

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa, instalacja i wdrożenie systemu

kontroli dostępu do sieci (NAC)

Część nr 2 zamówienia – Zadanie nr 5 wniosku o dofinansowanie (Obszar techniczny IT)

1. Informacje ogólne

Niniejszy Opis Przedmiotu Zamówienia (OPZ) określa minimalne wymagania techniczne i funkcjonalne dotyczące dostawy, instalacji, konfiguracji i uruchomienia systemu kontroli dostępu do sieci (NAC – Network Access Control) wraz z licencją wsparcia technicznego producenta oraz przeprowadzeniem szkoleń dla administratorów. System obejmuje kontrolę dostępu w szczególności infrastrukturę teleinformatyczną wykorzystywaną przy zbiorowym zaopatrzeniu w wodę, w tym środowisko Stacji Uzdatniania Wody oraz sieci OT infrastruktury wodociągowej.

Parametr	Wartość
Nazwa zamówienia	Dostawa, instalacja i wdrożenie systemu kontroli dostępu do sieci (NAC)
Typ systemu	Network Access Control (NAC) – sprzętowo-programowy lub wirtualny
Minimalna pojemność	Co najmniej 1000 jednoczesnych unikatowych autoryzacji w ciągu dnia
Skalowalność	Do co najmniej 5000 jednoczesnych unikatowych autoryzacji
Licencja systemu	Dożywotnia licencja systemu NAC
Wsparcie techniczne	24 miesiące wsparcia producenta oprogramowania
Szkolenie	2-dniowe warsztaty zdalne dla maksymalnie 4 administratorów
Język interfejsu	Co najmniej język polski i angielski
Dokumentacja powykonawcza	W terminie do 14 dni od zakończenia wdrożenia

2. Zakres przedmiotu zamówienia

Przedmiotem zamówienia jest:

- Dostawa dożywotniej licencji systemu NAC wraz z 24-miesięczną licencją wsparcia technicznego producenta.
- Instalacja i konfiguracja wstępna systemu NAC w środowisku Zamawiającego.
- Konfiguracja podstawowa systemu (integracja z domeną Active Directory, konfiguracja urzędu certyfikacji, uruchomienie wysokiej dostępności HA).
- Konfiguracja urządzenia firewall (dodanie VLAN-u gościnnego, ustawienie polityk).
- Import urządzeń końcowych i tożsamości z Active Directory oraz list dostarczonych przez Zamawiającego.
- Integracja dostarczanych urządzeń sieciowych (przełączniki, punkty dostępowe) z systemem NAC.
- Uruchomienie uwierzytelniania 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych (po jednym z każdej serii) wraz z testami.
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z DHCP, SNMP i skanem portów wraz z testami.

- Przeprowadzenie 2-dniowych warsztatów zdalnych dla maksymalnie 4 administratorów (po 6 godzin dziennie).
- Dostarczenie dokumentacji powykonawczej opisującej wykonane prace i konfigurację poszczególnych urządzeń.

3. Minimalne wymagania techniczne i funkcjonalne

Oferowany system musi spełniać łącznie wszystkie poniższe wymagania minimalne. Niespełnienie któregokolwiek z nich skutkuje odrzuceniem oferty jako niezgodnej z wymaganiami Zamawiającego.

3.1. Wymagania ogólne i architektura

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Kontrola dostępu	System musi posiadać funkcjonalność aktywnego zapobiegania dostępowi do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2	Multi-vendor	System musi współpracować z urządzeniami sieciowymi wielu producentów (multi-vendor).
3	Interfejs zarządzania	System musi być zarządzany wyłącznie z poziomu interfejsu graficznego (GUI) dostępnego przez przeglądarkę internetową (HTML5), bez konieczności instalacji dodatkowych wtyczek, z jednej konsoli.
4	Instalacja rozproszona	System musi wspierać instalację rozproszoną na wielu maszynach fizycznych lub wirtualnych w ramach jednej licencji.
5	Disaster Recovery	System musi wspierać mechanizm Disaster Recovery – tworzenia kopii lustrzanej systemu w celu zachowania ciągłości działania, w ramach jednej licencji.
6	Skalowalność licencji	System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7	Pojemność	System musi obsługiwać co najmniej 1000 jednoczesnych unikatowych autoryzacji do sieci (w tym gości) oraz być skalowalny do przynajmniej 5000 jednoczesnych autoryzacji.
8	Zwalnianie licencji	Licencja musi być zwalniana automatycznie po rozłączeniu urządzenia końcowego.
9	BYOD	System musi obsługiwać jednocześnie agenty oraz urządzenia BYOD (Bring Your Own Device) w liczbie co najmniej równej licencji na jednoczesne autoryzacje.
10	Wirtualizacja	System musi umożliwiać instalację na maszynie wirtualnej (VMware ESXi min. 5.x, Hyper-V min. 2012,

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
		Proxmox min. 5.x, KVM min. 7.x, Citrix XenServer min. 4.x), PaaS lub maszynie fizycznej.
11	Wbudowane serwery	System musi posiadać funkcjonalność następujących serwerów: RADIUS, OTP, Syslog, TACACS+, Monitoring, DHCP, polityk 802.1X, WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12	Wysoka dostępność	System musi umożliwiać wysoką dostępność elementów funkcjonalnych poprzez redundancję modułów dostępu do sieci i DHCP.
13	Język interfejsu	Interfejs graficzny systemu musi być dostępny co najmniej w języku polskim i angielskim.
14	Kontrola dostępu do GUI	System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
15	IPv6	System musi wspierać protokół IPv6 co najmniej dla: konsoli SSH, komunikacji RADIUS, NTP, SNMP oraz komunikacji z Microsoft Active Directory.

3.2. Uwierzytelnianie i integracja

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Uwierzytelnianie administratorów	System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów: OpenLDAP, Microsoft Active Directory, WebServices/API, RADIUS, relacyjne bazy danych (min. MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC).
2	Uwierzytelnianie urządzeń i tożsamości	System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów: OpenLDAP, Microsoft Active Directory, WebServices/API, RADIUS, relacyjnych baz danych.
3	Synchronizacja danych	System musi umożliwiać synchronizację danych (tożsamości, urządzenia, adresy MAC, jednostki OU, konta administracyjne) z Microsoft Active Directory.
4	API CRUD	System musi wspierać API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
5	NTLM / wiele AD	System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, również nie połączonymi relacjami zaufania.
6	Obsługa wielu PKI	System musi obsługiwać wiele PKI dla różnych grup użytkowników.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
7	Protokoły uwierzytelniania	System musi obsługiwać uwierzytelnianie w oparciu o: MAC, PAP/ASCII, CHAP, SNMP, 802.1X (w tym PEAP, EAP-TLS, EAP-TTLS, TEAP, MD5).
8	Suplikanci 802.1X	System musi wspierać implementację 802.1X z suplikantami: Windows 10/11, Apple macOS, Apple iOS, Google Android, Ubuntu.
9	Polityki uwierzytelniania	System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły: tożsamość, grupa, parametry urządzenia, atrybuty AD, urządzenia sieciowe, VLAN, data/czas, metoda autoryzacji.
10	Przypisywanie VLAN / VSA	System musi umożliwiać przypisywanie VLAN i/lub atrybutów RADIUS VSA (ACL, QoS) podczas autoryzacji dla min.: Cisco, Aruba, Extreme, HPE, Juniper, Ruckus, MikroTik, Ubiquiti.
11	IP-to-ID Mapping	System musi wspierać funkcjonalność IP-to-ID Mapping – łączenie tożsamości, adresu IP i adresu MAC.
12	Auto-rejestracja	System musi wspierać auto-rejestrację – łączenie tożsamości, urządzenia, adresu MAC podczas autoryzacji (SNMP, DHCP, NMAP, WMI).
13	Integracja MDM	System może umożliwiać integrację z zewnętrznymi rozwiązaniami MDM (np. Microsoft Intune) – funkcjonalność dodatkowa, niewymagana.
14	EDUROAM	Integracja z EDUROAM nie jest wymagana – funkcjonalność dodatkowa, niepodlegająca ocenie.
15	Zmiana atrybutów AD	System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (Login, Hasło, Imię, Nazwisko, Email, Status).

3.3. Captive Portal i dostęp gościnny

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Wbudowany Captive Portal	System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
2	Logowanie społecznościowe	Logowanie za pomocą portali społecznościowych nie jest wymagane – funkcjonalność dodatkowa, niepodlegająca ocenie.
3	Responsywność	Captive Portal musi automatycznie dostosowywać format do urządzenia końcowego (komputer, tablet, telefon).

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
4	Rejestracja gości / sponsor	Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor.
5	Dwuskładnikowe MFA	Captive Portal musi umożliwiać dwuskładnikowe uwierzytelnianie (OTP) za pomocą tokenu Google Authenticator lub bramki SMS.
6	Logowanie lokalne i AD	Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
7	Zmiana hasła	Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
8	HotSpot / kod dostępu	Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
9	Dynamiczne pola formularza	Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego (pole tekstowe, lista wyboru).
10	Języki	Interfejs Captive Portalu musi być dostępny co najmniej w: języku polskim, angielskim, niemieckim, hiszpańskim, francuskim i ukraińskim.
11	Personalizacja strony	System musi posiadać możliwość personalizacji strony gościnnej.
12	Usuwanie wygasłych kont	Captive Portal powinien obsługiwać automatyczne kasowanie wygasłych kont gościnnych na żądanie lub okresowo (wg zadanej liczby dni).
13	Limit nieudanych logowań	Captive Portal powinien umożliwiać konfigurację maksymalnej liczby nieudanych logowań.
14	Wysyłka danych dostępowych	System musi umożliwiać wysyłanie danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.

3.4. Serwer DHCP

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Zintegrowany serwer DHCP	System musi posiadać funkcję zintegrowanego serwera DHCP.
2	Uruchamianie per podsieć	Serwer DHCP musi umożliwiać uruchamianie usługi dla wybranych podsieci.
3	Statyczny przydział IP	Serwer DHCP musi umożliwiać przypisanie ustalonego adresu IP dla adresu MAC.
4	Różne IP dla tego samego MAC	Serwer DHCP musi obsługiwać przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
5	Filtrowanie MAC	Serwer DHCP musi umożliwiać zwracanie adresów IP wyłącznie dla wcześniej zdefiniowanej grupy adresów MAC oraz blokowanie określonych MAC.
6	Monitoring puli	Serwer DHCP musi zapewniać monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji.
7	Dodatkowe parametry zwrotne	Serwer DHCP musi umożliwiać ustawienie dodatkowych parametrów zwrotnych przesyłanych do klientów.
8	Wizualizacja adresacji IP	System musi umożliwiać podgląd obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego.
9	Zmiana bez restartu	Serwer DHCP musi umożliwiać zmianę przydziału dynamicznego na statyczny bez restartu usługi.

3.5. Serwer TACACS+

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Grupy uprawnień	System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych poprzez serwer TACACS+.
2	Lista komend	System musi umożliwiać tworzenie listy komend uprawnień dla administratorów.
3	Raportowanie komend	System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
4	Rotacja haseł	System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
5	Logowanie AD	System musi umożliwiać logowanie przez TACACS+ za pomocą poświadczeń Microsoft Active Directory.
6	OTP dla administratorów	System musi wspierać logowanie administratorów przez TACACS+ za pomocą tokenów OTP.
7	Atrybuty zwrotne VSA	System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji TACACS+.

3.6. Profilowanie i kontrola zgodności urządzeń końcowych

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Dedykowany agent	System musi posiadać dedykowanego agenta co najmniej dla systemów: Windows, macOS, Linux.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
2	Metody profilowania	System musi obsługiwać profilowanie urządzeń metodami: DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, RADIUS, WMI, MDM, WinRM, ONVIF.
3	Kontrola zgodności – aktualizacje	Agent musi sprawdzać czy system operacyjny jest aktualny z możliwością automatycznego naprawienia niezgodności.
4	Kontrola zgodności – firewall	Agent musi sprawdzać czy włączony jest firewall.
5	Kontrola zgodności – antywirus	Agent musi sprawdzać czy uruchomiony jest system antywirusowy i czy baza sygnatur jest aktualna.
6	Kontrola zgodności – szyfrowanie dysku	Agent musi sprawdzać czy włączone jest szyfrowanie dysku systemowego.
7	Kontrola zgodności – domena AD	Agent musi sprawdzać czy urządzenie jest przyłączone do domeny Microsoft Active Directory.
8	Kontrola zgodności – pliki/katalogi	Agent musi sprawdzać czy na dysku znajdują się wskazane przez administratora pliki lub katalogi.
9	Kontrola zgodności – procesy i usługi	Agent musi sprawdzać czy w systemie uruchomione są wskazane procesy i usługi, z możliwością automatycznego naprawienia niezgodności.
10	Kontrola zgodności – rejestr	Agent musi sprawdzać wpisy w rejestrze systemowym wg klucza, wartości i typu (Number, String, Version).
11	Autokonfiguracja sieci	System musi posiadać mechanizm autokonfiguracji sieci (przewodowej i bezprzewodowej) dla: Windows, macOS, iOS, Android – bez angażowania działu IT.
12	Instalacja certyfikatu przez autokonfigurację	System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci.

3.7. Certyfikaty CA

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Zintegrowany serwer CA	System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2	Generowanie i podpisywanie certyfikatów	Funkcja CA musi umożliwiać generowanie i podpisywanie certyfikatów dla tożsamości i urządzeń końcowych.
3	Bezpieczne przechowywanie	System musi zapewniać bezpieczne przechowywanie certyfikatów tożsamości i urządzeń końcowych.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
4	SCEP	System musi umożliwiać generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
5	OCSP	System musi obsługiwać usługę OCSP (Online Certificate Status Protocol).

3.8. Monitorowanie, raportowanie i alarmy

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Monitoring autoryzacji i zdarzeń	System musi umożliwiać monitoring: autoryzacji, zdarzeń systemowych, zdarzeń DHCP, tożsamości, urządzeń końcowych i sieciowych.
2	Raport stanu systemu	System musi generować raport stanu systemu (dane z węzłów, wykorzystanie polityk, błędy krytyczne, obciążenie CPU/RAM, zmiany konfiguracji) dostępny z poziomu konsoli CLI, interfejsu WWW oraz emaila.
3	Raport zdarzeń logowania	System musi generować raport zdarzeń logowania z informacją o nadanym adresie IP.
4	Raport logów DHCP	System musi generować raport z logów DHCP z informacją o polityce dostępu do sieci.
5	Graficzny podgląd przełącznika	System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
6	Graficzny podgląd stosów	System musi wspierać graficzny podgląd urządzeń sieciowych działających w stosie.
7	Monitoring drukarek	Graficzny monitoring zasobów drukarek sieciowych nie jest wymagany – funkcjonalność dodatkowa, niepodlegająca ocenie.
8	Podgląd tożsamości w czasie rzeczywistym	System musi umożliwiać podgląd tożsamości i urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym, z podziałem wg urządzeń sieciowych i kontrolerów WiFi.
9	Raport OTP	System musi generować raport z logów OTP z informacją o poprawnej i błędnej autoryzacji oraz wysłanym tokenie SMS.
10	Raport zdarzeń AD	System musi generować raport zdarzeń Microsoft Active Directory, w tym: logowania/wylogowania (w tym błędne), logowania do sieci 802.1X.
11	Alarmy e-mail / Syslog	System musi umożliwiać generowanie alarmów systemowych (e-mail, Syslog, notyfikacje) dla sytuacji krytycznych: liczba transakcji RADIUS, opóźnienie RADIUS, status krytyczny modułów.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
12	Narzędzia diagnostyczne	System musi posiadać narzędzia diagnostyczne: ping, traceroute, tcpdump (RADIUS, TACACS+), wyszukiwanie zdarzeń RADIUS z filtrowaniem po nazwie użytkownika, MAC, statusie, czasie.
13	Eksport do SIEM	System musi posiadać funkcjonalność wysyłania zdarzeń do systemów SIEM co najmniej protokołem Syslog.

3.9. Zarządzanie siecią i urządzeniami

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Monitoring SNMP	System musi umożliwiać monitoring urządzeń sieciowych i końcowych za pomocą protokołu SNMP.
2	Inwentaryzacja	System musi umożliwiać zbieranie danych inwentaryzacyjnych i sprawdzanie kondycji urządzeń za pomocą SNMP.
3	Zarządzanie portami	System musi zarządzać urządzeniami sieciowymi w zakresie: monitoringu, zapisu zmian konfiguracji, konfiguracji portów (VLANy, autoryzacja, status, opis).
4	Automatyczne egzekwowanie polityk	System musi obsługiwać automatyczne egzekwowanie zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
5	LLDP / CDP	System musi umożliwiać budowanie topologii sieci za pomocą protokołów LLDP i CDP.
6	Kwarantanna	System musi posiadać mechanizm rozłączania dostępu do sieci z możliwością dodania tożsamości/urządzenia/MAC do kwarantanny z poziomu interfejsu aplikacji.
7	Rozłączanie sesji	System musi obsługiwać rozłączanie sesji min.: SNMP, komend CLI, RADIUS CoA (RFC 5176).
8	Integracja zewnętrzna	System musi posiadać mechanizm integracji z systemami zewnętrznymi za pomocą: Syslog, SNMP Trap, REST API – w celu wykrywania anomalii i blokowania dostępu do sieci.
9	Serwer DHCP	System musi posiadać funkcjonalność konfiguracji serwera DHCP dla tworzonych podsieci IP.
10	Autodiscovery	System musi automatycznie wyszukiwać urządzenia sieciowe i końcowe w wybranych podsieciach minimum za pomocą SNMP v1, v2c i v3.
11	Kopia bezpieczeństwa	System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
12	Szablony e-mail i poświadczeń	System musi umożliwiać konfigurację własnych szablonów wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.

4. Wymagania dotyczące wdrożenia

Wykonawca zobowiązany jest zrealizować wdrożenie obejmujące co najmniej następujące etapy:

- Dostawa, instalacja i konfiguracja wstępna systemu NAC w środowisku Zamawiającego.
- Podstawowa konfiguracja systemu: integracja z domeną Active Directory, konfiguracja urzędu certyfikacji (CA), uruchomienie wysokiej dostępności (HA).
- Konfiguracja urządzenia firewall: dodanie VLAN-u gościnnego, ustawienie polityk dostępu.
- Import urządzeń końcowych i tożsamości z Active Directory oraz dostarczonych przez Zamawiającego list.
- Integracja dostarczanych urządzeń sieciowych (przełączniki, punkty dostępowe) z systemem NAC w ramach dostępnych funkcjonalności.
- Uruchomienie uwierzytelniania 802.1X (EAP-TLS) na urządzeniach wzorcowych (po jednym z każdej serii) wraz z testami potwierdzającymi poprawność działania.
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z DHCP, SNMP i skanem portów wraz z testami.
- Przeprowadzenie 2-dniowych warsztatów zdalnych dla maksymalnie 4 administratorów Zamawiającego (po 6 godzin dziennie), zakończonych wydaniem zaświadczeń.
- Opracowanie i dostarczenie dokumentacji powykonawczej w terminie do 14 dni od zakończenia wdrożenia.

5. Wymagania dotyczące szkoleń

Wykonawca w ramach wynagrodzenia zapewni:

- 2-dniowe warsztaty zdalne dla maksymalnie 4 administratorów Zamawiającego, po 6 godzin dziennie.
- Program warsztatów obejmujący co najmniej: konfigurację i administrację wdrożonym systemem NAC, zarządzanie użytkownikami i politykami, diagnostykę i rozwiązywanie problemów.
- Materiały szkoleniowe w języku polskim w formie elektronicznej dla każdego uczestnika.
- Zaświadczenia potwierdzające uczestnictwo w warsztatach i nabycie umiejętności obsługi systemu NAC dla każdego uczestnika.
- Szczegółowy plan, zakres i terminy warsztatów uzgodniony z Zamawiającym przed ich rozpoczęciem.

6. Wymagania dotyczące wsparcia technicznego

Wykonawca dostarczy, wraz z dożywotnią licencją systemu NAC, 24-miesięczną licencję na wsparcie techniczne producenta obejmującą co najmniej:

- Kontakt mailowy z działem wsparcia technicznego producenta w celu rozwiązywania problemów związanych z wdrożeniem lub obsługą systemu.
- Rozwiązywanie powtarzalnych i możliwych do odtworzenia problemów związanych z oprogramowaniem, a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów, pomoc w określaniu parametrów konfiguracyjnych oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej producenta.
- Dostęp do aktualizacji i poprawek oprogramowania dostępnych z poziomu interfejsu systemu.

7. Dokumentacja powykonawcza

Wykonawca zobowiązany jest do dostarczenia dokumentacji powykonawczej w terminie do 14 dni od daty zakończenia wdrożenia. Dokumentacja musi obejmować co najmniej:

- Opis zrealizowanych prac wdrożeniowych.
- Opis konfiguracji systemu NAC (parametry, polityki, integracje).
- Opis konfiguracji poszczególnych urządzeń sieciowych zintegrowanych z systemem.
- Schemat topologii sieci po wdrożeniu.
- Dane dostępowe do systemu (konta administracyjne, adresy URL konsoli zarządzania).