

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa urządzeń sieciowych wraz z akcesoriami i licencjami dla KW PSP w Białymstoku”

1. Przedmiot zamówienia

- 1.1. Dostawa **24** szt. przełączników sieciowych zgodnych z wymaganiami opisanymi w pkt 3.
- 1.2. Dostawa **22** licencji dostępowych na minimum **12** miesięcy, oraz 2 licencji dostępowych na minium 60 miesięcy, dla przełączników wymienionych w pkt 1.1. do systemu centralnego zarządzania, który jest zgodny z wymaganiami opisanymi w pkt 4.
- 1.3. Zamawiający wymaga, aby oferowane przełączniki sieciowe były w pełni kompatybilne, interoperacyjne i współpracowały bez ograniczeń funkcjonalnych z urządzeniami Juniper EX4650-48Y oraz Juniper EX4400-48MXP, stanowiącymi posiadaną infrastrukturę referencyjną, zarządzaną centralnie za pomocą platformy Juniper Mist.

Dopuszcza się zaoferowanie rozwiązań równoważnych. Za rozwiązanie równoważne Zamawiający uzna przełączniki innej marki, które zapewnią pełną, natywną współpracę z urządzeniami referencyjnymi bez konieczności dokupywania przez Zamawiającego dodatkowych licencji, konwerterów czy zewnętrznego oprogramowania integrującego. Ciężar udowodnienia równoważności spoczywa na Wykonawcy.

W przypadku zaoferowania systemu zarządzania innego niż system referencyjny, Wykonawca zobowiązany jest do przeprowadzenia w ramach wynagrodzenia szkolenia dla co najmniej 5 osób, w wymiarze minimum 3 dni szkoleniowych.

Szkolenie musi mieć charakter praktyczny i obejmować co najmniej:

- konfigurację i zarządzanie przełącznikami,
- konfigurację VLAN, portów, QoS/CoS oraz 802.1X,
- monitoring i diagnostykę urządzeń i sieci,
- analizę zdarzeń, alarmów i przyczyn problemów,
- wykorzystanie funkcji analitycznych i automatyzacji,
- zarządzanie użytkownikami, rolami i uprawnieniami,
- aktualizację oprogramowania oraz zarządzanie konfiguracją.

Co najmniej 50% czasu szkolenia musi stanowić część praktyczna. Wykonawca zapewni materiały szkoleniowe oraz imienne zaświadczenia potwierdzające ukończenie szkolenia. Koszt szkolenia musi być uwzględniony w cenie oferty i nie może generować dodatkowych kosztów po stronie Zamawiającego.

2. Wymagania Ogólne

- 2.1. Wszystkie urządzenia będą dostarczone jako fabrycznie nowe, nieużywane w innych projektach oraz nie starsze niż 12 miesięcy od daty produkcji.
- 2.2. Dostarczany sprzęt musi posiadać okablowanie, zasilacze oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie (np. przewody zasilające, zasilacze itp.).
- 2.3. Wszystkie dostarczane urządzenia i oprogramowanie będą pochodziły z oficjalnego kanału dystrybucji na Unię Europejską dla danego producenta.
- 2.4. Zarówno dostarczane Urządzenia, jak i ich elementy składowe wraz z systemami operacyjnymi oraz aplikacjami nie mogą znajdować się na aktualnej, na czas składania ofert, liście elementów producenta przewidzianych do wycofania z produkcji, sprzedaży lub serwisowania;
- 2.5. Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w pkt.3 i pkt.4. Wykonawca, który powołuje się na rozwiązania równoważne opisane przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

3. Minimalne wymagania dla przełączników

3.1. Parametry podstawowe

- 3.1.1. Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości nie większej niż 1U przystosowanym do montowania w szafie rack 19 cali. Zestaw montażowy do szafy rack musi znajdować się na wyposażeniu dostarczonego urządzenia.
- 3.1.2. Urządzenie musi być wyposażone we wbudowany zasilacz dostosowany do napięcia zmiennego 220-230V. Zasilacz ten musi być wbudowany, nie dopuszcza się zasilaczy zewnętrznych.
- 3.1.3. Urządzenie musi być chłodzone przepływem powietrza w schemacie od przodu do tyłu. Za przód urządzenia przyjmuje się stronę z zabudowanymi interfejsami tranzytowymi 1 oraz 10Gbps.

3.2. Interfejsy urządzenia

- 3.2.1. Przełącznik musi być wyposażony co najmniej w następujące interfejsy, zgodne z właściwymi standardami IEEE 802.3:
 - a) 48 portów 1 Gigabit Ethernet RJ-45 z obsługą PoE do poziomu 30W na port i budżetem mocy min. 740W
 - b) 4 porty 1/10 Gigabit Ethernet (oddzielne od portów wymienionych w poprzednim podpunkcie). Typ złącza interfejsu musi być określany przez

wymienny moduł SFP+. Lista kompatybilnych modułów SFP28 musi uwzględniać co najmniej:

- Dla prędkości 1Gbps: 1GBase-SX, 1GBase-LX, 1GBase-LH (do min. 70km)
- Dla prędkości 10Gbps: 10GBase-T, 10GBase-SR, 10GBase-BXD/U, 10GBase-LR, 10GBase-ER, 10GBase-ZR (80km), a także interfejsy typu direct attach (DA) o długościach kabli od 1m do nie mniej niż 5m, co najmniej 3 różne długości w tym zakresie

3.2.2. Przełącznik musi być wyposażony w co najmniej jeden interfejs zarządzania OOB GE 1GBase-T RJ-45 oraz port szeregowy konsoli zarządzającej.

3.3. Parametry podstawowe

- 3.3.1. Opisane w tym rozdziale funkcjonalności muszą zostać dostarczone wraz z właściwą licencją, jeżeli jest ona wymagana dla uruchomienia tej funkcjonalności.
- 3.3.2. Urządzenie musi obsługiwać funkcjonalności Fast PoE / Perpetual PoE umożliwiające podanie zasilania w trakcie uruchamiania urządzenia i bezprzerwowe zasilanie podłączonych urządzeń w trakcie restartu przełącznika.
- 3.3.3. Przełącznik musi obsługiwać ramki Jumbo o wielkości 9KB
- 3.3.4. Urządzenie musi obsługiwać sprzętowo ruting IPv4 oraz IPv6. Pakiety muszą być przełączane w warstwie drugiej i trzeciej modelu OSI bez udziału procesora zarządzającego urządzeniem.
- 3.3.5. Urządzenie musi obsługiwać ruting statyczny IPv4 i IPv6 oraz (jako opcjonalna rozbudowa licencyjna) ruting dynamiczny IPv4/IPv6, co najmniej dla protokołów routingu OSPF, IS-IS oraz BGP.
- 3.3.6. Urządzenie musi obsługiwać (jako opcjonalna rozbudowa licencyjna) mechanizm tworzenia wirtualnych ruterów (kontekstów / VRF-ów / ruterów logicznych) umożliwiający ruting pakietów w oparciu o niezależne tablice routingu.
- 3.3.7. Urządzenie wspiera agregację linków Ethernet, statyczną oraz z wykorzystaniem protokołu LACP.
- 3.3.8. Urządzenie musi obsługiwać protokół redundancji VRRP dla IPv4 i IPv6 - jako opcjonalna rozbudowa licencyjna.
- 3.3.9. Dla protokołów BGP, OSPF i IS-IS (w ramach opcjonalnej rozbudowy licencyjnej) musi być wspierany mechanizm BFD.
- 3.3.10. Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów (ACL) na podstawie informacji nagłówka IPv4 oraz IPv6. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza.
- 3.3.11. Urządzenie musi obsługiwać protokół SNMP w wersjach 1, 2 i 3. Urządzenie musi udostępniać za pomocą protokołu SNMP co najmniej liczniki ramek i bajtów wysłanych i odebranych na poszczególnych interfejsach tranzytowych.

- 3.3.12. Urządzenie wspiera funkcjonalność SPAN, tzn. wysłanie kopii ruchu na porcie/vlanie na inny port fizyczny. Ponadto musi istnieć możliwość wysłania kopii nagłówków przechwyconego ruchu do oprogramowania zarządzającego na podstawie żądania systemu telemetrycznego gRPC.
- 3.3.13. Urządzenie musi posiadać mechanizmy pozwalające na ograniczanie pasma dla ruchu wejściowego na wszystkich interfejsach tranzytowych (z uwzględnieniem filtrów ruchu – ACL).
- 3.3.14. Urządzenie musi posiadać mechanizmy klasyfikowania i znakowania ruchu w oparciu co najmniej o adresację z nagłówków L3 na wszystkich portach tranzytowych oraz dla poszczególnych sieci VLAN.
- 3.3.15. Urządzenie musi obsługiwać co najmniej 8 kolejek wyjściowych dla każdego portu tranzytowego z możliwością priorytetyzacji.
- 3.3.16. Urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1q. Urządzenie wspiera tunelowanie enkapsulacji 802.1Q (Q-in-Q).
- 3.3.17. Urządzenie musi obsługiwać protokoły Spanning Tree – zgodnie z co najmniej IEEE 802.1d, 802.1w i 802.1s. Ponadto przełącznik musi zapewniać kompatybilność z infrastrukturą pracującą zgodnie z protokołem Per-Vlan Spanning Tree.
- 3.3.18. Urządzenie musi wspierać protokół 802.1X w celu uwierzytelnienia dołączonego suplikanta (pojedynczego lub większej liczby per interfejs) na serwerze RADIUS oraz akceptować co najmniej przypisanie vlan-u, a także listy vlanów (formujących trunk) jako wyniku procesu autoryzacji. Dla urządzeń klienckich bez oprogramowania suplikanta, urządzenie musi wykonać uwierzytelnienie wykorzystując adres MAC, a także umożliwiać przekierowanie do portalu uwierzytelniającego (captive portal).
- 3.3.19. Urządzenie ma możliwość pracy jako pojedynczy, administrowany z pojedynczej konsoli i pod wspólnym adresem IP przełącznik logiczny w grupie do 6 urządzeń; dystans pomiędzy poszczególnymi urządzeniami fizycznymi może przekraczać 100m. Musi istnieć możliwość wizualnej identyfikacji pozycji i roli konkretnego urządzenia fizycznego w urządzeniu logicznym (np. jako która wirtualna karta jest on dostępny w zagregowanym urządzeniu logicznym) przez odpowiednią sygnalizację np. diodami LED lub wyświetlaczem.

3.4. Zarządzanie urządzeniem

- 3.4.1. Interfejsy zarządzające urządzeniem obejmują CLI (konsola szeregową oraz sesja SSH), wbudowane GUI, SNMP, netconf, telemetria gRPC.
- 3.4.2. Urządzenie wspiera uwierzytelnienie dostępu administracyjnego w zewnętrznej bazie użytkowników z wykorzystaniem protokołów RADIUS oraz TACACS+
- 3.4.3. Urządzenie umożliwia edycję konfiguracji wykonywalnej na urządzeniu bez natychmiastowego jej uruchamiania, blokowe uruchamianie zmian

konfiguracyjnych, cofanie zmian konfiguracyjnych do poprzedniej wersji, a także automatyczne cofnięcie się do poprzedniej wersji konfiguracji w przypadku np. utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany. W urządzeniu musi być przechowywanych automatycznie (tj. bez dodatkowych poleceń administracyjnych) nie mniej niż 20 poprzednich, kompletnych konfiguracji.

- 3.4.4. Urządzenie wspiera automatyzację i skryptowanie zarówno w zakresie off-box, jako zewnętrzne oprogramowanie komunikujące się z urządzeniem przez interfejs typu Netconf lub podobny, oraz on-box, jako skrypt podejmujący akcje administracyjne z uwzględnieniem zmiany konfiguracji wykonywalnej własnej lub innego urządzenia jako reakcja na zdarzenia definiowalne na urządzeniu.
- 3.4.5. Urządzenie obsługuje zero touch provisioning - przygotowana w systemie zarządzającym konfiguracja może zostać automatycznie dostarczona na urządzenie po jego włączeniu i dopięciu do reszty sieci IP bez konieczności jakiegokolwiek interwencji administratora bezpośrednio na urządzeniu. Na urządzeniu można - posiadając dostęp fizyczny do niego - wymusić ponowienie procesu inicjalizacji, np. przez wbudowany przycisk. Urządzenie wizualnie sygnalizuje prawidłowość połączenia z systemem zarządzającym, np. diodą LED lub informacją na wyświetlaczu.
- 3.4.6. Musi istnieć możliwość zarządzania przełącznikiem z poziomu centralnego systemu zarządzania tego samego producenta.
- 3.4.7. Centralny system zarządzania musi umożliwiać konfigurację dowolnych ustawień przełącznika, monitorowanie parametrów operacyjnych (nie mniej status interfejsów, obciążenie pamięci RAM, CPU, statystyk ruchu, liczników błędów, pobierania zasilania PoE), monitorowanie oraz alarmowanie o naruszeniach parametrów (dla przepustowości, uwierzytelnienia klientów 802.1x, osiągalności i poziomu obciążenia przełącznika).
- 3.4.8. System zarządzania musi tworzyć metryki KPI (Key Performance Indicators) odnoszące się do stanu infrastruktury przełączników sieciowych oraz jakości świadczonej usługi dostępu do sieci przewodowej. System musi wskazywać przyczyny, dla których wartości KPI odbiegają od oczekiwanych. Wśród mierzonych KPI muszą być nie mniej niż: przepustowość, stan przełączników, liczba udanych prób podłączenia się klientów do sieci, pasmo na przełącznikach.
- 3.4.9.** System zarządzania musi posiadać funkcję proaktywnego proponowania działań naprawczych dla zarejestrowanych problemów z funkcjonowaniem sieci przewodowych – między innymi związanymi z brakującymi sieciami VLAN na portach, nieudanymi transakcjami DHCP, nieudanymi próbami uwierzytelnienia, problemami na poziomie okablowania Ethernet, błędami autonegocjacji, pętlami w warstwie 2.

3.5. Parametry wydajnościowe oraz skalowalność

- 3.5.1. Zapisy o opcjonalnej rozbudowie licencyjnej z rozdziału III stosują się odpowiednio.
- 3.5.2. Urządzenie musi być wyposażone w nie mniej niż 4GB pamięci RAM oraz pamięć stałą (SSD/Flash) nie mniej niż 8GB
- 3.5.3. Przełącznik musi mieć przepustowość nie mniejszą niż 176 Gbps oraz obsługiwać nie mniej niż 130 Mpps (milionów pakietów na sekundę)
- 3.5.4. Urządzenie musi obsługiwać nie mniej niż:
 - a) 32 tysiące wpisów w tablicy adresów MAC
 - b) 4 tysiące wpisów w tablicy ARP
 - c) 1000 tras w tablicy forwardingu sprzętowego unicast IPv4,
 - d) 1000 wpisów w tablicy routingu multicast IPv4
 - e) 500 tras w tablicy forwardingu sprzętowego unicast IPv6 (można przyjąć prefiksy nie dłuższe niż /64)
 - f) 500 wpisów w tablicy routingu multicast IPv6
- 3.5.5. Urządzenie umożliwia konfigurację min. 10 instancji routingowych.
- 3.5.6. Agregacja portów: min. 8 portów per grupa oraz minimum 128 różnych grup per zagregowana grupa urządzeń.
- 3.5.7. VRRP, dla min. 100 rozłącznych grup.
- 3.5.8. BFD dla OSPF: nie mniej niż 30 jednoczesnych sesji.
- 3.5.9. Urządzenie musi pozwalać na skonfigurowanie i uruchomienie nie mniej niż 1000 sieci VLAN jednocześnie.

3.6. Warunki gwarancji

- 3.6.1. Gwarancja obowiązuje przez cały okres, w którym sprzęt jest posiadany przez klienta,
- 3.6.2. Wbudowane lub wymienne zasilacze oraz wentylatory w przełącznikach są objęte ograniczoną gwarancją wynoszącą minimum 5 lat,
- 3.6.3. Wsparcie i dostępność części/obsługa gwarancyjna wygasają po 5 latach od ogłoszenia wycofania produktu z oferty (End of Life),
- 3.6.4. Wysyłka jednostki zamiennej następuje w ciągu 1 dnia roboczego.

4. Minimalne wymagania dla systemu zarządzania

4.1. Ogólne właściwości systemu zarządzającego

- 4.1.1. W celu uproszczenia instalacji, wdrażania, utrzymania i skalowania, oferowane rozwiązanie musi się składać z przełączników, które zostaną podłączone do sieci w lokalizacjach Zamawiającego oraz z centralnego systemu zarządzania urządzeniami, kontroli dostępu oraz analityki zlokalizowanego w środowisku chmury obliczeniowej, udostępnionego przez producenta jako usługa.
- 4.1.2. Usługa zarządzania musi być realizowana na terenie Unii Europejskiej, a dane przetwarzane w zgodzie z regulacją GDPR.

- 4.1.3. Nie jest dopuszczalne rozwiązanie, w którym komponent systemu zarządzania będzie musiał znajdować się w lokalizacji Zamawiającego.
- 4.1.4. Platforma zarządzania musi zapewniać wydajność, skalę i niezawodność w wykorzystaniu mechanizmów natywnych dla środowiska chmurowego (np. microservices). Dostęp do platformy zarządzania oraz jej funkcji musi być precyzyjnie zdefiniowany poprzez np. licencje, subskrypcje itp. Nie jest dopuszczalne by sposób korzystania z platformy zarządzania przez Zamawiającego miał wpływ na bieżące bądź wnosił dodatkowe koszty rozwiązania podczas jego użytkowania.
- 4.1.5. Nie jest dopuszczalne rozwiązanie, w którym system zarządzania będzie realizowany przez oprogramowanie przeznaczone do instalacji w sieci lokalnej (on-premises) zainstalowane na maszynach wirtualnych w środowisku chmurowym, za które Zamawiający musiałby ponosić dodatkowe opłaty.
- 4.1.6. W celu obsługi w czasie rzeczywistym danych telemetrycznych zbieranych z zarządzanych urządzeń oraz ich prezentowania w sposób przyjazny dla użytkownika, platforma musi wykorzystywać nowoczesne metody przetwarzania zbiorów danych - nie mniej niż analitykę Big Data, machine learning (ML), Artificial Intelligence (AI).
- 4.1.7. Aktualizacje oprogramowania platformy zarządzania związane z nowymi funkcjami, poprawkami błędów i łataniami bezpieczeństwa muszą być udostępniane przez producenta nie rzadziej niż co 2 miesiące.
- 4.1.8. System zarządzania musi wspierać dostęp SSO z wykorzystaniem SAML i wspierać algorytmy SHA-512, SHA-384, SHA-256. System zarządzania musi wspierać mapowanie kont użytkowników do ról o różnym poziomie uprawnień. System zarządzania musi posiadać możliwość włączenia / wyłączenia dostępu wsparcia producenta do obszaru platformy zarządzania administrowanej przez Zamawiającego.
- 4.1.9. System musi generować logi audytowe dla każdej sesji administratora oraz dla zmian konfiguracyjnych. Logi audytowe nie mogą być modyfikowane przez żadnego użytkownika niezależnie od uprawnień administracyjnych. Logi audytowe muszą zawierać co najmniej: czas zdarzenia, nazwę konta użytkownika, typ dostępu (np. odczyt, zmiana konfiguracyjna), nazwę lokalizacji, szczegóły zmiany konfiguracyjnej). Musi być dostępna funkcja wyszukiwania w logach audytowych - nie mniej niż po dacie, nazwie administratora, lokalizacji, typie dostępu.
- 4.1.10. System musi zapewniać elastyczność w rozumieniu, że rozbudowa sieci Zamawiającego w celu obsługi nowych lokalizacji oraz podniesienia wydajności odbywać się będzie bez przerwy w ruchu i bez degradacji wydajności.
- 4.1.11. System musi wspierać mechanizm Zero Touch Provisioning (ZTP). Przetłaczalniki w konfiguracji fabrycznej muszą skontaktować się z platformą zarządzania przez Internet i ściągnąć docelową konfigurację.

- 4.1.12. Komunikacja między punktami dostępowymi i platformą zarządzania musi być nawiązywana wyłącznie na kierunku wychodzącym do Internetu, nie może wymagać dostrojenia reguł na firewallu Zamawiającego dla ruchu przychodzącego z Internetu.
- 4.1.13. Wszystkie ustawienia konfiguracyjne oraz wszystkie monitorowane dane muszą być dostępne przez interfejs API udostępniony przez producenta.
- 4.1.14. System zarządzania i monitorowania musi posiadać funkcję integracji z przełącznikami Ethernet tego samego producenta. Integracja musi polegać co najmniej na widoczności statusu podłączonych urządzeń, monitorowaniu ich parametrów oraz zmiany ustawień konfiguracyjnych podłączonych urządzeń.
- 4.1.15. System musi raportować status zarządzanych urządzeń, ich numery seryjne, zestawienie komponentów fizycznych (inventory), a także status poszczególnych interfejsów sieciowych. System musi na bieżąco raportować parametry operacyjne zarządzanych przełączników, włącznie z obciążeniem CPU, wykorzystaniem pamięci, ilości przesyłanego ruchu na poszczególnych portach oraz poborem mocy przez urządzenia zasilane z przełączników z PoE.
- 4.1.16. System musi posiadać funkcję aktualizowania systemu operacyjnego przełączników.
- 4.1.17. System musi posiadać funkcję zestawienia sesji SSH z zarządzanymi urządzeniami.
- 4.1.18. System zarządzania musi zarządzać konfiguracją na przełącznikach LAN w zakresie co najmniej sieci VLAN, adresacji IP, ustawień Class of Service, uwierzytelniania użytkowników (802.1X). posiadać możliwość konfiguracji protokołów routingu dynamicznego (co najmniej OSPF, BGP).
- 4.1.19. W celu automatyzacji wykonywania powtarzalnych czynności przez administratorów sieci LAN system musi posiadać mechanizm definiowania profili portów obejmujących typ pracy portu (dostępowy / trunk), sieci VLAN, ustawienia CoS, 802.1X. System musi udostępniać graficzne narzędzie do tworzenia profili portów oraz przypisywania profili do poszczególnych interfejsów fizycznych na przełącznikach. Profile muszą być przepisywane ręcznie oraz automatycznie na podstawie między innymi informacji z protokołu LLDP, Radius oraz adresu MAC urządzenia podłączonego do przełącznika. Musi być dostępna funkcja definiowania szablonów konfiguracyjnych do stosowania tych samych ustawień na wielu zarządzanych przełącznikach.
- 4.1.20. System musi posiadać funkcję wykrywania urządzeń końcowych w sieci LAN (na bazie adresów MAC i IP).
- 4.1.21. System musi tworzyć metryki KPI (Key Performance Indicators) odnoszące się do stanu infrastruktury przełączników sieciowych oraz jakości świadczonej usługi dostępu do sieci przewodowej. System musi wskazywać przyczyny, dla których wartości KPI odbiegają od oczekiwanych. Wśród mierzonych KPI muszą być nie

mniej niż: przepustowość, stan przełączników, liczba udanych prób podłączenia się klientów do sieci, pasmo na przełącznikach.

4.2. Wymagania dla systemu uwierzytelniającego

- 4.2.1. System zarządzania musi posiadać wbudowaną funkcję systemu uwierzytelniania i autoryzacji dla urządzeń końcowych podłączanych do przełączników Ethernet. W szczególności uwierzytelnienie nie może być wydzielone do odrębnego portalu administracyjnego.
- 4.2.2. Musi istnieć możliwość skorzystania z odrębnego, lokalnego serwera RADIUS zamiast uwierzytelnienia wbudowanego.
- 4.2.3. System zarządzania musi wspierać 802.1x dla uwierzytelnienia, accountingu, CoA i dynamicznego przypisywania sieci VLAN użytkownikom.
- 4.2.4. System uwierzytelniania musi obsługiwać protokół Radius oraz Radius over TLS (RadSec). Musi być dostępna możliwość obsługi funkcji Proxy Radius.
- 4.2.5. System musi wspierać uwierzytelnianie użytkowników i urządzeń końcowych protokołem 802.1X przy użyciu co najmniej następujących metod: EAP-TLS z wykorzystaniem certyfikatów, EAP-TTLS z wykorzystaniem hasła.
- 4.2.6. System musi wspierać uwierzytelnianie użytkowników i urządzeń końcowych bez wykorzystania protokołu 802.1X – w szczególności MAB.
- 4.2.7. System musi obsługiwać uwierzytelnianie przy użyciu certyfikatów X.509 i wspierać integrację z zewnętrznymi systemami PKI. System musi wspierać mechanizmy automatycznego unieważniania certyfikatów przy użyciu CRL i OCSP.
- 4.2.8. System uwierzytelniania musi obsługiwać integrację z zewnętrznymi systemami IdP (Identity Providers) przy użyciu protokołów Secure LDAP i OAuth 2.0. Wśród oficjalnie wspieranych zewnętrznych dostawców tożsamości muszą znajdować co najmniej Microsoft Entra ID (Microsoft Azure AD), Okta Identity.
- 4.2.9. System musi posiadać funkcję blokowania oraz zezwalania na dostęp do sieci, a także przypisywania atrybutów AAA (VLAN, rola) w zależności od nie mniej niż:
 - a) atrybutów AAA – nazwa użytkownika, VSA (Vendor Specific Attribute),
 - b) listy adresów MAC,
 - c) grupa z IdP,
 - d) atrybuty z certyfikatów: Common Name, Subject, Issuer, SAN (Subject Alternative Name).
- 4.2.10. System musi posiadać możliwość uwierzytelnienia użytkowników i urządzeń podłączanych do bezprzewodowych punktów dostępowych oraz przełączników Ethernet wyprodukowanych przez innych producentów.

- 4.2.11. System uwierzytelniania musi udostępniać graficzny interfejs użytkownika wykorzystujący przeglądarkę WWW, pozwalający na wykonanie następujących czynności:
- a) tworzenie i stosowanie reguł polityki dostępu do zasobów sieciowych,
 - b) zezwolenie na dostęp do sieci dla uwierzytelnionych użytkowników i urządzeń,
 - c) blokowanie dostępu do sieci określonym użytkownikom i urządzeniom,
 - d) dodawanie certyfikatów zaufanych centrów certyfikacyjnych (CA),
 - e) konfigurację dostawców tożsamości (IdP),
 - f) monitorowanie aktywności podłączonych klientów.
- 4.2.12. System posiada graficzne narzędzia do monitorowania zdarzeń związanych z udanymi i nieudanymi próbami uwierzytelniania klientów. Wśród pokazywanych informacji muszą się znaleźć między innymi szczegóły dotyczące certyfikatów, typ uwierzytelnienia, VLAN, Identity Provider oraz która z reguł polityki kontroli dostępu wygenerowała dane zdarzenie.
- 4.2.13. System musi tworzyć metryki KPI (Key Performance Indicators) związane przebiegiem procesu uwierzytelniania użytkowników oraz wskazywać przyczyny, dla których wartości KPI odbiegają od oczekiwanych. Wśród mierzonych KPI muszą być nie mniej niż: liczba połączeń do sieci zakończonych sukcesem, czas trwania procesu podłączenia do sieci.
- 4.2.14. System uwierzytelniania musi obsługiwać nie mniej niż 3000 aktywnych klientów jednocześnie. System musi zapewnić możliwość rozszerzenia do 5000 aktywnych klientów jednocześnie bez konieczności rozbudowy lokalnej infrastruktury (np. serwerów, kontrolerów itp.).