**Załącznik nr 3 – system NAC (Część 2)**

Infrastruktura, w której będzie wykonywane wdrożenie obejmuje:

- przełączniku sieciowe: DCN pietro2-95 S4600-52X-P-SI oraz przełączniki dostarczone w Części 1. Wszystkie przełączniki obsługujące gniazda abonenckie obsługują protokoły: Radius, 802.1X, MAB, TACACS

- AP Ubiquiti UniFi AP AC z kontrolerem programowym UniFi Network Application,

- stacje robocze użytkowników – 135,

- drukarki i urządzenia wielofunkcyjne TCP/IP – 35,

- urządzenia telefonii IP – 1,

- inne 2

- szacowana ilość jednocześnie logowanych użytkowników w sieciach WiFi 40 w tym 30 w sieci publicznie dostępnej.

Łączna ilość szacowanych jednoczesnych unikatowych logowań - 213

Zamawiający dysponuje serwerem o wydajności wystarczającej do zainstalowania i pracy oferowanego rozwiązania. W zakresie niezbędnym do wykonania zadania Zamawiający zapewni dostęp do pomieszczeń, infrastruktury technicznej i wyposażenia.

Zamawiający udostępni wszelkie pozostające w jego dyspozycji dokumenty i informacje dotyczące infrastruktury teleinformatycznej oraz funkcjonującego oprogramowania. Brakujące dokumenty, informacje i rysunki niezbędne do wykonania dokumentacji Wykonawca uzupełni we własnym zakresie.

Wykonawca przeszkoli administratorów – 3 osoby w czasie nie krótszym niż 8 godzin.

**Licencja dostarczonego rozwiązania powinna zapewnić:**

Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego poprzedzonego testami oprogramowania NAC.

Scenariusze testów wdrożonego systemu NAC:

1. Weryfikacja synchronizacji systemu z Active Directory i pobierania informacji o nowych użytkownikach/ urządzeniach.

2. Weryfikacja integracji systemu z urządzeniami sieciowymi.

3. Symulacja działania polityk 802.1x LAN/Wi-Fi użytkowników dla każdej stworzonej grup użytkowników.

4. Symulacja działania polityk 802.1x LAN/Wi-Fi urządzeń końcowych dla każdej stworzonej grupy urządzeń końcowych.

5. Symulacja działania polityk 802.1x/ MAC dla drukarek i urządzeń wielofunkcyjnych

6. Symulacja działania polityk MAC dla pozostałych urządzeń.

7. Symulacja dostępu gościnnego z wykorzystaniem Captive Portal.

**Podstawowa funkcjonalność systemu NAC:**

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 220 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 400 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 G Suite, 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.

**Pozostałe wymagania:**

1. Po zakończeniu realizacji zadania Wykonawca zobowiązany jest przekazać dokumentację powykonawczą w formie elektronicznej, zawierającą opis wykonanych prac oraz sposób konfiguracji poszczególnych urządzeń.
2. Zamawiający wymaga wsparcia technicznego na okres 12 m-cy, liczony od dnia zakończenia wdrożenia, potwierdzonego podpisaniem protokołu odbioru.
   1. Wsparcie techniczne obejmuje:
   * kontakt z działem wsparcia technicznego za pośrednictwem poczty elektronicznej lub innego uzgodnionego z Zamawiającym sposobu komunikacji;
   * pomoc techniczną mającą na celu rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem;
   * udzielanie wsparcia 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 technicznej;
   * dostęp do aktualizacji oraz poprawek oprogramowania;
   * rozpatrywanie wszystkich zdarzeń, które zostaną zgłoszone, w czasie nie przekraczającym 14 dni roboczych