Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy postępowania pn.:

„Dostawa i wdrożenie oprogramowania typu NAC na potrzeby Portu Lotniczego „Rzeszów – Jasionka" Sp. z o.o."

I. Przedmiot zamówienia

Przedmiotem zamówienia jest:

- Dostawa dożywotniej licencji oprogramowania wraz z 36 miesięczną licencją wsparcia technicznego producenta dla systemu NAC.
- Instalacja, wdrożenie i konfiguracja systemu NAC.
- Przygotowanie i dostarczenie dokumentacji – projektu wdrożenia, dokumentacji technicznej, dokumentacji dla użytkownika, dokumentacji powdrożeniowej.
- Szkolenie/warsztaty z obsługi systemu NAC.

Opis Przedmiotu Zamówienia zawiera minimalne wymagania jakie musi spełnić Wykonawca na potrzeby realizacji przedmiotu zamówienia.

Maksymalny czas realizacji przedmiotu zamówienia do 90 dni od daty podpisania umowy. **Oferent** jest zobligowany do podania harmonogramu czasu trwania poszczególnych etapów.

II. Opis infrastruktury Zamawiającego

Zamawiający zakłada w szczególności następujące zasoby IT, które będą objęte kontrolą dostępu do sieci:

ZASOBY IT
Pierwsze centrum autoryzacyjne – Sieć LAN
Drugie centrum autoryzacyjne – Sieć MONITORINGU WIZYJNEGO oraz SIEĆ OT

III. Wymagania dla rozwiązania NAC

1. Podstawowa funkcjonalność:

System musi umożliwiać zbudowanie dwóch centrum autoryzacji, niezależnych od siebie. Każde z nich musi zapewniać HA na poziomie wirtualizatora lub na poziomie sieciowym.

System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
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.
System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
System musi umożliwiać obsługę co najmniej 1000 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) w każdym centrum autoryzacji oraz zapewniać skalowalność do przynajmniej 10 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
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.
System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym: a. VM – min. VMWare ESXi co najmniej w wersji 8.x, Hyper-V w wersji min 2022, Proxmox w wersji min 6.x, KVM w wersji min 7.x b. Maszyny fizyczne - serwery wspierane przez producenta. c. Platform as a Service - Microsoft Azure.
System musi posiadać funkcjonalność serwerów: a. serwera RADIUS dla infrastruktury sieciowej, b. serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+, c. serwera VPN, d. serwera DNS, e. serwera SYSLOG, f. serwera TFTP, g. serwera TACACS+, h. serwera Monitoringu, i. serwera DHCP, j. serwera polityk uwierzytelniania i kontroli dostępu 802.1X, k. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
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.
System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z minimum systemów zewnętrznych: a. AirWatch b. IBM MaaS c. MobileIron d. Microsoft Intune e. Google G Suite f. Famoc g. Microsoft Active Directory h. Radius i. OpenLDAP j. Relacyjnych baz danych: MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC k. CheckPoint l. Service Now
Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, konfiguracji VPN, wysłania konfiguracji dostępowych poprzez email.
System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
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.
System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory minimum: a. Login b. Hasło c. Imię d. Nazwisko e. Email

f. Status
System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
System posiada identyfikacji urządzeń końcowych z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520.
System musi posiadać mechanizm podglądu, tworzenia map graficznych umiejscowienia urządzeń sieciowych, końcowych, gniazdek internetowych z podziałem na budynki, pokoje oraz węzły sieciowe.
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.
System musi zapewniać scentralizowane zarządzanie urządzeniami sieciowymi. Zarządzanie musi odbywać się bezagentowo, a w systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu: a. VLANów, b. Autoryzacji, c. Statusu, d. Opisu.
System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
System musi zapewniać funkcjonalność wizualizacji konfiguracji podsieci IP oraz przypisania jej do jednostek.
System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
System musi wspierać funkcjonalność włączania i wyłączania podsieci IP, adresów IP bez konieczności usuwania ich z systemu.

System musi posiadać funkcjonalność migracji sieci do sieci o większej masce wraz z dotychczasową konfiguracją sieci i ustalonymi powiązaniami adresów IP, MAC oraz konfiguracją serwera DHCP.
System musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja zainstalowanego oprogramowania (firmware), numer faktury zakupu, przypisane gwarancje wraz z powiadamianiem o zbliżającym się ich końcu.
System musi umożliwiać obsługę zdarzeń serwisowych, gwarancyjnych, reklamacyjnych urządzeń sieciowych oraz użytkownika min. rejestrowanie zdarzeń, zmianę statusu urządzenia.
System musi mieć możliwość oddelegowania wykonania zadań, mapowania ich z tożsamościami użytkowników, urządzeniami sieciowymi oraz urządzeniami końcowymi.
System musi posiadać funkcjonalność przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń sieciowych (min. w formacie tekstowym) oraz ich składowania na wewnętrznym serwerze TFTP.
System musi być wyposażony w funkcjonalność inwentaryzacji urządzeń w zakresie: umów, licencji, gwarancji, dostawców.
System musi posiadać funkcjonalność tworzenia kodów identyfikujących dla urządzeń (min. typu Barcode i QR Code) oraz ich wydruk w formacie obsługiwanym przez drukarki etykiet min. Zebra w formacie ZPL.
System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
System musi posiadać mechanizm automatyzacji wg harmonogramu z możliwością symulacji działania, min: a. Włączenie wskazanych portów urządzeń sieciowych, b. Wyłączenie wskazanych portów urządzeń sieciowych, c. Wykonania komend na wskazanych urządzeń sieciowych, d. Dodanie znalezionych urządzeń sieciowych w skazanych podsieciach z możliwością sklonowania konfiguracji z podanego urządzenia sieciowego wg podanych parametrów jak: parametry dostępowe SNMP w wersji 1, 2c, 3, producenta, modelu urządzenia.
System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP.
System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i

urządzeń końcowych (BYOD).
System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google.
System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS.
System musi posiadać funkcję personalizacji strony gościnnej.
Captive Portal musi umożliwiać obsługę instalacji agentów, dystrybucji certyfikatów użytkowników oraz generowania autokonfiguratorów sieci.
System musi posiadać mechanizm zarządzania uprawnieniami użytkowników, którzy będą mogli rejestrować swoje urządzenia, pobierać certyfikaty, agenty oraz uruchamiać autokonfiguratorów sieci.
Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS.
Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
Captive Portal powinien umożliwiać podgląd ostatnich 10 logowań do sieci.
Captive Portal powinien umożliwiać zmianę konfiguracji numeru portów HTTP i HTTPS.
Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.

Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
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, co najmniej: a. Palo Alto b. Fortigate c. Sophos d. FlowMon e. ESET NOD32 f. CheckPoint
System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
System musi obsługiwać metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej: a. DHCP Fingerprinting b. DHCP SPAN c. SNMP d. Vendor OUI e. TCP f. Active Directory g. CDP/LLDP h. HTTP/S i. DNS j. Radius k. WMI l. MDM m. WinRM n. ONVIF
System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM co najmniej: a. AirWatch

b. IBM MaaS c. MobileIron d. Microsoft Intune e. Google G Suite f. Famoc
System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: a. FortiGate b. Pulse Secure c. OpenVPN d. Palo Alto e. Cisco ASA
System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej: a. Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności b. Czy włączony jest firewall c. Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur d. Czy jest włączone szyfrowanie dysku systemowego e. Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory f. Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora g. Czy w systemie są uruchomione procesy wskazane przez administratora h. Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności i. Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem: j. Wartości klucza rejestru k. Typu wartości: Number, String, Version
System musi posiadać obsługę realizowaną przez dedykowanego agenta przełączanie VLANów na określonych portach urządzeń sieciowych.
System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
System musi współpracować z serwerem tokenów.
System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej: a. Microsoft Windows b. Mac OS c. iOS d. Android

System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
System musi umożliwiać wsparcie dla systemów typu HOT-SPOT oraz serwisami umożliwiającym oferowanie materiałów promocyjnych.
System musi posiadać wbudowany skaner sieciowy umożliwiający co najmniej weryfikacje otwartych portów urządzenia końcowego oraz zainstalowany system operacyjny.
System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

2. Mechanizmy uwierzytelniania

System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.dla zewnętrznego serwera RADIUS.
System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły: a. MAC, b. PAP/ASCII, c. CHAP, d. SNMP, e. 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), itp.
System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
System musi wspierać implementację protokołu 802.1X z różnymi suplikantam i (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).
a. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły: b. Tożsamość/Urządzenie końcowe, c. Grupa tożsamości/urządzeń końcowych, d. Parametry urządzeń końcowych, min: system operacyjny, wersja, e. Atrybuty Active Directory, f. Jednostka organizacyjna tożsamości/urządzeń końcowych, g. Urządzenia sieciowe sieci przewodowej, bezprzewodowej, h. Grupy urządzeń sieciowych, i. Porty urządzeń sieciowych, j. Grupy portów urządzeń sieciowych, k. Jednostka organizacyjna portów,

l. Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID), m. Data, czas ważności polityki, n. Wewnętrzny Captive Portal, o. Metoda autoryzacji.
System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: a. Cisco Networks b. Aruba Networks c. Extreme Networks d. Hewlett Packard Enterprise e. Juniper Networks f. Ruckus Networks g. MicroTik h. Ubiquiti Networks
System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
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.
System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
System musi umożliwiać automatyczną konfigurację parametrów dostępowych do serwerów VPN z poziomu tożsamości.
System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów

MAC.
System musi pozwalać na weryfikację zalogowanego urządzenia końcowego IoT (Internet of Things) minimum za pomocą mechanizmów SNMP, DHCP, NMAP, Agenta oraz wywołania akcji: powiadomienie administratorów i/lub zablokowanie i rozłączenie sesji.
System musi umożliwiać automatyczną generację certyfikatów z poziomu tożsamości i urządzeń końcowych.
System musi posiadać funkcjonalność testowania poprawności polityk z poziomu interfejsu graficznego dla wybranych tożsamości bądź urządzeń końcowych wraz z informacją zwrotną, za pomocą, której polityki zostanie przydzielony dostęp do sieci.
System musi wspierać funkcjonalność różnych typu 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.
System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
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.

3. Obsługa serwerów certyfikatów CA

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

4. Obsługa serwerów VPN

System musi posiadać funkcję zintegrowanego serwera VPN oraz zapewniać współpracę z zintegrowanym oraz zewnętrznym serwerem CA,
System musi umożliwiać wystawianie konfiguracji klienckich, certyfikatów dla serwerów VPN.

System musi logować wszelkie próby autoryzacji do serwerów VPN.
System musi zapewniać przynajmniej następujące funkcjonalności serwera VPN: a. Logowanie do zasobów firmy, b. Obsługę OTP, c. Przypisanie ustalonego adresu IP.

5. Obsługa serwerów DNS

System musi posiadać funkcję zintegrowanego serwera DNS
System musi umożliwiać graficzne zarządzanie serwerami DNS.
System musi zapewniać przynajmniej następujące funkcjonalności serwera DNS: a. Zarządzanie strefami, b. Zarządzanie rekordami stref, c. Zatwierdzanie przez administratorów moderowanych rekordów stref, d. Weryfikacja konfiguracji przed instalacją, **e.** Instalacja konfiguracji na serwerach DNS.

6. Obsługa serwerów DHCP

System musi posiadać funkcję zintegrowanego serwera DHCP.
System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP: a. Uruchamianie usługi dla wybranych podsieci, b. Przypisanie ustalonego adresu IP dla adresu MAC. c. Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci, d. Możliwość zwracania adresów IP wyłącznie dla wybraneji wcześniej zdefiniowanej grupy adresów MAC, e. Możliwość określania braku dostępu dla wybranych adresów MAC, f. Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC, g. Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP, h. Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego, i. Możliwość zmiany przydziału dynamicznego na statyczny j. Dokonywanie zmian bez konieczności wyłączania usług.

7. Obsługa serwerów TACACS+

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

System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
System musi umożliwiać tworzenia haseł administratorom.
System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
System musi wspierać logowanie administratorów za pomocą tokenów OTP.

8. Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

Monitoring autoryzacji: a. Top 10 uwierzytelnień pomyślnych (zaakceptowanych autoryzacji), b. Top 10 autoryzacji odrzuconych, c. Top 10 urządzeń sieciowych z największą liczbą autoryzacji, d. Top 10 urządzeń sieciowych z największą liczbą autoryzacji odrzuconych, e. Top 10 SSID z największą liczbą autoryzacji, f. Top 10 SSID z największą liczbą autoryzacji odrzuconych, g. Autoryzacje zaakceptowane w ciągu ostatnich 30 dni, h. Autoryzacje odrzucone w ciągu ostatnich 30 dni, i. Obciążenie serwera autoryzacji, j. Ostatnie 100 zdarzeń autoryzacji, k. Top 10 unikalnych urządzeń końcowych wg. tożsamości.
Monitoring dla zdarzeń systemowych: a. Ostatnie 100 zdarzeń systemowych, b. Top 10 zdarzenia typu error z Sysloga, c. Top 10 zdarzenia typu TopSeverity z Sysloga, d. Obciążenie serwera Syslog.
Monitoring dla zdarzeń DHCP: a. Wykorzystanie podsieci statyczne i dynamiczne, b. Ilość używanych adresów DHCP,

c. Ostatnie 100 zdarzeń DHCP, d. Procentowe wykorzystanie serwera DHCP, e. Top 10 DHCP z największą liczbą przyznanych adresów, f. Top 10 DHCP z największą liczbą kolizji IP, g. Top 10 DHCP z największą liczbą odrzuconych IP, h. Top 10 DHCP z wykorzystaną pulą IP, i. Obciążenie serwera DHCP.
Monitoring dla tożsamości: a. Podział tożsamości ze względu na typ konta, b. Podział tożsamości ze względu na tożsamości aktywne i nieaktywne, c. Podział tożsamości ze względu na serwer autoryzacji, d. Podział tożsamości ze względu na konta, które straciły ważność, e. Wykorzystanie kont gościnnych z dostępem czasowym.
Monitoring dla urządzeń końcowych: a. Podział urządzeń ze względu na ich status, b. Podział urządzeń ze względu na ich typ, c. Podział urządzeń ze względu na serwer autoryzacji, d. Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.
Monitoring dla urządzeń sieciowych: a. Podział urządzeń ze względu na urządzenia aktywne i nieaktywne. b. Podział urządzeń ze względu na ich typ.
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.
Raport ze zdarzeń logowania z informacją o nadam adresie IP.
Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych
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.
System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.

Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
Raport zdarzeń Microsoft Active Directory, minimum: a. Logowania, wylogowania z system w tym błędne logowania b. Logowania do sieci 802.1X

9. Alarmy

System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: a. wiadomości e-mail, b. Syslog, c. notyfikacji systemowych.
Alarmy mogą być generowane w sytuacjach, min: a. Ilości obsługiwanych transakcji RADIUS, b. Opóźnienie obsługi transkacji RADIUS, c. Statusu krytycznego modułów.
System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: a. badanie łączności IP za pomocą ping, traceroute, b. tcpdump protokołów RADIUS, TACACS+, c. 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, d. wykonanie zdalnego polecenia na urządzeniu sieciowym.

IV. Wymagania dotyczące wdrożenia i harmonogram ramowy

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
- 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 dostarczanych urządzeń sieciowych (ok. 20 sztuk różnych typów) (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.
- Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6h dziennie.
- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.

V. Szkolenia/warsztaty

- Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC
- Warsztaty zostaną przeprowadzone dla maksymalnie 4 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.

VI. Dokumentacja

- Wykonawca dostarczy dokumentację obejmującą:
  - projekt wdrożenia rozwiązania w infrastrukturze Zamawiającego,
  - dokumentacja powdrożeniową,
  - dokumentację techniczną umożliwiająca Zamawiającemu samodzielną administracje rozwiązaniem,
- a także przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji.
- Wszelka dokumentacja wytworzona przez Wykonawcę musi być sporządzona w języku polskim.
- Dokumentacja musi być w formacie Microsoft Word z obsługą trybu rejestracji zmian.
- Wszelka dokumentacja musi charakteryzować się wysoką jakością i czytelnością.

VII. Licencja wsparcia technicznego producenta oprogramowania

Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 36 miesięczną licencje na wsparcie producenta oprogramowania. Licencja ta powinna 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.

VIII. Bezpieczeństwo przetwarzanych danych

- Wykonawca zobowiązany jest do przestrzegania, przekazanych w trakcie realizacji przedmiotu zamówienia, zasad i przepisów dotyczących bezpieczeństwa informacji oraz

systemów informatycznych, obowiązujących u Zamawiającego, oraz innych zasad związanych z wykonywaniem czynności na terenie obiektów Zamawiającego. Zobowiązanie to dotyczy wszystkich osób, z pomocą których Wykonawca będzie realizował przedmiot zamówienia.

- System NAC musi być w pełni zgodny z zasadami bezpieczeństwa zdefiniowanymi w przekazanych przez Zamawiającego instrukcjach i procedurach. Z uwagi na zakres Polityki Bezpieczeństwa Danych Osobowych (PBDO) Zamawiającego, zasady i reguły określone w PBDO podlegają ochronie przed ujawnieniem lub udostępnieniem nieupoważnionej lub nieuprawnionej osobie lub nieuprawnionemu podmiotowi zewnętrznemu, dlatego dokumenty te zostaną przekazane Wykonawcy po podpisaniu Umowy na realizację przedmiotu zamówienia.
- Przesyłanie danych w obrębie systemu NAC musi odbywać się w dedykowanej sieci Zamawiającego - bezpiecznymi kanałami, szyfrowanymi i chronionymi przed nieuprawnionym dostępem oraz zapewniającymi poufność, integralność i dostępność danych osobowych.
- Wszystkie dane, które będą udostępnione w systemie NAC muszą być chronione przed nieuprawnionym odczytem poprzez mechanizmy logowania z wykorzystaniem unikalnego identyfikatora oraz hasła. Wytyczne dotyczące sposobu budowania identyfikatorów i haseł zostaną przekazane przez Zamawiającego.
- System NAC musi zapewniać logowanie wszystkich udanych i nieudanych prób dostępu do systemu z uwzględnieniem informacji o użytkowniku końcowym, dacie i czasie logowania oraz adresu IP z którego nastąpiła próba logowania.