OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa i wdrożenie systemu kontroli dostępu do sieci (NAC) dla sieci biurowej

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji dożywotniej (bezterminowej) systemu kontroli dostępu do sieci klasy NAC (Network Access Control), zwanego dalej „Systemem", przeznaczonego do ochrony sieci biurowej Zamawiającego (przewodowej i bezprzewodowej), wraz z 12-miesięczną licencją wsparcia technicznego producenta oprogramowania, wdrożeniem Systemu oraz szkoleniem dla 2 osób w wymiarze 4 godzin.

1.2. Zakres ilościowy zamówienia:

Lp.	Element przedmiotu zamówienia	Ilość
1	Licencja dożywotnia (bezterminowa) Systemu NAC na co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości), z możliwością rozbudowy do co najmniej 200 – zgodnie z rozdz. 4	1 kpl.
2	Licencja wsparcia technicznego producenta oprogramowania na okres 12 miesięcy – zgodnie z rozdz. 7	1 kpl.
3	Usługa wdrożenia Systemu w sieci biurowej Zamawiającego – zgodnie z rozdz. 5	1 usługa
4	Szkolenie z administrowania Systemem – 4 godziny zegarowe, 2 osoby, forma stacjonarna lub zdalna – zgodnie z rozdz. 6	1 usługa

1.3. Kody CPV: 48000000-8 Pakiety oprogramowania i systemy informatyczne; 48730000-4 Pakiety oprogramowania zabezpieczającego; 72263000-6 Usługi wdrażania oprogramowania; 80533100-0 Usługi szkolenia komputerowego.

2. Opis środowiska Zamawiającego

2.1. System zostanie wdrożony w sieci biurowej Zamawiającego. Środowisko obejmuje w szczególności:

- liczba stanowisk pracy i użytkowników: do 25; szacunkowa liczba urządzeń końcowych (komputery, drukarki, telefony VoIP, urządzenia mobilne, inne): 100;
- przełączniki sieciowe: TP-Link, NetGear
- kontroler Wi-Fi / punkty dostępowe (producent, model, liczba), SSID: brak;
- platforma wirtualizacyjna przeznaczona dla Systemu: VMware ESXi / Hyper-V / Proxmox;
- zapora sieciowa / koncentrator VPN: UTM;
- system SIEM / serwer Syslog: w trakcie wdrażania; system MDM: brak;

2.2. Szczegółowe informacje o konfiguracji sieci zostaną przekazane Wykonawcy po zawarciu umowy i podpisaniu zobowiązania do zachowania poufności.

3. Wymagania ogólne

3.1. Wykonawca dostarczy licencje fabrycznie nowe, pochodzące z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, udzielone na rzecz Zamawiającego.

3.2. Licencja Systemu musi być dożywotnia (bezterminowa). Po upływie okresu wsparcia technicznego producenta System musi zachować pełną funkcjonalność w zakresie dostarczonej wersji, bez ograniczenia liczby obsługiwanych autoryzacji.

3.3. Zamawiający zapewni zasoby infrastruktury wirtualizacyjnej dla Systemu. Wykonawca wskaże w ofercie minimalne wymagania sprzętowe (vCPU, RAM, przestrzeń dyskowa) dla oferowanej konfiguracji, w tym dla instalacji rozproszonej i mechanizmu Disaster Recovery.

3.4. Wszystkie licencje niezbędne do realizacji wymagań z rozdz. 4 muszą być dostarczone w ramach zamówienia. Zamawiający nie dopuszcza konieczności zakupu dodatkowych licencji lub modułów w celu spełnienia wymagań, z wyjątkiem licencji rozszerzających liczbę autoryzacji powyżej wartości z pkt 1.2 lp. 1.

3.5. Dokumentacja techniczna Systemu musi być dostępna w języku polskim lub angielskim; dokumentacja powykonawcza i materiały szkoleniowe – w języku polskim.

3.6. Wymagania sformułowane w rozdz. 4 słowem „musi" są wymaganiami obowiązkowymi – ich niespełnienie skutkuje odrzuceniem oferty. Wymagania sformułowane słowem „powinien" (pkt 49, 50, 52, 53, 54) są wymaganiami pożądanymi – ich niespełnienie nie skutkuje odrzuceniem oferty.

4. Wymagania funkcjonalne i techniczne Systemu

Wymagania dotyczące wartości liczbowych są wymaganiami minimalnymi; dopuszcza się parametry lepsze.

Lp.	Wymaganie minimalne		
0	Producent, nazwa i wersja oferowanego oprogramowania NAC oraz nazwa/oznaczenie oferowanej licencji i licencji wsparcia technicznego producenta.		
A. Podstawowa funkcjonalność systemu NAC			
1	System musi posiadać funkcjonalność aktywnego zapobiegania dostępowi do sieci nieautoryzowanych użytkowników i urządzeń końcowych.		
2	System musi współpracować z urządzeniami wielu producentów (tzw. multi-vendor).		
3	System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli; interfejs WEB w wersji HTML5 niewymagający obsługi dodatkowych wtyczek.		
4	System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.		
5	System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.		
6	System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.		
7	System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do co najmniej 200 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.		
8	Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.		
9	System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) w liczbie co najmniej równej liczbie licencji na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.		
10	System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:		

Lp.	Wymaganie minimalne		
	– VM – min. VMware ESXi co najmniej w wersji 5.x, Hyper-V w wersji min. 2012, Proxmox w wersji min. 5.x, KVM , Citrix XenServer w wersji min. 4.x, – maszyny fizyczne – serwery wspierane przez producenta.		
11	System musi posiadać funkcjonalność serwerów: – serwera RADIUS dla infrastruktury sieciowej, – serwera OTP dla infrastruktury VPN, Captive Portal, TACACS+, – serwera SYSLOG, – serwera TACACS+, – serwera monitoringu, – serwera DHCP, – serwera polityk uwierzytelniania i kontroli dostępu 802.1X, – serwera WWW (HTTP/HTTPS) dla uwierzytelniania gościnnego.		
12	System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.		
13	System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji, w tym OpenLDAP, Microsoft Active Directory, WebServices/API, RADIUS, relacyjnych baz danych: min. MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.		
14	System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji, w tym OpenLDAP, Microsoft Active Directory, Google G Suite, WebServices/API, RADIUS, relacyjnych baz danych: min. MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.		
15	System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, RADIUS, OpenLDAP, relacyjne bazy danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), Check Point, ServiceNow).		
16	Podczas synchronizacji system musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenie lokalnych haseł, certyfikatów oraz wysyłanie konfiguracji dostępowych poprzez e-mail.		
17	System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.		
18	System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także niepołączonymi relacjami zaufania.		
19	System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.		
20	System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.		
21	System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. login, hasło, imię, nazwisko, e-mail, status).		
22	System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji i kasowania.		
23	Interfejs graficzny systemu musi być dostępny w różnych wersjach językowych (min. w języku polskim i angielskim).		

Lp.	Wymaganie minimalne		
24	System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.		
25	System musi posiadać możliwość raportowania podłączonych tożsamości i urządzeń końcowych podłączonych do sieci, min.: tożsamość, adres MAC, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony VLAN z przydzielonym adresem IP.		
26	System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny z podglądem wszystkich portów i modułów zarządzanego urządzenia.		
27	System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.		
28	System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.		
29	System musi posiadać funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu zmian konfiguracji oraz konfiguracji ustawień portu w zakresie min. VLAN-ów, autoryzacji, statusu, opisu.		
30	System musi obsługiwać automatyczne egzekwowanie zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.		
31	System musi posiadać możliwość konfiguracji serwera DHCP dla utworzonych podsieci IP.		
32	System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.		
33	System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach, minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.		
34	System musi posiadać funkcjonalność wysyłania zdarzeń, np. do systemów SIEM, minimum protokołem Syslog, z informacjami z serwerów autoryzacji, DHCP, VPN, OTP, TACACS+.		
35	System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.		
36	System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).		
37	System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook, Google i LinkedIn.		
38	System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez e-mail, bramkę SMS oraz zapasową bramkę SMS.		
39	System musi posiadać funkcję personalizacji strony gościnnej.		
40	Captive Portal musi się automatycznie dostosowywać formatem do podłączonego urządzenia końcowego, min.: komputer, tablet, telefon.		
41	Captive Portal musi umożliwiać rejestrację gości potwierdzaną przez konta typu sponsor.		
42	Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego w Google Authenticator lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.		

Lp.	Wymaganie minimalne		
43	Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.		
44	Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.		
45	Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.		
46	Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np. pole tekstowe, lista wyboru.		
47	Interfejs graficzny Captive Portalu musi być dostępny w różnych wersjach językowych (min. w języku polskim, angielskim, niemieckim, hiszpańskim, francuskim i ukraińskim).		
48	Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.		
49	Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie oraz okresowo, wg zadanej liczby dni.		
50	Captive Portal powinien umożliwiać konfigurację maksymalnej liczby nieudanych logowań.		
51	System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP i CDP.		
52	System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołów, min. Syslog, SNMP Trap, REST API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.		
53	System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością dodania tożsamości, urządzenia końcowego lub adresu MAC do kwarantanny.		
54	System powinien posiadać mechanizm rozłączania sesji min. przez SNMP, komendy CLI, RADIUS CoA zgodnie z RFC 5176.		
55	System musi posiadać dedykowanego agenta min. dla systemów Windows, macOS, Linux w celu profilowania urządzeń końcowych.		
56	System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia i systemu operacyjnego, co najmniej przez: DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, RADIUS, WMI, MDM, WinRM, ONVIF.		
57	System musi umożliwiać integrację z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).		
58	System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum dla systemów: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.		
59	System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa, co najmniej: – czy system jest aktualny – z możliwością automatycznego naprawienia niezgodności, – czy włączona jest zapora sieciowa (firewall), – czy uruchomiony jest system antywirusowy i czy baza sygnatur jest aktualna, – czy włączone jest szyfrowanie dysku systemowego, – czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory, – czy na dysku znajdują się pliki lub katalogi wskazane przez administratora,		

Lp.	Wymaganie minimalne		
	– czy w systemie są uruchomione procesy wskazane przez administratora, – czy w systemie są uruchomione usługi wskazane przez administratora – z możliwością automatycznego naprawienia niezgodności, – czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem: • wartości klucza rejestru, • typu wartości: Number, String, Version.		
60	System musi posiadać możliwość wysyłania komunikatów do użytkowników min. za pomocą agenta i Captive Portalu.		
61	System musi współpracować z serwerem tokenów.		
62	System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników dział IT, co najmniej dla systemów: – Microsoft Windows, – macOS, – iOS, – Android.		
63	System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).		
64	System musi wspierać protokół IPv6 min. dla konsoli SSH, komunikacji RADIUS, NTP, SNMP oraz komunikacji z Microsoft Active Directory.		
B. Mechanizmy uwierzytelniania			
65	System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.		
66	System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły: – MAC, – PAP/ASCII, – CHAP, – SNMP, – 802.1X, wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania, np. IEEE 802.1X (PEAP), IEEE 802.1X (EAP-TLS), IEEE 802.1X (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP itp.		
67	System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.		
68	System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.		
69	System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows 10, Windows 11, Apple macOS Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).		
70	System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły: – tożsamość/urządzenie końcowe, – grupa tożsamości/urządzeń końcowych, – parametry urządzeń końcowych, min.: system operacyjny, wersja, – atrybuty Active Directory, – jednostka organizacyjna tożsamości/urządzeń końcowych,		

Lp.	Wymaganie minimalne		
	– urządzenia sieciowe sieci przewodowej i bezprzewodowej, – grupy urządzeń sieciowych, – porty urządzeń sieciowych, – grupy portów urządzeń sieciowych, – jednostka organizacyjna portów, – punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID), – data, czas ważności polityki, – wewnętrzny Captive Portal, – metoda autoryzacji.		
71	System musi umożliwiać przypisywanie sieci VLAN i/lub zwrotnych atrybutów RADIUS VSA podczas etapu autoryzacji, np. ACL, Quality of Service, co najmniej dla następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MikroTik, Ubiquiti Networks.		
72	System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP i adresu MAC.		
73	System musi wspierać funkcjonalność autorejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego i adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.		
74	System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.		
75	System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.		
76	System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.		
77	System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.		
78	System musi umożliwiać tworzenie hasła dnia dla tożsamości zarejestrowanych przez wewnętrzny Captive Portal.		
79	System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.		
80	System musi wspierać uwierzytelnianie urządzeń końcowych na podstawie adresów MAC zawartych w lokalnej bazie.		
81	System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal WWW.		
82	System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.		
83	System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP, zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.		
C. Obsługa serwerów certyfikatów CA			
84	System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.		

Lp.	Wymaganie minimalne		
85	Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać co najmniej następujące funkcjonalności: – możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych, – możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych, – możliwość generowania certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol), – usługę OCSP (Online Certificate Status Protocol).		
D. Obsługa serwerów DHCP			
86	System musi posiadać funkcję zintegrowanego serwera DHCP.		
87	System musi wspierać funkcjonalność autorejestracji, polegającą na łączeniu urządzenia końcowego i adresu MAC podczas pracy serwera DHCP.		
88	System musi zapewniać co najmniej następujące funkcjonalności serwera DHCP: – uruchamianie usługi dla wybranych podsieci, – przypisanie ustalonego adresu IP dla adresu MAC, – przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci, – możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC, – możliwość określania braku dostępu dla wybranych adresów MAC, – monitoring obciążenia pul dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC, – możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP, – możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego, – możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi, – dokonywanie zmian bez konieczności wyłączania usług.		
E. Obsługa serwerów TACACS+			
System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu do urządzeń sieciowych, w tym:			
89	System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.		
90	System musi umożliwiać tworzenie haseł administratorom.		
91	System musi umożliwiać tworzenie listy komend uprawnień dla administratorów.		
92	System musi raportować wszystkie wydane komendy na kontrolowanych urządzeniach sieciowych.		
93	System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.		
94	System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.		
95	System musi wspierać logowanie administratorów za pomocą tokenów OTP.		
96	System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.		
F. Raportowanie i monitoring			
System musi umożliwiać generowanie raportów oraz monitoring co najmniej następujących parametrów:			

Lp.	Wymaganie minimalne		
97	Monitoring autoryzacji.		
98	Monitoring zdarzeń systemowych.		
99	Monitoring zdarzeń DHCP.		
100	Monitoring tożsamości.		
101	Monitoring urządzeń końcowych.		
102	Monitoring urządzeń sieciowych.		
103	Raport stanu systemu (min. szczegółowe dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostatnie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenie portów – przepustowość, liczba autoryzacji), dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu e-mail.		
104	Raport ze zdarzeń logowania z informacją o nadanym adresie IP.		
105	Raport stanu systemu z poziomu konsoli CLI, min.: obciążenie procesora, pamięci, przestrzeni dyskowej, działanie usług.		
106	Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.		
107	System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.		
108	System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.		
109	System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności VLAN-ów w urządzeniach sieciowych działających w środowisku.		
110	System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.		
111	System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych, w tym: podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min.: system operacyjny, wersja.		
112	System musi umożliwiać podgląd tożsamości i urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych i kontrolerów Wi-Fi.		
113	Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji oraz o tokenach wysłanych przez bramkę SMS.		
114	Raport zdarzeń Microsoft Active Directory, minimum: – logowania i wylogowania z systemu, w tym błędne logowania, – logowania do sieci 802.1X.		
G. Alarmy i diagnostyka			
115	System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: – wiadomości e-mail, – Syslog, – notyfikacji systemowych.		

Lp.	Wymaganie minimalne		
116	Alarmy muszą móc być generowane co najmniej w sytuacjach: – przekroczenia ilości obsługiwanych transakcji RADIUS, – opóźnienia obsługi transakcji RADIUS, – statusu krytycznego modułów.		
117	System musi posiadać zestaw narzędzi diagnostycznych do rozwiązywania problemów, w tym: – badanie łączności IP za pomocą ping, traceroute, – tcpdump protokołów RADIUS, TACACS+, – wyszukiwanie zdarzeń RADIUS z uwzględnieniem: • nazwy użytkownika, • adresu MAC, • statusu uwierzytelnienia (udane lub nieudane), • powodu, jeżeli uwierzytelnienie było nieudane, • zakresu czasowego, co do dnia, godziny i minuty, – wykonanie zdalnego polecenia na urządzeniu sieciowym.		

Wraz z ofertą Wykonawca złoży:

- wypełnioną tabelę wymagań załączoną do formularza ofertowego (zał. 2.1.) (kolumny „Spełnia” i „Parametry oferowane / sposób spełnienia”), ze wskazaniem producenta, nazwy i wersji oferowanego oprogramowania;
- kartę katalogową, specyfikację techniczną lub inny dokument producenta potwierdzający spełnienie wymagań (w języku polskim lub angielskim).

5. Wdrożenie Systemu

5.1. Analiza przedwdrożeniowa

- Wykonawca w terminie do 10 dni od zawarcia umowy przeprowadzi analizę środowiska (urządzenia sieciowe, segmentacja VLAN, Active Directory, rodzaje urządzeń końcowych, w tym urządzenia nieobsługujące 802.1X).
- Na jej podstawie Wykonawca opracuje projekt techniczny wdrożenia, obejmujący m.in. architekturę Systemu, politykę dostępu dla poszczególnych grup, plan etapowania i plan wycofania zmian. Projekt wymaga akceptacji Zamawiającego.

5.2. Instalacja

- Instalacja Systemu na infrastrukturze wirtualizacyjnej Zamawiającego, w tym konfiguracja instalacji rozproszonej / wysokiej dostępności i Disaster Recovery.
- Aktualizacja do najnowszej stabilnej wersji, zabezpieczenie konfiguracji (hardening), ograniczenie dostępu do panelu administracyjnego do segmentu zarządzania, konfiguracja kont administratorów i ról.
- Konfiguracja cyklicznej kopii bezpieczeństwa i przeprowadzenie testu odtworzenia.

5.3. Integracje

- Integracja z Microsoft Active Directory, przełącznikami i kontrolerem Wi-Fi/punktami dostępowymi wskazanymi w pkt 2.1 (RADIUS, RADIUS CoA, SNMP).
- Przekazywanie zdarzeń do systemu SIEM / serwera Syslog Zamawiającego.
- Integracja z systemem MDM, zaporą sieciową / VPN (OTP) i serwerem DHCP.

5.4. Polityki dostępu

- Pracownicy i komputery służbowe – uwierzytelnianie 802.1X (EAP-TLS z certyfikatami lub PEAP z przypisaniem VLAN/ACL.
- Urządzenia bez suplikanta 802.1X (drukarki, telefony VoIP, urządzenia IoT) – uwierzytelnianie MAC z profilowaniem urządzeń.
- Goście – Captive Portal z rejestracją potwierdzaną przez sponsora, osobny VLAN z dostępem wyłącznie do Internetu; BYOD – rejestracja urządzeń prywatnych.
- Agent i badanie zgodności (posture) dla komputerów służbowych, VLAN kwarantanny i komunikaty dla użytkowników.

5.5. Uruchomienie etapowe

- System zostanie najpierw uruchomiony w trybie monitorowania (bez blokowania dostępu) na okres nie krótszy niż 14 dni, w celu inwentaryzacji urządzeń i weryfikacji polityk.
- Włączanie egzekwowania polityk odbywać się będzie stopniowo (np. według przełączników lub segmentów), w oknach serwisowych uzgodnionych z Zamawiającym, z zachowaniem planu wycofania zmian.

5.6. Testy odbiorowe

- Testy obejmą co najmniej: dostęp pracownika (802.1X), dostęp urządzenia bez suplikanta (MAC), odmowę dostępu dla nieznanego urządzenia, przypisanie do VLAN kwarantanny dla urządzenia niezgodnego z polityką, rejestrację gościa przez Captive Portal, rozłączenie sesji (CoA), przekazanie zdarzeń do SIEM, odtworzenie z kopii bezpieczeństwa oraz procedurę awaryjną.
- Scenariusze testów Wykonawca przedstawi do akceptacji Zamawiającego przed ich przeprowadzeniem.

5.7. Dokumentacja powykonawcza

- Wykonawca przekaże w języku polskim dokumentację powykonawczą zawierającą m.in.: opis architektury i konfiguracji, polityki dostępu, konfigurację urządzeń sieciowych w zakresie NAC, procedury administracyjne, procedurę kopii bezpieczeństwa i odtwarzania oraz procedurę awaryjną (przywrócenie dostępu do sieci w przypadku niedostępności Systemu).
- Wykonawca przekaże Zamawiającemu wszystkie hasła i poświadczenia utworzone w trakcie wdrożenia.

5.8. Prace wykonywane będą w siedzibie Zamawiającego lub zdalnie, wyłącznie za pośrednictwem kanału dostępu wskazanego i kontrolowanego przez Zamawiającego. Osoby realizujące wdrożenie podpiszą zobowiązanie do zachowania poufności.

6. Szkolenie

6.1. Wykonawca przeprowadzi szkolenie w zakresie użytkowania i administrowania wdrożonym Systemem NAC dla **2 osób** wskazanych przez Zamawiającego.

6.2. Szkolenie odbędzie się w wymiarze **4 godzin zegarowych** (1 godzina = 60 minut), w jednym dniu roboczym, w godzinach 8:00–16:00. Czas przerw nie wlicza się do czasu szkolenia.

6.3. Szkolenie zostanie przeprowadzone w jednej z następujących form, **według wyboru Zamawiającego**:

- **stacjonarnej** – w siedzibie Zamawiającego; Zamawiający zapewni salę, a Wykonawca ponosi wszelkie koszty związane z dojazdem i pobytem prowadzącego;
- **zdalnej (online)** – w czasie rzeczywistym, z udziałem prowadzącego, z możliwością zadawania pytań i udostępniania ekranu, za pośrednictwem platformy zapewnionej przez Wykonawcę, niewymagającej zakupu licencji ani instalacji płatnego oprogramowania po stronie Zamawiającego. Zamawiający nie dopuszcza szkolenia w formie nagrania lub kursu e-learningowego.

6.4. Zamawiający poinformuje Wykonawcę o wybranej formie szkolenia przy uzgadnianiu terminu, nie później niż 5 dni roboczych przed terminem szkolenia.

6.5. Szkolenie odbędzie się po zakończeniu wdrożenia Systemu i będzie uwzględniać konfigurację wdrożoną u Zamawiającego. Ćwiczenia praktyczne prowadzone będą na wdrożonym Systemie lub na środowisku testowym, w sposób niezakłócający pracy sieci produkcyjnej.

6.6. Szkolenie przeprowadzi osoba posiadająca praktyczną wiedzę w zakresie oferowanego Systemu (np. certyfikat producenta lub doświadczenie we wdrożeniach Systemu).

6.7. Ramowy program szkolenia (szczegółowy program Wykonawca przedstawi do akceptacji Zamawiającego nie później niż 5 dni roboczych przed terminem szkolenia):

Lp.	Zakres tematyczny	Czas (orientacyjnie)
1	Architektura i elementy wdrożonego Systemu, konsola zarządzania, konta i uprawnienia administratorów	30 min
2	Polityki uwierzytelniania i autoryzacji: 802.1X, uwierzytelnianie MAC, przypisywanie VLAN/ACL, kwarantanna, rozłączanie sesji (CoA)	60 min
3	Obsługa gości i BYOD: Captive Portal, konta sponsorskie, autokonfiguratory sieci, certyfikaty (CA)	30 min
4	Profilowanie urządzeń, agent i badanie zgodności (posture)	30 min
5	Monitoring, raporty, alarmy, przekazywanie zdarzeń do SIEM	30 min
6	Utrzymanie Systemu: kopie bezpieczeństwa i odtwarzanie, aktualizacje, narzędzia diagnostyczne, procedura awaryjna	30 min
7	Pytania uczestników, podsumowanie	30 min
	Razem	**240 min**

6.8. Wykonawca dostarczy każdemu uczestnikowi materiały szkoleniowe w języku polskim w postaci elektronicznej, najpóźniej w dniu szkolenia. Zamawiający może je wykorzystywać na potrzeby własne bez ograniczeń czasowych.

6.9. Po zakończeniu szkolenia uczestnicy otrzymają imienne zaświadczenia potwierdzające uczestnictwo w szkoleniu oraz nabycie umiejętności obsługi Systemu NAC.

6.10. Szczegółowy plan i termin szkolenia zostaną uzgodnione przez Wykonawcę z Zamawiającym. Potwierdzeniem realizacji szkolenia będzie lista obecności (w formie zdalnej – raport uczestnictwa z platformy) oraz protokół odbioru szkolenia.

7. Licencja wsparcia technicznego producenta

7.1. Wykonawca dostarczy wraz z dożywotnią licencją Systemu NAC 12-miesięczną licencję na wsparcie producenta oprogramowania, liczoną od dnia podpisania protokołu odbioru końcowego. Licencja ta musi obejmować co najmniej:

- kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą Systemu NAC,
- rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem, a także wsparcie przy identyfikacji problemów trudnych do powtórzenia,
- wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów konfiguracji oprogramowania, a także wstępne obejścia dla wykrytych problemów,

- dostęp do dokumentacji i instrukcji na stronie internetowej,
- dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

7.2. Zgłoszenia mogą być składane w języku polskim lub angielskim.

8. Termin realizacji i odbiór

8.1. Dostawa licencji (przekazanie kluczy licencyjnych i dostępu do portalu producenta): do [●] dni od zawarcia umowy.

8.2. Wdrożenie Systemu: do 30 dni od zawarcia umowy – z uwzględnieniem analizy przedwdrożeniowej i okresu monitorowania z pkt 5.5.

8.3. Szkolenie: do 7 dni od dnia odbioru wdrożenia, w terminie uzgodnionym z Zamawiającym.

8.4. Odbiór realizowany będzie protokołami: odbioru dostawy licencji, odbioru wdrożenia (po pozytywnych testach z pkt 5.6), odbioru szkolenia oraz protokołem odbioru końcowego. Zamawiający może odmówić odbioru w przypadku stwierdzenia niezgodności z OPZ.

9. Rozwiązania równoważne

9.1. Wskazane w OPZ nazwy systemów, produktów i producentów (np. Microsoft Active Directory, Microsoft Intune, FortiGate, Cisco) określają systemy i urządzenia, z którymi oferowany System musi współpracować, i nie stanowią wskazania przedmiotu zamówienia.

9.2. Jeżeli w OPZ wskazano znak towarowy, patent, pochodzenie lub normę w odniesieniu do przedmiotu zamówienia, Zamawiający dopuszcza rozwiązania równoważne, zapewniające co najmniej parametry i funkcjonalności opisane w OPZ (art. 99 ust. 5 i 6 ustawy Pzp). Wykazanie równoważności spoczywa na Wykonawcy.