***Nr sprawy: 19/P/2024***

**Rozbudowa infrastruktury serwerowej i sieciowej OR POLATOM w podziale na części**

# Załącznik A do SWZ

## Spis treści


Wymagania ogólne ..... 3
1. Rozbudowa sieci LAN (Część 1) ..... 5
1.1. Oprogramowanie do zarządzania siecią, zarządzania dostępem, analizowania zdarzeń. ..... 7
1.2. Oprogramowanie do zarządzania dostępem (NAC). ..... 10
1.3. Kontroler do zarządzania sieci bezprzewodowej ..... 14
1.4. Przełączniki rdzeniowe 54 portowe – 6 sztuk: ..... 16
1.5. Przełączniki brzegowe 48 portowe – 14 sztuk, ..... 18
1.6. Przełączniki brzegowe 24 portowe – 8 sztuk ..... 20
1.7. Przełączniki brzegowe 12 portowe – 8 sztuk, ..... 22
1.8. Punkty dostępowe sieci bezprzewodowej - 32 sztuki wraz z centralnym kontrolerem sieci bezprzewodowej ..... 24
1.9. Akcesoria ..... 26
1.10. Zamówienie opcjonalne dla części 1 ..... 26
2. Urządzenia serwerowe (Część 2) ..... 28
2.1. Obudowa serwerów kasetowych ..... 28
2.2. Serwer kasetowy na potrzeby bazy danych SQL o parametrach minimalnych: ..... 30
2.3. Serwer kasetowy na potrzeby wirtualizacji o parametrach minimalnych: ..... 30
2.4. Serwer kasetowy na potrzeby systemów operacyjnych Windows o parametrach minimalnych: 31
2.5. Zamówienie opcjonalne dla części 2 ..... 32
Obudowa na serwery kasetowe. 1 sztuka (Specyfikacja jak punkt 2.1) ..... 32
Serwery kasetowe dla wirtualizacji o parametrach minimalnych ..... 32
Serwery kasetowe na potrzeby systemów operacyjnych Windows o parametrach minimalnych ..... 32
3. Rozbudowa sieci SAN i przestrzeni dyskowej (Część 3) ..... 33
3.1. Przełączniki szkieletowe sieci SAN-FC ..... 33
3.2. Macierz dyskowa SAN-FC z przeznaczeniem na aplikacje bazodanowe i wirtualizacje. ..... 33
3.3. Macierz dyskowa SAN-FC z przeznaczeniem na przechowywanie kopii zapasowych ..... 34
3.4. Macierz dyskowa SAN-FC dedykowana do obsługi bazy danych. ..... 35
3.5. Zamówienie opcjonalne dla części 3 ..... 36

Macierz dyskowa SAN-FC z przeznaczeniem na aplikacje bazodanowe i wirtualizacje. 1 sztuka (Specyfikacja jak punkt 3.2) ..... 36
Dodatkowa półka dyskowa do macierzy z punktu 3.3. Macierz dyskowa SAN-FC z przeznaczeniem na przechowywanie kopii zapasowych o parametrach: ..... 36
Macierz dyskowa FC SAN z przeznaczeniem na aplikacje bazodanowe i wirtualizacje. ..... 36

## Wymagania ogólne

Dostarczony sprzęt winien być sprawny, fabrycznie nowy, nie plombowany (z możliwością bez narzędziowej ingerencji we wnętrze obudowy), a data produkcji nie może być wcześniejsza niż 8 miesięcy od daty dostawy. Wszystkie urządzenia, zamówione w liczbie większej niż 1 sztuka, muszą być takie same pod względem modelu/wyposażenia/koloru, wzajemnie kompatybilne i zapewniać wzajemną zamienność technologiczną podzespołów. Urządzenia muszą być dostarczone w stanie wolnym od wad technicznych oraz prawnych i formalnych odnośnie uprawnień do gwarancji i aktualizacji. Całość dostarczanego sprzętu musi zostać dostarczona do siedziby Zamawiającego.

W celu zapewnienia gwarancji realizowanej przez jeden podmiot, całość dostawy musi pochodzić z oficjalnego kanału dystrybucji adresowanego na rynek polski. Gwarancja na całość dostarczanego sprzętu w ramach części postępowania musi być realizowana przez jeden podmiot, to znaczy przez producenta sprzętu bądź partnera posiadającego autoryzację producenta. Informacja o możliwych formach kontaktu z serwisem musi znajdować się na stronach internetowych producenta sprzętu.

Zamawiający wymaga, aby całość dostarczanego sprzętu i oprogramowania pochodziła z autoryzowanego kanału sprzedaży producenta i wymaga by do oferty dołączyć certyfikat legalności produktów lub równoważny - pismo potwierdzające od Producenta producenta, że dostawca jest autoryzowanym parterem oraz że produkty i wsparcie oferowane klientowi pochodzą z autoryzowanego i legalnego kanału sprzedaży oraz posiadają wsparcie producenta. Oferowane przełączniki LAN i elementy sieci WLAN, wkładki optyczne oraz system zarządzania muszą pochodzić od jednego, tego samego, Producenta oraz muszą być wzajemnie kompatybilne.

Wszystkie dostarczone funkcjonalności wbudowane w urządzenia muszą być dostępne bezterminowo. Zamawiający dopuszcza licencjonowanie terminowe tylko w sytuacji, kiedy dotyczy ono oprogramowania do centralnego zarządzania, a funkcje na urządzeniach będą nadal działały tylko wymagając większego nakładu pracy w celu rekonfiguracji. Zamawiający dopuszcza dostawę urządzenia, którego funkcjonalność będzie ograniczona terminem tylko w sytuacji dostarczenia oprogramowania do zarządzania z minimalnie 10 letnim wsparciem, chyba że wskazano inaczej w specyfikacji przy urządzeniu.

Wykonawca zagwarantuje wsparcie serwisowe oraz techniczne producenta sprzętu. Wsparcie to musi być zapewnione poprzez wskazany dedykowany numer telefoniczny oraz adres e-mail dla wsparcia technicznego i informacji produktowej. W ramach wsparcia Zamawiający wymaga możliwości weryfikacji na stronie producenta sprzętu komputerowego: konfiguracji fabrycznej zakupionego sprzętu, wykupionej gwarancji na każdy dostarczony towar oraz statusu naprawy urządzeń. Zamawiający wymaga również możliwości pobierania sterowników dla zamawianego sprzętu przez stronę producenta po podaniu indywidualnego numeru seryjnego oraz poprzez dedykowane oprogramowanie.

Wszystkie dostarczone na przełączniku sieciowym funkcje (tak wyspecyfikowane jak i niewyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne). Wymaga się, aby dostawca zaznaczył, czy licencje na oprogramowanie są udzielane na czas określony lub nieokreślony.

Dostarczany sprzęt wraz z dostawą musi posiadać deklaracje zgodności CE oraz potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki lub równoważne.

W przypadku napraw realizowanych przez autoryzowanych partnerów, wymaga się przedstawienia dokumentów wystawionych przez producenta sprzętu, potwierdzających autoryzowane partnerstwo.

Ponadto, Wykonawca zapewni, że producent sprzętu w przypadku niewywiązywania się serwisu z obowiązków gwarancyjnych, przejmie on wszelkie zobowiązania związane z serwisem zgodnie z udzieloną gwarancją i zgodnie z wykupionymi przez Wykonawcę u producenta dodatkowymi opcjami serwisowymi, mającymi spełnić stawiane wymagania.
Wymagany okres gwarancji oraz wymagany czas naprawy urządzeń został określony w minimalnych wymaganiach technicznych. **Zgłoszenia usterek będą przyjmowane w cyklu 24 godziny na dobę przez 7 dni w tygodniu.** Zamawiający dopuszcza przysłanie przez serwis części zamiennej w celu szybszego usunięcia usterki przez lokalny zespół wsparcia reprezentowany przez dział Systemów Teleinformatycznych OR POLATOM.
W przypadku braku możliwości naprawy sprzętu w wymaganym przedziale czasowym (72 h) w okresie gwarancyjnym, Zamawiający wymaga aby na czas naprawy udzielono nieodpłatnego wypożyczenia urządzenia o porównywalnych parametrach, umożliwiających uruchomienie konfiguracji z posiadanego urządzenia z kopii zapasowej. Zamawiający wymaga, aby serwis posiadał historię wymiany sprzętu, jeżeli zmienią się numery seryjne przy wymianie urządzenia. Zamawiający podczas zgłoszenia serwisowego nie będzie wysyłał dokumentów potwierdzających jego zakup.
**Podczas naprawy bądź wymiany urządzenia, dyski twarde i inne nośniki danych wykorzystywane w urządzeniach przetwarzających dane nie mogą opuścić terenu NCBJ OR POLATOM.** Dopuszczalne jest wysłanie samej elektroniki z dysku magnetycznego, jeżeli nie posiada on wbudowanej pamięci cache lub SSD, jako potwierdzenie uszkodzenia i nieużywania nośnika przez OR POLATOM. W przypadku awarii dysku twardego, pozostaje on u Zamawiającego bez naliczania dodatkowych opłat.

Numery seryjne przypisane do dostarczonych produktów wraz z numerami akcesoriów należy dostarczyć elektronicznie w postaci tabelarycznej umożliwiającej zaimportowanie do zewnętrznych systemów. Przykładowo xlsx lub csv. Wykaz ten zostanie wykorzystany również w celu weryfikacji gwarancji na dostarczony sprzęt u producentów urządzeń. Tabela musi zawierać co najmniej: l.p., nazwę produktu, numer seryjny.
Zamawiający wymaga, aby sprzęt zakupiony przez zamawiającego był zarejestrowany w systemach producenta bezpośrednio na Zamawiającego jako klienta końcowego.

W celu sprawdzenia zgodności oferowanego sprzętu z wymaganiami SWZ, wymagane jest podanie w ofercie (w formularzu asortymentowo-cenowym) przez Wykonawcę: modelu, symbolu oraz nazwy producenta oferowanego sprzętu.

Uruchomienie systemu może być zrealizowane przez Wykonawcę wraz z pracownikami producenta. Wykonawca musi zapewnić Zamawiającemu możliwość kontaktu z inżynierami producenta w celu omówienia funkcji posiadanych przez dostarczane rozwiązanie.

**Wymagania dodatkowe na wezwanie przed podpisaniem umowy:**
Certyfikat ISO 9001 dla producenta sprzętu w zakresie wytwarzania i świadczenia usług serwisowych.

**Wymagania dodatkowe na etapie składania ofert:**
Certyfikat ISO 9001 dla Wykonawcy zamówienia w zakresie świadczenia usług serwisowych.
Oświadczenie producenta potwierdzające, że serwis urządzeń będzie realizowany bezpośrednio przez producenta i/lub we współpracy z autoryzowanym partnerem serwisowym.

## 1. Rozbudowa sieci LAN (Część 1)

W związku z rozbudową istniejącej sieci, Zamawiający wymaga, aby produkt był fabrycznie nowy, nieużywany przez innych klientów w celu zachowania gwarancji wieczystej realizowanej przez producenta sprzętu.

Minimum 5 lat gwarancji producenta, obejmującej wszystkie elementy przełącznika, punktu dostępowego, dostarczanego oprogramowania (również zasilacze i wentylatory) zapewniającą dostawę sprawnego sprzętu, z wysyłką, na wymianę w maksymalnie następny dzień roboczy gdzie produkt dotrze do Zmawiającego maksymalnie w 7 dni roboczych.

Minimum 5 lat wsparcia na dostarczane licencje uprawniające do aktualizacji do najnowszej wersji.

Zakończenie gwarancji nie może spowodować utraty dostępu do oprogramowania firmware urządzenia. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika, również po wygaśnięciu kontraktu serwisowego.

Wymagana jest dostępność usługi gwarancyjnej w trybie co najmniej 24x7. Serwis musi być świadczony bezpośrednio przez producenta sprzętu lub autoryzowanego partnera. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i wskazanym serwisem w języku polskim.

W związku z tym, iż większość producentów aktualnie proponuje oprogramowanie ograniczone czasem (model subskrypcyjny licencji) należy dostarczyć oprogramowanie z terminem ważności licencji oraz ważnym wsparciem technicznym i prawem aktualizacji oprogramowania do najnowszej dostępnej u producenta wersji, wykupionym na okres minimum 5 lat.

Od Wykonawcy będzie wymagane dostarczenie urządzeń wraz z odpowiednim oprogramowaniem niezbędnym okablowaniem i uruchomieniem dostarczanych urządzeń wraz z Działem Systemów Teleinformatycznych OR POLATOM we wskazanych miejscach na terenie NCBJ OR POLATOM w lokalizacji OTWOCK-Świerk. Wymagane jest, żeby dostawca zapewnił wszelkie akcesoria takie jak wkładki SFP, SFP+, kable światłowodowe, zasilające w ilości nie mniejszej niż zaplanowana przez Zamawiającego.

Zamawiający przez uruchomienie dostarczanych urządzeń rozumie zbudowanie bezpiecznego, odpornego na awarię oraz wypełni zautomatyzowanego szkieletu sieci LAN rozpiętego na trzy budynki. (opcjonalnie na cztery budynki)
Aktualnie posiadana infrastruktura jest zbudowana z dwóch przełączników rdzeniowych ARUBA 5400R umieszczonych w serwerowni głównej. Połączenia światłowodowe pomiędzy budynkami zrealizowane są w architekturze gwiazdy. Zamawiający oczekuje przekształcenia topologii gwiazdy w topologię mieszaną pierścienia i gwiazdy, a więc zaproponowane rozwiązanie musi zapewniać możliwość zbudowania sieci w dowolnej topologii połączeń (wszystkie połączenia aktywne) pomiędzy przełącznikami rdzeniowymi. Mieszana topologia gwiazdy i pierścienia zostanie zrealizowana w zależności od dostępności połączeń pomiędzy budynkami OR POLATOM. Zaproponowana technologia użyta w urządzeniach nie może mieć ograniczeń, jeśli chodzi o zastosowaną topologię połączeń pomiędzy poszczególnymi urządzeniami sieciowymi. Transmisja danych musi się odbywać najkrótszą drogą, ale jednocześnie musi zapewniać uwzględnienie przepustowości łączy (przykładowo droga przez

dwa przełączniki połączone interfejsami 100G może być „krótsza/szybsza” niż droga bezpośrednia poprzez łącze 10G). Wszystkie połączenia sieciowe pomiędzy budynkami powinny być zrealizowane w technologii 100G na światłowodach jednomodowych z wykorzystaniem złączy LC, które zamawiający posiada jako zakończenie okablowania światłowodowego w budynkach. Pojedyncze połączenie 100G nie może wykorzystywać więcej niż dwa włókna światłowodowe.
Zbudowana sieć rdzeniowa musi zapewniać szybką konfigurację usług sieciowych działających na warstwie L2, L3 oraz obsługiwać transport ruchu multicast zarówno na warstwie L2 jak i L3. Konfiguracja usług sieciowych na dostarczanych urządzeniach musi być realizowana na brzegu sieci bez konieczności konfiguracji urządzeń znajdujących się pomiędzy punktami sieci, gdzie ma być zapewniona usługa. Główny routing sieci musi odbywać się na dostarczanych przełącznikach nie obciążając aktualnie posiadanych routerów.
Architektura sieci rdzeniowej musi zapewnić możliwość konfiguracji dwóch przełączników pracujących w redundancji i zapewniających możliwość przyłączenia dowolnych innych urządzeń sieciowych obsługujących standardowy protokół agregacji łączy IEEE 802.3ad z obsługą protokołu LACP. Urządzenia rdzeniowe muszą zapewniać możliwość skonfigurowania tej samej sieci VLAN przychodzącej do przełącznika rdzeniowego na różnych portach do różnych usług L2. Warstwa kontrolna nowo budowanej sieci powinna być wbudowana w urządzenia sieciowe. Jeśli warstwa kontrolna jest realizowana za pomocą zewnętrznych kontrolerów to musi być zapewniona redundancja tych urządzeń oraz redundancja połączenia kontrolerów do poszczególnych przełączników sieciowych. (kontrolery realizujące warstwę kontrolną mogą być licencjami ograniczonymi czasowo, ale ich minimalny dostarczony okres licencjonowania nie może być krótszy niż 10 lat).

Dostarczone rozwiązanie musi zapewniać możliwość połączenia usług sieciowych (min. usług L2) wytwarzanych na przełącznikach brzegowych, które nie są częścią tego projektu (przykładowo ARUBA 2920, 2930), do przełączników szkieletowych.
Rozwiązanie ma zapewnić możliwość przeniesienia miejsca konfiguracji usług sieciowych na dostarczane przełączniki.
Jedną z bardzo istotnych usług realizowanych w sieci LAN jest konieczność zapewnienia transmisji ruchu multicast z kamer monitoringu. Coraz większa liczba kamer oraz konieczność oglądania obrazu w różnych miejscach sieci przy jednoczesnym zminimalizowaniu retransmisji tego samego strumienia wideo w sieci wymaga uruchomienia na kamerach transmisji wideo w trybie multicast. Nowo budowana sieć szkieletowa musi zapewniać prostą realizację transmisji ruchu multicast zarówno w sieci L2 jak i w sieci L3. Dodatkowym atutem całego rozwiązania będzie realizacja routingu multicast w sieci bez konieczności konfiguracji protokołów routingu multicast, który wymaga dodatkowych nakładów konfiguracyjnych oraz dodatkowych konfiguracji w celu zapewnienia redundancji.

Dostarczane urządzenia muszą być zarządzane przez oprogramowanie pozwalające na:

- Zarządzanie konfiguracją sieci przewodowej i bezprzewodowej
- Zarządzanie dostępem do sieci przewodowej i bezprzewodowej
- Monitorowanie stanu infrastruktury

Oprogramowanie nie może być wymagane do działania dostarczanych urządzeń. Wyłączenie dostarczanego oprogramowania nie może wpływać na działanie dowolnej funkcji uruchomionej na przełącznikach, a wszystkie funkcje skonfigurowane przez oprogramowanie na przełączniku można wykonać z linii komend na poszczególnych urządzeniach.

Oprogramowanie musi być dostarczone w formie wirtualnej maszyny niewymagającej dodatkowych licencji na system operacyjny na którym jest uruchomione. Wirtualna maszyna musi uruchamiać się na wirtualizacji VmWare posiadanym przez Zamawiającego.

Wirtualna maszyna, na której jest uruchomione oprogramowanie musi zapewniać możliwość skalowania liczby obsługiwanych urządzeń, punktów dostępowych oraz klientów bezprzewodowych poprzez zmianę udostępnianych zasobów w środowisku wirtualnym. Wymagane jest, aby wirtualna maszyna mogła zapewnić możliwość pracy w klastrze odpornym na awarie. W ramach postępowania należy dostarczyć niezbędną liczbę kontrolerów niezbędnych do pracy w klastrze. Należy dostarczyć instrukcję przywracania maszyny po awarii.

## 1.1. Oprogramowanie do zarządzania siecią, zarządzania dostępem, analizowania zdarzeń.

1) Oprogramowanie do zarządzania 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;
2) Oprogramowanie do zarządzania musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS;
3) Oprogramowanie do zarządzania musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli;
4) Oprogramowanie do zarządzania musi zarządzać wszystkimi oferowanymi urządzeniami oraz wszystkimi dostarczonymi punktami dostępowymi;
5) Oprogramowanie do zarządzania musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników;
6) Oprogramowanie do zarządzania musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius;
7) Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze;
8) Oprogramowanie do zarządzania musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3;
9) SNMPv3 musi wspierać szyfrowanie z wykorzystaniem DES oraz AES jak również uwierzytelnianie za pomocą MD5 oraz SHA;
10) Oprogramowanie do zarządzania 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;
11) Oprogramowanie do zarządzania musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów;
12) Oprogramowanie do zarządzania musi posiadać możliwość kompilowania SNMP MIB innych producentów;
13) Oprogramowanie do zarządzania musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II;
14) Oprogramowanie do zarządzania musi zapewniać możliwość importu dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych;
15) Oprogramowanie do zarządzania musi posiadać wbudowany Syslog serwer i pozwalać na gromadzenie logów przesyłanych przez urządzenia;

16) Oprogramowanie do zarządzania musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps;
17) Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych;
18) Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia;
19) Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
    a) Wysłanie e-mail do wskazanej grupy adresowej
    b) Wysłanie informacji SYSLOG do wskazanego serwera
    c) Wysłanie TRAP SNMP do wskazanego adresu IP
    d) Uruchomienie skryptu w systemie operacyjnym Linux
    e) Uruchomienie automatyzacji w oprogramowaniu do zarządzania
20) Oprogramowanie do zarządzania musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera;
21) Oprogramowanie do zarządzania musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji (SNMP System Location) i kontaktu do administratora (SNMP Contact);
22) Oprogramowanie do zarządzania musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach w celu przeprowadzania konfiguracji grup urządzeń lub portów;
23) Oprogramowanie do zarządzania musi zapewniać możliwość wizualizacji sieci przedstawiającej urządzenia i uwzględniającej:
    a) połączenia pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu
    b) konfigurację sieci VLAN
24) Oprogramowanie do zarządzania musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh (z wykorzystaniem consoli Web) oraz http/https;
25) Oprogramowanie do zarządzania musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
    a) adres IP urządzenia
    b) adres MAC urządzenia
    c) nazwę urządzenia
    d) wersję oprogramowania
    e) wersję bootrom
    f) lokalizację urządzenia
    g) dane kontaktowe administratora
    h) numer seryjny
    i) numer inwentaryzacyjny – możliwość wprowadzenia własnej numeracji urządzeń w ramach inwentaryzacji sprzętu
26) Oprogramowanie do zarządzania musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:

a) możliwość automatycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie;
b) możliwość realizacji backup'u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych;
c) możliwość odtworzenia wskazanej konfiguracji urządzenia na nowo podpięte;
d) możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami;
e) możliwość obsługi backup'u urządzeń sieciowych różnych producentów;
f) możliwość generowania alarmu w przypadku zmiany konfiguracji;

27) Oprogramowanie do zarządzania musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie;
28) Oprogramowanie do zarządzania musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych;
29) Oprogramowanie do zarządzania musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Produkcja, Pomiarowa, CCTV, Access Point, Drukarka, Telefon VoIP itp.;
30) Oprogramowanie do zarządzania musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:
    a) przyłączenia do sieci VLAN
    b) przyłączenia do serwisu w ramach utworzonej topologii sieci
    c) konfiguracji Quality of Service
    d) konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
    e) 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.
31) Oprogramowanie do zarządzania musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
    a) 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. Oprogramowanie Zarządzające po zlokalizowaniu użytkownika musi wskazać, gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
    b) 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).
    c) wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.;
    d) generowanie raportów;
32) Oprogramowanie do zarządzania musi zapewniać zarządzenia siecią bezprzewodową;
    Minimalne funkcje realizowane:
    a) Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa);

b) 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
c) Musi być zapewniona widzialność parametrów wszystkich kontrolerów; bezprzewodowych zawierających między innymi adres IP kontrolera, liczba obsługiwanych klientów, szczytowe wartości zajmowanego pasma, wersja oprogramowania;
d) Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających między innymi 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;
e) Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających minimum 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;
f) Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Na mapie musi być uwidoczniony obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości, zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem, lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych;

## 1.2.Oprogramowanie do zarządzania dostępem (NAC).

1) System zarządzania tożsamością musi zapewniać bieżącą widzialność wszystkich uwierzytelnionych urządzeń i umożliwiać podgląd adresu MAC, adresu IP, nazwa hosta, typ klienta oraz systemu operacyjnego, nazwa urządzenia, do którego podłączony jest klient (nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika), identyfikacje portu, do którego dołączony jest klient, typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, nazwa przydzielonej polityki bezpieczeństwa.
2) 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.
3) System musi zapewniać możliwość konfiguracji okresu za jaki będą zbierane informacje historyczne
4) 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 musi zapewniać możliwość konfiguracji mechanizmu CoA np. SNMP, RADIUS CoA (RFC5176), zmianę statusu portu UP/Down, formatu MAC adresu wysyłanego w ramach żądania.
5) System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:

a) 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.;
b) Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP, Grupy przekazanej w ramach atrybutu RADIUS lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika;
c) Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC, lub sprawdzenia wskazanego atrybutu w ramach LDAP dla danej stacji końcowej;
d) 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;
e) Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia;

6) System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do użytkowników (MAC adres urządzenia, z którego korzysta użytkownik). 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, grupa punktów dostępowych, grupa kamer itp.;
7) 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;
8) System do zarządzania tożsamością musi zapewniać możliwość przydzielenia urządzenia do systemu ze wskazaniem wielu obsługiwanych serwerów RADIUS, włączenie obsługi RADIUS Accounting oraz wskazanie atrybutów RADIUS wysyłanych do urządzenia wraz z mapowaniem ich do zmiennych przechowywanych w systemie - chodzi np. o możliwość definiowania wysyłanych atrybutów RADIUS rozumianych przez dane urządzenie – przykładowo przydział VLAN dla danego urządzenia może odbywać się przez RFC 3580, a dla innego urządzenia może być to przykładowo RFC 4675;
9) System do 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;
10) System do zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS;
11) System do zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. id pracownika, adres email, numer telefonu, adres email osoby zapraszającej;
12) System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy;
13) System do zarządzania musi posiadać portal 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;
14) System do zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:

a) liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.;
b) liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.;
c) liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android;
d) liczbę urządzeń z przydziałem profilu np. Urządzenie MFP, Drukarka Zebra, Drukarka Canon;
e) liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa;
f) liczbę urządzeń z podziałem na obszary np. budynek A, budynek B;

15) System do zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów – przykładowo musi zapewniać możliwość uruchomienia skryptu po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication;
16) System do zarządzania tożsamością musi realizować funkcje uwierzytelniania za pomocą dedykowanych maszyn wirtualnych lub osobnego systemu Linux dla zapewnienia odpowiedniej skalowalności Oprogramowania Zarządzającego i Systemu Zarządzania Tożsamością;
17) Konieczne jest zapewnienie min. 2 maszyn uwierzytelniających dla zapewnienia odporności na awarię, a system musi zapewniać możliwość rozbudowy o kolejne maszyny, które np. będą zlokalizowane w oddziale dla zapewnienia lokalnego uwierzytelniania użytkowników w przypadku awarii łącza do centralnych maszyn uwierzytelniających;
18) System do zarządzania tożsamością musi zapewniać realizację odporności na awarie oraz skalowalność poprzez uruchamianie dodatkowych jednostek zarządzanych z Oprogramowania Zarządzającego;
19) tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 1000 urządzeń klienckich (adresów MAC) z możliwością rozbudowy do minimum 3000;
20) System do zarządzania musi współpracować z dostarczonymi urządzeniami pozwalając na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej;
21) 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 informacje ilościowe ruchu poszczególnych aplikacji;
22) 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;
23) System analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS;
24) System analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji;
25) Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji
26) 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;

27) System analityki musi zapewniać możliwość tworzenia raportów;
28) System analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail;
29) 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 do zarządzania, systemie analityki, systemie zarządzania tożsamością;
30) System do zarządzania musi posiadać możliwość uruchomienie skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora);
31) 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;
32) System do zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu;
33) System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki;
34) System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów (należy dostarczyć wraz z dostawą rozwiązania pełną dokumentację i prawo do korzystania z API):
    a) Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall takimi jak: Palo Alto, Fortinet, Sonicwall, Checkpoint;
    b) 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;
    c) Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune;

## 1.3. Kontroler do zarządzania sieci bezprzewodowej

1) Kontroler musi pochodzić od producenta oferowanych punktów dostępowych.
2) Kontroler musi być dostarczony formie klastra wysokiej dostępności i zapewniać skalowalność do min. 100 punktów dostępowych i 1 tys. klientów bezprzewodowych.
3) Kontroler musi zostać dostarczony wraz z licencjami pozwalającymi na zarządzanie 32 punktami dostępowymi.
4) Kontroler musi zapewniać obsługę sieci VLAN zgodnych z IEEE 802.1Q.
5) Kontroler musi być zarządzany przez przeglądarkę www bez konieczności instalacji dedykowanej aplikacji na stacji zarządzającej jak np. Java.
6) Kontroler musi zapewniać obsługę wielu Lokalizacji z wizualizacją ich stanu, liczby sieci bezprzewodowych (SSID) oraz liczby obsługiwanych punktów dostępowych w każdej lokalizacji.
7) Kontroler musi zapewniać możliwość konfiguracji planów poszczególnych pięter budynków oraz umieszczenie punktów dostępowych na planie.
8) Kontroler musi zapewniać możliwość nanoszenia na plany budynków ścian i pozwalać na wizualizację zasięgu poszczególnych punktów dostępowych umieszczonych na planie.
9) Kontroler musi zapewniać możliwość importu planów jak również wczytywanie planów piętra z plików graficznych.
10) 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;
11) Kontroler musi zapewniać możliwość filtracji prezentowanych informacji o punktach dostępowych na podstawie dowolnych parametrów z uwzględnieniem warunków logicznych np. wszystkie punkty w lokalizacji Otwock pracujące na kanale 36.
12) Modyfikacja konfiguracji musi się automatycznie propagować na podłączone punkty dostępowe;
13) Obraz systemu operacyjnego musi się automatycznie propagować na wszystkie kompatybilne punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję;
14) Kontroler musi zapewniać możliwość konfiguracji sieci bezprzewodowych, ich przydziału do grup punktów dostępowych, a następnie do lokalizacji;
15) Kontroler musi zapewniać automatyczne wykrywanie i automatyczną konfigurację nowych punktów dostępowych zgodnie z zadanymi warunkami (Zero Touch);

16) Kontroler musi być zarządzany przez SNMPv1/v2/v3 oraz SSHv2;
17) Kontroler musi obsługiwać RADIUS authentication oraz RADIUS accounting;
18) Kontroler musi zapewniać obsługę: 802.11i, WPA2, TKIP oraz AES, WPA3;
19) Kontroler musi zapewniać obsługę IEEE 802.1x oraz uwierzytelnienie: EAP-TLS, EAP-SIM, EAP-TTLS, EAP-AKA, PEAP, EAP-MD5, EAP-FAST;
20) Kontroler musi zapewniać obsługę uwierzytelniania MAC authentication;
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 do tunelu VXLAN terminowanego w sieci LAN na urządzeniu wspierającym tunelowanie VXLAN – np. na przełączniku;
22) Kontroler bezprzewodowy musi zapewniać możliwość ustawiania następujących parametrów w ramach każdej sesji klienckiej:
    a) indywidualne reguły filtrowania ruchu
    b) przypisanie sieci VLAN
    c) QoS
    d) ograniczenia transmisji wejściowej i wyjściowej
    e) wyboru topologii
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 konfiguracji danych niezbędnych dla rejestracji np.: Imię, Nazwisko, email, numer telefonu, id pracownika, itp.
26) Portal rejestracji gości musi zapewniać możliwość stworzenia i akceptacji regulaminu przez rejestrujących się gości;
27) Kontroler musi zapewniać przynajmniej podstawową konfigurację wyglądu Captive Portal – zmiana kolorów, zmiana stylów CSS, dodanie loga firmy;
28) 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;
29) Captive Portal musi zapewniać wsparcie min. języka polskiego, angielskiego i niemieckiego;
30) Captive Portal musi zapewniać obsługę urządzeń mobilnych;
31) Kontroler musi zapewniać rejestrację gości z wykorzystaniem portali społecznościowych;
32) Kontroler musi zapewniać możliwość automatycznej, centralnej aktualizacji oprogramowania punktów dostępowych zaadoptowanych do kontrolera;
33) Kontroler musi zapewniać możliwość konfiguracji blokowania ruchu pomiędzy klientami sieci bezprzewodowej;

34) Kontroler musi zapewniać autoryzację użytkowników IEEE 802.1x w oparciu o zewnętrzny serwer RADIUS z możliwością definicji różnych serwerów RADIUS dla różnych identyfikatorów SSID;
35) Kontroler musi zapewniać przydzielanie klientów do wskazanych sieci wirtualnych na podstawie informacji przesyłanej z serwera RADIUS zgodnie z RFC3580;
36) Kontroler musi zapewniać możliwość uwierzytelniania z wykorzystaniem Microsoft Active Directory;
37) Kontroler musi zapewniać możliwość przydzielania do sieci VLAN na podstawie przynależności klientów bezprzewodowych do grup użytkowników zdefiniowanych w LDAP;
38) 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;
39) Kontroler musi zapewniać konfigurację roamingu pomiędzy punktami dostępowymi;
40) Kontroler musi zapewniać konfigurację oszczędzania energii;
41) Kontroler musi obsługiwać QBSS (informacja o zbyt dużym obciążeniu zostanie przekazana klientowi dla obsługi inteligentnego roamingu);
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;

## 1.4. Przełączniki rdzeniowe 54 portowe – 6 sztuk:

- 6 sztuk 56 portowych przełączników chłodzonych od tyłu do przodu.
    1) Minimum 48 portów 10/25 G (SFP/SFP+/SFP28);
    2) Minimum 6 portów 40/100 G (QSFP+/QSFP28);
    3) 2 sztuki wkładek 100G umożliwiających połączenie pomiędzy budynkami;
    4) 20 sztuk wkładek 10 G umożliwiających podłączenie urządzeń w zasięgu 300 metrów na (OM3);
    5) Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów;
    6) Zainstalowane porty nie mogą utrudniać wyjęcia wkładki SFP, jeżeli wyjmowanie wkładek jest utrudnione należy dostarczyć narzędzie do wysuwania wkładek;
    7) Wbudowana diagnostyka wkładek SFPxx;
    8) Wszystkie porty muszą być od siebie niezależne, nie dopuszcza się portów typu Combo
    9) Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem – ang. „out of band management”;
    10) Dwa redundantne zasilacze AC, posiadające możliwość wymiany bez wyłączania urządzenia (ang. hot swap). (Zainstalowane dwa zasilacze w każdej ze sztuk);
    11) Redundantne wentylatory (wymienne typu hot-swap);
    12) Przepływ powietrza w kierunku do tyłu od przodu przełącznika. Zamawiający nie dopuszcza przełącznika z mieszanym przepływem powietrza;
    13) Wysokość w szafie 19” – 1U o głębokości maksymalnie 60cm;
    14) Port konsoli RJ45 lub USB;
    15) Przepustowość minimum 952 Mpps dla pakietów 64 bajtowych;
    16) Wydajność nie mniejszą niż 4 Tbps;
    17) Przełączanie w warstwie 3 modelu OSI;

18) Nie mniej niż 16GB RAM pamięci operacyjnej;
19) Nie mniej niż 64GB SSD na wewnętrzny system operacyjny;
20) Możliwość przechowywania w pamięci przełącznika kilku wersji konfiguracji;
21) Przełącznik musi pozwalać na połączenie przełączników tworząc logicznie jedno urządzenie. Musi istnieć możliwość połączenia minimum 2 urządzeń w jeden klaster; Klaster powinien zostać utworzony tak aby zapewniać redundancję logiczną i możliwość połączenia z nimi urządzeń w trybie LACP;
22) Obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB;
23) Obsługa LLDP Media Endpoint Discovery (LLDP-MED);
24) Statyczne przyłączania portu do grupy multicast;
25) Filtrowanie IGMP;
26) Obsługa RIP;
27) Obsługa VRRP IPv4 oraz IPv6;
28) Obsługa OSPFv3;
29) Obsługa ISIS;
30) Obsługa opcji 82 dla DHCP Relay IPv6;
31) Obsługa IGMP v3 - RFC 3376;
32) Obsługa IGMP v3 snooping;
33) Obsługa MLDv2 snooping;
34) Obsługa logowania do sieci Network Login;
    a) IEEE 802.1x based Network Login;
    b) MAC address-based Network Login;
35) Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants);
36) Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x;
37) Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication;
38) Automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA;
39) Automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA;
40) Przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA, np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który "przejmie" rolę uwierzytelniania klientów;
41) Obsługa Guest VLAN dla IEEE 802.1x;
42) Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu - CoA RFC 5176;
43) Obsługa wymuszania ponownego periodycznego uwierzytelnienie (Reauthentication);
44) Obsługa RADIUS Authentication over TLS (RadSec);
45) Obsługa RADIUS Accounting over TLS (RadSec);
46) Dwukierunkowe listy kontroli dostępu ACL realizowane bez zmniejszenia wydajności przełącznika;
47) Możliwość mirrorowania portu;
48) Obsługa sieci wirtualnych IEEE 802.1Q;
49) Obsługa wykrywania periodycznego zaniku linku (Port-Flap):
    a) możliwość zdefniowania liczby zaniku linku w czasie określonego czasu;
    b) możliwość automatycznej reakcji polegającej na wyłączeniu portu;
    c) możliwość raportowania zdarzenia poprzez SNMP;
50) Obsługa Trused DHCP Server;
51) Obsługa DHCP Snooping and Guard;
52) Obsługa Gratuitous ARP Protection;
53) Obsługa DHCP Secured ARP/ARP Validation;

54) Obsługa IP Source Guard;
55) Obsługa SSH;
56) Obsługę ramek Jumbo;
57) Obsługę Quality of Service;
58) Obsługa ograniczenia przepustowości na portach wyjściowych;
59) Obsługa STP (Spanning Tree Protocol) IEEE 802.1D;
60) Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w;
61) Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s;
62) Obsługa min. 12 instancji MSTP;
63) Obsługa Link Aggregation IEEE 802.3ad wraz z LACP;
    a) obsługa min. 52 grup łączy typu Link Aggregation;
    b) obsługa umożliwiająca zgrupowanie min. 8 portów;
64) Obsługę protokołu sFlow;
65) Obsługę Network Time Protocol (NTP) lub Simple Network Time Protocol (SNTP);
66) Obsługę Syslog (TLS);
67) Obsługa komendy PING dla IPv4 i IPv6;
68) Obsługa transferu plików: TFTP, SFTP, FTP, SCP;
69) Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników;
70) Wbudowany DHCP Server;
71) Wbudowany DHCP Client;
72) Wbudowany klient DNS;
73) Obsługa skryptów CLI;
74) Opcjonalnie możliwość rozbudowy o funkcjonalność uruchamiania maszyn wirtualnych na przełączniku o funkcjonalność IPSec lub maszynę z Wireshark.
75) Wsparcie VXLAN;

## 1.5. Przełączniki brzegowe 48 portowe – 14 sztuk.

- 8 sztuk 48 portowych przełączników sieci LAN z umieszczonymi z przodu obudowy portami 10/100/1000 MB i 4 portami SFP+ 1/10GBE (zainstalowane 2 wkładki 10G, 300m, (OM3);
- 6 sztuk 48 portowych przełączników sieci LAN z umieszczonymi z przodu obudowy portami 10/100/1000 MB i 4 portami SFP+ 1/10GBE z obsługą PoE+ o budżecie 350W:
    1) Wysokość urządzenia 1U - montaż w standardowej szafie 19";
    2) Głębokość urządzenia nie większa niż 35 cm wraz z połączeniami z tyłu;
    3) Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex Zakres;
    4) Wydajność przełączania sięgająca minimum 176 Gbps;
    5) Temperatura pracy przełącznika: 0 - 50 stopni C;
    6) Pamięć operacyjna: min. 1 GB pamięci DRAM;
    7) Pamięć flash: min. 1 GB pamięci Flash;
    8) Możliwość monitorowania CPU i pamięci przełącznika;
    9) Możliwość połączenia do 8 przełączników w stos za pomocą portów SFP+;
    10) Dedykowany port konsoli szeregowej RS-232 (RJ45);
    11) Możliwość budowy stosu za pomocą portów 10G SFP+;
    12) Możliwość włączenia minimum 2 zagregowanych linków LACP zawierających po dwa porty;
    13) Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów;
    14) Obsługa STP (Spanning Tree Protocol) IEEE 802.1D;
    15) Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w;
    16) Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s;
    17) Obsługa min. 64 instancji MSTP;

18) Obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB;
19) Obsługa LLDP Media Endpoint Discovery (LLDP-MED);
20) Obsługa CDPv1 oraz CDPv2;
21) Możliwość ograniczenia liczby pakietów Multicast na porcie;
22) Możliwość ograniczenia liczby pakietów Broadcast na porcie;
23) Możliwość ograniczenia liczby pakietów Unknown Unicast na porcie;
24) Przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP;
25) Obsługa routingu statycznego IPv4;
26) Obsługa routingu dynamicznego IPv4 - RIP v1/v2, OSPFv2;
27) Obsługa redundancji routingu VRRP dla IPv4 i IPv6;
28) Policy Based Routing dla IPv4 I IPv6;
29) Obsługa DHCP Relay;
30) Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów;
31) Obsługa Opcji 82 dla DHCP;
32) Statyczne przyłączania portu do grupy multicast;
33) Filtrowanie IGMP;
34) Obsługa IGMP v3 - RFC 3376;
35) Obsługa IGMP v3 snooping;
36) Obsługa MLDv2 snooping;
37) Obsługa MVR (Multicast VLAN Registration);
38) Obsługa logowania do sieci Network Login;
    a) IEEE 802.1x based Network Login;
    b) MAC address based Network Login;
    c) Web based Network Login;
39) Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants);
40) Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation;
41) Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x;
42) Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication;
43) Obsługa Guest VLAN dla IEEE 802.1x;
44) Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci;
45) Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu - CoA RFC 5176;
46) Obsługa wymuszania ponownego periodycznego uwierzytelnienie (Reauthentication)
47) Obsługa RADIUS Authentication (RFC 2865);
48) Obsługa RADIUS Accounting (RFC 2866);
49) Obsługa RADIUS Per-Command Authentication - uwierzytelnianie każdej komendy wydawanej przez administratora w serwerze RADIUS;
50) Obsługa RADIUS Authentication over TLS (RadSec);
51) Obsługa RADIUS Accounting over TLS (RadSec);
52) Bezpieczeństwo MAC adresów
    a) ograniczenie liczby MAC adresów na porcie;
    b) zatrzaśnięcie MAC adresów na porcie;
    c) możliwość wpisania statycznych MAC adresów na port/vlan;
53) Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning);
54) Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4
    a) Adres MAC źródłowy i docelowy plus maska;
    b) Adres IP źródłowy i docelowy plus maska dla IPv4;
    c) Adres IP źródłowy i docelowy plus maska dla IPv6;
    d) Protokół - np.. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.;

e) Numery portów źródłowych i docelowych TCP, UDP;
f) Zakresy portów źródłowych i docelowych TCP, UDP;
g) Identyfikator sieci VLAN - VLAN ID;
h) Quality of Service IEEE 802.1p;
i) Quality of Service DiffServ/DSCP;
j) Flagi TCP;

55) Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika;
56) Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI;
57) Wsparcie 8 tys. wpisów ACL na wejściu (Ingress);
58) Wsparcie 1 tys. wpisów ACL na wyjściu (Egress);
59) Obsługa Trused DHCP Server;
60) Obsługa DHCP Snooping and Guard;
61) Obsługa Gratuitous ARP Protection;
62) Obsługa DHCP Secured ARP/ARP Validation;
63) Obsługa IP Source Guard;
64) Ograniczenie przepustowości (rate limiting) na portach wyjściowych;
65) Ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL;
66) Obsługa SNMP;
67) Obsługa klienta NTP i SNTP;
68) Obsługa klienta DNS;
69) Obsługa klienta i serwera SSH, Telnet;
70) Obsługa transferu plików poprzez TFTP, SFTP, SCP;
71) Obsługa SYSLOG (TLS);
72) Obsługa ping i traceroute dla IPv4 i IPv6;
73) Możliwość rozbudowy przełącznika o wsparcie szyfrowania AES-256;
74) Zasilanie 230V 50/60Hz;

## 1.6. Przełączniki brzegowe 24 portowe – 8 sztuk

- 3 sztuki 24 portowych przełączników sieci LAN z umieszczonymi z przodu obudowy portami 10/100/1000 MB i 4 portami SFP+ 1/10GBE;
- 5 sztuk 24 portowych przełączników sieci LAN z umieszczonymi z przodu obudowy portami 10/100/1000 MB i 4 portami SFP+ 1/10GBE z obsługą PoE+ 350W:
    1) Wysokość urządzenia 1U - montaż w standardowej szafie 19";
    2) Głębokość urządzenia nie większa niż 35 cm;
    3) Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex Zakres ;
    4) Wydajność przełączania sięgająca minimum 128 Gbps;
    5) Temperatura pracy przełącznika: 0 - 50 stopni C
    6) Pamięć operacyjna: min. 1 GB pamięci DRAM;
    7) Pamięć flash: min. 1 GB pamięci Flash;
    8) Możliwość monitorowania CPU i pamięci przełącznika;
    9) Możliwość połączenia do 8 przełączników w stos za pomocą portów SFP+;
    10) Dedykowany port konsoli szeregowej RS-232 (RJ45);
    11) Możliwość budowy stosu za pomocą portów 10G SFP+;
    12) Możliwość włączenia minimum 2 zagregowanych linków LACP zawierających po dwa porty;
    13) Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów;

14) Obsługa STP (Spanning Tree Protocol) IEEE 802.1D;
15) Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w;
16) Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s;
17) Obsługa min. 64 instancji MSTP;
18) Obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB;
19) Obsługa LLDP Media Endpoint Discovery (LLDP-MED);
20) Obsługa CDPv1 oraz CDPv2;
21) Możliwość ograniczenia liczby pakietów Multicast na porcie;
22) Możliwość ograniczenia liczby pakietów Broadcast na porcie;
23) Możliwość ograniczenia liczby pakietów Unknown Unicast na porcie;
24) Przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP;
25) Obsługa routingu statycznego IPv4;
26) Obsługa routingu dynamicznego IPv4 - RIP v1/v2, OSPFv2;
27) Obsługa redundancji routingu VRRP dla IPv4 i IPv6;
28) Policy Based Routing dla IPv4 I IPv6;
29) Obsługa DHCP Relay;
30) Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów;
31) Obsługa Opcji 82 dla DHCP;
32) Statyczne przyłączania portu do grupy multicast;
33) Filtrowanie IGMP;
34) Obsługa IGMP v3 - RFC 3376;
35) Obsługa IGMP v3 snooping;
36) Obsługa MLDv2 snooping;
37) Obsługa MVR (Multicast VLAN Registration);
38) Obsługa logowania do sieci Network Login;
39) IEEE 802.1x based Network Login;
40) MAC address based Network Login;
41) Web based Network Login;
42) Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants);
43) Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation;
44) Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x;
45) Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication;
46) Obsługa Guest VLAN dla IEEE 802.1x;
47) Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci;
48) Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu - CoA RFC 5176;
49) Obsługa wymuszania ponownego periodycznego uwierzytelnienie (Reauthentication);
50) Obsługa RADIUS Authentication (RFC 2865);
51) Obsługa RADIUS Accounting (RFC 2866);
52) Obsługa RADIUS Per-Command Authentication - uwierzytelnianie każdej komendy wydawanej przez administratora w serwerze RADIUS;
53) Obsługa RADIUS Authentication over TLS (RadSec);
54) Obsługa RADIUS Accounting over TLS (RadSec);
55) Obsługa TACACS+ (RFC 1492);
56) Bezpieczeństwo MAC adresów;
57) ograniczenie liczby MAC adresów na porcie;
58) zatrzaśnięcie MAC adresów na porcie;
59) możliwość wpisania statycznych MAC adresów na port/vlan;
60) Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning);

61) Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4;
62) Adres MAC źródłowy i docelowy plus maska;
63) Adres IP źródłowy i docelowy plus maska dla IPv4;
64) Adres IP źródłowy i docelowy plus maska dla IPv6;
65) Protokół - np.. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.;
66) Numery portów źródłowych i docelowych TCP, UDP;
67) Zakresy portów źródłowych i docelowych TCP, UDP;
68) Identyfikator sieci VLAN - VLAN ID;
69) Quality of Service IEEE 802.1p;
70) Quality of Service DiffServ/DSCP;
71) Flagi TCP;
72) Obsługa Jumbo pakietów;
73) Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika;
74) Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI;
75) Wsparcie 8 tys. wpisów ACL na wejściu (Ingress);
76) Wsparcie 1 tys. wpisów ACL na wyjściu (Egress);
77) Obsługa Trused DHCP Server;
78) Obsługa DHCP Snooping and Guard;
79) Obsługa Gratuitous ARP Protection;
80) Obsługa DHCP Secured ARP/ARP Validation;
81) Obsługa IP Source Guard;
82) Ograniczenie przepustowości (rate limiting) na portach wyjściowych;
83) Ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL;
84) Obsługa SNMP;
85) Obsługa klienta NTP i SNTP;
86) Obsługa klienta DNS;
87) Obsługa klienta i serwera SSH, Telnet;
88) Obsługa transferu plików poprzez TFTP, SFTP, SCP;
89) Obsługa SYSLOG (TLS);
90) Obsługa ping i traceroute dla IPv4 i IPv6;
91) Możliwość rozbudowy przełącznika o wsparcie szyfrowania AES-256;
92) Zasilanie 230V 50/60Hz;

## 1.7.Przełączniki brzegowe 12 portowe – 8 sztuk

- 4 sztuki 12 portowych przełączników sieci LAN 10/1000/1000 MB z 2 portami mini-GBIC;
- 4 sztuki 12 portowych przełączników sieci LAN o tych samych parametrach z obsługą PoE+:
    1) Wysokość urządzenia 1U - montaż w standardowej szafie 19";
    2) Głębokość urządzenia nie większa niż 30 cm;;
    3) Przełącznik musi posiadać wbudowany zasilacz AC 230V
    4) Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex Zakres;
    5) Wydajność przełączania sięgająca minimum 104 Gbps;
    6) Temperatura pracy przełącznika: 0 - 50 stopni C;
    7) Pamięć operacyjna: min. 1 GB pamięci DRAM;
    8) Pamięć flash: min. 1 GB pamięci Flash;
    9) Możliwość monitorowania CPU i pamięci przełącznika;
    10) Możliwość połączenia do 8 przełączników w stos za pomocą portów SFP+;
    11) Dedykowany port konsoli szeregowej RS-232 (RJ45);
    12) Możliwość budowy stosu za pomocą portów 10G SFP+ ;

13) Możliwość włączenia minimum 2 zagregowanych linków LACP zawierających po dwa porty;
14) Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów;
15) Obsługa STP (Spanning Tree Protocol) IEEE 802.1D;
16) Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w;
17) Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s;
18) Obsługa min. 64 instancji MSTP;
19) Obsługa Link Aggregation Discovery Protocol LLDP IEEE 802.1AB;
20) Obsługa LLDP Media Endpoint Discovery (LLDP-MED);
21) Obsługa CDPv1 oraz CDPv2 ;
22) Możliwość ograniczenia liczby pakietów Multicast na porcie;
23) Możliwość ograniczenia liczby pakietów Broadcast na porcie;
24) Możliwość ograniczenia liczby pakietów Unknown Unicast na porcie;
25) Przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP;
26) Obsługa routingu statycznego IPv4;
27) Obsługa routingu dynamicznego IPv4 - RIP v1/v2, OSPFv2;
28) Obsługa redundancji routingu VRRP dla IPv4 i IPv6;
29) Policy Based Routing dla IPv4 I IPv6;
30) Obsługa DHCP Relay;
31) Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów
32) Obsługa Opcji 82 dla DHCP;
33) Statyczne przyłączania portu do grupy multicast;
34) Filtrowanie IGMP;
35) Obsługa IGMP v3 - RFC 3376;
36) Obsługa IGMP v3 snooping;
37) Obsługa MLDv2 snooping;
38) Obsługa MVR (Multicast VLAN Registration);
39) Obsługa logowania do sieci Network Login;
40) IEEE 802.1x based Network Login;
41) MAC address based Network Login;
42) Web based Network Login;
43) Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants);
44) Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation;
45) Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x;
46) Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication;
47) Obsługa Guest VLAN dla IEEE 802.1x;
48) Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci;
49) Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu - CoA RFC 5176;
50) Obsługa wymuszania ponownego periodycznego uwierzytelnienie (Reauthentication)
51) Obsługa RADIUS Authentication (RFC 2865);
52) Obsługa RADIUS Accounting (RFC 2866);
53) Obsługa RADIUS Per-Command Authentication - uwierzytelnianie każdej komendy wydawanej przez administratora w serwerze RADIUS;
54) Obsługa RADIUS Authentication over TLS (RadSec);
55) Obsługa RADIUS Accounting over TLS (RadSec);
56) Obsługa TACACS+ (RFC 1492);
57) Bezpieczeństwo MAC adresów;

58) ograniczenie liczby MAC adresów na porcie;
59) zatrzaśnięcie MAC adresów na porcie;
60) możliwość wpisania statycznych MAC adresów na port/vlan;
61) Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning);
62) Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4
    - Adres MAC źródłowy i docelowy plus maska;
    - Adres IP źródłowy i docelowy plus maska dla IPv4;
    - Adres IP źródłowy i docelowy plus maska dla IPv6;
    - Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.;
    - Numery portów źródłowych i docelowych TCP, UDP;
    - Zakresy portów źródłowych i docelowych TCP, UDP;
    - Identyfikator sieci VLAN - VLAN ID;
    - Quality of Service IEEE 802.1p;
    - Quality of Service DiffServ/DSCP;
    - Flagi TCP;
63) Obsługa Jumbo pakietów;
64) Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika;
65) Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI;
66) Wsparcie 8 tys. wpisów ACL na wejściu (Ingress);
67) Wsparcie 1 tys. wpisów ACL na wyjściu (Egress);
68) Obsługa Trused DHCP Server;
69) Obsługa DHCP Snooping and Guard;
70) Obsługa Gratuitous ARP Protection;
71) Obsługa DHCP Secured ARP/ARP Validation;
72) Obsługa IP Source Guard;
73) Ograniczenie przepustowości (rate limiting) na portach wyjściowych;
74) Ograniczenie przepustowości (rate limiting) ruchu wybranego przez ACL;
75) Obsługa SNMP;
76) Obsługa klienta NTP i SNTP;
77) Obsługa klienta DNS;
78) Obsługa klienta i serwera SSH, Telnet;
79) Obsługa transferu plików poprzez TFTP, SFTP, SCP;
80) Obsługa SYSLOG (TLS);
81) Obsługa ping i traceroute dla IPv4 i IPv6;
82) Opcjonalnie możliwość rozbudowy przełącznika o wsparcie szyfrowania AES-256;
83) Bez wentylatorowy;
84) Wbudowany zasilacz 230V 50/60Hz. Nie dopuszcza się zasilacza zewnętrznego.

## 1.8. Punkty dostępowe sieci bezprzewodowej - 32 sztuki wraz z centralnym kontrolerem sieci bezprzewodowej

1) Licencje umożliwiające na wpięcie do oprogramowania do zarzadzania (kontrolera)
2) Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków.
3) Punkt dostępowy musi być wyposażony w dwie wersje oprogramowania firmware. W sytuacji, kiedy aktualizacja do nowszej wersji się nie powiedzie to punkt dostępowy uruchomi się z ostatnim dobrym oprogramowaniem firmware.
4) Punkt dostępowy musi posiadać trzy interfejsy radiowe pozwalające na obsługę:
   a) pasma 2.4 GHz min. 2x2:2 MIMO
   b) pasma 5 GHz min. 2x2:2 MIMO

c) pasma 6GHz min . 2x2:2 MIMO

5) Punkt dostępowy musi posiadać port usb lub rs232 do zarządzania bezpośredniego
6) Punkt dostępowy musi być wyposażony w 2 interfejsy Ethernet z czego jeden musi zapewniać minimalnie tryby pracy 1G/2.5G Base-T, a drugi minimalnie 100M/1G Base-T.
7) Punkt dostępowy musi umożliwiać pracę na wszystkich radiach WiFi w trybie 2x2:2 MIMO przy jednoczesnym zasileniu go przez standardowe PoE (IEEE 802.3af – max. 15.4W).
8) Punkt dostępowy musi być zgodny ze standardem WiFi6E.
9) Punkt dostępowy musi zapewniać możliwość użycia go jako klienta sieci WiFi lub trybie Mesh.
10) Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:
11) Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP.
12) Punkt dostępowy musi obsługiwać nie mniej niż 6 niezależnych SSID.
13) Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.
14) Możliwość podłączenia się pod zewnętrzny portal uwierzytelniający.
15) Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
    a) Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe.
    b) Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu.
    c) Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma.
    d) Wykrywanie interferencji oraz miejsc bez pokrycia sygnału.
    e) Automatyczne przekierowywanie/przełączanie klientów, którzy mogą pracować w pasmie 5GHz.
    f) Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac/ax oraz starszych (802.11b/g).
    g) Wsparcie dla 802.11d oraz 802.11h.
    h) Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane.
16) Minimalizacja interferencji związanych z sieciami 3G/4G LTE.
17) Obsługa roamingu 802.11r, 802.11v, 802.11k dla klientów w warstwie 2.
18) Obsługa monitoringu przez SNMP.
19) Obsługa logowania na kontroler lokalny.
20) W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
21) W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
22) Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax.
23) Możliwość ustawienia VHT – kanały 20/40/80/160MHz dla 802.11ac.
24) Możliwość ustawienia HE – kanały 20/40/80/160MHz dla 802.11ax.
25) Wsparcie dla technologii DFS (Dynamic Frequency Selection).
26) Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac.
27) Moc transmisji konfigurowalna przez administratora.
28) Punkt dostępowy musi posiadać co najmniej:

a) 1 interfejs 1G z funkcją auto-sensing link oraz MDI/MDX i obsługą PoE/PoE+ dla standardu 802.3az Energy Efficient Ethernet (EEE).
b) 1 interfejs konsoli RS-232 (RJ-45) lub USB.
c) ukryty przycisk przywracający konfigurację fabryczną.
d) slot zabezpieczający przed kradzieżą Keningston.

29) Parametry pracy urządzenia:
a) Temperatura otoczenia (zakres minimalny): 0-50 º C.
b) Wilgotność (zakres minimalny): 5% - 92%.

30) Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni.

## 1.9. Akcesoria

- 12 sztuk kabli DAC 10G o długości 1m z przeznaczeniem na stworzenie stosu przełączników.
- 8 sztuk kabli DAC 10G o długości 3m z przeznaczeniem na stworzenie stosu przełączników.
- 20 sztuk wkładek SFP 10G /LC z zasięgiem minimum 300 metrów na kabel wielomodowy (OM3)
- 8 sztuk wkładek SFP 100G /LC z zasięgiem minimum 700 metrów na kabel jednodomowy
- 30 sztuk kable połączeniowe światłowodowe pomiędzy panelem krosowym (złącze LC duplex) a dostarczanymi modułami.
- 15 sztuk zasilaczy PoE do dostarczanych punktów dostępowych zasilacze będą instalowane przy przełącznikach sieciowych nie posiadających PoE.

  Wymagane jest, aby moduły po zainstalowaniu go w przełączniku sieciowym poprawnie pracowały a błędy powstałe podczas jego pracy były wspierane przez serwis producenta.

  Moduły sieciowe SFP+ muszą być wyposażone w złącze LC.

## 1.10. Zamówienie opcjonalne dla części 1

Zamawiający zastrzega sobie prawo do skorzystania z prawa opcji. Zamawiający uzależnia skorzystanie z prawa opcji od własnych potrzeb w zakresie wskazanym w Specyfikacji technicznej, stanowiącej załącznik A do SWZ w okresie **do 12 miesięcy** od daty złożenia zamówienia w okresie do 12 miesięcy od daty podpisania protokołu odbioru bez uwag zamówienia podstawowego.

Zamówienie opcjonalne obejmuje dodatkowe urządzenia i rozwiązania, które w części znajdą się w czwartym budynku Zamawiającego Sprzęt jest tego samego typu co dostarczany w części 1.

Specyfikacja wymienionych poniżej urządzeń znajduje się w punktach ujętych w nawiasie.

Należy dodać wymagane licencje na zaproponowane oprogramowanie.

- 56 portowy przełącznik rdzeniowy 2 sztuki (Specyfikacja jak punkt 1.4.)
- 48 portowe przełączniki brzegowe 10 sztuk bez PoE (Specyfikacja jak punkt 1.5.)
- 24 portowe przełączniki brzegowe 2 sztuki z PoE (Specyfikacja jak punkt 1.6.)
- 24 portowe przełączniki brzegowe 3 sztuki bez PoE (Specyfikacja jak punkt 1.6.)
- punkty dostępowe WiFi 8 sztuk (Specyfikacja jak punkt 1.7.)

Wszystkie urządzenia w ramach zamówienia opcjonalnego muszą zostać dostarczone wraz z akcesoriami umożliwiającymi montaż oraz uruchomienie urządzeń w pełnej funkcjonalności.

### 1.11. Akcesoria dostarczane w ramach zamówienia opcjonalnego

- 15 sztuk kabli DAC 10GBE o długości 1m z przeznaczeniem na stworzenie stosu przełączników.
- 8 sztuk kabli DAC 10GBE o długości 5m z przeznaczeniem na stworzenie stosu przełączników.
- 30 sztuk wkładek SFP 10GBE z zasięgiem minimum 300 metrów na kabel wielomodowy.
- 8 sztuk wkładek SFP 100GBE z zasięgiem minimum 700 metrów na kabel jednomodowy.
- 30 sztuk kable połączeniowe światłowodowe pomiędzy panelem krosowym (złącze LC duplex) a dostarczanymi modułami.

Wymagane jest, aby moduł poprawnie pracował po zainstalowaniu go w przełączniku sieciowym i błędy powstałe podczas jego pracy były wspierane w rozwiązywaniu problemów / usuwaniu usterek / naprawiane przez serwis producenta.

Moduły sieciowe SFP+ muszą być wyposażone w złącze LC.

## 2. Urządzenia serwerowe (Część 2)

Każdy serwer kasetowy musi być wyposażony w rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną do zdalnego zarządzania (konsoli) pozwalającej na:

a. włączenie, wyłączenie i restart serwera;
b. podgląd logów sprzętowych serwera i karty;
c. przejęcie zdalnej pełnej konsoli graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS);
d. zdalne podłączenie wirtualnych napędów CD/DVD/ISO;
e. integrację z Active Directory;
f. powiadamianie o zdarzeniach za pomocą poczty email;
g. współdzielenie jednej zdalnej konsoli graficznej przez 2 użytkowników;
h. szyfrowanie połączeń za pomocą protokołu TLS do karty zdalnego zarządzania.
i. aktualizacje oprogramowania układowego;

Do oferty należy dodać licencje na oprogramowanie do zarządzania serwerami. Zamawiający dopuszcza dostarczenie oprogramowania w postaci maszyny wirtualnej przygotowanej przez producenta serwerów. Oprogramowanie ma integrować dostarczane serwery:

- monitorowanie ich stanu dysków, kontrolerów, zasilaczy, uplinków, wentylatorów, procesorów, Pamięci RAM
- bezpośrednie zalogowanie się z oprogramowania do zdalnego zarządzania w celu wykonania operacji administracyjnych.

### 2.1. Obudowa serwerów kasetowych

W związku z rozbudową istniejącej infrastruktury, Zamawiający wymaga, aby produkt był fabrycznie nowy, nie przeznaczony dla innych klientów w celu zachowania prawa do gwarancji producenta objętej dedykowanym kontraktem. Do serwerów należy dostarczyć najnowszej generacji kompatybilną obudowę mieszczącą minimum wymaganą ilość serwerów, instalowaną w szafie RACK. Głębokość obudowy nie może przekraczać 1000mm i mieścić się w szafie o głębokości 1200mm wraz z wymaganymi połączeniami z tyłu. Obudowa będzie podłączona do infrastruktury sieci LAN czteroma przewodami o prędkości 100G po dwa od każdego przełącznika, do dwóch przełączników rdzeniowych poprzez agregację łączy LACP. Siec SAN będzie podłączona do szkieletu FC składającego się z dwóch niezależnych przełączników pracujących jako fabric A i fabric B za pomocą czterech przewodów o prędkości 32G każdy. Obudowa i zainstalowany w niej osprzęt nie może posiadać ograniczeń licencyjnych na aktywne porty ich rodzaje i limity prędkości.

Obudowa musi posiadać minimum 8 miejsc na serwery i być wyposażona minimum w:

- 2 sztuki przełączników 100G sieci LAN obsługujące wszystkie wnęki serwerów z prędkością co najmniej 25G i porty wychodzące na zewnątrz z prędkością 100G znajdujące się w przełączniku. Przełączniki muszą umożliwiać przydzielanie adresów MAC serwerom zainstalowanym w obudowie. Możliwość tworzenia niezależnych VLAN tak aby między wydzielonymi sieciami nie było komunikacji.
- 2 sztuki przełączników 32G sieci FC - SAN działające z przełącznikami firmy BROCADE obsługujące wszystkie wnęki serwerów i porty wychodzące znajdujące się w przełączniku.

- 2 sztuki modułów zarządzających wyposażonych w dedykowany port Ethernet pracujących nadmiarowo umożliwiających dostęp do zarządzania i monitorowania każdego obszaru obudowy z jednego miejsca. Z modułu zarządzania musi być możliwość monitorowania stanu przełączników zainstalowanych w obudowie.
- Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów
- Pełny komplet zasilaczy Hot Plug w konfiguracji nadmiarowej obsługujących wszystkie wnęki serwerów i elementy zainstalowane w obudowie (nie dopuszcza się pozostawienie pustych wnęk na zasilacze).
- Pełny komplet wentylatorów obsługujących wszystkie wnęki serwerów i elementów wstawionych do obudowy (nie dopuszcza się pozostawienie pustych wnęk na wentylatory).
- Pola nie wykorzystane należy zaślepić dedykowanymi zaślepkami usuwanymi bez narzędziowo (jeżeli są wymagane narzędzia należy je dostarczyć w ilości 3 kompletów do każdej dostarczonej obudowy).

W obudowie musi istnieć możliwość rozbudowy poprzez dołożenie dodatkowych dwóch przełączników LAN lub SAN.

Podczas świadczenia gwarancji Zamawiający dopuszcza możliwość wysłania przez serwis części zamiennych, które zespół IT wymieni na miejscu samodzielnie nie tracąc gwarancji i skracając czas na usunięcie zgłoszonej usterki.

Licencje dostarczone w ramach części 2 przedmiotu zamówienia muszą być udzielone na czas nieokreślony i upoważniają Zamawiającego do korzystania na warunkach eksploatacji określonych przez producenta oprogramowania.

Zamawiający wymaga przeprowadzenia testów dostarczanego sprzętu, test polegać ma na:

- dwutygodniowym uruchomieniu dostarczonych serwerów i obciążeniu ich procesorów w zakresie 50-80%.
- odłączeniu zasilania częściowo, przywróceniu zasilania (weryfikacja odporności na awarię przynajmniej dwóch zasilaczy zainstalowanych w klatce)
- odłączeniu zasilania całkowicie, przywróceniu zasilania

Oczekiwanym efektem po powrocie zasilania jest automatyczne i prawidłowe uruchomienie serwerów.

a) Wykonawca dokonał instalacji dwu serwerowego klastra SQL przeprowadził testy wysokiej dostępności wraz z zespołem działu informatyki OR POLATOM oraz wykonał migrację baz danych z posiadanego serwera SQL 2012 firmy Microsoft uruchomionego w klastrze wysokiej dostępności na systemie operacyjnym wersji 2012R2. Zamawiający posiada odpowiednie licencje firmy Microsoft.
b) Wykonawca dokonał instalacji systemu operacyjnego VmWare wraz z zespołem działu informatyki OR POLATOM przeprowadził testy odporności na awarię pojedynczego serwera z systemem operacyjnym firmy VmWare. Test polegać będzie na uruchomieniu sześciu maszyn wirtualnych i weryfikacja czy po odłączeniu jednego z serwerów wirtualizujących pozostałe dwa przejmą działanie uruchomionych na wyłączanej maszynie testowych maszyn wirtualnych.

Zamawiający wymaga, aby nowo zamontowane serwery przeszły dwutygodniowe testy sprawności działania. Wymaga się, aby po zakończonym sukcesem dwutygodniowym teście Wykonawca dokonał instalacji:

a) dwu serwerowego klastra SQL. Po instalacji Wykonawca wraz z zespołem działu informatyki OR POLATOM przeprowadzi testy wysokiej dostępności oraz wykona migrację baz danych z posiadanego serwera SQL 2012 firmy Microsoft uruchomionego w klastrze wysokiej dostępności na systemie operacyjnym wersji 2012R2. Zamawiający posiada odpowiednie licencje firmy Microsoft.
b) systemu operacyjnego VmWare. Po instalacji Wykonawca wraz z zespołem działu informatyki OR POLATOM przeprowadzi testy odporności na awarię pojedynczego serwera z systemem operacyjnym firmy VmWare. Test polegać będzie na uruchomieniu sześciu maszyn wirtualnych i weryfikacji czy po odłączeniu jednego z serwerów wirtualizujących pozostałe dwa przejmą działanie uruchomionych na wyłączanej maszynie, testowych maszyn wirtualnych.

## 2.2. Serwer kasetowy na potrzeby bazy danych SQL o parametrach minimalnych:

| Ilość | 2 szt. |
|---|---|
| Obudowa | Kompatybilna z obudową typu Blade |
| Typ i liczba zainstalowanych dysków | 2x Hot Swap M.2 SSD 480GB NVMe Gen3 |
| Obsługa RAID | Obsługa RAID 0, 1 na minimum 2 dyskach |
| Karta sieciowa | 2x25/50Gb |
| Procesor | Intel Xeon-Gold 6444Y 3.6GHz 16-core 270W |
| Liczba procesorów | 1 z możliwością rozszerzenia do 2 |
| Pamięć | 128GB (4x32GB) DDR5-4800 EC8 |
| Ilość gniazd pamięci | 16 |
| Zarządzanie infrastrukturą | Z wymaganymi licencjami, zintegrowany z obudową typu BLADE system KVM wraz funkcjami zarządzania energią serwera |
| Rozszerzenia | Podwójny adapter magistrali hosta 32 Gb Fibre Channel dla serwerów typu Blade |
| Bezpieczeństwo | Moduł TPM 2.0 |
| Porty | 1x USB |
| Zarządzanie | Karta KVM |
| Zasilacz | ND |
| Wsparcie | System operacyjny Red HAT, Ubuntu, Windows 2019/2022 |
| Gwarancja | 5 lat, 24/7/4 (DMR dyski pozostają u Zamawiającego) |
| System operacyjny | brak |

## 2.3. Serwer kasetowy na potrzeby wirtualizacji o parametrach minimalnych:

| Ilość | 3 szt. |
|---|---|
| Obudowa | Kompatybilna z obudową typu Blade |
| Typ i liczba zainstalowanych dysków | 2x Hot Swap M.2 SSD 480GB NVMe Gen3 |
| Obsługa RAID | Obsługa RAID 0, 1 na minimum 2 dyskach |
| Karta sieciowa | 2x 25/50Gb |
| Procesor | 2x Intel Xeon-Gold 6444Y 3.6GHz 16-core 270W |
| Liczba procesorów | 2 |
| Pamięć | 512GB DDR5-4800 EC8 |
| Ilość gniazd pamięci | 16 |
| Zarządzanie infrastrukturą | Z wymaganymi licencjami, zintegrowany z obudową typu BLADE system KVM wraz funkcjami zarządzania energią serwera |
| Rozszerzenia | Podwójny adapter magistrali hosta 32 Gb Fibre Channel dla serwerów typu Blade |
| Wsparcie | System operacyjny VmWare 7 U3, do najnowszej aktualne dostępnej |
| Zasilacz | ND |
| Gwarancja | 5 lat, 24/7/4 (DMR dyski pozostają u Zamawiającego) |
| System operacyjny | VmWare vSphere Standard 8 - 32 rdzenie z 3 letnim wsparciem licencja rejestrowana w portalu producenta systemu operacyjnego |

## 2.4. Serwer kasetowy na potrzeby systemów operacyjnych Windows o parametrach minimalnych:

| | |
|---|---|
| **Ilość** | **4 szt.** |
| **Obudowa** | Kompatybilna z obudową typu Blade |
| **Typ i liczba zainstalowanych dysków** | 2x Hot Swap M.2 SSD 480GB NVMe Gen3 |
| **Obsługa RAID** | Obsługa RAID 0, 1 na minimum 2 dyskach |
| **Karta sieciowa** | 2x10/25Gb |
| **Procesor** | Intel Xeon-Gold 5415+ 2.9GHz 8-core 150W |
| **Liczba procesorów** | 1 z możliwością rozszerzenia do 2 |
| **Pamięć** | 16GB DDR5-4800 EC8 (2 serwery z Pamięcią 32GB DDR5-4800 EC8) |
| **Ilość gniazd pamięci** | 16 |
| **Zarządzanie infrastrukturą** | Z wymaganymi licencjami, zintegrowany z obudową typu BLADE system KVM wraz funkcjami zarządzania energią serwera |
| **Rozszerzenia** | Podwójny adapter magistrali hosta 32 Gb Fibre Channel dla serwerów typu Blade |
| **Rozszerzenia** | Adapter magistrali hosta 32 Gb Fibre Channel dla serwerów typu Blade |
| **Wsparcie** | System operacyjny Red HAT, Ubuntu, Windows 2019/2022 |
| **Zasilacz** | ND |
| **Gwarancja** | 5 lat, 24/7/4 (DMR dyski pozostają u Zamawiającego) |
| **System operacyjny** | brak |

## 2.5.Zamówienie opcjonalne dla części 2

Zamawiający zastrzega sobie prawo do skorzystania z prawa opcji. Zamawiający uzależnia skorzystanie z prawa opcji od własnych potrzeb w zakresie wskazanym w Specyfikacji technicznej, stanowiącej załącznik A do SWZ w okresie **do 12 miesięcy** od daty złożenia zamówienia w okresie do 12 miesięcy od daty podpisania protokołu odbioru bez uwag zamówienia podstawowego.

Zamawiający wymaga w zamówieniu opcjonalnym polegającym na dostawie serwerów przeprowadzenia dwutygodniowego testu działania sprzętu.

### Obudowa na serwery kasetowe. 1 sztuka (Specyfikacja jak punkt 2.1)

### Serwery kasetowe dla wirtualizacji o parametrach minimalnych

| Ilość | 2 szt. |
|---|---|
| Obudowa | Kompatybilna z obudową typu Blade |
| Typ i liczba zainstalowanych dysków | 2x Hot Swap M.2 SSD 480GB NVMe Gen3 |
| Obsługa RAID | Obsługa RAID 0, 1 na minimum 2 dyskach |
| Karta sieciowa | 2x 25/50Gb |
| Procesor | 2x Intel Xeon-Gold 6444Y 3.6GHz 16-core 270W |
| Liczba procesorów | 2 |
| Pamięć | 256GB DDR5-4800 EC8 |
| Ilość gniazd pamięci | 16 |
| Zarządzanie infrastrukturą | Z wymaganymi licencjami, zintegrowany z obudową typu BLADE system KVM wraz funkcjami zarządzania energią serwera |
| Rozszerzenia | Podwójny adapter magistrali hosta 32 Gb Fibre Channel dla serwerów typu Blade |
| Wsparcie | System operacyjny VmWare 7 U3, do najnowszej aktualne dostępnej |
| Zasilacz | ND |
| Gwarancja | 5 lat, 24/7/4 DMR |
| System operacyjny | VmWare vSphere Standard 8 - 32 rdzenie z 3 letnim wsparciem licencja rejestrowana w portalu producenta systemu operacyjnego |

### Serwery kasetowe na potrzeby systemów operacyjnych Windows o parametrach minimalnych

| Ilość | 3 szt. |
|---|---|
| Obudowa | Kompatybilna z obudową typu Blade |
| Typ i liczba zainstalowanych dysków | 2x Hot Swap M.2 SSD 480GB NVMe Gen3 |
| Obsługa RAID | Obsługa RAID 0, 1 na minimum 2 dyskach |
| Karta sieciowa | 2x10/25Gb |
| Procesor | Intel Xeon-Gold 5415+ 2.9GHz 8-core 150W |
| Liczba procesorów | 1 z możliwością rozszerzenia do 2 |
| Pamięć | 32GB DDR5-4800 EC8 |
| Ilość gniazd pamięci | 16 |
| Zarządzanie infrastrukturą | Z wymaganymi licencjami, zintegrowany z obudową typu BLADE system KVM wraz funkcjami zarządzania energią serwera |
| Rozszerzenia | Podwójny adapter magistrali hosta 32 Gb Fibre Channel dla serwerów typu Blade |
| Rozszerzenia | Adapter magistrali hosta 32 Gb Fibre Channel dla serwerów typu Blade |
| Wsparcie | System operacyjny Red HAT, Ubuntu, Windows 2019/2022 |
| Zasilacz | ND |
| Gwarancja | 5 lat, 24/7/4 DMR |
| System operacyjny | Microsoft standard 2022 zakupiony w licencji grupowej wraz z SA licencja rejestrowana w portalu producenta systemu operacyjnego |

# 3. Rozbudowa sieci SAN i przestrzeni dyskowej (Część 3)

Zamawiający zamierza zrealizować połączenie sieci SAN FC pomiędzy dwoma budynkami. W każdym budynku będą się znajdowały dwa przełączniki tworzące niezależne fabric A i fabric B. Połączenie obu budynków będzie realizowane przez wykorzystanie istniejących 8 włókien światłowodowych połączonych w dupleksowe pary złączami LC. Wykorzystując to okablowanie Zamawiający zamierza stworzyć dla każdego fabrica redundantne połączenia o przepustowości 32G. Połączenie to ma służyć udostępnianiu zasobów macierzy do serwerów z drugiej lokalizacji, przesyłaniu danych związanych z synchroniczną replikacją macierzy dyskowych oraz przesyłaniu kopii zapasowych do drugiego budynku.

Zamawiający wymaga przeniesienia danych z serwerów plików Windows, hostów wirtualizujących VmWare znajdujących się na macierzach IBM SW z serii v7000 oraz HPE 3par z serii 7200 na nową dostarczoną macierz.

Przełączniki mają umożliwiać podłączenie w sieć SAN FC: bibliotek taśmowych, macierzy dyskowych, serwerów, innych przełączników firmy BROCADE posiadanych przez Zamawiającego.

Do wykonawcy należy wraz z lokalnym zespołem IT budowa nowego szkieletu sieci SAN składającej się z dwóch FABRIC-ów o przepustowości łącznej 128G pomiędzy budynkami.

Do oferty należy dodać licencje na oprogramowanie do zarządzania macierzami. Zamawiający dopuszcza dostarczenie oprogramowania w postaci maszyny wirtualnej przygotowanej przez producenta macierzy. Oprogramowanie ma integrować dostarczane macierze dyskowe i umożliwiać:

- monitorowanie ich stanu dysków, kontrolerów, zasilaczy, uplinków, wentylatorów

- bezpośrednie zalogowanie się z oprogramowania do macierzy w celu wykonania operacji administracyjnych.

## 3.1. Przełączniki szkieletowe sieci SAN-FC

| Ilość | 4 szt. |
|---|---|
| Obudowa | Instalowana w szafie RACK 1U |
| Chłodzenie | Umożliwiające instalacje przełącznika z tyłu szafy RACK |
| Zarządzanie | Poprzez GUI, SSH, port szeregowy oraz opcjonalnie poprzez dedykowane oprogramowanie |
| Karta sieciowa | 1 x RJ 45 do podłączenia modułu zarzadzania |
| Wyposażenie | 24 wkładki FC 32G |
| Licencje | Umożliwiające korzystanie z wszystkich portów |
| Licencje | Umożliwiające połączenie z posiadanymi przełącznikami firmy BROCADE |
| Rozszerzenia | Na wyposażeniu wszystkie porty obsadzone modułami gibic 32G |
| Rozszerzenia | 8 sztuk transciver Fibre Channel 32G do połączenia z drugim budynkiem na odległość ok 700m światłowodu jednmodowego |
| Zasilacz | Po 2 sztuki zasilaczy na każdy przełącznik |
| Gwarancja | 5 lat, 24/7 DMR z prawem aktualizacji firmware |

## 3.2. Macierz dyskowa SAN-FC z przeznaczeniem na aplikacje bazodanowe i wirtualizacje.

| Ilość | 1 szt. |
|---|---|
| Obudowa | Instalowana w szafie RACK |
| Kontrolery | 2 sztuki pracujące w trybie Active – Active<br>Oba kontrolery pracują na wydajność (w każdym kontrolerze musi być co najmniej 192 GB RAM wspierających odczyt i zapis z zabezpieczeniem bateryjnym w celu przeniesienia danych na pamięć nie ulotną podczas awarii zasilania) |
| | |

| | |
|---|---|
| **Rodzaj dysku** | Typu MVMe |
| **Przestrzeń dyskowa fizyczna** | 180 TB brutto (fizyczna) |
| **Przestrzeń dyskowa netto** | Minimalna przestrzeń netto 130 TiB/ bez kompresji I deduplikacja (bez redukcji danych) |
| **Obsługa RAID** | Obsługa RAID 6 z zabezpieczeniem minimum 2 dysków |
| **Karta sieciowa** | 2 x GbE do podłączenia modułów zarzadzania |
| **Rozbudowa** | Możliwość rozbudowy do 4 kontrolerów |
| **Rozbudowa** | Możliwość rozbudowy do 72 sztuk |
| **Zarządzanie infrastrukturą** | Poprzez dedykowane wbudowane kontrolery |
| **Tryb pracy klastrowej** | Praca z drugą macierzą w trybie synchronicznym wykorzystując FC poprzez dostarczane przełączniki (Zamawiający dopuszcza macierz wykorzystująca siec LAN na potrzeby synchronizacji, ale w przypadku skorzystania z prawa opcji wymaga dostarczenia osprzętu umożliwiającego połączenie obu macierzy pomiędzy budynkami) |
| **Funkcje** | Obsługa tylko dysków SSD lub modułów flash (nie dopuszcza się dostarczenia dysków talerzowych) |
| **Funkcje** | Obsługa minimum 500 LUNs |
| **Funkcje** | Obsługa minimum 500 kopii migawkowych przez system |
| **Funkcje** | Kontrolery muszą działać w sposób redundantny - tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych - praca w trybie Active/Active |
| **Funkcje** | Macierz musi umożliwiać budowę jednego obszaru danych na wszystkich dyskach zainstalowanych wewnątrz macierzy. Dyski muszą być skonfigurowane w taki sposób, aby utrata dowolnego z nich zapewniła ciągłość dostępu do danych. |
| **Funkcje** | Bez sterownikowe wsparcie dla systemu Windows serwer2022, VmWare 6.x i nowsze |
| **Funkcje** | Możliwość rozszerzenia wielkości LUN podczas pracy systemu bez przerywania pracy systemom operacyjnym (Windows serwer2022, VmWare 6.x i nowsze) |
| **Funkcje** | Wsparcie dla vVols minimum 800 sztuk. |
| **Funkcje** | Możliwość rozszerzania grupy dysków (puli dysków) podczas pracy systemu |
| **Funkcje** | Obsługa dysków NVMe |
| **Funkcje** | Dodatkowe pułki dyskowe musza być przyłączane poprzez NVMe |
| **Funkcje** | Obsługa protokołu NVMe-oF/FC |
| **Funkcje** | Pełny monitoring wszystkich dysków |
| **Funkcje** | Pełny monitoring wszystkich podzespołów znajdujących się w obudowie. |
| **Funkcje** | Połączenie pomiędzy półkami a kontrolerami musi być wykonane redundantnie i nie może ograniczać wydajności podłączonej drugiej półki. |
| **Funkcje** | Możliwość zbudowania puli dyskowej o pojemności 1PB |
| **Rozszerzenia** | Dwie niezależne karty FC na kontroler |
| **Rozszerzenia** | 8 sztuk transciver Fibre Channel 32 Gb |
| **Wydajność** | Wydajność dostarczanej konfiguracji macierzy ok +/- 5% 185000Iops (blok 8KiB w proporcji 80 na 20) |
| **Wydajność** | Redukcja danych deduplikacja i kompresja włączona - ok +/- 5% 145000Iops (blok 8KiB w proporcji 80 na 20) |
| **Gwarancja** | 5 lat 24/7 z 24 godzinnym gwarantowanym czasem naprawy i usunięciem usterki krytycznej, z prawem aktualizacji firmware (DMR dyski pozostają u Zamawiającego) |
| **Gwarancja obsługa** | w języku polskim |
| **Gwarancja** | Możliwość wyłączenia i włączenia automatycznego zgłaszania usterek do serwisu. |
| **Gwarancja** | Podczas gwarancji wsparcie inżyniera w trakcie planowania wgrania krytycznej aktualizacji firmware oraz podczas aktualizacji. |

## 3.3. Macierz dyskowa SAN-FC z przeznaczeniem na przechowywanie kopii zapasowych

| **Ilość** | **1 szt.** |
|---|---|
| **Obudowa** | Instalowana w szafie RACK |
| **Kontrolery** | 2 sztuki pracujące w trybie Active – Pasive dla wystawionego LUN |
| **Typ i liczba zainstalowanych dysków** | 24 x Hot Swap 16TB NLSAS 7200rpm |
| **Obsługa RAID** | Obsługa RAID 0, 1, 5, 6, 10, |
| **Karta sieciowa** | 2 x do podłączenia modułów zarzadzania |
| **Ilość gniazd na dyski** | Minimum 24 z możliwością rozbudowy do 100 sztuk |
| **Zarządzanie infrastrukturą** | Poprzez dedykowane wbudowane kontrolery |
| **Funkcje** | Obsługa minimum 500 LUNs |
| **Funkcje** | Obsługa minimum 500 kopii migawkowych przez system |
| **Funkcje** | Możliwość rozszerzenia wielkości LUN podczas pracy systemu bez przerywania pracy systemom operacyjnym (Windows serwer2022, VmWare 6.x i nowsze) |
| **Funkcje** | Możliwość wskazania jednego z kontrolerów jako głównego dla danego wolumenu |
| **Funkcje** | Możliwość rozszerzania grupy dysków |
| **Funkcje** | Obsługa dysków HDD i SSD |

| | |
|---|---|
| **Funkcje** | Możliwość zbudowania puli dyskowej do pojemności 1PB |
| **Funkcje** | Kontrolery muszą działać w sposób redundantny - tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych |
| **Funkcje** | Macierz musi umożliwiać budowę jednego obszaru danych na wszystkich dyskach zainstalowanych wewnątrz macierzy. Dyski muszą być skonfigurowane w taki sposób, aby utrata dowolnego z nich zapewniła ciągłość dostępu do danych. |
| **Wydajność** | Wydajność dostarczanej konfiguracji macierzy ok +/- 5% 2500Iops (blok 8KiB w proporcji 80 na 20) |
| **Rozszerzenia** | 4 sztuki gniazd 16 Gb Fibre Channel na kontroler |
| **Rozszerzenia** | 8 sztuk transciver Fibre Channel 16 Gb |
| **Wsparcie** | Dla systemu VmWare i Microsoft Windows |
| **Rozbudowa** | Możliwość rozbudowy do 120 dysków |
| **Zasilacz** | Po 2 sztuki zasilaczy na każda dostarczoną półkę z dyskami i kontrolerami |
| **Gwarancja** | 5 lat, 24/7 z prawem aktualizacji firmware (DMR dyski pozostają u Zamawiającego) |

## 3.4. Macierz dyskowa SAN-FC dedykowana do obsługi bazy danych.

| **Ilość** | **1 szt.** |
|---|---|
| **Obudowa** | Instalowana w szafie RACK |
| **Kontrolery** | 2 sztuki pracujące w trybie Active – Pasive dla wystawionego LUN |
| **Typ i liczba zainstalowanych dysków** | 12 x Hot Swap 1,9TB SSD SAS 12G M2 |
| **Obsługa RAID** | Obsługa RAID 0, 1, 5, 6, 10, |
| **Karta sieciowa** | 2 x do podłączenia modułów zarzadzania |
| **Ilość gniazd na dyski** | Minimum 24 z możliwością rozbudowy do 90 sztuk |
| **Zarządzanie infrastrukturą** | Poprzez dedykowane wbudowane kontrolery |
| **Funkcje** | Obsługa minimum 500 LUNs |
| **Funkcje** | Obsługa minimum 500 kopii migawkowych przez system |
| **Funkcje** | Możliwość rozszerzenia wielkości LUN podczas pracy systemu bez przerywania pracy systemom operacyjnym (Windows serwer2022, VmWare 6.x i nowsze) |
| **Funkcje** | Możliwość wskazania jednego z kontrolerów jako głównego dla danego wolumenu |
| **Funkcje** | Możliwość rozszerzania grupy dysków |
| **Funkcje** | Kontrolery muszą działać w sposób redundantny - tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych |
| **Funkcje** | Macierz musi umożliwiać budowę jednego obszaru danych na wszystkich dyskach zainstalowanych wewnątrz macierzy. Dyski muszą być skonfigurowane w taki sposób, aby utrata dowolnego z nich zapewniła ciągłość dostępu do danych. |
| **Funkcje** | Możliwość zbudowania puli dyskowej do pojemności 0,6 PB |
| **Funkcje** | Połączenie pomiędzy półkami a kontrolerami musi być wykonane redundantnie |
| **Wydajność** | Wydajność dostarczanej konfiguracji macierzy ok +/- 5% 5000Iops (blok 8KiB w proporcji 80 na 20) |
| **Rozszerzenia** | 2 sztuki gniazd 16 Gb Fibre Channel na kontroler |
| **Rozszerzenia** | 4 sztuki transciver Fibre Channel 16 Gb |
| **Zasilacz** | Po 2 sztuki zasilaczy na każda dostarczoną półkę z dyskami i kontrolerami |
| **Gwarancja** | 5 lat, 24/7  z prawem aktualizacji firmware (DMR dyski pozostają u Zamawiającego) |

## 3.5.Zamówienie opcjonalne dla części 3

Zamawiający zastrzega sobie prawo do skorzystania z prawa opcji. Zamawiający uzależnia skorzystanie z prawa opcji od własnych potrzeb w zakresie wskazanym w Specyfikacji technicznej, stanowiącej załącznik A do SWZ w okresie **do 12 miesięcy** od daty złożenia zamówienia w okresie do 12 miesięcy od daty podpisania protokołu odbioru bez uwag zamówienia podstawowego.

Zamówienie opcjonalne obejmuje dodatkowe urządzenia i rozwiązania, które w części znajdą się w czwartym budynku Zamawiającego.

### Macierz dyskowa SAN-FC z przeznaczeniem na aplikacje bazodanowe i wirtualizacje. 1 sztuka (Specyfikacja jak punkt 3.2):

| | |
|---|---|
| **Tryb pracy klastrowej** | Praca z drugą macierzą (jak punkt 3.2) w trybie synchronicznym wykorzystując FC poprzez dostarczane przełączniki (Zamawiający dopuszcza macierz wykorzystująca siec LAN na potrzeby synchronizacji, ale wymaga do tego dostarczenia macierzy wraz z osprzętem umożliwiającym połączenie obu macierzy pomiędzy budynkami)<br>Do macierzy dyskowej będącej drugim elementem klastra należy dodać serwer, który będzie pełnił funkcje koordynatora działania klastra. Zamawiający przewiduje miejsce 1U na wstawienie takiego rozwiązania w trzeciej serwerowni. |

### Dodatkowa półka dyskowa do macierzy z punktu 3.3. Macierz dyskowa SAN-FC z przeznaczeniem na przechowywanie kopii zapasowych o parametrach:

| | |
|---|---|
| **Ilość** | 2 szt. |
| **Obudowa** | Instalowana w szafie RACK |
| **Kontrolery** | Nd |
| **Typ i liczba zainstalowanych dysków** | 12 x Hot Swap 16TB NLSAS 7200rpm |
| **Karta rozszerzeń** | 2 x do podłączenia z macierzą z punktu 3.3. |
| **Kable** | Kable pozwalające na podłączenie pułki do macierzy z punktu 3.3 |
| **Ilość gniazd na dyski** | 12 |
| **Zasilacz** | Po 2 sztuki zasilaczy na każda dostarczoną półkę z dyskami i kontrolerami |
| **Gwarancja** | 5 lat, 24/7 z prawem aktualizacji firmware (DMR dyski pozostają u Zamawiającego) |

### Macierz dyskowa FC SAN z przeznaczeniem na aplikacje bazodanowe i wirtualizacje:

| | |
|---|---|
| **Ilość** | **1 szt.** |
| **Obudowa** | Instalowana w szafie RACK |
| **Kontrolery** | 2 sztuki pracujące w trybie Active – Pasive |
| **Typ i liczba zainstalowanych dysków** | 24 x Hot Swap 8TB SAS 7200rpm |
| **Typ i liczba zainstalowanych dysków** | 12 x Hot Swap 0,9TB SSD SAS 12G M2 |
| **Obsługa RAID** | Obsługa RAID 0, 1, 5, 6, 10, |
| **Karta sieciowa** | 2 x do podłączenia modułów zarzadzania |
| **Ilość gniazd na dyski** | Minimum 48 |
| **Zarządzanie infrastrukturą** | Poprzez dedykowane wbudowane kontrolery |
| **Funkcje** | Obsługa minimum 500 LUNs |
| **Funkcje** | Obsługa minimum 500 kopii migawkowych przez system |
| **Funkcje** | Możliwość rozszerzenia wielkości LUN podczas pracy systemu bez przerywania pracy systemów operacyjnych |
| **Funkcje** | Możliwość wskazania jednego z kontrolerów jako głównego dla danego wolumenu |
| **Funkcje** | Możliwość rozszerzania grupy dysków |
| **Funkcje** | Obsługa dysków HDD i SSD |
| **Funkcje** | Możliwość zbudowania puli dyskowej do pojemności 1PB |
| **Funkcje** | Połączenie pomiędzy półkami a kontrolerami musi być wykonane redundantnie |
| **Rozszerzenia** | 4 sztuki gniazd 16 Gb Fibre Channel na kontroler |
| **Rozszerzenia** | 4 sztuki transciver Fibre Channel 16 Gb |
| **Wsparcie** | Dla systemu VmWare i Microsoft Windows |
| **Rozbudowa** | Możliwość rozbudowy do 100 dysków |
| **Zasilacz** | Po 2 sztuki zasilaczy na każda dostarczoną półkę z dyskami i kontrolerami |
| **Gwarancja** | 5 lat, 24/7 z prawem aktualizacji firmware (DMR dyski pozostają u Zamawiającego) |
| **Gwarancja** | 5 lat, 5/9 NBD |