WL-IV.272.9.2026 zał. 1B do swz

Opis Przedmiotu Zamówienia / specyfikacja techniczna

(Cz. II zamówienia)

Przedmiotem zamówienia jest wykonanie przez Wykonawcę projektu technicznego wdrożenia, dostawa, instalacja, konfiguracja i uruchomienie systemu klasy NAC (Network Access Control) przeznaczonego do zarządzania dostępem do sieci przewodowej i bezprzewodowej w środowisku Zamawiającego. Środowisko wirtualizacyjne (serwery fizyczne oraz platforma wirtualizacyjna) zostanie zapewnione przez Zamawiającego. Wykonawca otrzyma dostęp administracyjny do wirtualizatora w celu instalacji systemu. System musi być wdrożony w architekturze rozproszonej, z zapewnieniem wysokiej dostępności (HA) oraz integracją z infrastrukturą Zamawiającego. Rozwiązanie powinno posiadać funkcjonalności systemów klasy PacketFence lub równoważnych. Minimalne wymagania funkcjonalne:

- Obsługa kontroli dostępu do sieci LAN/WLAN dla użytkowników wewnętrznych, gości oraz urządzeń niezarządzanych (BYOD, IoT).
- Obsługa wielu lokalizacji fizycznych (multi-site), z centralnym zarządzaniem politykami i lokalną egzekucją dostępu.
- Wysoka dostępność usług (HA) w każdej lokalizacji – zapewnienie działania systemu również w przypadku utraty łączności z lokalizacją centralną.
- Obsługa uwierzytelniania 802.1X (EAP-PEAP, EAP-TLS) oraz MAC Authentication Bypass (MAB).
- Rejestracja użytkowników i urządzeń za pomocą Captive Portalu z funkcją potwierdzeń mail/SMS.
- Możliwość dynamicznego przypisywania VLAN do portów/przełączników lub punktów dostępowych na podstawie polityk dostępu.
- Integracja z katalogiem użytkowników (np. Microsoft Active Directory lub LDAP).
- Integracja z infrastrukturą klucza publicznego (PKI), w szczególności: obsługa certyfikatów X.509, weryfikacja certyfikatów przez CRL i/lub OCSP, integracja z zewnętrznym lub lokalnym CA.
- Obsługa dzienników dostępu i raportowania zgodności z politykami bezpieczeństwa.
- Centralny, webowy interfejs zarządzający dostępny przez HTTPS, z autoryzacją i rolami użytkowników.

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

Minimalne wymagania techniczne i funkcjonalne:

Lp.	Wymaganie techniczne i funkcjonalne	Wartość minimalna	Nie potrzebne skreślić*
1.	Architektura	Rozproszona (multi-site) z lokalną redundancją	Spełnia/ Nie spełnia*
2.	Wysoka dostępność	HA w wielu lokalizacjach, odporność na awarie łącza z centralą	
3.	Obsługiwane protokoły	802.1X (EAP-PEAP, EAP-TLS), MAB, RADIUS, SNMP, HTTPS	
4.	Obsługa VLAN	Dynamiczne przypisywanie VLAN (CoA) na przełącznikach i WiFi	
5.	Captive Portal	Z możliwością uwierzytelniania, rejestracji	
6.	Integracja z Active Directory / LDAP	Tak	
7.	Integracja z PKI (CA lokalne / zewnętrzne)	Tak, pełne wsparcie dla EAP-TLS, CRL, OCSP	
8.	Sprzęt	Instalacja na wirtualizatorze Zamawiającego	
9.	Zgodność sprzętowa	Integracja z: kontrolerem WiFi Aruba, przełącznikami Zamawiającego	
10.	Interfejs zarządzania	Webowy (HTTPS), z wielopoziomową kontrolą dostępu	
11.	Licencja	Oprogramowanie typu open source lub licencja komercyjna z wieczystym bezpłatnym dostępem do aktualizacji	

Zakres realizacji:

- Instalacja i pełna konfiguracja systemu klasy NAC (PacketFence lub równoważny) na środowisku wirtualnym Zamawiającego.
- Integracja z kontrolerem WiFi Aruba (ArubaMC-VA,8.6.0.18) oraz przełącznikami – obecnie zamawiający posiada wyłącznie przełączniki zarządzalne marki Cisco lub HP (Aruba) warstwy 2 lub 3.
- Wdrożenie integracji z usługą katalogową (AD/LDAP) oraz infrastrukturą PKI Zamawiającego. Konfiguracja supplicanta 802.1X na urządzeniach końcowych

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

przyłączonych do domeny Active Directory, w tym przygotowanie i wdrożenie polityk grupowych (GPO) automatyzujących konfigurację uwierzytelniania sieciowego.

- Skonfigurowanie polityk dostępu, ról użytkowników, VLAN, Captive Portalu oraz inspekcji urządzeń.
- W ramach wdrożenia Wykonawca skonfiguruje autoryzację urządzeń infrastrukturalnych Zamawiającego w oparciu o protokół 802.1X z wykorzystaniem metody EAP-TLS dla telefonów IP marki Cisco tj. konfiguracja uwierzytelniania 802.1X z wykorzystaniem certyfikatu urządzenia (EAP-TLS), punkty dostępowe WiFi Aruba poprzez uwierzytelnianie po certyfikacie urządzenia (EAP-TLS), zgodne z polityką bezpieczeństwa Zamawiającego,
- Wykonawca zapewni odpowiednią konfigurację NAC oraz współpracę z infrastrukturą PKI Zamawiającego, w tym proces wystawiania i instalacji certyfikatów X.509 dla urządzeń.
- W ramach wdrożenia Wykonawca przeprowadzi analizę infrastruktury i wskaże urządzenia nieobsługujące uwierzytelniania 802.1X. Dla tych urządzeń zostanie zaproponowane alternatywne rozwiązanie kontroli dostępu, np. oparte na adresach MAC lub inne równoważne.
- Przeprowadzenie testów poprawności działania zgodnie ze scenariuszem z załącznika.
- Przeprowadzenie szkolenia 6 administratorów (min. 1 dzień).
- Przekazanie dokumentacji technicznej i powdrożeniowej.
- Wykonawca zobowiązany jest po wdrożeniu do przedłożenia oświadczenia, że wdrożony system umożliwia realizację polityk bezpieczeństwa zgodnych z NIS2, w tym przez dostarczenie odpowiednich konfiguracji oraz dokumentacji wspierającej ocenę zgodności, gwarantujące możliwie najwyższy poziom bezpieczeństwa.
- Wykonawca zapewni podstawowy okres wsparcia technicznego od dnia podpisania bezusterkowego, protokolarnego odbioru przedmiotu zamówienia do dnia 30 czerwca 2026 r. oraz w okresie 12 miesięcy od zakończenia podstawowego okresu, tj. od dnia 01 lipca 2026 r. Wsparcie techniczne w dni robocze (poniedziałek–piątek) w godzinach 7:30–15:30. Wsparcie nie może być limitowane liczbą zgłoszeń. Wsparcie techniczne obejmuje również aktualizacje i pomoc przy błędach konfiguracji.

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.