETTO we wskazanej walucie** | **Wartość podatku VAT we wskazanej walucie** | **Ogółem wartość BRUTTO we wskazanej walucie** |
| Sieć komputerowa |  |  |  |  |

**Całkowita wartość zamówienia brutto słownie:**

1. **Ceny wskazane w tabeli uwzględniają wszystkie koszty związane z wykonaniem przedmiotu zamówienia i są cenami stałymi w okresie obowiązywania umowy.**
2. Cały przedmiot zamówienia będzie posiadał aktualne atesty i certyfikaty bezpieczeństwa poświadczające zgodność z normami obowiązującymi w Unii Europejskiej oraz zgodności i certyfikaty określone w zapytaniu ofertowym.
3. Zobowiązujemy się do wykonania przedmiotu zamówienia z zastosowaniem następujących urządzeń i materiałów:

(***W każdym wierszu tabeli należy podać informację czy/jak oferowany sprzęt spełnia wymagania Zamawiającego. Dopuszcza się wypełnienie wierszy w formule TAK/NIE. W przypadku braku zamieszczenia informacji (braku wypełnienia) w którymkolwiek z obowiązkowych pól, oferta zostanie odrzucona. Wykonawca tam gdzie jest to możliwe wskazuje również „Typ/model oferowanego urządzenia” oraz „Producenta”).***

|  |  |  |
| --- | --- | --- |
| **Lp** | **Parametry techniczne przedmiotu zamówienia** | **Potwierdzenie spełnienia /**  **Parametry oferowane[[1]](#footnote-2)** |
| **1.** | **Urządzenie typu Firewall – 2 sztuki** | Typ:  Model:  Producent: |
| 1. Typ urządzenia:  a. Urządzenie klasy UTM (Unified Threat Management)  b. Urządzenie typu wolnostojącego appliance  2. Wyposażenie:  a. 4 interfejsy LAN typu 1000Base-T oraz dwa interfejsy 10 Gbps SFP+  b. 2 interfejsy WAN 10Gbps SFP+ oraz dwa interfejsy WAN RJ45 2.5Gbps  c. Interfejs USB do podłączenia modemu 3G/4G/LTE  d. Dysk twardy o pojemności 1TB  3. Parametry wydajnościowe:  a. Wydajność zapory ogniowej L3 z NAT 5 Gbps  d. Wydajność urządzenia z włączonymi wszystkimi funkcjami bezpieczeństwa (NAT, VPN (Split-tunnel), filtrowanie treści, traffic shaping, anti-virus/anti-phishing, IPS): 2 Gbps  e. Maksymalna ilość połączeń: 250000  g. Przepustowość dla ruch VPN: 2Gbps  h. Maksymalna liczba sesji VPN: 1000  4. Parametry fizyczne  a. wysokość 1RU  b. możliwość montażu w szafie 19”  c. praca w temperaturach 0 – 40 st.C  d. waga do 5kg  e. urządzenie wyposażone w dwa zasilacze 230V AC  5. Urządzenie realizuje funkcje zintegrowanego systemu zarządza¬nia zagrożeniami 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. Tworzenie niezależnego filtru blokującego ruch sieciowy w warstwie 3 dla ruchu kierowanego do łącza komórkowego 3G/4G/LTE  c. Możliwość zablokowania lub ograniczenia dla określonych adresów IP odpowiedzi na ICMP ping oraz odpowiedzi do wbudowanego serwera WEB dla interfejsów zewnętrznych  d. Firewalling ruchu aplikacyjnego wg. typu aplikacji w warstwie 7:  · Blogging  · Email  · File Sharing  · Gaming  · News  · Online backup  · Peer-to-peer  · Social web  · 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 pochodzącego lub wysyłanego do danego kraju  · Możliwość blokowania ruchu internetowego niepochodzącego lub wysyłanego do danego kraju  · Możliwość blokowania ruchu poprzez podanie zakresów adresów IP i portów  e. Ograniczanie ruchu sieciowego (traffic shaping):  · Na łączach WAN niezależnie dla każdego łącza poprzez podanie z granularnością do 1 Mb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz)  · Na łączu komórkowym 3G/4G/LTE poprzez podanie z granularnością do 1 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz)  · Na użytkownika sieci poprzez podanie limitu z granularnością do 1 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz)  · Dla określonego ruchu aplikacyjnego w warstwie 7 określonego powyżej w punkcie 5d z granularnością do 1 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz). Urządzenie umożliwia tworzenie do 8 reguł ograniczających ruch sieciowy, z których każda może się składać z dowolnej kombinacji aplikacji sieciowych. Dla każdej z reguł jest możliwość priorytetyzacji ruchu (wysoki priorytet, normalny priorytet, niski priorytet) oraz oznaczania ruchu danym znacznikiem DSCP (od 0 do 7)  f. 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, usługi finansowe, hazard, gry, strony wulgarne, strony hakerskie, rasizm oraz szerzenie nienawiści, myślistwo oraz wędkarstwo, strony nielegalne, wyszukiwarki zdjęć oraz filmów, keyloggery oraz monitory stacji, źródła malware, wojskowość i militaria, oprogramowanie peer to peer, strony płatne, blogi, phishing i inne zagrożenia internetowe, 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, poczta webowa  g. Blokowanie treści dla dorosłych w wynikach działania najpopularniejszych wyszukiwarek internetowych: Google, Yahoo, Bing – funkcja działa dla wyszukiwania niezaszyfrowanego  h. Blokowanie dostępu do zaszyfrowanego wyszukiwania treści internetowych w serwisie Google.  i. Funkcja YouTube for Schools  j. Możliwość definiowana własnej listy zabronionych (czarna lista) lub dozwolonych (biała lista) stron URL  k. Wykrywanie i ochrona przed malware  l. Ochrona antywirusowa i antyphishingowa  m. Ochrona IPS i IDS  6. Urządzenie realizuje monitoring i analizę ruchu sieciowego w zakresie:  a. Wykres ilości ruchu generowanego przez wszystkich użytkowników, jednego użytkownika lub grupę użytkowników w ciągu dwóch ostatnich godzin, ostatniego dnia, ostatniego tygodnia i ostatniego miesiąca  b. Wykres ilości użytkowników podłączonych do sieci chronionej w ciągu dwóch ostatnich godzin, ostatniego dnia, ostatniego tygodnia i ostatniego miesiąca  c. Dokłada informacja, jakie aplikacje sieciowe używają użytkownicy w sieci chronionej dla wszystkich użytkowników lub dla wybranego użytkownika z podaniem wolumenu przesłanego ruchu  7. Urządzenie realizuje funkcje koncentratora VPN(dla IKEv1 oraz dla IKEv2) dla łączenia ze sobą placówek (site-to-site vpn przy użyciu tuneli IPSEC) 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  · konfiguracja sieci VPN typu site-to-site jest bardzo prosta i wymaga tylko podania:  · Trybu pracy tuneli  · Topologii sieci VPN  · Wybrania urządzenia centralnego dla topologii gwiazdy  · Wybrania, które sieci lokalne w danej placówce mają możliwość komunikacji z siecią VPN  Cała reszta konfiguracji sieci VPN dokonywana jest automatycznie przez oprogramowanie zarządzające i obejmuje między innymi: konfigurację tuneli VPN, konfigurację protokołów IKE/IPSec oraz wymiana kluczy i update tablic routingu,  · Urządzenie posiada możliwość blokowania ruchu sieciowego na poziomie reguła 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 oraz dedykowanego klienta opartego po połączenie SSL.  · Automatyczna rejestracja do dynamicznego DNS na potrzeby dostępu VPN dla Klientów (Client VPN) z możliwością zdefiniowana nazwy dla każdego z linków WAN niezależnie  · Możliwość tworzenia kont na lokalnych zasobach systemu do zarządzania oraz możliwość integracji z serwerem RADIUS oraz Acrive Directory  c. Możliwość tworzenia tuneli IPSec do urządzeń innych producentów  d. Możliwość pracy w parze niezawodnościowej w trybie WARM dla potrzeb koncentracji ruchu VPN  8. Urządzenie realizuje funkcje routera do sieci Internet w zakresie:  a. Fizyczne podłączenie do łącza lub łączy internetowych operatora (2 x WAN )+ interfejs USB do podłączenia modemu 3G/4G/LTE  b. NAT / PAT  c. Tryb pracy przeźroczystej (Bridge warstwy 2)  d. Serwer DHCP  · Konfiguracja czasu dzierżawy,  · Konfiguracja serwerów DNS lub użycie serwerów podanych przez nadrzędny serwer DHCP lub użycie serwerów publicznych np. Google Public DNS lub Open DNS  · Konfiguracja opcji DHCP  · Konfiguracja zakresów adresów zarezerwowanych lub przydzielanych statycznie  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 z możliwością określenia proporcji wynikających np. z różnej prędkości łączy  · 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. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu np. tworzącymi VPN bez ograniczeń ilościowych w zakresie:  a. Monitoring  · Monitoring stanu i kondycji jednego urządzenia lub wielu urządzeń w jednym widoku  · Monitoring statusu tuneli VPN w zakresie:  · Status połączenia (stan tunelu) przez ostatni dzień lub ostatni tydzień lub ostatnie 30 dni  · Ilość ruchu przesłanego przez VPN dla danej placówki przez ostatni dzień lub ostatni tydzień  a. Sumaryczna  b. W relacji do innej placówki  · Opóźnienie dla ruchu przesłanego przez VPN dla danej placówki przez ostatni dzień lub ostatni tydzień  a. Średnie  b. W relacji do innej placówki  · W zakresie jednego urządzenia monitoring:  · Status urządzenia  · Numer seryjny  · Przypisane znaczniki wyszukiwania  · Adres pocztowy instalacji urządzenia  · Status interfejsów WAN wraz z przypisanymi adresami IP  · Zarejestrowana nazwa w dynamicznym DNS  · 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  · Uruchomienie PING z danego urządzenia do innego urządzenia poprzez podanie nazwy hosta w Internecie, adresu IP lub adresu MAC  · Traceroute z podaniem linku WAN, który ma być użyty do wyznaczania ścieżki  · Możliwość przełączenia diod LED w tryb mrugania w celu oznaczenia urządzenia  · Możliwość restartu zdalnego urządzenia  · Wysyłania alertów mailowych do wszystkich lub wybranych administratorów sieci w przypadku, gdy:  · Urządzenie jest niedostępne (offline) przez 5 lub 10 lub 15 lub 30 lub 60 minut  · Zmieni się status podstawowego łącza WAN  · Nastąpi wyczerpanie puli adresów IP serwera DHCP  · Stwierdzono konflikt adresów IP w sieci  · Zmienił się status łącza komórkowego  · Został wykryty w sieci nielegalny serwer DHCP  · W przypadku pracy urządzenia w układzie niezawodnościowym z drugim urządzeniem nastąpi wykrycie awarii i zmian ról urządzeń  b. Konfiguracja  · Konfiguracja i uruchomienie sieci VPN site-to-site  · Konfiguracja i zmiana ustawień jednego lub wielu urządzeń na raz w zakresie:  · Tryb pracy, jako router lub bridge warstwy 3  · NAT  · Routing statyczny/dynamiczny 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:  · Godziny i dni tygodnia dostępności lub niedostępności dostępu do sieci  · Ograniczenie pasma transmisji z granularnością do 1 Kb/s określonych wartości dla kierunku UP (na zewnątrz) oraz DOWN (do wewnątrz)  · Określenie reguł firewallingu w warstwie 3 i 7  · Określenie reguł ograniczania ruchu sieciowego (traffic shaping)  · Określenie reguł filtracji stron i treści internetowych  · Określenie listy dozwolonych i niedozwolonych adresów URL  · Uruchomienie lub wyłączenie filtrowania wyników przeszukiwania w wyszukiwarkach internetowych  · Włączenie lub wyłączenie funkcji filtrowania treści YouTube  · System posiada mechanizm konfiguracji party o szablony umożliwiający łatwe instalowanie wielu urządzeń sieciowych w wielu lokalizacjach i jednoczesną zmianę parametrów konfiguracyjnych wielu urządzeń na raz  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. Uproszczona instalacja urządzenia, która wymaga jedynie:  a. podłączenie do sieci Internet  b. podanie jego numeru seryjnego w systemie zarządzania i monitorowania siecią oraz  c. wskazanie sieci / lokalizacji, która określa jego konfigurację  11. Urządzenie obsługuje SNMP v2c oraz SYSLOG  12. Urządzenie obsługuje PPPoE dla łącza WAN  13. Urządzenia muszą pracować jako urządzenia wysokiej dostępności.  14. Urządzenie wymaga licencji czasowych na wykorzystanie w zakresie wymaganej funkcjonalności :  · filtrowania treści  · filtrowania geograficznego  · ochrony IDS/IPS  · Blokowania treści dla dorosłych w wynikach działania najpopularniejszych wyszukiwarek internetowych  · Blokowania dostępu do zaszyfrowanego wyszukiwania treści internetowych w serwisie Google.  · Funkcji YouTube for Schools  · Definiowana własnej listy zabronionych (czarna lista) lub dozwolonych (biała lista) stron URL  · Wykrywania i ochrony przed malware  · Ochrony antywirusowej i antyphishingowej  15. Wykonawca musi dostarczyć licencje na okres 5 lat (lub jeśli to możliwewykorzystać licencję Zamawiającego - Meraki MX105 Advanced Security License and Support). Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania.  16. Urządzenie objęte jest przez producenta sprzętu pełną gwarancją lifetime warranty (nie krótszą niż 5 lat). |  |
|  |
| **2.** | **Urządzenie typu 1 - przełącznik– 2 sztuki** | Typ:  Model:  Producent: |
| 1. Typ i liczba portów:   12 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 możliwe do obsadzenia następującymi rodzajami wkładek:   * 10Gigabit Ethernet 10GBase-SR, * 10Gigabit Ethernet 10GBase-LR, * 10Gigabit Ethernet typu twinax (SFP+ - SFP+),  1. Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb): 2. 8x1/10/25G typu SFP/SFP+/SFP28 3. 2x40G QSFP 4. Porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia następującymi rodzajami wkładek:  * 10GBASE-SR * 10GBASE-LR * QSFP-40G-CSR4 * 10GSFP+Cu(Twinax)  1. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:  * Przepustowość w ramach stosu – minimum 480Gb/s, * 8 urządzeń w stosie, * Zarządzanie przełącznikiem poprzez dedykowany panel zarządzania w chmurze producenta. * Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, * Możliwość współdzielenia mocy zasilaczy (grupa do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania” mocy dla innych jednostek w stosie),  1. Zasilanie i chłodzenie: 2. Redundantne i wymienne moduły wentylatorów, 3. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), 4. Parametry wydajnościowe:   · Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):  · Przepustowość przełącznika (switching capacity): ] 900 Gb/s (bez podłączenia do stosu)  · Prędkość przesyłania (forwarding rate): 740 Mpps (bez podłączenia do stosu),  · Bufor pakietów – 16MB   1. Pamięć DRAM – 16 GB 2. Pamięć flash – 16GB 3. Obsługa: 4. 1000 aktywnych sieci VLAN 5. 32000 adresów MAC 6. 8192 tras IPv4 7. 256 interfejsów L3 8. Jumbo frame 9198B 9. Obsługa IGMP/ PIM-SM lub PIM-ASM/RFC4604/ 10. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: 11. IEEE 802.1w Rapid Spanning Tree 12. Per-VLAN Rapid Spanning Tree (PVRST+) 13. IEEE 802.1s Multi-Instance Spanning Tree 14. Obsługa protokołu LLDP (IEEE 802.1ab) 15. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego 16. Możliwość uruchomienia funkcji serwera DHCP 17. Mechanizmy związane z bezpieczeństwem sieci:   · Wiele poziomów dostępu administracyjnego - RBAC. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu.  · Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,  · Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,  · Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,  · Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,  · Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,  · Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,  · Funkcjonalność flexible authentication (możliwość wyboru uwierzytelniania – 802.1X i/lub uwierzytelnianie w oparciu o MAC adres  · Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection ,  · Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard   1. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:  * sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, * bezpieczna sekwencja uruchamiania, * sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia. * Mechanizmy związane z zapewnieniem jakości usług w sieci: * Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, * Kontrola sztormów dla ruchu broadcast/multicast/unicast, * Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;  1. Obsługa protokołów i mechanizmów routingu:  * Routing statyczny dla IPv4 i IPv6, * Routing dynamiczny – OSPF  1. Przełącznik 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  * Przełącznik 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.),  1. Parametry fizyczne:  * Możliwość montażu w szafie rack 19”, * Wysokość urządzenia 1 RU, * Głębokość chassis urządzenia z wentylatorami i zasilaczami mniejsza niż 50 cm,  1. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników(jeśli wymaga to dodatkowej licencji nie jest to wymagane na tym etapie postępowania):  * Statycznie w oparciu o port do którego podłączona jest stacja, * Statycznie w oparciu o VLAN, w którym pracuje stacja, * Statycznie w oparciu o adres IP stacji, * Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;  1. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu (jeśli wymaga to dodatkowej licencji nie jest to wymagane na tym etapie postępowania), 2. Wyposażenie urządzenia:  * Przełącznik wyposażony w zasilacz redundantny o mocy identyczny jak zasilacz podstawowy, * Przełącznik wyposażony jest w moduł do łączenia w stos data wraz z kablem stakującym o długości 50 cm * Przełącznik wyposażony jest w kabel o długości 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną, * Przełącznik wyposażony jest w następujące moduły/interfejsowe SFP+ pochodzące z oferty producenta przełącznika lub kompatybilne z dostarczonym urządzeniem: * 10GBASE-LR – 8 sztuk  1. Licencje dostępne muszą być dostarczone w na okres 5 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania. 2. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu. 3. Urządzenie musi zostać objęte jest gwarancją lifetime warranty oraz serwisem wymiany urządzenia z możliwa wysyłka na następny dzień roboczy przez producenta sprzętu |  |
| **3.** | **Urządzenie typu 2 - przełącznik– 6 sztuk** | Typ:  Model:  Producent: |
| 1. Typ i liczba portów:  • 48 portów 10/100/1000BaseT RJ-45 ze wsparciem PoE/PoE+, budżet mocy dla PoE/PoE+ wymagany jest na poziomie 370W  2. Przełącznik wyposażony musi być w moduł/porty zainstalowane na stałe – 4x10G  3. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:  • Przepustowość w ramach stosu - 80Gb/s,  • Do 8 jednostek w stosie  4. Wydajność przełączania min 176 Gbps  5. Obsługa:  • warstwy trzeciej L3 i routingu statycznego  • uwierzytelnienia 802.1X  • protokołu RSTP  • DHCP snooping  • Dynamic ARP Inspection  • 802.1q VLAN  • listy kontroli dostępu ACL IPv4 oraz IPv6  • QoS dla głosu i video  • Broadcast Storm Control  6. Zarządzenie oraz integracja:  • możliwość dodania lokalizacji na mapie  • automatyczne umiejscowienie w topologii sieciowej L2 w systemie zarządzającym,  • możliwość przygotowania konfiguracji urządzenia, zanim zostanie podłączone do sieci, urządzenie zaciągnie konfigurację automatycznie po podłączeniu.  • raportowanie o odłączeniu urządzenia od sieci (e-mail).  • możliwość zdalnej diagnozy problemów np. narzędzia do zdalnego przechwytywania pakietów, ping  • możliwość zarządzania portami przez graficzny interfejs  • statystyki ruchu na portach oraz analizy ruchu użytkowników  • bezpieczne aktualizacje oprogramowania firmware z możliwością ustalenia harmonogramu  • Wyposażenie dodatkowe: kabel zasilający  7. Wsparcie:  • dostęp do pomocy producenta 24/7, przez czas trwania licencji  • usługa instalacji i konfiguracji zestawu w siedzibie zamawiającego.  8. Wbudowany zasilacz.  9. Przełącznik musi zostać dostarczony wraz z kablami do stack. Kable muszą pochodzić od producenta sprzętu.  10. Przełącznik wyposażony jest w następujące moduły/interfejsowe SFP+ pochodzące z oferty producenta przełącznika lub kompatybilne z dostarczonym urządzeniem:  a. 10GBASE-LR – 2 sztuki  11. Licencje dostępne muszą być dostarczone w na okres 5 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania.  12. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu.  13. Urządzenie musi zostać objęte gwarancją lifetime warranty oraz serwisem wymiany urządzenia z możliwa wysyłka na następny dzień roboczy przez producenta sprzętu |  |
| **4.** | **Urządzenie typu 3 - przełącznik– 2 sztuki** | Typ:  Model:  Producent: |
| 1. Typ i liczba portów:  • 48 portów 10/100/1000BaseT RJ-45 ze wsparciem PoE/PoE+, budżet mocy dla PoE/PoE+ wymagany jest na poziomie 740W  2. Przełącznik wyposażony musi być w moduł/porty zainstalowane na stałe – 4x10G  3. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:  • Przepustowość w ramach stosu - 80Gb/s,  • Do 8 jednostek w stosie  4. Wydajność przełączania min 176 Gbps  5. Obsługa:  • warstwy trzeciej L3 i routingu statycznego  • uwierzytelnienia 802.1X  • protokołu RSTP  • DHCP snooping  • Dynamic ARP Inspection  • 802.1q VLAN  • listy kontroli dostępu ACL IPv4 oraz IPv6  • QoS dla głosu i video  • Broadcast Storm Control  6. Zarządzenie oraz integracja:  • możliwość dodania lokalizacji na mapie  • automatyczne umiejscowienie w topologii sieciowej L2 w systemie zarządzającym,  • możliwość przygotowania konfiguracji urządzenia, zanim zostanie podłączone do sieci, urządzenie zaciągnie konfigurację automatycznie po podłączeniu.  • raportowanie o odłączeniu urządzenia od sieci (e-mail).  • możliwość zdalnej diagnozy problemów np. narzędzia do zdalnego przechwytywania pakietów, ping  • możliwość zarządzania portami przez graficzny interfejs  • statystyki ruchu na portach oraz analizy ruchu użytkowników  • bezpieczne aktualizacje oprogramowania firmware z możliwością ustalenia harmonogramu  • Wyposażenie dodatkowe: kabel zasilający  7. Wsparcie:  • dostęp do pomocy producenta 24/7, przez czas trwania licencji  • usługa instalacji i konfiguracji zestawu w siedzibie zamawiającego.  8. Wbudowany zasilacz.  9. Przełącznik wyposażony jest w następujące moduły/interfejsowe SFP+ pochodzące z oferty producenta przełącznika lub kompatybilne z dostarczonym urządzeniem:  a. 10GBASE-LR – 2 sztuki  10. Licencje dostępne muszą być dostarczone w na okres 5 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania.  11. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu.  12. Urządzenie musi zostać objęte gwarancją lifetime warranty oraz serwisem wymiany urządzenia z możliwa wysyłka na następny dzień roboczy przez producenta sprzętu |  |
| **5.** | **Urządzenie typu 4 - przełącznik– 2 sztuki** | Typ:  Model:  Producent: |
|  | 1. Typ i liczba portów:  • 24 porty 10/100/1000BaseT RJ-45 ze wsparciem PoE/PoE+, budżet mocy dla PoE/PoE+ wymagany jest na poziomie 370W  2. Przełącznik wyposażony musi być w moduł/porty zainstalowane na stałe – 4x10G  3. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:  • Przepustowość w ramach stosu - 80Gb/s,  • Do 8 jednostek w stosie  4. Wydajność przełączania min 128 Gbps  5. Obsługa:  • warstwy trzeciej L3 i routingu statycznego  • uwierzytelnienia 802.1X  • protokołu RSTP  • DHCP snooping  • Dynamic ARP Inspection  • 802.1q VLAN  • listy kontroli dostępu ACL IPv4 oraz IPv6  • QoS dla głosu i video  • Broadcast Storm Control  6. Zarządzenie oraz integracja:  • możliwość dodania lokalizacji na mapie  • automatyczne umiejscowienie w topologii sieciowej L2 w systemie zarządzającym,  • możliwość przygotowania konfiguracji urządzenia, zanim zostanie podłączone do sieci, urządzenie zaciągnie konfigurację automatycznie po podłączeniu.  • raportowanie o odłączeniu urządzenia od sieci (e-mail).  • możliwość zdalnej diagnozy problemów np. narzędzia do zdalnego przechwytywania pakietów, ping  • możliwość zarządzania portami przez graficzny interfejs  • statystyki ruchu na portach oraz analizy ruchu użytkowników  • bezpieczne aktualizacje oprogramowania firmware z możliwością ustalenia harmonogramu  • Wyposażenie dodatkowe: kabel zasilający  7. Wsparcie:  • dostęp do pomocy producenta 24/7, przez czas trwania licencji  • usługa instalacji i konfiguracji zestawu w siedzibie zamawiającego.  8. Wbudowany zasilacz.  9. Przełącznik wyposażony jest w następujące moduły/interfejsowe SFP+ pochodzące z oferty producenta przełącznika lub kompatybilne z dostarczonym urządzeniem:  a. 10GBASE-LR – 2 sztuki  10. Licencje dostępne muszą być dostarczone w na okres 5 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania.  11. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu.  12. Urządzenie musi zostać objęte gwarancją lifetime warranty oraz serwisem wymiany urządzenia z możliwa wysyłka na następny dzień roboczy przez producenta sprzętu |  |
| **6.** | **Urządzenie typu 4 - przełącznik– 1 sztuka** | Typ:  Model:  Producent: |
| 1. Typ i liczba portów:  • 24 porty 10/100/1000BaseT RJ-45  2. Przełącznik wyposażony musi być w moduł/porty zainstalowane na stałe – 4x10G  3. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:  • Przepustowość w ramach stosu - 80Gb/s,  • Do 8 jednostek w stosie  4. Wydajność przełączania min 128 Gbps  5. Obsługa:  • warstwy trzeciej L3 i routingu statycznego  • uwierzytelnienia 802.1X  • protokołu RSTP  • DHCP snooping  • Dynamic ARP Inspection  • 802.1q VLAN  • listy kontroli dostępu ACL IPv4 oraz IPv6  • QoS dla głosu i video  • Broadcast Storm Control  6. Zarządzenie oraz integracja:  • możliwość dodania lokalizacji na mapie  • automatyczne umiejscowienie w topologii sieciowej L2 w systemie zarządzającym,  • możliwość przygotowania konfiguracji urządzenia, zanim zostanie podłączone do sieci, urządzenie zaciągnie konfigurację automatycznie po podłączeniu.  • raportowanie o odłączeniu urządzenia od sieci (e-mail).  • możliwość zdalnej diagnozy problemów np. narzędzia do zdalnego przechwytywania pakietów, ping  • możliwość zarządzania portami przez graficzny interfejs  • statystyki ruchu na portach oraz analizy ruchu użytkowników  • bezpieczne aktualizacje oprogramowania firmware z możliwością ustalenia harmonogramu  • Wyposażenie dodatkowe: kabel zasilający  7. Wsparcie:  • dostęp do pomocy producenta 24/7, przez czas trwania licencji  • usługa instalacji i konfiguracji zestawu w siedzibie zamawiającego.  8. Wbudowany zasilacz.  9. Licencje dostępne muszą być dostarczone w na okres 5 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania.  10. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu.  11. Urządzenie musi zostać objęte gwarancją lifetime warranty oraz serwisem wymiany urządzenia z możliwa wysyłka na następny dzień roboczy przez producenta sprzętu |  |
| **7.** | **Specyfikacja – punkt dostępowy typu 1 – 10 szt. (biuro)** | Typ:  Model:  Producent: |
| 1. Obudowa:  • Z przeznaczeniem do wewnątrz;  • Możliwość umieszczenie na suficie (mocowanie ścienne/sufitowe na wyposażeniu);  • Możliwość zainstalowania fizycznego zabezpieczenia (np. Kensington Lock);  • Posiada przycisk reset  • Posiada diode/diody LED informujące o stanie pracy radia: uruchomiony/połączony/brak połączenia/ aktualizacji oprogramowania/online  2. Antena:  • Wewnętrzna, dookólna, zintegrowana  • 2.4 GHz: osiągalnym zyskiem min. 3 dBi, antena wewnętrzna, dookólna w azymucie  • 5 GHz: osiągalnym zyskiem min. 5 dBi, antena wewnętrzna, dookólna w azymucie  • 6 GHz: osiągalnym zyskiem min. 4 dBi, antena wewnętrzna, dookólna w azymucie  3. Radio:  • 2.4 GHz 802.11b/g/n/ax  • 5 GHz 802.11a/n/ac/ax  • 6 GHz 802.11ax  • 2.4 GHz, 5 GHz, and 6 GHz trójzakresowy Air Marshal WIDS/WIPS  • 2.4 GHz Bluetooth Low Energy z obsługą beacon oraz ei skanowaniem umożliwiającym jednoczesną pracę wszystkich pięciu radiach.  4. Interfejsy:  • 1x 100/1000/2.5G BASE-T Ethernet (RJ45)  • 1x złącze zasilania  • USB 2.0 z możliwym budżetem mocy 4,5 W  5. Bezpieczeństwo:  • Zintegrowana zapora sieciowa warstwy 7 z zarządzaniem polityką urządzeń mobilnych  • WIDS/WIPS w czasie rzeczywistym 24x7 z alarmowaniem i automatycznym powstrzymywaniem obcych punktów dostępowych za pośrednictwem dedykowanego radia skanującego  • Elastyczny dostęp dla gości z izolacją urządzeń  • Znakowanie VLAN (802.1q) i tunelowanie za pomocą IPsec VPN  • Raportowanie zgodności PCI  • WPA2-PSK, WPA2-Enterprise, WPA3 - Personal, WPA3 - Enterprise, WPA3 - Enhanced Open (OWE)  • Uwierzytelnianie lokalne EAP – EAP-TTLS/PAP, PEAP-GTC, EAP-TLS  • Zaawansowany standard szyfrowania (AES)  6. System bezprzewodowy musi obsługiwać stanową zaporę ogniową warstwy aplikacji, która potrafi identyfikować, klasyfikować i priorytetyzować aplikacje, wykorzystując inteligencję warstwy 7. Aplikacje powinny być kształtowane ruchowo, aby zapewnić, że aplikacje rekreacyjne (takie jak BitTorrent, Pandora, Spotify itp.) nie zużywają całej dostępnej przepustowości.  7. System bezprzewodowy musi obsługiwać identyfikację typów urządzeń klienckich (np. iPad, Android, iPhone, Windows itp.) i stosować ustawienia zabezpieczeń do tych urządzeń bez konieczności używania dodatkowych urządzeń czy licencji. Na przykład: iPady w sieci SSID dla uczniów mogą mieć dostęp tylko do internetu, z ograniczeniem prędkości do 512 kbps i bez ruchu peer-to-peer.  8. Usługi bramkowe umożliwiające płynne działanie Airplay, drukowania, iTunes i innych usług opartych na Bonjour w sieci bezprzewodowej  9. System bezprzewodowy powinien mieć wbudowany dostęp gościnny, bez potrzeby stosowania dodatkowych urządzeń lub licencji dla użytkowników gościnnych.  10. Punkty dostępowe muszą mieć możliwość uruchamiania lokalnych reguł zapory ogniowej warstw 2, 3 i 7.  11. Punkty dostępowe muszą obsługiwać co najmniej 15 SSID jednocześnie.  12. Możliwości i kompatybilność ze standardami 802.11 ax, 802.11ac Wave 2 i 802.11n:  • UL/DL-OFDMA  • TWT  • BSS coloring - zmniejszenie negatywne zakłóceń pochodzących od innych komórek sieci WLAN działających w tym samym pasmie częstotliwości (Funkcję może być włączona poprzez aktualizacje oprogramowania sprzętowego)wsparcie SU-MIMO i DL MU-MIMO  • MRC  • 802.11ax wykorzystującą technologie beamforming  • kanały 20 and 40 MHz (802.11n)  • kanały 20, 40, 80 MHz (802.11ac Wave 2)  • kanały 20, 40, 80, and 160 MHz (802.11ax)  • Wsparcie do 1024-QAM dla 2.4 GHz, 5 GHz, i 6 GHz  • Wykorzystanie metod agregacji ramek A-MPDU, A-MSDU  • 2.4 GHz 2x2 multiple-input, multiple-output (MIMO) z 2 strumienieniami przestrzennymi  • 5 GHz: 4x4 multiple-input, multiple-output (MIMO) z 4 strumienieniami przestrzennymi  • 6 GHz: 4x4 multiple-input, multiple-output (MIMO) z 4 strumienieniami przestrzennymi  13. Zarządzanie i integracja:  • Możliwość dodania lokalizacji na mapie  • analiza połączeń urządzeń do sieci bezprzewodowej - L2, DHCP, DNS.  • Możliwość przygotowania konfiguracji urządzenia, zanim zostanie podłączone do sieci, urządzenie zaciągnie konfigurację automatycznie po podłączeniu.  • Raportowanie o odłączeniu urządzenia od sieci (e-mail).  • Dostępna odseparowana sieć dla gości.  • Możliwość dostępu do sieci bezprzewodowej po podaniu danych w captive portalu  14. Obsługa standardu 802.11ax (Wi-Fi 6E) :  • 4x4:4 uplink/downlink MU-MIMO z czterema strumienieniami przestrzennymi (5 GHz and 6 GHz)  • 2x2:2 uplink/downlink MU-MIMO z dwoma strumienieniami przestrzennymi (2.4 GHz)  • przepustowość zagregowana 7.49 Gbps (PHY data rates)  15. Zasilanie:  • Zasilanie przez Ethernet: 42 - 57V (zgodne z PoE+ i UPoE)  • Możliwość użycia zasilacza DC (54V) – nie jest wymagany  • Pobór mocy: 30,5 W z obsługą USB (UPOE) i 25 W bez obsługi USB (PoE+)  16. Waga:  • nie więcej niż 1,61 kg  17. Wymiary:  • maksymalne wymiary 241.5 mm x 241.5 mm x 57.4 mm  18. Opcjonalna funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;  19. Licencje dostępne muszą być dostarczone w na okres 5 lat. Licencje oprócz wyżej wymienionych funkcjonalności muszą gwarantować dostęp do chmurowego zarządzania, wsparcia producenta oraz aktualizacji oprogramowania.  20. Urządzenie zarządzane i monitorowane jest poprzez aplikację zarządzającą dostępną w chmurze. Za pomocą tej aplikacji możliwe jest zarządzanie wieloma urządzeniami danego typu. Zarządzanie musi odbywać się z poziomu tej samej aplikacji zarówno dla firewall jak i dla przełączników.  21. Urządzenie musi zostać objęte gwarancją lifetime warranty oraz serwisem wymiany urządzenia z możliwa wysyłka na następny dzień roboczy przez producenta sprzętu. |  |
| **8.** | **Punkt dostępowy typu 2 – 31 szt. (magazyn)** | Typ:  Model:  Producent: |
| • Punkt dostępu bezprzewodowego:  · obsługa standardów IEEE 802.11a/b/g/n/ac/ax  · obsługa OFDMA (uplink/downlink), TWT, BSS Coloring  · obsługa MU-MIMO – min. 4x4:4 (w 2,4 GHz oraz 5 GHz)  · obsługa kanałów 20, 40 MHz dla 802.11n  · obsługa kanałów 20, 40, 80,160 MHz dla 802.11ac/ax  · obsługa prędkości PHY do 3,4 Gbps (ac)  · obsługa prędkośći PHY do 5,3 Gbps (ax)  · obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)  · obsługa beamforming 802.11 ac/ax  · obsługa MRC (Maximal Ratio Combining)  · konfigurowalna moc nadajnika  · dla zakresu 2.4 GHz: do 100 mW  · dla zakresu 5GHz: do 200 mW  · praca dwuzakresowa w pasmach: 2,4 GHz oraz 5 GHz  · zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:  · 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  · uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w  · obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)  · 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 pod kątem zagrożeń bezpieczeństwa (wykrywanie obcych AP oraz klientów)  · 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:  · ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik, per SSID  · obsługa WMM, TSPEC, U-APSD  · wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM  · obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting  · wsparcie IEEE 802.11i, WPA2, WPA3  · wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)  · obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS  · obsługa blokowania ruchu Peer-to-Peer  · analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)  · obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:  · sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia  · bezpieczna sekwencja uruchamiania  · sprawdzenie autentyczności urządzenia  • wbudowana funkcjonalność wykrywająca zakłócenia na obsługiwanym kanale radiowym (w pasmach 2,4 oraz 5 GHz), typu: kuchenka mikrofalowa, continuous wave (rejestrator AV, elektroniczna niańka), SI-FHSS (urządzenia Bluetooth, DECT)  • interfejs MultiGigabit Ethernet (100/1000/2500) zgodny z IEEE 802.3bz  • interfejs konsoli RJ45  • port USB 2.0  • 2 GB RAM, 1 GB Flash  • pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at), możliwość uruchomienia AP z wykorzystaniem PoE (802.3af) z ograniczonymi funkcjonalnościami (m.in.: redukcja układów radiowych do trybu 2x2)  • wyposażony w złącza typu RP-TNC dla anten zewnętrznych  • obudowa przystosowana do pracy w zakresie temperatur -20 – 50oC  • diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji  • certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi 6, Wi-Fi Enhanced Open, WMM, WMM-PS  • wbudowane radio Bluetooth Low Energy (BLE) 5.0  • Wraz z urządzeniem należy dostarczyć zewnętrzne anteny, wybór anten jest po stronie Wykonawcy w związku z koniecznością wykonania planowania radiowego.  • Należy dostarczyć również komplet uchwytów montażowych. |  |
| **9.** | **Punkt dostępowy typu 2 – 20 szt. (magazyn)** | Typ:  Model:  Producent: |
| Punkt dostępu bezprzewodowego:  · obsługa standardów IEEE 802.11a/b/g/n/ac/ax  · obsługa OFDMA (uplink/downlink), BSS Coloring  · obsługa MU-MIMO – min. 2x2:2 (w 2,4 GHz oraz 5 GHz)  · obsługa kanałów 20, 40 MHz dla 802.11n  · obsługa kanałów 20, 40, 80 MHz dla 802.11ac/ax  · obsługa prędkości PHY do 866 Mbps (ac)  · obsługa prędkośći PHY do 1,4 Gbps (ax)  · obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)  · obsługa beamforming 802.11ac/ax  · obsługa MRC (Maximal Ratio Combining)  · konfigurowalna moc nadajnika  · dla zakresu 2.4 GHz: do 100 mW  · dla zakresu 5GHz: do 100 mW  · praca dwuzakresowa w pasmach: 2,4 GHz oraz 5 GHz  · zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:  · 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  · uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w  · obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)  · 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 pod kątem zagrożeń bezpieczeństwa (wykrywanie obcych AP oraz klientów)  · 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:  · ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik, per SSID  · obsługa WMM, TSPEC, U-APSD  · wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM  · obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting  · wsparcie IEEE 802.11i, WPA2, WPA3  · wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)  · obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS  · obsługa blokowania ruchu Peer-to-Peer  · analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)  · obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:  · sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia  · bezpieczna sekwencja uruchamiania  · sprawdzenie autentyczności urządzenia  · interfejs GigabitEthernet (10/100/1000)  · interfejs konsoli RJ45  · zabezpieczenie typu Kensington przed kradzieżą/demontażem  · pełna funkcjonalność AP przy zasilaniu przez PoE (802.3af)  · anteny zintegrowane o zysku min. 4 dBi dla pasma 2,4 GHz oraz 5 dBi dla pasma 5 GHz  · obudowa przystosowana do pracy w zakresie temperatur 0 – 50oC  · diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji  · certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi 6, Wi-Fi Enhanced Open, WMM, WMM-PS  · wbudowane radio Bluetooth Low Energy (BLE) 5  · Należy dostarczyć również komplet uchwytów montażowych. |  |
| **10.** | **Punkt dostępowy typu 3 – zewnętrzny - 3 szt. (magazyn)** | Typ:  Model:  Producent: |
|  | Punkt dostępowy przeznaczony do montażu zewnętrznego. Nie dopuszcza się stosowania punktów dostępowych wewnętrznych montowanych w skrzynkach termicznych/technicznych. Punkt dostępowy musi pochodzić od tego samego producenta sprzętu co punkty wewnętrze.  Należy dostarczyć komplet montażowy do zamontowania punktów dostępowych.  Zewnętrzny punkt dostępu bezprzewodowego z wbudowanymi antenami:  · obsługa standardów 802.11a/b/g/n/ac/ax  o obsługa OFDMA (uplink/downlink), TWT, BSS Coloring  o obsługa MU-MIMO (uplink/downlink) 4x4:4 (w 2,4 GHz oraz 5GHz)  o obsługa kanałów 20 i 40 MHz dla 802.11n  o obsługa kanałów 20, 40, 80 MHz dla 802.11ac/ax  o obsługa prędkośći PHY do 2,9 Gbps (ax)  o obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)  o obsługa beamforming dla klientów 802.11a/g/n/ac/ax  o obsługa MRC (Maximal Ratio Combining)  · programowe ustawianie mocy wyjściowej  o do 30 dBm (do 1W) dla pasma 5 GHz  o do 30 dBm (do 1W) dla pasma 2,4 GHz  · praca dwuzakresowa w pasmach: 2,4 GHz oraz 5 GHz  · zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:  o automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN  o optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)  o obsługa min. 16 BSSID  o definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID  o uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w  o obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)  o możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników  o obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6  o jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN)  o obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h  o obsługa IPv6  o obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r  o obsługa mechanizmów QoS:  § ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik  § obsługa WMM, TSPEC, U-APSD  o wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM  o obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting  o wsparcie IEEE 802.11i, WPA3, WPA2, WPA  o wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)  o obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS  o obsługa blokowania ruchu Peer-to-Peer  o analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)  · możliwość pracy w trybie kratowym (część AP dołączona do sieci kablowej, pozostałe formujące sieć w oparciu o medium radiowe)  o komunikacja między punktami dostępowymi bez medium kablowego  o autoryzacja punktów dostępowych w oparciu o certyfikaty, adresy MAC  o separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)  o automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)  o automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)  o automatyczna ochrona kryptograficzna (AES) ruchu pomiędzy AP  · obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:  o sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia  o bezpieczna sekwencja uruchamiania  o sprawdzenie autentyczności urządzenia  · zintegrowany moduł radiowy pełniący funkcję analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz):  o dokładność analizy (kwant próbkowania) max. 200 kHz  o zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych  o automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.)  o współpraca z mechanizmami optymalizacji wykorzystania pasma radiowego w celu szybkiej reakcji w wyniku wykrycia interferencji  o 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  · interfejs MultiGigabit Ethernet (100/1000/2500) zgodny z IEEE 802.3bz  · interfejs światłowodowy (1000BaseX – styk definiowany przez wkładkę typu SFP)  · interfejs GigabitEthernet 100/1000BASE-T dostarczający zasilanie PoE 802.3af (PoE-out) do podłączanego urządzenia (np.: kamery)  · interfejs konsoli RJ45  · zróżnicowane możliwości zasilania:  o obsługa wszystkich funkcjonalności przy zasilaniu 802.3bt lub zasilaniu DC: 24-56V  o możliwość uruchomienia urządzenia przy zasilaniu 802.3at, w układzie radiowym 2x2, z ograniczonymi funkcjonalnościami  o możliwość uruchomienia urządzenia przy zasilaniu 802.3af, bez obsługi układów radiowych, z ograniczonymi funkcjonalnościami  · obudowa odporna na warunki atmosferyczne, przystosowana do pracy zewnętrznej  o wymiary nie przekraczające 26 x 24 x 9 cm (bez elementów montażowych)  o praca przy temperaturach między -40oC a 55oC  o odporność na wiatr o prędkości min. 150 km/h (stała prędkość) / 250 km/h (porywy)  o zgodność z IP67  · diodowa sygnalizacja stanu urządzenia  · certyfikacja Wi-Fi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi6, WMM  · anteny wbudowane kierunkowe o zysku min. 8 dBi dla pasma 2,4GHz oraz 5GHz  · wbudowany moduł Bluetooth Low Energy (BLE) 5.0 z anteną o zysku 4 dBi  · nakładka maskująca punkt dostępowy (z możliwością pomalowania w celu lepszego wtopienia się w otaczające tło)  · uchwyt pozwalający na pionowy montaż (z możliwością pochylenia) punktu dostępowego na słupie o średnicy 51-127mm lub na ścianie, |  |
| **11.** | **Punkt dostępowy typu 4 – 2 szt. (biuro przy magazynie)** | Typ:  Model:  Producent: |
|  | Punkt dostępu bezprzewodowego:  • obsługa standardów 802.11a/b/g/n/ac/ax  • obsługa MU-MIMO – min. 4x4:4  • obsługa kanałów 20, 40 MHz dla 802.11n  • obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax  • obsługa prędkości PHY do 3,47 Gbps (ac)  • obsługa prędkośći PHY do 5,38 Gbps (ax)  • obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)  • obsługa beamforming dla klientów 802.11a/g/n/ac/ax  • obsługa MRC (Maximal Ratio Combining)  • obsługa szerokiego zakresu kanałów radiowych:  • dla zakresu 2.4 GHz: min. 13 kanałów  • dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów  • dla zakresu 5GHz (extended UNII-2): min. 8 kanałów  • konfigurowalna moc nadajnika  • dla zakresu 2.4 GHz: do 100 mW  • dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW  • dla zakresu 5GHz (extended UNII-2): do 200 mW  • zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:  • 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  • uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w  • obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)  • 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, wireless IDS)  • 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:  • ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik  • obsługa WMM, TSPEC, U-APSD  • współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne  • wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM  • wsparcie IEEE 802.11i, WPA2, WPA  • wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)  • interfejs MultiGigabit Ethernet (100/1000/2500) - IEEE 802.3bz  • interfejs konsoli RJ45  • port USB 2.0 (funkcjonalność dostępna w przyszłych wersjach oprogramowania)  • 2 GB RAM, 1 GB Flash  • zasilanie przez PoE+ (IEEE 802.3at)  • anteny zintegrowane o zysku:  • dla modułu 2,4 GHz 3 dBi  • dla modułu 5 GHz: min. 4dBi  • obudowa przystosowana do pracy w zakresie temperatur 0 – 50oC  • diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji  • wbudowane radio Bluetooth Low Energy (BLE) 5.0 |  |
| **12.** | **Kontroler sieci bezprzewodowej – sztuk 2** | Typ:  Model:  Producent: |
|  | • urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:  o zarządzanie politykami bezpieczeństwa  o wykrywanie zagrożeń w sieci bezprzewodowej  o zarządzanie pasmem radiowym  o zarządzanie mobilnością  o zarządzanie jakością transmisji  zgodnie z protokołem CAPWAP (RFC 5415)  • obsługa 6000 punktów dostępowych  • dostarczenie licencji na obsługę AP wszytkach zaproponowanych punktów dostępowych wraz ze wsparciem producenta na okres 5  • wspierane tryby uruchomienia:  o na platformach wirtualizacyjnych (chmura prywatna): ESXi, KVM, Hyper-V  o w chmurze publicznej: AWS (Amazon Web Services), GCP (Google Cloud Platform)  • wydajność centralnego przełączania ruchu 1,5 Gbps (dotyczy platform ESXi, KVM, HyperV), przy zastosowaniu SR-IOV wydajność do 5Gbps (dotyczy platform ESXi, KVM)  • 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)  • obsługa 64000 klientów sieci bezprzewodowej  • zarządzanie pasmem radiowym punktów dostępowych:  o automatyczna adaptacja do zmian w czasie rzeczywistym  o optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)  o dynamiczne przydzielanie kanałów radiowych  o wykrywanie, eliminacja i unikanie interferencji  o równoważenie obciążenia punktów dostępowych  o tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych  o automatyczna dystrybucja klientów pomiędzy punkty dostępowe  o mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych  o dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe  • mapowanie SSID do segmentów VLAN w sieci przewodowej  o 1:1  o 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)  o możliwość tunelowania ruchu klientów do kontrolera (dotyczy platform ESXi, KVM, HyperV) oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)  • obsługa sieci kratowych (dotyczy platform ESXi, KVM, HyperV)  o komunikacja między punktami dostępowymi bez medium kablowego  o separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)  o automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)  o automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)  o autoryzacja punktów dostępowych w oparciu o certyfikaty, adresy MAC  • obsługa mechanizmów bezpieczeństwa:  o 802.11i, WPA3, WPA2, WPA  o 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)  o obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników  o kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID  o obsługa profilowania użytkowników:   przydział sieci VLAN   przydział list kontroli dostępu (ACL)  o uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w  o uwierzytelnianie punktów dostępowych w oparciu o certyfikaty  o obsługa list kontroli dostępu (ACL)  o obsługa list kontroli dostępu opartych o nazwy domenowe (DNS ACL)  o obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X  o wykrywanie i dezaktywacja obcych punktów dostępowych  o możliwość budowania reguł klasyfikacji obcych punktów dostępowych w oparciu o nazwę SSID, wybrany ciąg znaków w SSID, siłę sygnału RSSI, minimalną ilość podłączonych urządzeń  o ochrona kryptograficzna (DTLS) ruchu użytkowników (dotyczy platform ESXi, KVM, HyperV) oraz ruchu kontrolnego CAPWAP  o DHCP proxy, wsparcie dla DHCP Option 82  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)  • zabezpieczenia zapewniające autentyczność sprzętową oraz software’ową:  o kryptograficzne podpisywanie obrazów oprogramowania  o bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych  • 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  • obsługa ruchu unicast IPv4 i IPv6  • zgodność z funkcjonalnościami IPv6 pod kątem RFC: 4191, 6980, 8200, 8201 (dotyczy platform ESXi, KVM, HyperV)  • obsługa ruchu multicast IPv4 i IPv6 (dotyczy platform ESXi, KVM, HyperV)  o IGMP / MLD snooping  o optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)  o obsługa konwersji ruchu multicast do unicast  • obsługa mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami (dotyczy platform ESXi, KVM, HyperV))  • obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k  • obsługa mechanizmów QoS  o 802.1p  o WMM, TSpec, U-APSD  o Ograniczanie pasma per użytkownik  o Call Admission Control, SIP CAC, Call Snooping  o równomierna obsługa klientów sieci bezprzewodowej w oparciu o utylizację czasu antenowego  o kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID  o zbiór wbudowanych profili do automatycznej konfiguracji ustawień QoS  • 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)  • 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)  • obsługa dostępu gościnnego (IPv4 i IPv6)  o przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony)  o przekierowanie użytkowników do strony logowania na zewnętrznym serwerze  o obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta  o 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)  • obsługa NTP (IPv4 oraz IPv6), możliwość ustawienia różnych serwerów NTP dla wybranych grup AP  • możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania (dni tygodnia, godziny)  • obsługa EoGRE w celu tunelowania ruchu z kontrolera do dedykowanego koncentratora (np. na routerze) (dotyczy platform ESXi, KVM, HyperV)  • wsparcie dla IEEE 802.11u  • obsługa Hotspot 2.0 (dotyczy platform ESXi, KVM, HyperV)  • obsługa redundancji rozwiązania (N+1)  • obsługa redundancji 1:1 (Active/Standby) zapewniającej (dotyczy platform ESXi, KVM, HyperV):  o utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera  o synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej  • zarządzanie przez HTTPS, SNMP, SSH, NETCONF, wirtualny port konsoli  • obsługa logowania Syslog, wsparcie dla IPSec w celu zabezpieczenia Syslog (dotyczy platform ESXi, KVM, HyperV)  • obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020)  • wbudowana baza najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem  • 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)  • Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 5 lat  • Urządzenie dostarczone w formie maszyny wirtualnej na platformę: ESXi / Hyper-V |  |

1. Oświadczam, że zapoznałem się z treścią zapytania ofertowego oraz że nie wnoszę zastrzeżeń do jego treści i zdobyłem wszelkie informacje niezbędne do sporządzenia oferty i wykonania zamówienia. Złożona oferta spełnia wszelkie parametry i warunki zapytania ofertowego.
2. Oświadczam, że akceptuję termin związania ofertą wynoszący 30 dni od dnia upływu terminu składania ofert, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
3. Zobowiązuje się wykonać zamówienie w terminach wskazanych w Zapytaniu ofertowym,
4. W przypadku wyboru mojej oferty zobowiązuję się do zawarcia umowy na wykonanie przedmiotu zamówienia w miejscu i terminie wskazanym przez Zamawiającego.
5. Umowa będzie opiewać na kwotę brutto.
6. Znajduję się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
7. Posiadam wiedzę i doświadczenie niezbędne do realizacji przedmiotu zamówienia.
8. Wyrażam zgodę na przetwarzanie przez Zamawiającego danych osobowych na potrzeby realizacji niniejszego postępowania zgodnie z art. 23 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 ze zm.) do celów związanych z przeprowadzeniem niniejszego postępowania. Moja zgoda obejmuje również przetwarzanie danych w przyszłości pod warunkiem, że nie zostanie zmieniony cel przetwarzania.
9. Jestem świadomy/-a odpowiedzialności karnej za fałszywe zeznania wynikające z art. 233 (podanie nieprawdy lub zatajenie nieprawdy) ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r., Nr 88, poz. 553 ze zm.), a zawarte w ofercie informacje są zgodne z prawdą oraz stanem faktycznym.

………….……………………………

Czytelny podpis osoby uprawnionej do reprezentowania podmiotu

Załączniki:

1. Załącznik nr 2 – oświadczenie Wykonawcy – warunki udziału w postępowaniu
2. Załącznik nr 3 – wykaz dostaw
3. Załącznik nr 4 – wykaz personelu

1. Zakres danych i informacji musi także potwierdzać **równoważność** oferowanych urządzeń, w stosunku do wymagań wskazanych przez Zamawiającego [↑](#footnote-ref-2)