ZAŁĄCZNIK NR 5 – OPIS PRZEDMIOTU ZAMÓWIENIA

I. Podstawowa funkcjonalność systemu:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu 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 niewymagających 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 500 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1000 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) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
    - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min. 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, 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 uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.

13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, 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 ActiveDirectory, Google Workspace, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, 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, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
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 nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę 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, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, 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, na którym dostępny jest podgląd 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. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych 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 informacji 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, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
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 dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, 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, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, 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 określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje 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, minumum na systemach: 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 włączony jest firewall
    - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
    - Czy jest włączone szyfrowanie dysku systemowego
    - Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
    - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora

- 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 Portal.
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 Zespołu Informatyków dla systemów co najmniej:
    - Microsoft Windows
    - Mac OS
    - 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, komunikację z Microsoft Active Directory.

II. Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. 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.
3. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
4. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
5. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).

6. 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,
    - Urządzenia sieciowe sieci przewodowej, 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.
7. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Netgear, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
8. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
9. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
10. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
11. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
12. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
14. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
15. 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.

16. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
17. 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.
18. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
19. 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.

III. Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
    - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
    - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
    - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
    - usługę OCSP (Online Certificate Status Protocol).

IV. Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej 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 puli 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.

V. Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów.
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

VI. Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadam adresie IP.

9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. 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.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
    - Logowania, wylogowania z system w tym błędne logowania
    - Logowania do sieci 802.1X

VII. Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
    - wiadomości e-mail,
    - Syslog,
    - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min.:
    - Ilości obsługiwanych transakcji RADIUS,
    - Opóźnienie obsługi transkacji RADIUS,
    - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla 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 (udana lub nieudana),
– powodu, jeżeli uwierzytelnienie nieudane,
– zakresu czasowego, co do dnia, godziny i minuty,

- wykonanie zdalnego polecenia na urządzeniu sieciowym.

VIII. Wymagania dotyczące wdrożenia i harmonogram ramowy:

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku Zamawiającego.
- Dostawa jednego zarządzanego przełącznika gigabitowego PoE min. 8 port (w tym min. 4 porty PoE) w obudowie typu biurkowego, ze wsparciem dla SNMP v1/v2c/v3, RMON IEEE 802.3i, IEEE 802.3u, IEEE 802.1x, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3af, VLAN, QoS, Spanning Tree.
- Dostawa jednego zarządzanego przełącznika gigabitowego PoE min. 16 port (w tym min. 8 porty PoE) w obudowie typu biurkowego, ze wsparciem dla SNMP v1/v2c/v3, RMON IEEE 802.3i, IEEE 802.3u, IEEE 802.1x, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3af, VLAN, QoS, Spanning Tree.
- Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
- Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.).
- Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
- Integracja posiadanych przez Zamawiającego urządzeń sieciowych (switche, AP itp.) z systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.
- Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

IX. Szkolenia/warsztaty:

- Wykonawca zapewni 2-dniowe szkolenia (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC
- szkolenia zostaną przeprowadzone dla 3 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC

- Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC
- Warsztaty odbędą się w formie zdalnej.
- Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
- Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym

X. Licencja i wsparcie techniczne producenta oprogramowania:

Wykonawca dostarczy dożywotnią licencję systemu NAC oraz wsparcie producenta oprogramowania do 8 maja 2026 r. Wsparcie musi obejmować minimum:

- 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 dla konfiguracji oprogramowania oraz 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.