Nr sprawy: DZ.22.23.2023

Załącznik nr 1 do SWZ

Dostawa sprzętu sieciowego i oprogramowania do Instytutu Łączności – Państwowego Instytutu Badawczego

I. Wymagania ogólne

1. Przedmiotem zamówienia jest dostawa sprzętu sieciowego i oprogramowania do Instytutu Łączności – Państwowego Instytutu Badawczego, ul. Szachowa 1, 04-894 Warszawa.
2. Wszystkie urządzenia muszą być fabrycznie nowe i posiadać oznaczenie CE producenta.
3. Jeśli w wymaganiach szczegółowych nie wskazano inaczej, dostarczany sprzęt musi być objęty min. pięcioletnią gwarancją producenta NBD (Next Bussines Day). Zamawiający rozumie przez to gwarancję naprawy lub wymiany sprzętu na nowy w następnym dniu roboczym od momentu zgłoszenia awarii. Naprawa lub wymiana sprzętu na nowy musi mieć miejsce w siedzibie Zamawiającego.
4. Bieg gwarancji rozpoczyna się z dniem dostawy. W dniu dostawy Wykonawca dostarczy niezbędne dokumenty gwarancyjne.
5. W ramach gwarancji/wsparcia serwisowego:
    a. wykonawca udostępni pojedynczy punkt przyjmowania zgłoszeń przez telefon, fax, email
    b. zgłoszenia będą przyjmowane i obsługiwane przez całą dobę (w trybie 24x7x365)
    c. usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) zostanie wykonana przez wykonawcę w następnym dniu roboczym. (realizacja napraw sprzętowych będzie realizowana w trybie 8x5xNBD)
    d. w okresie gwarancji wykonawca zapewni dostęp do aktualizacji oprogramowania do najnowszej oraz rekomendowanej przez producenta.
6. Wykonawca zobowiązany jest załączyć do oferty szczegółowy opis techniczny i funkcjonalny oferowanych produktów wskazujące w szczególności oferowany typ, rodzaj, model, producenta, numer katalogowy, charakterystykę produktu oraz dokładne nazwy oraz wersje oferowanego oprogramowania/licencji pozwalające na ocenę zgodności oferowanego przedmiotu zamówienia z wymaganiami SWZ.
7. Ilekroć w opisie przedmiotu zamówienia użyte zostało określenie standardu, Zamawiający dopuszcza zastosowanie tego standardu lub równoważnego.

II. Wymagania szczegółowe

Dostawa obejmuje:

A. Dwa (2) kontrolery sieci WiFi 6E o następujących minimalnych parametrach technicznych:

1. Urządzenie ma zapewniać centralną kontrolę punktów dostępowych WiFi:
    a) zarządzanie politykami bezpieczeństwa,
    b) wykrywanie zagrożeń w sieci bezprzewodowej,
    c) zarządzanie pasmem radiowym,
    d) zarządzanie mobilnością,
    e) zarządzanie jakością transmisji zgodnie z protokołem CAPWAP (RFC 5415).
2. Obsługa 250 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia do 500 przez dodanie odpowiedniej licencji.

3. Urządzenie wyposażone w 25 licencji na obsługę punktów dostępowych określonych w pkt. B oraz dodatkowe 25 licencji mające obsługiwać obecnie wykorzystywane punkty dostępowe Cisco AP 1832 i AP 2702 wraz ze wsparciem producenta na okres 5 lat.
4. Wyposażone w 4 interfejsy 2.5G/1G oraz 2 interfejsy 10G/1G (SFP/SFP+).
5. Obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć sieć bezprzewodową przed awarią pojedynczego interfejsu.
6. Obsługa ruchu tunelowanego o przepustowości 5 Gb/s z możliwością rozszerzenia do 10 Gb/s przez dodanie licencji.
7. Obsługa do 5000 klientów sieci bezprzewodowej.
8. Zarządzanie pasmem radiowym punktów dostępowych:
   a) automatyczna adaptacja do zmian w czasie rzeczywistym,
   b) optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia),
   c) dynamiczne przydzielanie kanałów radiowych,
   d) wykrywanie, eliminacja i unikanie interferencji,
   e) równoważenie obciążenia punktów dostępowych,
   f) tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych,
   g) automatyczna dystrybucja klientów pomiędzy punkty dostępowe,
   h) mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych,
   i) dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe.
9. Mapowanie SSID do segmentów VLAN w sieci przewodowej:
   a) 1:1,
   b) 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty),
   c) możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego, terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID).
10. Obsługa sieci kratowych,
    a) komunikacja między punktami dostępowymi bez medium kablowego,
    b) separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi),
    c) automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo),
    d) automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji),
    e) autoryzacja punktów dostępowych w oparciu o certyfikaty, adresy MAC.
11. Obsługa mechanizmów bezpieczeństwa:
    a) 802.11i, WPA3, WPA2, WPA,
    b) 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST),
    c) obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników,
    d) kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID,
    e) obsługa profilowania użytkowników:
       - przydział sieci VLAN,
       - przydział list kontroli dostępu (ACL),
    f) uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w,
    g) uwierzytelnianie punktów dostępowych w oparciu o certyfikaty,

h) obsługa list kontroli dostępu (ACL),
i) obsługa list kontroli dostępu opartych o nazwy domenowe,
j) obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X,
k) wykrywanie i dezaktywacja obcych punktów dostępowych,
l) możliwość budowania reguł klasyfikacji obcych punktów dostępowych w oparciu o nazwę SSID, wybrany ciąg znaków w SSID, siłę sygnału RSSI, minimalną ilość podłączonych urządzeń,
m) ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP,
n) DHCP proxy, wsparcie dla DHCP Option 82,
o) obsługa polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa z wykorzystaniem mechanizmu out-of-band, który przekazuje mapowania aktualnych adresów IP stacji i znacznika.

12. Zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową:
    a) kryptograficzne podpisywanie obrazów oprogramowania,
    b) bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych,
    c) wbudowany moduł sprzętowy unikalnie identyfikujący urządzenie i jego pochodzenie.
13. Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak: VLAN, polityka QoS, lista kontroli dostępu, czas trwania sesji.
14. Obsługa ruchu unicast IPv4 i IPv6.
15. Zgodność z funkcjonalnościami IPv6 pod kątem RFC: 4191, 6980, 8200, 8201.
16. Obsługa ruchu multicast IPv4 i IPv6:
    a) IGMP/MLD snooping,
    b) optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym),
    c) obsługa konwersji ruchu multicast do unicast.
17. Obsługa mobilności (roamingu) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami)
18. Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k.
19. Obsługa mechanizmów QoS:
    a) 802.1p,
    b) WMM, TSpec, U-APSD,
    c) ograniczanie pasma per użytkownik,
    d) Call Admission Control, SIP CAC, Call Snooping,
    e) równomierna obsługa klientów sieci bezprzewodowej w oparciu o utylizację czasu antenowego,
    f) kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID,
    g) zbiór wbudowanych profili do automatycznej konfiguracji ustawień QoS.
20. Analiza ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu; rozpoznawanie aplikacji; współpraca z serwerami autoryzacyjnymi w celu przypisania odpowiednich polityk kontroli ruchu aplikacji per użytkownik/grupa użytkowników.
21. Obsługa protokołu Bonjour poprzez wbudowany mDNS (multicast DNS) Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów.
22. Obsługa dostępu gościnnego (IPv4 i IPv6):
    a) przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony),

b) przekierowanie użytkowników do strony logowania na zewnętrznym serwerze,
c) obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta,
d) obsługa konfiguracji jako dedykowany kontroler do obsługi ruchu gości – całość ruchu z SSID dostępu gościnnego zebranego na pozostałych kontrolerach musi być przesyłana do tego kontrolera w sposób zapewniający logiczną separację od ruchu wewnętrznego,

23. Obsługa NTP (IPv4 oraz IPv6).
24. Możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania (dni tygodnia, godziny).
25. Obsługa EoGRE w celu tunelowania ruchu z kontrolera do dedykowanego koncentratora (np. na routerze),
26. Wsparcie dla IEEE 802.11u.
27. Obsługa Hotspot 2.0.
28. Obsługa redundancji 1:1 (active/standby) zapewniającej:
    a) utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera,
    b) synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej.
    c) dedykowany interfejs 1 Gb/s typu RJ-45 służący do połączenia dwóch kontrolerów w redundantną parę 1:1.
29. Urządzenie wyposażone w dedykowany interfejs 1 Gb/s typu RJ-45 do zarządzania.
30. Urządzenie wyposażone w port konsoli.
31. Zarządzanie przez HTTPS, SNMP, SSH, NETCONF, port konsoli szeregowej.
32. Obsługa logowania syslog, wsparcie dla IPSec w celu zabezpieczenia syslog.
33. Obsługa wbudowanego interpretera języka PYTHON.
34. Obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020).
35. Wbudowana baza najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem.
36. Zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow, w tym również informacji zawartych w pakiecie od warstw 2 do 7 (w szczególności informacji o aplikacjach).
37. Urządzenie wyposażone jest w licencję subskrypcyjną na wymagane funkcjonalności na okres 5 lat.

B. Dwadzieścia pięć (25) punktów dostępowych sieci WiFi 6E o następujących minimalnych parametrach technicznych:

1. Obsługa IEEE 802.11ax i wcześniejszych standardów:
    a) obsługa OFDMA (uplink/downlink), TWT, BSS Coloring,
    b) obsługa MU-MIMO (uplink/downlink) – min. 8x8:8 (5 GHz),
    c) obsługa MU-MIMO (uplink/downlink) – min. 4x4:4 (2,4 GHz oraz 6 GHz),
    d) obsługa kanałów 20, 40 MHz dla 802.11n,
    e) obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac,
    f) obsługa kanałów 20, 40, 80, 160 MHz (dla 6 GHz) oraz 20, 40, 80, 80+80 MHz (dla 5 GHz) dla 802.11ax,
    g) obsługa prędkości PHY do 3,4 Gbps (ac),
    h) obsługa prędkośći PHY do 10,2 Gbps (ax) (4x4 160MHz w paśmie 6GHz, 8x8 80MHz w paśmie 5GHz, 4x4 20 MHz w paśmie 2,4 GHz),
    i) obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx),
    j) obsługa beamforming dla klientów 802.11ac/ax,
    k) obsługa MRC (Maximal Ratio Combining).

2. Konfigurowalna moc nadajnika:
   a) dla zakresu 2,4 GHz: do 100 mW,
   b) dla zakresu 5 GHz: do 400 mW,
   c) dla zakresu 6 GHz: do 200 mW.
3. Praca trójzakresowa w pasmach: 2,4GHz oraz 5GHz oraz 6GHz
4. Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
   a) automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN,
   b) optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany),
   c) obsługa min. 16 BSSID,
   d) definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID,
   e) uwierzytelnianie ruchu kontrolnego (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w,
   f) obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN),
   g) możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników,
   h) obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6,
   i) jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN),
   j) obsługa Dynamic Frequency Selection (DFS) oraz Transmit Power Control (TPC) zgodnie z IEEE 802.11h,
   k) obsługa IPv6,
   l) obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r,
   m) obsługa mechanizmów QoS:
      - ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik,
      - obsługa WMM, TSPEC, U-APSD
   n) wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM,
   o) obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting,
   p) wsparcie IEEE 802.11i, WPA3, WPA2, WPA,
   q) wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP),
   r) obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS,
   s) obsługa blokowania ruchu Peer-to-Peer,
   t) analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie),
5. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware w tym:
   a) sprawdzanie autentyczności systemu operacyjnego urządzenia przed uruchomieniem urządzenia,
   b) bezpieczna sekwencja uruchamiania,
   c) sprawdzenie autentyczności urządzenia.

6. Zintegrowany moduł radiowy pełniący funkcję analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz, 5GHz oraz 6GHz):
   a) zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych,
   b) automatyczne wykrywanie i klasyfikacja źródeł interferencji (Bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.),
   c) umożliwia skanowanie off-channel (funkcjonuje niezależnie od pracy modułów radiowych transmitujących do klientów) zapewniając dodatkową analizę pasma radiowego pod kątem, m.in.: wykrywania sygnałów DFS, zarządzania ustawieniami parametrów radiowych, zbierania pakietów do lokalizacji urządzeń mobilnych,
7. Wyposażone w:
   a) 2 interfejsy MultiGigabit Ethernet (100M/1G/2.5G/5G) zgodne z IEEE 802.3bz:
      - umożliwiają agregację (LAG – Link Aggregation) – redundancja połączeń,
      - pozwalają na uzyskanie redundancji zasilania w przypadku awarii jednego z połączeń.
   b) interfejs konsoli,
   c) port USB 2.0,
   d) 2 GB RAM,
   e) 1 GB Flash.
8. Umożliwiające zróżnicowane możliwości zasilania:
   a) przy zasilaniu przez 802.3bt: pełna funkcjonalność AP,
   b) przy zasilaniu przez 802.3at: praca w trybie 2x2 w paśmie 2,4GHz, w trybie 4x4 w paśmie 5GHz, w trybie 2x2 w paśmie 6GHz, z jednym pracującym interfejsem przewodowym o prędkości 2,5 Gb/s oraz wyłączonym portem USB,
   c) przy zasilaniu przez 802.3af: możliwość uruchomienia AP w celach diagnostycznych bez pracujących modułów radiowych.
9. Anteny zintegrowane o zysku min. 4 dBi dla pasma 2,4 GHz, 5 dBi dla pasma 5GHz, 6 dBi dla pasma 6GHz.
10. Certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi6, Wi-Fi Enhanced Open, WMM, WMM-PS.
11. Wbudowane radio Bluetooth Low Energy (BLE) 5.0.
12. Wbudowane sensory do pomiaru: temperatury, wilgotności powietrza, jakości powietrza.

C. Dwa (2) przełączniki Multigigabit Ethernet PoE 48 portów o następujących minimalnych parametrach technicznych:

1. Liczba portów – 48 portów RJ-45 PoE+ oraz 4 porty SFP+ w tym:
   a) 12 portów RJ-45 Multigigabit 10G/5G/2.5G/1G/100M,
   b) 36 portów RJ-45 2.5G/1G/100M.
2. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
   a) Gigabit Ethernet 1000Base-T,
   b) Gigabit Ethernet 1000Base-SX,
   c) Gigabit Ethernet 1000Base-LX/LH,
   d) Gigabit Ethernet 1000Base-BX-D/U,
   e) 10Gigabit Ethernet 10GBase-SR,
   f) 10Gigabit Ethernet 10GBase-LR,
   g) 10Gigabit Ethernet 10GBase-BX-D/U,
   h) 10Gigabit Ethernet typu twinax (SFP+ - SFP+).
3. Możliwość połączenia przełączników w stos z zapewnieniem następujących funkcjonalności:
   a) przepustowość w ramach stosu – 320Gb/s,
   b) możliwość połączenia do 8 urządzeń w stosie,
   c) zarządzanie poprzez jeden adres IP,

d) możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
e) wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),
f) urządzenia powinny zostać dostarczone wraz modułami i przewodami pozwalającymi na połącznie w stos.

4. Zasilanie i chłodzenie
   a) dwa redundantne zasilacze dostarczające co najmniej:
      - 675W dla PoE w przypadku pracy jednego zasilacza,
      - 1700W dla PoE w przypadku pracy dwóch zasilaczy,
   b) możliwość wymiany zasilaczy na gorąco,
   c) możliwość podtrzymania zasilania z portów PoE podczas restartu urządzenia,
   d) wsparcie IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),
   e) redundantne i wymienne moduły wentylatorów.
5. Parametry wydajnościowe:
   a) szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):
      - przepustowość przełącznika (switching capacity):
        – minimum 390 Gb/s (bez podłączenia do stosu),
        – minimum 790 Gb/s (z podłączeniem do stosu),
      - prędkość przesyłania (forwarding rate):
        – 350 Mpps (bez podłączenia do stosu),
        – 580 Mpps (z podłączeniem do stosu).
   b) bufor pakietów – 16MB,
   c) pamięć DRAM – 8GB,
   d) pamięć flash – 16GB,
   e) obsługa:
      - minimum 1000 aktywnych sieci VLAN,
      - 32 000 adresów MAC,
      - 8 000 tras IPv4,
      - 4 000 tras IPv6,
      - 5 000 wpisów w listach kontroli dostępu Security ACL,
      - 5 000 wpisów w listach kontroli dostępu QoS ACL,
      - 1 000 interfejsów SVI L3,
      - 128 interfejsów L3,
      - jumbo frame 9198 B,
      - 128 połączeń zagregowanych typu „port channel”,
      - 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
6. Obsługa protokołu NTP.
7. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping.
8. Spanning Tree:
   a) obsługa IEEE 802.1w Rapid Spanning Tree,
   b) obsługa Per-VLAN Rapid Spanning Tree (PVRST+),

c) IEEE 802.1s Multi-Instance Spanning Tree,
d) obsługa 128 instancji protokołu STP.

9. Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED.
10. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
11. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
12. Możliwość uruchomienia funkcji serwera DHCP.
13. Obsługa mechanizmów związanych z bezpieczeństwem sieci:
    a) wiele poziomów dostępu administracyjnego poprzez konsolę; przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    b) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    c) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    d) obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    e) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    f) możliwość uwierzytelniania użytkowników w oparciu o portal WWW dla klientów bez suplikanta 802.1X,
    g) możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
    h) możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
    i) funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
    j) obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection oraz IP Source Guard,
    k) zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
    l) możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
    m) obsługa list kontroli dostępu (ACL) następujących typów:
        - port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
        - VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
        - routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
        - możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
    n) możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128),
    o) wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
    p) funkcja Private VLAN.

14. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    a) sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    b) bezpieczna sekwencja uruchamiania,
    c) sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
15. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    a) implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    b) implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
    c) możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    d) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    e) możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
    f) kontrola sztormów dla ruchu broadcast/multicast/unicast,
    g) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
16. Obsługa protokołów i mechanizmów routingu:
    a) routing statyczny dla IPv4 i IPv6,
    b) routing dynamiczny – RIP, OSPF do 1000 tras, PIM Stub do 1000 tras,
    c) policy-based routing (PBR),
    d) obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,
    e) obsługa 10 tuneli GRE (Generic Routing Encapsulation);
17. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN.
18. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
19. Zarządzanie:
    a) port konsoli,
    b) dedykowany port Ethernet do zarządzania out-of-band,
    c) plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
    d) obsługa protokołów SNMPv3, SSHv2, SCP, SFTP (SSH File Transfer Protocol), HTTPS, syslog,
    e) możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
    f) wsparcie dla protokoły RESTCONF,
    g) przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
    h) port USB umożliwiający podłączenie zewnętrznego nośnika danych; urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.

20. Wbudowany interfejs webowy zarządzania przełącznikiem umożliwiający:
    a) monitoring pracy przełącznika w zakresie:
        - użycie CPU,
        - użycie pamięci,
        - temperatura pracy,
        - podstawowe informacje systemowe: rodzaj sprzętu, czas pracy, czas systemowy, oprogramowanie, data i czas ostatniej zmiany konfiguracji,
        - obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, wykorzystanie PoE,
        - informacji o urządzeniach sąsiednich podłączonych do przełącznika,
        - statystyki ruchu (RX/TX) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN,
        - statystyki ruchu (RX/TX) na poszczególnych portach L3,
        - informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
    b) konfigurację przełącznika w zakresie:
        - konfiguracja interfejsów L2,
        - konfiguracja interfejsów L3,
        - tworzenie i konfiguracja sieci VLAN,
        - konfiguracja protokołu STP,
        - tworzenie i konfiguracja wirtualnych instancji routingu (VRF),
        - konfiguracja routingu statycznego,
        - uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
        - tworzenie i przypisanie list kontroli dostępu ACL,
        - konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
        - konfiguracja i uruchomienie NetFlow,
    c) administracja przełącznika w zakresie:
        - zdalnego uruchamia komend linii poleceń,
        - ustawiania czasu systemowego, w tym obsługi protokół NTP,
        - obsługi kont administracyjnych,
        - upgrade'u oprogramowania,
        - backupu konfiguracji,
        - zdalnego restart urządzenia,
        - konfiguracji i dostępu przez SNMP,
        - narzędzi PING i TRACEROUTE,
        - przeglądania logów systemowych.
21. Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU.
22. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow –obsługa 64000 strumieni (flow).
23. Obsługa rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych.
24. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
25. Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku.
26. Przełącznik musi być wyposażony w:

a) moduł do łączenia w stos wraz z kablem stakującym o długości 50 cm,
b) 4 moduły 10Gigabit Ethernet 10GBase-SR,
c) licencję subskrypcyjną na wymagane funkcjonalności na okres co najmniej 5 lat,
d) zestaw do montażu w szafie rack 19".

27. Przełącznik musi współpracować z systemem rancid wykorzystywanym przez zamawiającego do backupu konfiguracji.

D. System zarządzania siecią o następujących minimalnych parametrach technicznych:

1. Dostarczony jako komponent sprzętowy albo jako maszyna wirtualna (virtual appliance).
2. Zapewniający zarządzanie i monitorowanie sieci Zamawiającego przy użyciu interfejsu graficznego.
3. Musi obsługiwać punkty dostępowe Cisco AIR-AP1832I-E-K9 będące w posiadaniu zamawiającego.
4. Musi pozwolić na zaimportowanie map, wraz z naniesionymi punktami dostępowymi WiFi, z systemu Cisco Prime 3.8.x Zamawiającego.
5. Funkcjonalności podstawowe z zakresu monitoringu sieci:
   a) zbieranie i zapamiętywanie do 30 dni wstecz danych telemetrycznych o działaniu sieci, urządzeń sieciowych przewodowych i bezprzewodowych, użytkowników i aplikacji z różnych źródeł danych: SNMP, Syslog, NetFlow,
   b) analiza i korelacja wskazanych powyżej danych,
   c) wyznaczenie na postawie analizy danych telemetrycznych dla każdego z urządzeń sieciowych, grupy użytkowników, pojedynczego użytkownika oraz grupy aplikacji lub pojedynczej aplikacji indeksu liczbowego określającego jakość pracy danego monitorowanego obiektu, monitorowanych obiektów,
   d) wizualizacja topologii sieci wraz połączeniami oraz wizualizacją indeksu jakości pracy danego monitorowanego obiektu,
   e) wyznaczenie i wizualizacja indeksów jakości pracy dla grup urządzeń sieciowych wg:
      - typów urządzeń: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, kontroler WLAN, radiowy punkt dostępowy - w przedziałach czasowych ostatnie 7 dni, ostatnie 24h, ostatnie 3h, zadany przedział czasowy w okresie ostatnich 30 dni,
      - lokalizacji geograficznych,
   f) wizualizacja na skali czasu zmiany wartości indeksów jakości pracy dla grup urządzeń sieciowych;
   g) wyznaczenie i wizualizacja indeksów jakości pracy dla grup użytkowników z rozbiciem na użytkowników przewodowych oraz bezprzewodowych wraz z wizualizacją na skali czasu zmiany wartości indeksów jakości pracy dla grup użytkowników;
   h) dla użytkowników przewodowych szczegółowa informacja o ilości użytkowników podłączonych do sieci oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci z podaniem typowych przyczyn braku podłączenia np. problem z otrzymaniem adresu z serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej; szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP,
   i) dla użytkowników bezprzewodowych szczegółowa informacja o ilości użytkowników podłączonych do sieci z rozbiciem na grupę użytkowników o dobrej jakości i złej jakości pracy oraz ilości użytkowników, którzy mieli problemy z podłączeniem do sieci bezprzewodowej z podaniem typowych przyczyn braku podłączenia np. problem z otrzymaniem adresu z

serwera DHCP, problem z uwierzytelnieniem, informacja o lokalizacjach i urządzeniach, gdzie takie problemy występują najczęściej; szczegółowa lista użytkowników zaliczonych do danej kategorii np. użytkownicy z problemem z usługą DHCP,

j) generowanie automatycznych komunikatów o stwierdzonych nieprawidłowościach w pracy sieci w oparciu o skorelowane informacje zbierane przez system z urządzeń sieciowych wraz z sugestią przyczyny, sposobu rozwiązania problemu oraz dalszych krokach diagnostycznych dla poszczególnych urządzeń sieciowych,

k) narzędzie do śledzenia ścieżki sieciowej dla danego ruchu w sieci np. w relacji pomiędzy dwoma hostami wraz podanie informacji o wszystkich węzłach na ścieżce, ich indeksie jakości pracy, topologii fizycznej i logicznej np. zaznaczenie tunelowania ruchu bezprzewodowego, dokładną informacją o interfejsach, przez który płynie ruch, z zaznaczeniem lokalizacji list ACL, które dokonują filtracji danego ruchu,

6. Wykrywanie i analiza problemów w sieci:
   a) automatyczna analiza zdarzeń w sieci oraz identyfikacja i wyświetlanie na tej podstawie problemów w działaniu sieci na poziomie całej sieci lub poszczególnych monitorowanych obiektów np. problemy związane z danym urządzeniem, użytkownikiem lub aplikacją,
   b) automatyczna priorytetyzacja problemów,
   c) dla danego problemu, podanie opisu problemu, dostarczenie informacji kontekstowej umożliwiającej identyfikację i rozwiązanie problemu, określenie lokalizacji, urządzeń oraz użytkowników dotkniętych problemem, propozycja sugerowanych działań umożliwiających rozwiązanie problemu wraz z możliwością dostępu do urządzeń sieciowych w celu natychmiastowego dostarczenia danych diagnostycznych,
7. Monitoring urządzeń:
   a) monitoring dostępności i osiągalności poszczególnych urządzeń sieciowych,
   b) w zakresie sieci bezprzewodowej:
      - wykres ilości aktywnych i nieaktywnych punktów radiowych z podaniem dokładnej listy urządzeń w każdej z kategorii;
      - lista radiowych punktów dostępowych wg ilości podłączonych klientów bezprzewodowych;
      - lista radiowych punktów dostępowych wg poziomu zakłóceń i interferencji funkcji pasma transmisji 2.4 GHz, 5 GHz;
   c) pełna lista wszystkich monitorowanych urządzeń sieciowych w całej sieci lub w danej domenie lub lokalizacji z podaniem modelu urządzenia, wersji systemu operacyjnego, adresu IP, indeksu jakości pracy, osiągalności, ilości zidentyfikowanych problemów, lokalizacji geograficznej; możliwość eksportu danych w postaci pliku CSV,
   d) możliwość łatwego filtrowania listy urządzeń wg kryteriów:
      - typ urządzenia: router, przełącznik rdzeniowy, przełącznik dystrybucyjny, przełącznik dostępowy, radiowy punkt dostępowy, kontroler WLAN,
      - stan jakości pracy urządzenia: jakość niska, średnia, wysoka,
      - lokalizacja,
      - model urządzenia,
      - wersja systemu operacyjnego,
      - adres IP,
   e) szczegółowy monitoring każdego z urządzeń sieciowych obejmujący:
      - wykres zmian indeksu jakości pracy urządzenia w zadanym okresie czasu do 30 dni wstecz,

- szczegółowa informacja o następujących parametrach pracy urządzenia w dowolnym momencie pracy urządzenia do 30 dni wstecz; monitorowane parametry: wykorzystanie pamięci i procesora, dostępność łączy uplinkowych (w górę sieci), poziom błędów na łączach, skojarzone zdarzenia zarejestrowane w systemie,
- szczegółowa lista wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 30 dni wstecz) o problemach skojarzonych z danym urządzeniem,
- schemat topologii sieci, w której znajduje się urządzenie,
- dostęp do zdarzeń zarejestrowanych w systemie związanych z danym urządzenie z możliwością filtrowanie wg Ważności,
- możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia do danego innego miejsca w sieci (adresu IP),
- możliwość bezpośredniego, z poziomu konsoli graficznej systemu zarządzania i monitorowania, dostępu do konsoli urządzenia lub narzędzia umożliwiającego zdalne wydawanie komend na urządzeniu,
- szczegółowe informacje o urządzeniu obejmujące:
  - wykresy czasowe: wykorzystania procesora, pamięci, dostępności i temperatury urządzenia,
  - informacje o poszczególnych interfejsach urządzeń w uwzględnieniem: stanu interfejsu, typu, numer skonfigurowanej sieci VLAN, MAC adresu podłączonego urządzenia, prędkość linku, FDX/HDX,
  - dla każdego z monitorowanych interfejsów wykresy czasowe: dostępności interfejsu, jego wykorzystania oraz poziomu błędów,

8. Monitoring użytkowników:
   a) Szczegółowe informacje o użytkowniku końcowym i urządzeniach, na których pracuje takie jak:
      - identyfikator użytkownika,
      - nazwa, adres MAC, adres IPv4 lub IPv6 komputera lub urządzenia, na których pracuje,
      - typ urządzenia,
      - urządzenie sieciowe, do którego jest podłączone dane urządzenie końcowe wykorzystywane przez użytkownika,
      - lokalizacja geograficzna,
   b) szczegółowa informacja o następujących parametrach pracy urządzenia końcowego wykorzystywanego przez użytkownika w dowolnym momencie do 30 dni wstecz; monitorowane parametry: stan podłączenia do sieci, dla urządzeń bezprzewodowych: poziom sygnału RSSI, poziom szumów SNR, przepustowość połączenia, ilość danych otrzymanych i nadawanych, SSID sieci, do której jest podłączone urządzenie końcowe, nazwa radiowego punktu dostępowego, wykorzystywany kanał radiowy i pasmo,
   c) szczegółowa lista wszystkich bieżących oraz historycznych (dla zadanego okna czasowego w okresie do 7 dni wstecz) problemów skojarzonych z danym urządzeniem końcowym,
   d) schemat topologii sieci z zaznaczeniem urządzenia dostępowego, do którego jest podłączony dane urządzenie końcowe,
   e) dostęp do zdarzeń zarejestrowanych w systemie związanych z danym urządzenie z możliwością filtrowanie wg ważności,
   f) możliwość uruchomienia narzędzia do analizy ścieżki od danego urządzenia do danego innego miejsca w sieci (adresu IP);

g) informacje o generowanym ruchu sieciowym przez użytkownika na danym urządzeniu końcowym z podziałem na aplikacje biznesowe oraz niebiznesowe; szczegółowe informacje dla każdej z aplikacji takie jak: nazwa aplikacji, indeks jakości działania aplikacji w sieci, ruch (w bajtach), średnia przepustowość (w bps), parametry QoS faktyczne oraz oczekiwane, straty pakietów (maksymalne i średnie), opóźnienie sieciowe (maksymalne i średnie), jitter (maksymalny i średni),
h) Szczegółowe informacje o urządzeniu końcowym wykorzystywanym przez użytkownika:
   - wykres czasowy ilości danych nadawanych i otrzymywanych,
   - wykres czasowy ilości generowanych zapytań DNS i otrzymywanych odpowiedzi,
   - dla urządzeń bezprzewodowych wykres czasowy zmian wartości mocy sygnału radiowego RSSI oraz zmian wartości poziomu szumów SNR.

9. Monitoring aplikacji:
   a) szczegółowe informacje o aplikacjach wykorzystywanych w sieci takie jak: lista wszystkich wykrytych aplikacji z podaniem nazw aplikacji, klas ruchu, ilości ruchu generowanego, średniej przepustowości, straty pakietów, opóźnienia sieciowego oraz wykrytych problemów związanych z daną aplikacją,
   b) szczegółowe wykresy czasowe parametrów działania każdej z aplikacji z uwzględnieniem: przepustowości wykorzystywanej przez daną aplikację, strat pakietów, jitter, opóźnienia sieciowego, opóźnienia sieciowego po stronie klienta, opóźnienia sieciowego po stronie serwera, opóźnienia generowanego przez serwer aplikacyjny,
   c) szczegółowa lista wszystkich użytkowników wykorzysujących daną aplikację w sieci z podaniem urządzenia końcowego, który wykorzystuje daną aplikację.
10. Monitoring i zarządzanie siecią bezprzewodową:
   a) Wizualizacja graficzna rozmieszczenia poszczególnych radiowych punktów dostępowych, oraz klientów sieci bezprzewodowej na mapie budynku:
      - graficzne planowanie i zarządzanie siecią bezprzewodową (hierarchiczne mapy lokalizacji, mapy zasięgu) z wykorzystaniem własnych planów budynków,
      - tworzenie i wyświetlanie trójwymiarowych map teoretycznego zasięgu sieci bezprzewodowej dla częstotliwości dostępnych w monitorowanej sieci bezprzewodowej, wizualizacja dla RSSI, SNR oraz interferencji,
      - narzędzie do wizualizacji zmiany teoretycznego zasięgu sieci bezprzewodowej (planowanie) przy dołożeniu dodatkowych (wirtualnych) punktów dostępowych na mapie,
      - monitorowanie informacji takich jak: poziom szumu, poziom sygnału, interferencje sygnału pochodzących z punktów dostępowych,
      - współpraca z systemami lokalizacji urządzeń radiowych (punktów dostępowych, klientów, tagów) z prezentacją graficzną na mapie,
   b) monitoring usług sieciowych takich jak: usługi uwierzytelniania i kontroli dostępu (AAA) oraz DHCP w zakresie:
      - ilość udanych i nieudanych transakcji,
      - średnie opóźnienie,
      - lista lokalizacji o największym opóźnieniu oraz największej ilości nieudanych transakcji łącznie lub per serwer,
   c) narzędzie pozwalające na wykonywanie testów poprawności pracy sieci bezprzewodowej poprzez generowanie syntetycznego ruchu przez punkty dostępowe pozwalające na badanie/wykonanie testu:

- czasu podłączania się do sieci: asocjacja, uwierzytelnienie, adresacja z DHCP,
- pracy usług: DNS, RADIUS, dostępność bramy, dostępność określonych adresów IP,
- pracy aplikacji: POP3, IMAP, Outlook Web Access, FTP, HTTP, HTTPS,

d) możliwość określenia czasu lub częstotliwości wykonywania testów,
e) narzędzie pozwalające na monitoring i zarządzanie zagrożeniami w sieci bezprzewodowej uwzględniające wrogie punkty dostępowe (Rogue AP) oraz ataki identyfikowane przez sygnatury (Wireless IPS/IDS):
   - wyświetlanie zdarzeń bezpieczeństwa w zadanym oknie czasowym: ostatnich 3 godzin, 24 godzin lub 7 do 14 dni wstecz,
   - wyświetlanie szczegółowej listy indywidualnych zagrożeń wraz z informacją o ich: szkodliwości, typie, lokalizacji, czasie wykrycia oraz nazwie AP który je wykrył,
   - konfiguracja profili WIPS, które pozwalają na: określenie typów obsługiwanych sygnatur, wartości progów liczbowych wyzwalających daną sygnaturę oraz czy ma zostać zebrany materiał dowodowy (plik pcap) z danego zdarzenia,
   - konfiguracja reguł klasyfikacji wrogich punktów dostępowych (Rogue AP) w oparciu o: nazwę SSID, siłę sygnału RSSI (Received Signal Stength Indicator), to czy dane SSID jest szyfrowane czy nie, minimalną liczbę podłączonych urządzeń,
   - generowanie raportów z informacjami o zdarzeniach bezpieczeństwa w formie pliku CSV lub JSON,
f) narzędzie do tworzenia konfiguracji na kontrolerach i punktach dostępowych w zakresie:
   - tworzenie sieci WLAN (SSID) typu: sieć oparta o 802.1X oraz sieć gościnna,
   - tworzenie profili ustawień radiowych uwzględniających takie parametry jak: obsługiwane kanały radiowe, wspierane prędkości radiowe, parametry wykrywania dziur w pokryciu, itp.,
   - tworzenie list kontroli dostępu,
   - tryb pracy tunelowania ruchu w sieci bezprzewodowej.

11. Funkcjonalności z zakresu zarządzania siecią:
    a) hierarchizacja zarządzania siecią odzwierciedlająca hierarchię geograficzną tj. możliwość podziału sieci na kilka poziomów geograficznych np. miasto, budynek, piętro,
    b) wizualizacja graficzna na mapie lokalizacji poszczególnych urządzeń sieciowych – automatyczne rozmieszczanie urządzeń na postawie adresów pocztowych,
    c) możliwość wgrywania własnych planów budynków z dokładnością do poszczególnych pięter,
    d) obsługa REST API,
    e) integracja z systemem uwierzytelniania AD w celu otrzymywania informacji o tym jaki użytkownik jest związany z jakim urządzeniem, szczegółowej informacji o przebiegu procesu uwierzytelniania do sieci; uwzględnienie tych danych w procesie wyznaczania indeksów jakości pracy użytkowników jak również w procesie diagnostyki problemów w sieci,
    f) mechanizm automatycznej aktualizacji wersji systemu,
    g) wbudowane narzędzia do automatycznego tworzenia polityki QoS dla całej sieci w oparciu o wbudowane wzorce aplikacji, z możliwością tworzenia własnych wzorców; możliwości dokonywania zmian w polityce i jej szybkiej implementacji oraz możliwość cofania zmian bez konieczności ręcznej rekonfiguracji urządzeń sieciowych,
    h) funkcjonalność automatycznego wykrywania urządzeń sieciowych w oparciu o SNMP, CLI, HTTP, SSH,
    i) możliwość tworzenia parametryzowanych wzorców konfiguracyjnych dla urządzeń w oparciu o język skryptowy,

j) inwentaryzacja urządzeń oraz oprogramowania w zakresie minimum:
   - nazwa urządzenia,
   - adresy IP i MAC urządzenia,
   - typ urządzenia,
   - lokalizacja,
   - osiągalność oraz uptime,
   - numer seryjny,
   - wersja oprogramowania oraz zgodność oprogramowania z obowiązującą wersją,
   - indeks jakości pracy,
   - współczynnik zgodności z przyjętymi kryteriami (compliance),

k) zarządzanie wersjami oprogramowania z możliwością wskazania wersji obowiązujących,

l) narzędzie do aktualizacji oprogramowania na urządzeniach umożliwiające:
   - weryfikację warunków technicznych do wykonania aktualizacji (ilość wolnego miejsca, weryfikacja ustawień konfiguracji startowej, warunki do wykonania aktualizacji bezprzerwowej ISSU – In Service Software Upgrade),
   - przeprowadzenie aktualizacji na wybranych urządzeniach lub grupie urządzeń, w tym bezprzerwowej aktualizacji ISSU dla urządzeń, które wspierają taką funkcję,
   - wykonanie predefiniowanych i możliwość dodania własnych komend kontrolnych (sprawdzeń) przed i po wykonaniu aktualizacji,
   - funkcja zaprogramowania daty i czasu wykonania aktualizacji,
   - funkcja usunięcia z pamięci flash urządzenia nieaktualnych wersji oprogramowania po aktualizacji,
   - raport z aktualizacji obejmujący wynik aktualizacji i jej przebieg, status wykonania komend kontrolnych oraz raport niezgodności,

m) narzędzie do archiwizacji konfiguracji urządzeń umożliwiające:
   - stworzenie kopii zapasowej konfiguracji,
   - możliwość ustalenia dnia i godziny automatycznego backupu,
   - wyświetlanie na osi czasu punktów, w których została dokonania kopia konfiguracji razem z wyświetleniem różnic między wersjami,

n) narzędzie do zdalnego uruchamiania aplikacji i zarządzania nimi na urządzeniach sieciowych wyposażonych w taką funkcjonalność,

o) możliwość definiowania profili sieciowych oraz parametrów sieciowych takich jak: serwery TACACS+, RADIUS, NTP, syslog, NetFlow, DNS, DHCP dla poszczególnych poziomów hierarchii sieciowej niezależnie lub dziedziczenie tych ustawień z poziomu wyższego w dół hierarchii; centralne zarządzanie parametrami dostępowymi do urządzeń wraz z możliwością ich zmiany dla jednego urządzenia, grupy urządzeń lub całej sieci.

12. Gwarancja na system zarządzania siecią, obejmująca aktualizacje oprogramowania i niezbędne licencje subskrybcyne związane z wyżej określonymi funkcjonalnościami na okres 3 lat.

E. Serwer autoryzacji o następujących minimalnych parametrach technicznych:

1. Obudowa rack, wielkość maksymalnie 2U.
2. Komplet szyn umożliwiających montaż w szafie rack 19” i wysuwanie serwera w celach serwisowych.
3. Płyta główna z możliwością zainstalowania minimum dwóch procesorów, dedykowana do pracy w serwerach.

4. Chipset dedykowany przez producenta procesora do pracy w serwerach wieloprocesorowych.
5. Zainstalowane dwa (2) procesory serwerowe, co najmniej szesnastordzeniowe, klasy x86 (64-bit), o wydajności w teście PassMark CPU Mark nie mniejszej niż 62 000 pkt. (mierzonych dla konfiguracji dwuprocesorowej),
6. Zainstalowane min. 256 GB pamięci RAM, z możliwością rozbudowy co najmniej do 1 TB RAM bez usuwania pierwotnie zainstalowanych układów pamięci.
7. Zainstalowane 2 dyski SSD o pojemności min. 128 GB działające w konfiguracji RAID-1.
8. Zainstalowane min. 4 interfejsy 10/25 Gigabit Ethernet SFP28 obsadzone modułami SFP 28 LR
9. Serwery wyposażone w dwa redundantne zasilacze Hot Plug zapewniające prawidłową pracę serwera przy maksymalnym obciążeniu w oferowanej konfiguracji.
10. Wyposażone w redundantną wentylację Hot Plug w konfiguracji wystarczającej do redundantnego chłodzenia obudowy.
11. Panel LCD lub diody LED umieszczone na froncie obudowy, umożliwiający wyświetlenie informacji o stanie serwera.
12. Serwer musi posiadać oficjalne wsparcie producenta dla następujących systemów:
    a) Microsoft Windows Server z Hyper-V
    b) VMware ESXi
13. Karta zarządzająca, niezależna od zainstalowanego systemu operacyjnego, o następującej minimalnej funkcjonalnosci:
    a) zdalny dostęp do graficznego interfejsu Web karty zarządzającej,
    b) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera),
    c) szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika,
    d) możliwość podmontowania zdalnych wirtualnych napędów,
    e) wirtualną konsolę z dostępem do myszy, klawiatury,
    f) wsparcie dla IPv6,
    g) wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, SSH,
    h) integracja z Active Directory,
    i) możliwość obsługi przez dwóch administratorów jednocześnie,
    j) wsparcie dla dynamic DNS,
    k) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
14. Wymagane jest dostarczenie wszystkich licencji niezbędnych do korzystania z powyższych funkcjonalności.
    a) Wraz z serwerem muszą zostać dostarczone licencje MS Windows Server Datacenter Edition w wersji Accademic lub równoważne na liczbę rdzeni zainstalowanych w serwerze. Przez oprogramowanie równoważne Zamawiający rozumie oprogramowanie spełniające następujące wymagania:
        - możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek;
        - możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;
        - możliwość uruchomienia kontrolera domeny będącego w pełni zgodnym z domeną AD pracującą w oparciu o minimum system Windows Server 2012 R2 (poziom funkcjonalności

- możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
- możliwość uruchomienia usługi DFS zgodnej z min. Windows Server 2012 R2;
- możliwość uruchomienia serwera usług terminalowych (RemoteApp) zgodnego z min. Windows Server 2008 R2;
- obsługa zdalnego pulpitu;
- możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
- obsługa PowerShell 4.0;
- obsługa certyfikatów w AD.