# Znak sprawy: ZP/220/136/23

Załącznik nr 2.1. do SWZ

# **Zadanie nr 1**

**Dostawa systemu NAC**

Spis treści

[Wstęp 3](#_Toc148442027)

[System NAC 1 szt. 3](#_Toc148442028)

[Wdrożenie 11](#_Toc148442029)

## Wstęp

W ramach zadania wykonawca dostarczy oprogramowanie wyszczególnione w niniejszym dokumencie oraz dokona wdrożenia zgodnego z opisem w sekcji „Wdrożenie”.

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

1. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
2. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane
3. Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;
4. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
5. Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
6. Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:
7. połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),
8. łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,
9. zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,
10. wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,
11. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ±10%, 50Hz;

## System NAC 1 szt.

* Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.
  + Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare i/lub HyperV
  + Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
* Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
* Aplikacja zarządzająca musi zarządzać wszystkimi posiadanymi przez zamawiającego urządzeniami: 100 punktami dostępowymi firmy Extreme Networks oraz 70 przełącznikami sieciowymi Extreme Networks.
* Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
* Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników logujących się do systemu zarządzającego z wykorzystaniem LDAP i/lub Radius.
* Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
* Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
* Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
* Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
* Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
* Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
* Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych.
* Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email’a, wysłanie trapu SNMP, wpisu do Syslog’a lub uruchomienie automatyzacji (skryptu).
* Aplikacja musi posiadać wbudowany Syslog serwer.
* Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie otrzymywanych SNMP Traps
* Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych.
* Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia.
* Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
  + Wysłanie e-mail do wskazanej grupy adresowej
  + Wysłanie informacji SYSLOG do wskazanego serwera
  + Wysłanie TRAP SNMP do wskazanego adresu IP
  + Uruchomienie skryptu w systemie operacyjnym Linux
  + Uruchomienie skryptu skonfigurowanego w systemie zarządzającym
* Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
* Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
* Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
* Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
  + połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu. Połączenia pomiędzy urządzeniami muszą być wyświetlane automatycznie na podstawie informacji uzyskiwanych z protokołu LLDP.
  + konfiguracji sieci VLAN
* Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https
* Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
  + adres IP urządzenia
  + adresu MAC urządzenia
  + nazwy urządzenia
  + wersji oprogramowania
  + wersji bootrom
  + lokalizacji urządzenia
  + danych kontaktowych administratora
  + numeru seryjnego
  + numeru inwentaryzacyjnego – własna numeracja
* Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
  + możliwość automatycznej periodycznej realizacji backup’u konfiguracji urządzeń o wskazanym czasie
  + możliwość realizacji backup’u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych
  + możliwość odtworzenia wskazanej konfiguracji urządzenia
  + możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami
  + możliwość obsługi backup’u urządzeń sieciowych różnych producentów
* Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
* Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
* Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
* Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Studenci, Kadra, Goście, Zarząd, Kamera CCTV, Telefon, Access Point itp.
* Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:
  + przyłączenia do sieci VLAN
  + przyłączenia do serwisu w ramach „Fabric” z wykorzystaniem IEEE 802.1Qcj,
  + konfiguracji Quality of Service
  + konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
  + możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej.
* Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
  + szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
  + wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
  + wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
  + generowanie raportów
* Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.
  + Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
  + Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax
  + Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
    - adres IP kontrolera
    - liczba obsługiwanych klientów
    - szczytowe wartości zajmowanego pasma
    - wersja oprogramowania
  + Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
    - adres IP punktu dostępowego
    - MAC adres punktu dostępowego
    - wersja oprogramowania
    - typ punktu dostępowego
    - kanały pracy poszczególnych interfejsów radiowych
    - szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
  + Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
    - adres IP klienta
    - MAC adres klienta
    - nazwa użytkownika
    - nazwa punktu dostępowego, do którego dołączony jest użytkownik
    - BSSID, do którego dołączony jest użytkownik
    - SSID, do którego dołączony jest użytkownik
  + Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
    - zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
    - zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem
    - lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych
* Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:
  + adresu MAC
  + adresu IP
  + nazwy komputera
  + typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
  + nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
  + adres IP urządzenia, do którego dołączony jest klient.
  + identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
  + typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
  + nazwa przydzielonej polityki bezpieczeństwa.
* System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.
* System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
* System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:
  + Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.
  + Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.
  + Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC
  + Realizacji przyłączenia do sieci ze wskazanej „lokalizacji” – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.
  + Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia
* System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.
* Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń.
* System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
* System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS
* System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.
* System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy.
* System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa.
* System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
  + liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
  + liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
  + liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
  + liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
  + liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
* System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication
* System zarządzania tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. **1000** urządzeń klienckich (adresów MAC).
* System zarządzania musi posiadać przy współpracy z dostarczonymi urządzeniami pozwalając na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej
* Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.
* Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.
* System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos
* System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.
* Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.
* System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.
* System Analityki musi zapewniać możliwość tworzenia raportów.
* System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail.
* System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością.
* System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)
* System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie.
* System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu
* System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki
* System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:
  + Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall takimi jak: Palo Alto, Fortinet, Checkpoint
  + Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny
  + Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune, AirWatch MDM

Funkcjonalność kontrolera sieci bezprzewodowej:

1. Kontroler bezprzewodowy instalowany jako maszyn wirtualna

2. Kontroler bezprzewodowy musi wspierać instalację w systemie VMWare oraz HyperV

3. Kontroler musi zapewniać możliwość skalowania liczby obsługiwanych punktów dostępowych oraz klientów bezprzewodowych poprzez zmianę udostępnianych zasobów w środowisku wirtualnym

4. Kontroler musi obsługiwać posiadane przez zamawiającego Access Pointy Extreme Networks AP305C-1-WR, AP310i-WR i WS-AP3915i-ROW w ilości: 70 sztuk

5. Kontroler musi być dostarczony w trybie pracy klastra odpornym na awarie (należy dostarczyć minimum 2 kontrolery zapewniające redundancje)

6. Kontroler musi zapewniać skalowalność do min. 1000 punktów dostępowych i 16 tys. klientów bezprzewodowych

7. Kontroler musi zapewniać obsługę sieci VLAN zgodnych z IEEE 802.1Q

8. Kontroler musi być zarządzany przez przeglądarkę www bez konieczności instalacji aplikacji na stacji zarządzającej jak np. Java

9. Kontroler musi zapewniać obsługę wielu Lokalizacji z wizualizacją ich stanu, liczby sieci bezprzewodowych (SSID) oraz liczby obsługiwanych punktów dostępowych w każdej lokalizacji.

10. Kontroler musi posiadać integrację z systemem map pozwalających na wizualizację poszczególnych lokalizacji na mapie i określeniem lokalizacji poprzez jej wskazanie na mapie lub wpisanie współrzędnych geograficznych

11. Kontroler musi zapewniać możliwość konfiguracji planów poszczególnych pięter budynków oraz umieszczenie punktów dostępowych na planie

12. Kontroler musi zapewniać możliwość nanoszenia na plany budynków ścian i pozwalać na wizualizację zasięgu poszczególnych punktów dostępowych umieszczonych na planie.

13. Kontroler musi zapewniać możliwość importu planów z systemu planowania Ekahau (ESX) jak również wczytywanie planów piętra z plików graficznych

14. Kontroler musi zapewniać widzialność wszystkich dołączonych do kontrolera punktów dostępowych z następującymi informacjami:

a. Nazwa punktu dostępowego – konfigurowalna nazwa punktu (Host Name)

b. Typ punktu dostępowego

c. Numer seryjny punktu dostępowego

d. MAC adres punktu dostępowego

e. Adres IP punktu dostępowego

f. Status punktu dostępowego

g. Przypisanie do lokalizacji

h. Informacje o kanałach pracy poszczególnych interfejsów radiowych

i. Informacje o liczbie klientów na poszczególnych interfejsach radiowych

j. Informacje o aktualnej mocy ustawionej na poszczególnych interfejsach radiowych

k. Informacji o szerokości kanału ustawionej na poszczególnych interfejsach radiowych

l. Informacji o statusie portów Ethernet i ewentualnej konfiguracji połączeń Link Aggregation na portach Etherent punktów dostępwowych

m. Informacji o poziomie szumu dla poszczególnych interfejsów radiowych

15. Kontroler musi zapewniać możliwość konfiguracji sieci bezprzewodowych, ich przydziału do grup punktów dostępowych, a następnie do lokalizacji

16. Kontroler musi zapewniać automatyczne wykrywanie nowych punktów dostępowych

17. Kontroler musi być zarządzany przez SNMPv1/v2/v3 oraz SSHv2.

18. Kontroler musi obsługiwać RADIUS authentication oraz RADIUS accounting.

19. Kontroler musi zapewniać obsługę: 802.11i, WPA, WPA2, TKIP oraz AES, WPA3

20. Kontroler musi zapewniać obsługę IEEE 802.1x oraz autentykację: EAP-TLS, EAP-TTLS, PEAP, EAP-MD5 oraz EAP-SIM.

21. Kontroler musi zapewniać przesyłanie danych z sieci WLAN do sieci przewodowej w następujących architekturach:

a. bridging na kontrolerze – kontroler zapewnia przełączanie ruchu z sieci bezprzewodowej do wskazanej sieci wirtualnej przewodowej dołączonej do kontrolera

b. bridging na punkcie dostępowym – w tym trybie ruch z sieci bezprzewodowej jest kierowany bezpośrednio do wskazanej sieci wirtualnej przyłączonej bezpośrednio do punktu dostępowego

c. bridging na punkcie dostępowym wraz z sygnalizacją niezbędnych sieci VLAN z wykorzystaniem IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging (PBB)

d. bridging na punkcie dostępowym z zapewnieniem tunelowania ruchu poprzez VxLAN

22. Kontroler bezprzewodowy musi zapewniać możliwość ustawiania następujących parametrów w ramach każdej sesji klienckiej:

a. indywidualne raguły filtrowania ruchu

b. przypisanie sieci VLAN

c. QoS

d. ograniczenia transmisji wejściowej i wyjściowej

e. wyboru topologii (bridging na kontrolerze, bridging na punkcie dostępowym, tunel VxLAN, IEEE 802.1Qcj)

23. Kontroler musi zapewniać obsługę Captive Portal pozwalającego na obsługę gości jak i uwierzytelnianie klientów bezprzewodowych z wykorzystaniem Captive Portal – np. nie posiadających suplikanta IEEE 802.1x

24. Kontroler musi zapewniać możliwość rejestracji gości w oparciu o portal www znajdujący się na kontrolerze.

25. Portal rejestracji gości musi zapewniać możliwość stworzenia i akceptacji regulaminu przez rejestrujących się gości

26. Kontroler musi zapewniać przynajmniej podstawową konfigurację wyglądu Captive Portal – zmiana kolorów, zmiana stylów CSS, dodanie loga.

27. Captive Portal musi posiadać możliwość obsługi wielu języków wybieranych automatycznie na podstawie ustawień przeglądarki klienta bezprzewodowego jak również za pomocą np. combo box na portalu.

28. Captive Portal musi zapewniać wsparcie min. języka polskiego, angielskiego i niemieckiego.

29. Captive Portal musi zapewniać obsługę urządzeń mobilnych

30. Kontroler musi zapewniać rejestrację gości z wykorzystaniem portali społecznościowych np. Facebook, Google

31. Kontroler musi zapewniać możliwość automatycznej, centralnej aktualizacji oprogramowania punktów dostępowych zaadoptowanych do kontrolera.

32. Kontroler musi zapewniać możliwość konfiguracji blokowania ruchu pomiędzy klientami sieci bezprzewodowej.

33. Kontroler musi zapewniać autoryzację użytkowników IEEE 802.1x w oparciu o zewnętrzny serwer RADIUS z możliwością definicji różnych serwerów RADIUS dla różnych identyfikatorów SSID

34. Kontroler musi zapewniać przydzielanie klientów do wskazanych sieci wirtualnych na podstawie informacji przesyłanej z serwera RADIUS zgodnie z RFC3580

35. Kontroler musi zapewniać możliwość uwierzytelniania z wykorzystaniem Microsoft Active Directory

36. Kontroler musi zapewniać możliwość przydzielania do sieci VLAN na podstawie przynależności klientów bezprzewodowych do grup użytkowników zdefiniowanych w LDAP

37. Kontroler musi zapewniać przydzielanie polityki zawierającej QoS (Quality of Service), list kontroli dostępu ACL. Przydzielane polityki muszą być realizowane na punktach dostępowych w przypadku ruchu, który jest wpuszczany do sieci bezpośrednio na punkcie dostępowym.

38. Kontroler musi zapewniać konfigurację roamingu pomiędzy punktami dostępowymi.

39. Kontroler musi zapewniać konfigurację oszczędzania energii UAPSD (Unscheduled Automatic Power Save Delivery).

40. Kontroler musi obsługiwać QBSS (informacja o zbyt dużym obciążeniu zostanie przekazana klientowi dla obsługi inteligentnego roamingu)

41. Kontroler musi obsługiwać funkcjonalność FCA (Flexible Client Access) zwiększającą prędkość transmisji klientów IEEE 802.11n w sieci z urządzeniami IEEE 802.11/a/b/g.

42. Kontroler musi obsługiwać funkcjonalność CAC (Call Admission Control), pozwalającą na sprawdzenie, czy zestawienie nowego połączenia telefonii VoIP nie wpłynie na jakość dotychczasowych połączeń.

43. Kontroler musi zapewniać obsługę preferencji pasma polegającą na automatycznym przenoszeniu klientów na pasmo 5 GHz.

44. Kontroler musi zapewniać możliwość uruchamianie sieci bezprzewodowych wg. skonfigurowanego planu bazującego na kalendarzu.

45. Kontroler musi być w pełni zintegrowany z dostarczanym oprogramowaniem zarządzającym

* Zamawiający dopuszcza licencje czasowe na oprogramowanie zarządzające w formie subskrypcji, ale na okres nie krótszy niż 2 lat
* System zarządzania musi być objęty 2 letnim wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.

## Wdrożenie

1. Instalacja oferowanego oprogramowania na zasobach zamawiającego
2. Podłączenie wszystkich posiadanych przełączników oraz punktów dostępowych do systemu
3. Uruchomienie kontroli dostępu do sieci (NAC) z wykorzystaniem standardu 802.1x
4. Konfiguracja harmonogramu wykonywania kopii zapasowej konfiguracji przełączników
5. Stworzenie portalu dla dostępu gości do sieci LAN
6. Stworzenie polityk dostępu do sieci LAN opierających się o reputacje urządzeń i użytkowników podłączanych do sieci
7. Uruchomienie systemu kontroli dostępu do sieci NAC w trybie passthrough w celu zlokalizowania wszystkich urządzeń podłączonych do sieci
8. Stworzenie polityk, które muszą umożliwiać wielowarstwową klasyfikację ramek pozwalającą administratorowi kontrolować ruch za pomocą reguł klasyfikacji w punkcie wejścia dla systemu końcowego. Funkcjonalność musi pozwalać na dynamiczną implementację dowolnej liczby akcji w dowolnej kombinacji atrybutów warstwy 2, 3 lub 4 w pakietach. Zastosowanie polityk musi umożliwić także Multi-User Authentication oraz Multi-Method Authentication czyli uwierzytelnienie wielu użytkowników na jednym porcie przy zastosowania różnych metod uwierzytelniania, przy zastosowaniu następujących akcji: odrzucanie ruchu, zezwalanie na ruch, wprowadzanie priorytetyzacji ruchu, przypisanie do VLAN