Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

ZAŁĄCZNIK NR 1 DO SWZ

Opis Przedmiotu Zamówienia

W PROJEKTACH

„tytuł projektu: POPC.04.01.01-00-0073/22 „Finansowanie zaplecza technicznego i szkoleniowego dla Urzędu Komunikacji Elektronicznej w 2023 r.”

tytuł projektu: POPC.02.01.00-00-0136/21 „Dostęp do bieżącej informacji o jakości usług IAS w oparciu o system monitorowania jakości Internetu SMJI”

tytuł projektu: POPC.04.01.01-00-0041/20 „Rozbudowa Systemu Punktu Informacyjnego ds. Telekomunikacji etap II w latach 2020-2023”

DO POSTĘPOWANIA NA:

„Dostawa i wdrożenie serwerów, urządzeń sieciowych wraz z systemem do zarządzania i analizy oraz usługą wsparcia technicznego i gwarancją producenta na okres 36 miesięcy na dostarczony sprzęt”

Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

Data: …/…/…

Spis treści

Spis treści

1. Słownik 4
2. Ogólne wymagania Przedmiotu Zamówienia 9
3. Szczegółowa organizacja wdrożenia PZ 10
   1. Wymagania funkcjonalne 10
   2. Harmonogram wdrożenia 12
   3. Instalacja i Wdrożenie 14
   4. Procedura testowania 15
   5. Instruktaże stanowiskowe 16
   6. Odbiór końcowy 18
4. Specyfikacja techniczna sprzętu i oprogramowania 19
   4.1 Specyfikacja ilościowa Zamówienia podstawowego 21
   4.2 Specyfikacja techniczna Infrastruktury sieciowej 22
      4.2.1 Przełącznik sieciowy Typ A 22
      4.2.2 Przełącznik sieciowy Typ B 28
      4.2.3 Przełącznik sieciowy Typ C 37
      4.2.5 Przełącznik sieciowy Typ D 47
      4.2.7 Przełącznik sieciowy Typ E 52
      4.2.8 Urządzenie ochrony przed rozproszonymi atakami sieciowymi 57
      4.3.1 Systemy analizy, zarządzania i monitorowania 65
   4.3 Specyfikacja techniczna Infrastruktury serwerowej 81
      4.3.2 Serwer Rack 82
      4.3.3 Przełącznik SAN 87
      4.3.4 Macierz typ 1 90
      4.3.5 Macierz typ 2 95
   4.4 Specyfikacja techniczna Infrastruktury wskazanej w prawie opcji 101
      4.4.1 Serwer Rack – Prawo Opcji 101
      4.4.2 Przełącznik sieciowy Typ B – Prawo Opcji 107
      4.4.3 Przełącznik sieciowy Typ C – Prawo Opcji 117
      4.4.4 Przełącznik sieciowy Typ D – Prawo Opcji 127

Spis tabel 132

1. Słownik

Lp.	Nazwa parametru	Opis parametru
1.	**Analiza przedwykonawcza**	etap realizacji Zamówienia, na który składa się cykl prac analitycznych i organizacyjnych realizowany przez Wykonawcę we współpracy z Zamawiającym mający na celu przeprowadzenie analizy biznesowej i systemowej na potrzeby wdrożenia Rozwiązania u Zamawiającego. Analiza Przedwykonawcza ma na celu ustalenie szczegółowego sposobu spełnienia wymagań określonych w OPZ oraz sposobu realizacji Przedmiotu Zamówienia. Analiza Przedwykonawcza powinna zakończyć się dostarczeniem Dokumentacja Analizy Przedwykonawcza
2.	**Awaria**	Należy przez to rozumieć: kategorię Wady w obszarze Infrastruktury i Oprogramowania skutkującą całkowitym brakiem działania lub skutkującą niemożliwością realizowania ważnych funkcjonalności Przedmiotu Zamówienia
3.	**Błąd**	Należy przez to rozumieć Wadę w obszarze Infrastruktury i Oprogramowania, oznaczającą jego funkcjonowanie niezgodne z opisem w Dokumentacji lub SWZ uniemożliwiające działanie pojedynczych funkcjonalności w Przedmiocie Zamówienia lub powodujące ryzyko bądź zagrożenie nieuprawnionego dostępu do Rozwiązania
4.	**Czas Naprawy**	Należy przez to rozumieć czas, jaki upływa pomiędzy pierwszym Zgłoszeniem Wady, a Usunięciem Wady.
5.	**Czas Reakcji Wykonawcy**	Należy przez to rozumieć potwierdzenie przyjęcia zgłoszenia serwisowego przez Wykonawcę oraz potwierdzenie, że Wykonawca przystąpił do diagnozy przyczyn Usterki/Awarii oraz rozwiązywania problemu.
6.	**Dokumentacja Przedmiotu Zamówienia (Dokumentacja, Dokumentacja PZ, DPZ)**	Wszelka dokumentacja wytworzona, dostarczona i utrzymywana przez Wykonawcę w formatach danych (wymaga się, aby dany dokument został dostarczony w jednym z formatów w zależności od zawartości) doc, docx, xls, xlsx, pdf, dwg (każdorazowo sformatowana do wydruku na stronach A4 i/lub A3) dotycząca PZ i powstała w wyniku realizacji Umowy zawartej pomiędzy Zamawiającymi, a Wykonawcą. Dokumentacja zawiera: 1. Dokumentację Analizy Przedwykonawcza (DAP) 2. Dokumentację Powykonawczą (DPO) Odebrana wersja dokumentacji powinna zostać dostarczona w formie elektronicznej w formie uniemożliwiającej zmiany tj. na trwałym nośniku optycznym lub w wersji podpisanej elektronicznie przez osobę upoważnioną.

7.	**Dokumentacja Analizy Przedwykonawcza (DAP)**	Uzgodniona wspólnie z Zamawiającymi dokumentacja opracowana przez Wykonawcę wraz z późniejszymi zmianami, na podstawie której będzie realizowany organizacyjnie i technicznie PZ, która będzie podlegała akceptacji Zamawiających zawierająca w szczególności: 1. Część zarządcza: 1.1 Skład i struktura organizacyjna Zespołu Zarządzania Projektem i Zespołu Wdrożeniowego z podziałem na role i zadania poszczególnych członków zespołu, 1.2 Ogólny plan komunikacji w Projekcie, 1.3 Sposób obsługi zmian projektowych, 1.4 Ogólny plan zarządzania ryzykiem w Projekcie 1.5 Szczegółowy Harmonogram Wdrożenia zgodny z OPZ i zawierający elementarne zadania do wykonania podczas realizacji PZ 2. Część techniczna: 1.1 Podział PZ na Produkty 1.2 Karty katalogowe Infrastruktury 1.3 Plan dostaw 1.4 Plan oraz opis modernizacji i budowy Infrastruktury wraz z Oprogramowaniem, 1.5 Szczegółowe uzgodnienia Stron Umowy dotyczące zakresu i sposobu integracji dostarczanych rozwiązań z Istniejącymi Systemami Informatycznymi, 1.6 Zakres prac realizowanych przez podwykonawców, 1.7 Plan Instruktaży 1.8 Plan testów
8.	**Dokumentacja Powykonawcza (DPO)**	Należy przez to rozumieć Dokumentację właściwą dla danego Zamawiającego, zawierającą dokładną konfigurację rozwiązania na moment podpisania Protokołu Odbioru Końcowego, w tym co najmniej: 1. DPR zaktualizowana na termin Protokołu Odbioru Końcowego 2. Schematy architektury Infrastruktury wraz z połączeniami poszczególnych ich elementów; 3. Szczegółowy wykaz i opis wszystkich elementów Infrastruktury i Oprogramowania wraz z numerami katalogowymi, numerami seryjnymi, numerami niezbędnymi do kontaktu z serwisem producenta

		4. Opis konfiguracji Infrastruktury i Oprogramowania adresowany do Administratorów, pozwalający na samodzielne administrowanie przez Zamawiających Sprzętem po zakończeniu realizacji PZ; 5. Instrukcje instalacji, obsługi, zarządzania i konfiguracji wszystkich elementów Infrastruktury i Oprogramowania w wersji dostarczanej przez producenta - dopuszczana w wersji angielskiej, jeśli producent nie udostępnia w wersji polskiej 6. Inne dokumenty wytworzone w trakcie realizacji projektu uzgodnione z Zamawiającymi dotyczące rozwiązań technicznych i projektowych PZ
9.	**Dni Robocze**	Dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy, wskazanych w ustawie z dnia 18 stycznia 1951 r o dniach wolnych od pracy (Dz. U. z 2015 r. poz. 90)
10.	**Etap**	Zdeterminowany w Harmonogramie Wdrożenia okres podczas, którego Wykonawca realizuje określony zakres Przedmiotu Zamówienia podlegający odbiorowi
11.	**Harmonogram Wdrożenia**	Harmonogram prac Wykonawcy zawarty w Opisie Przedmiotu Zamówienia
12.	**Infrastruktura, Infrastruktura Sprzętowa(Sprzęt)**	Sprzęt informatyczny wyspecyfikowany w OPZ wchodzący w skład Rozwiązania w tym Infrastruktura Serwerowa i Infrastruktura Sieciowa
13.	**Instruktaż Stanowiskowy**	Należy przez to rozumieć konsultacje indywidualne lub grupowe dotyczące użytkowania uruchomionego i wdrażanego Sprzętu udzielane przez Wykonawcę Użytkownikom Zamawiającego w trakcie realizacji PZ
14.	**Odbiór**	Należy przez to rozumieć Odbiór Etapu, Odbiór Produktu lub Odbiór Końcowy
15.	**Odbiór Etapu**	Należy przez to rozumieć odbiór Etapu Umowy, zgodny z SWZ i Dokumentacją Analizy Przedwykonawczej. W ramach Odbioru Etapu następuje również odbiór produktów, wyszczególnionych dla danego Etapu w Analizie Przedwykonawczej
16.	**Odbiór Końcowy**	Należy przez to rozumieć odbiór końcowy PZ zgodny z wymogami SWZ i z postanowieniami Dokumentacji Analizy Przedwykonawczej
17.	**Oprogramowanie**	Należy przez to rozumieć System analizy i zarządzania
18.	**Prace Serwisowe**	Prace serwisowe to prace wykonywane w ramach świadczenia usług gwarancji. Prace muszą być realizowane w godzinach preferowanych przez Zamawiającego.

19.	**Produkt**	Elementarny efekt działań/prac/dostaw objętych całym zakresem Przedmiotu Zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach
20.	**Protokół Odbioru**	1. **Etapu –** Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego stanowi potwierdzenie wykonania prac przewidzianych w ramach Etapów określonych w SWZ i uszczegółowionych w Dokumentacji Analizy Przedwykonawczej. 2. **Produktu –** Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego stanowi potwierdzenie dostarczenia Produktu 3. **Końcowego –** Protokół, który po podpisaniu bez zastrzeżeń przez Zamawiającego, stanowi potwierdzenie wykonania i odbioru Przedmiotu Zamówienia.
21.	**PU**	Przedmiot Umowy, równoznaczne z Przedmiotem Zamówienia (PZ)
22.	**PZ**	Przedmiot Zamówienia „Zakup sprzętu i oprogramowania dla rozbudowy infrastruktury serwerowej Urzędu Komunikacji Elektroniczne
23.	**PZP**	Ustawa Prawo zamówień publicznych
24.	**Rozwiązanie**	oznacza całość infrastruktury oraz oprogramowania wskazanego w PZ
25.	**Rozwiązanie Zastępcze**	Należy przez to rozumieć awaryjne procedury postępowania w wykorzystaniu Infrastruktury i Oprogramowania lub dodatkowe oprogramowanie dostarczone przez Wykonawcę, które ma za zadanie podtrzymać ciągłość działania Infrastruktury lub Oprogramowania do czasu usunięcia Wady
26.	**System Zgłoszeń (SZ)**	Aplikacja informatyczna dostępna poprzez sieć Internet dostarczona przez Wykonawcę dla Zamawiających na okres realizacji Projektu oraz gwarancji wynikającej z Umowy stanowiąca repozytorium Dokumentacji, umożliwiająca zgłaszanie oraz obsługę uwag do prac Wykonawcy oraz zgłaszanie i obsługę Wad. Dopuszcza się rozdzielenie funkcjonalności na grupę systemów.
27.	**Szczegółowy Harmonogram Wdrożenia**	Harmonogram prac Wykonawcy określony na Etapie Dokumentacji Analizy Przedwykonawczej
28.	**SWZ**	Specyfikacja Warunków Zamówienia dla postępowania pn.: Zakup sprzętu i oprogramowania dla rozbudowy infrastruktury serwerowej Urzędu Komunikacji Elektronicznej”

29.	**Umowa**	Ilekroć w tekście niniejszego dokumentu zostanie przywołany wyraz “umowa” bez wyraźnego wskazania jej numeru lub daty zawarcia, należy go interpretować, jako odwołanie bezwzględne do umowy zawartej w ramach tego postępowania.
30.	**Usterka**	Należy przez to rozumieć kategorię Wady w Oprogramowaniu lub Infrastrukturze oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SWZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego, utrudniającą pracę Użytkownikowi Zamawiającego.
31.	**Wada**	Należy przez to rozumieć Awarię, Błąd, Usterkę
32.	**Wdrożenie**	Szereg uporządkowanych i zorganizowanych działań mających na celu wprowadzenie do użytkowania przez Zamawiającego opisanego w niniejszym dokumencie PZ.
33.	**Wykonawca**	Należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która ubiega się o udzielenie zamówienia publicznego, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego.
34.	**Zamawiający**	Oznacza Urząd Komunikacji Elektronicznej
35.	**Zgłoszenie**	przekazanie Wykonawcy przez uprawnioną osobę po stronie Zmawiającego informacji o konieczności naprawy lub modyfikacji oprogramowania. W przypadku zgłoszeń dotyczących modyfikacji musi być ono zaakceptowane przez obie strony.
36.	**Zgłoszenie Wady**	Zdarzenie, w wyniku którego nastąpiło powiadomienie Wykonawcy o zaistniałej Wadzie

2. Ogólne wymagania Przedmiotu Zamówienia

1) Wykonawca jest zobowiązany do realizacji PZ w uzgodnieniu z Zamawiającym oraz zgodnie z wymaganiami SWZ na każdym Etapie jego realizacji.
2) Wykonawca zaplanuje koncepcje wdrożenia, dostarczy, zainstaluje, skonfiguruje, przeprowadzi Testy i wdroży wszystkie PZ zgodnie z wymaganiami SWZ.
3) PZ musi być zrealizowany kompleksowo w lokalizacjach Zamawiającego znajdujących się na terenie Warszawy oraz na obszarze w promieniu 60 km od Warszawy.
4) Wszystkie nazwy własne oprogramowania i sprzętu użyte w OPZ należy rozumieć wyłącznie jako określenie standardów parametrów technicznych, użytkowych, funkcjonalnych i jakościowych oczekiwanych przez Zamawiającego i należy odczytywać łącznie z wyrazami „lub równoważne" chyba że dotyczącą rozbudowy konkretnego rozwiązania posiadanego przez Zamawiającego.
5) Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych wszystkim rozwiązaniom wskazanym w OPZ.
6) Wykonawca oferując rozwiązanie równoważne do opisanego w specyfikacji jest zobowiązany wykazać równoważność w zakresie parametrów technicznych, użytkowych, funkcjonalnych i jakościowych, które muszą być spełnione na poziomie nie niższym niż parametry wskazane przez Zamawiającego.
7) PZ obejmuje:
   a) Opracowanie Analizy Przedwykonawczej, obejmującej:
      i Projekt wdrożenia i integracji dostarczanej Infrastruktury z zasobami Zamawiającego,
      ii Szczegółowy Harmonogram Wdrożenia
   b) Dostawy, instalacje, konfiguracje i wdrożenia Infrastruktury i Oprogramowania
      iii Dostawy, instalacje, konfiguracje i wdrożenia i Oprogramowania
      iv Wsparcie Zamawiającego w rekonfiguracji i dostosowanie sieci u Zamawiającego dla właściwego działania i funkcjonowania Oprogramowania i Sprzętu
   c) Przeprowadzenie Testów
   d) Opracowanie Dokumentacji Przedmiotu Zamówienia,
   e) Przeprowadzenie Instruktażu Stanowiskowego,
   f) Pozostałe dostawy i usługi opisane w SWZ.

3. Szczegółowa organizacja wdrożenia PZ

1. Wymagania funkcjonalne

1) Celem wdrożenia Infrastruktury i Oprogramowania jest przygotowanie wydajnej i bezpiecznej platformy sprzętowo-programowej dla obsługi usług świadczonych przez UKE. Musi ona być zbudowana zgodnie z najlepszymi praktykami w zakresie projektowania i zabezpieczania tego typu systemów.
2) Docelowa architektura fizyczna i logiczna Zamawiającego musi składać się z dostarczanych elementów Infrastruktury, elementów istniejących oraz umożliwić prawidłowe i efektywne działanie u każdego Uczestnika. Dostarczona Infrastruktura musi działać w sposób kompatybilny z posiadaną przez Zamawiającego infrastrukturą w sposób opisany w niniejszym dokumencie.
3) Wszystkie działania Wykonawcy podczas Etapów muszą zostać przeprowadzone zgodnie z Harmonogramem Wdrożenia i zakończone pozytywnym wynikiem testów oraz odbiorem.
4) Zamawiający ma prawo do odstąpienia od poniższych wymogów, ich zmiany lub zaproponowania nowych w uzgodnieniu z Wykonawcą na etapie opracowania Dokumentu Analizy Przedwykonawczej.
5) Wykonawca wykona instalację, konfigurację i wdrożenie i testy dla Infrastruktury i Oprogramowania
6) Dokona montażu fizycznego wszystkich dostarczonych produktów w miejscu uzgodnionym z Zamawiającym.
7) Dostarczy wszystkie Urządzenia i Oprogramowanie z najnowszą - dostępną na termin dostawy - wersją oprogramowania . Na pisemny wniosek Zamawiającego wersja ta może zostać zmieniona do wersji starszej niż aktualnie dostępna (jeśli istnieje taka możliwość).
8) Podłączy dostarczaną Infrastrukturę serwerową i sieciową do instalacji zasilającej Zamawiającego oraz dostarczy i podłączy okablowaniem sygnałowym dostarczaną Infrastrukturę sieciową i serwerową (dla urządzeń tego wymagających) do istniejącej infrastruktury Zamawiającego (jeśli konieczne). Zamawiający zapewni punkt styku z obecną infrastrukturą w danej lokalizacji (jeśli konieczne). Wykonawca przygotuję fizyczny port w urządzeniu w celu podłączenia obecnej infrastruktury (jeśli konieczne).
9) Użyje jednoznacznego oznaczenia okablowania oraz sprzętu w celu uniknięcia błędów w podłączeniu dostarczonych produktów. Poprzez oznaczenie rozumie umieszczenie flagi na każdym zakończeniu kabla oraz oznakowaniu każdego urządzenia w widocznym miejscu zarówno z przodu jak i z tyłu urządzenia. Oznakowanie musi być na tyle trwałe, aby wytrzymało warunki pomieszczeń technicznych typu serwerownia czy węzeł sieciowy.
10) Wszystkie elementy sprzętowe dostarczonej Infrastruktury muszą być wyposażone w komplet akcesoriów niezbędnych do instalacji tak, aby po uruchomieniu osiągnęły wymaganą funkcjonalność.
11) Wykonawca nie jest zobowiązany do rekonfiguracji jakichkolwiek urządzeń niebędących w zakresie dostawy niniejszego postępowania

Infrastruktura Sprzętowa

1) Infrastruktura zostanie dostarczona i wdrożona do wskazanych lokalizacji w porozumieniu z Zamawiającym. Zadanie to wymaga odpowiedniego zaplanowania dostaw i prac w taki sposób, aby nie kolidowało to z bieżącą pracą Zamawiającego.
2) Wykonawca zapewni wniesienie dostarczonego Sprzętu do wskazanych pomieszczeń.
3) Wykonawca dostarczy Sprzęt sukcesywnie w terminie bezpośrednio poprzedzającym jego instalację i wdrożenie, w sposób dopasowany do możliwości logistycznych Zamawiającego. Zakres i wielkości dostaw należy każdorazowo uzgodnić z Zamawiającym.
4) Przedstawiciel Wykonawcy będzie obecny osobiście w miejscu każdej dostawy przewidzianej w PZ w obiektach Zamawiającego.
5) Dla całej Infrastruktury sprzętowej, we wszystkich Obiektach Wykonawca dostarczy, zamontuje, skonfiguruje i dostroi Sprzęt i Oprogramowanie.
6) Wdrożenie Infrastruktury zostanie wykonane przez specjalistów przeszkolonych i doświadczonych w tym zakresie.
7) Wykonawca będzie odpowiadać za utrzymanie w sprawności technicznej Infrastruktury Sprzętowej dostarczonej i uruchomionej u Zamawiającego przez okres do dnia podpisania protokołu Odbioru Końcowego PZ,

Oprogramowanie

1) Oprogramowanie zostanie dostarczone i wdrożone na dostarczonym Sprzęcie oraz w taki sposób, aby zapewnić prawidłowe funkcjonowanie Oprogramowania.
2) Dostawa i wdrożenie zostaną wykonane w lokalizacjach zgodnych z instalacją Sprzętu oraz zgodnie z ustaleniami DAP.
3) Instalacja i wdrożenie Oprogramowania zostaną wykonane przez specjalistów posiadających wiedzę praktyczną z wdrażania zaoferowanego Oprogramowania.
12) Oprogramowanie musi zostać wdrożone w taki sposób, aby działało poprawnie zgodnie z jego przeznaczeniem i architekturą Systemu.

2. Harmonogram wdrożenia

1. Przedmiot Zamówienia będzie realizowany w oparciu o opracowany przez Wykonawcę i zaakceptowany przez Zamawiającego Szczegółowy Harmonogram Wdrożenia , na podstawie Harmonogramu Wdrożenia zawartego w Tabeli poniżej. Szczegółowy Harmonogram Wdrożenia będzie aktualizowany w trakcie wykonywania PZ.
2. Wykonawca zapewni synchronizację działań i zależności pomiędzy wdrożeniem Infrastruktury i wdrożeniem Oprogramowania.

Tabela 1 Harmonogram wdrożenia

Numer ETAPU	**Zakres ETAPU**	**Całkowity czas realizacji Umowy (liczony w tygodniach od dnia podpisania Umowy)**							
Przedmiot zamówienia		1	2	3	4	5	6	7	8
1	Przeprowadzenie Analizy Przedwykonawczej oraz dostawa Dokumentacja Analizy Przedwykonawczej	**X**	**X**						
2	Dostawa Infrastruktury i Oprogramowania, instalacja, konfiguracja, wdrożenie, przeprowadzenie Testów Infrastruktury i Oprogramowania		**X**	**X**	**X**	**X**	**X**	**X**	**X**
3	Przeprowadzenie Instruktaży Stanowiskowych oraz dostawa Dokumentacji Powykonawczej i Podpisanie Protokołu Odbioru Końcowego.							**X**	**X**

3. Instalacja i Wdrożenie

1. W ramach Wdrożenia PZ Wykonawca dostarczy wszystkie niezbędne materiały pomocnicze dla Infrastruktury sieciowej takich jak:
    a) wkładki światłowodowe – wymagane jest dostarczenie wkładek dla wszystkich portów obsługujących wkładki światłowodowe w dostarczanej Infrastrukturze sieciowej. Dobór poszczególnych wkładek zostanie przeprowadzony w uzgodnieniu z Zamawiającym na etapie DAP. Dobór wkładek dotyczy także urządzeń Firewall. Zakłada się możliwość doboru wkładek o różnych przepustowościach (np. 1 Gbit, 10 Gbit) oraz o dowolnych parametrach obsługiwanych przez dostarczaną Infrastrukturę sieciową. Zamawiający dopuszcza dostawę wkładek nie pochodzących od producenta dostarczanego sprzętu pod warunkiem braku ograniczania gwarancji urządzenia poprzez wykorzystanie niniejszych wkładek oraz pełnej kompatybilności ze sprzętem.
    b) kable sygnałowe – wymagane jest dostarczenie wszystkich niezbędnych kabli sygnałowych (zarówno miedzianych jak i światłowodowych) wymaganych do uruchomienia dostarczanej Infrastruktury serwerowej i sieciowej w miejscu jej instalacji. Dodatkowo wymaga się dostarczenie patchcordów miedzianych i światłowodowych w liczbie pozwalającej do przekrosowania wszystkich gniazd w przełącznikach dostępowych dostarczanych w ramach postępowania. Długość i kolor zostaną dobrane w uzgodnieniu Zamawiającym na etapie DAP. Nie przewiduję się dostarczania patchcordów dłuższych niż 10m do przekrosowania przełączników.
    c) kable zasilające, organizery, trwałe etykiety itp. wymagane do uzyskania opisanych funkcjonalności w SWZ i DAP.
2. Dostarczone kable sygnałowe muszą mieć parametry nie gorsze niż parametry i klasa okablowania strukturalnego niskoprądowego dostarczonego przez Wykonawcę części pasywnej projektu (klasa nie niższa niż 6A).

4. Procedura testowania

1. W ramach zadania zostaną przeprowadzone wszystkie testy opisane w DAP. Celem testów jest weryfikacja przez Zamawiającego, czy wszystkie prace wykonane w trakcie realizacji PZ zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad, dla poszczególnych Produktów oraz całego PZ, jest warunkiem niezbędnym aby dokonać odbiorów w ramach poszczególnych Etapów (Etapu 2 i 3) oraz Odbioru końcowego.
3. Procedura dotyczy Testów funkcjonalnych poprzedzających Odbiór, zgodnie z Harmonogramem Wdrożenia.

   4. Termin i czas przeprowadzenia poszczególnych testów funkcjonalnych zostanie określony w Szczegółowym Harmonogramie Wdrożenia.

5. Instruktaże stanowiskowe

1) Instruktaże Stanowiskowe są elementem wdrożenia i mają zapewnić zapoznanie użytkowników i w efekcie ich sprawne korzystanie z dostarczanego Oprogramowania i Sprzętu.
2) Wykonawca zaplanuje w uzgodnieniu z Zamawiającym Instruktaże Stanowiskowe w wymiarze co najmniej wskazanym w ofercie jednak nie mniej niż wskazano w poniższej tabeli.
   a) Instruktaże Stanowiskowe będą prowadzone natywnie w języku polskim i obejmą zakresem użytkowanie Oprogramowania
   b) Budowę, architekturę i konfigurację Infrastruktury,
   c) Asystę Uruchomieniową,

Tematyka instruktażu stanowiskowego musi obejmować wszelkie czynności niezbędne do poprawnej eksploatacji dostarczonej Infrastruktury, w tym modyfikacje topologii połączeń i architektury, wymiany komponentów sprzętowych oraz obsługę interfejsów zarządzających (zarówno poprzez konsolę graficzną jak i tekstową). Instruktaże stanowiskowe będą prowadzone natywnie w języku polskim.

3) Wymiar Instruktaży stanowiskowych nie może być mniejszy niż (w godzinach):
   a) Infrastruktura– 15 godzin
   b) Oprogramowanie– 5 godzin

4) Wykonawca uzgodni z Zamawiającym Plan Instruktaży Stanowiskowych w Etapie wykonania Dokumentacji DAP z zachowaniem zgodności z Harmonogramem Wdrożenia

5) Plan Instruktaży Stanowiskowych będzie zawierać między innymi:

a) nazwy, zakresy tematyczne oraz grupy Użytkowników Wewnętrznych poszczególnych Instruktaży Stanowiskowych,

b) podział Instruktaży Stanowiskowych na Etapy realizacji Przedmiotu zamówienia uwzględniając: dostawy/przygotowanie, wdrożenie, użytkowanie po wdrożeniu,

c) lokalizację Instruktaży,

d) daty i godziny Instruktaży.

8) Wykonawca będzie prowadził rejestr wykonanych Instruktaży Stanowiskowych w układzie zgodnym z planem Instruktaży Stanowiskowych.
9) W przypadku potrzeby Zamawiający zapewniają we własnym zakresie pomieszczenia dla przeprowadzenia Instruktaży stanowiskowych. Wykonawca może realizować Instruktaże stanowiskowe również na stanowiskach pracy pracowników PL.
10) Instruktaże Stanowiskowe zostaną przeprowadzone przez doświadczonych specjalistów w zakresie Sprzętu lub Oprogramowania, który podlega Instruktażowi Stanowiskowemu.

11) Instruktaże Stanowiskowe zostaną przeprowadzone w miejscach instalacji lub innych uzgodnionych z Zamawiającym w tym Zamawiający może dopuścić możliwość przeprowadzenia Instruktaży poprzez wideokonferencję. Ewentualna zmiana miejsca przeprowadzenia Instruktaży jest warunkowana zapewnieniem przez Wykonawcę odpowiednich pomieszczeń i stanowisk pracy, a jeśli będzie taka potrzeba, Wykonawca nieodpłatnie zapewni odpowiednią ilość licencji oprogramowania niezbędną do przeprowadzenia Instruktaży Stanowiskowych w każdym Etapie realizacji PZ.
12) Każdy Instruktaż Stanowiskowy musi być potwierdzony pisemnym protokołem z obowiązkowym podpisem Użytkownika Wewnętrznego biorącego udział w Instruktażu Stanowiskowym z podaniem zakresu tematycznego, ilości godzin i lokalizacji Instruktażu Stanowiskowego oraz danych prowadzącego.

6. Odbiór końcowy

1) Odbiór końcowy PZ ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy i SWZ w tym odebrania wszystkich Produktów/Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji. Dokonanie Odbioru Końcowego zakończy realizację PZ.

4. Specyfikacja techniczna sprzętu i oprogramowania

W niniejszym dziale przedstawiono minimalne parametry urządzeń. W przypadku, gdy nie określono, że parametr określa maksymalną wartość jest to jego wartość minimalna. Wartość ta określa zawsze parametr korzystniejszy dla Zamawiającego.

Wymagania ogólne:

1. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producenta.
2. Całość dostarczanej infrastruktury serwerowej i sieciowej , tzn. każde z dostarczonych urządzeń, musi być fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach. Nie dopuszcza się urządzeń typu refubrished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta). Zamawiający zastrzega sobie możliwość sprawdzenia stanu urządzenia u producenta, w przypadku wątpliwości Zamawiającego, co do pochodzenia Przedmiotu Zamówienia na podstawie jego numerów seryjnych. W takim przypadku Wykonawca dostarczy na żądanie Zamawiającego dokument od producenta lub przedstawiciela producenta w Polsce (oficjalnego biura producenta w Polsce) potwierdzający stan urządzeń z dokładnością do pojedynczych modułów/kart zainstalowanych w urządzeniu.
3. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu, producenta, jak i daty produkcji (dopuszczalna data jednoznacznie określona w BIOS/Firmware).
4. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie elektronicznej w języku polskim lub angielskim. Wersja angielska dopuszczalna jest w przypadku braku dostępności wersji polskiej dokumentacji. Nie dopuszcza się przesłania dokumentacji w formacie linków do stron czy też w formie wymagającej posiadanie płatnego oprogramowania/ posiadania konta w portalu producenta w celu jej odczytania.
5. Do każdego urządzenia musi być dostarczony niezbędny sprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu dostawy wskazanym przez Zamawiającego. Sprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
6. Wszystkie urządzenia muszą posiadać oznakowanie CE.
7. Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL) lub nie może być wskazana data wejścia urządzenia w EOL (brak wsparcia producenta lub wycofanie urządzenia z oficjalnej dystrybucji).
8. Wszystkie urządzenia elektryczne muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
9. Wszystkie dostarczane urządzenia muszą być publicznie dostępne. Zamawiający nie dopuszcza stosowania urządzeń dedykowanych, stworzonych na potrzeby niniejszego zamówienia.

10. Wszystkie odpady związane z dostawami i realizacją Przedmiotu Zamówienia Wykonawca usunie na własny koszt, poza teren Zamawiającego, zgodnie z przepisami obowiązującymi na terenie Rzeczpospolitej Polski.
11. Do wszystkich urządzeń posiadających gniazda na wkładki należy dostarczyć komplet wkładek w celu obsadzenia wszystkich gniazd. Wraz z gniazdami należy dostarczyć niezbędne licencję bezterminowe w celu aktywacji gniazda jeśli takie są wymagane.
12. Dla sprzętu sieciowego należy dostarczyć komplet przewodów sygnałowych (patchcordy miedziane, światłowodowe itp.) w celu poprawnego podłączenia urządzeń w miejscu instalacji.
13. Wymagane jest, aby składnikami oferowanej infrastruktury serwerowej były urządzenia zintegrowane i zwalidowane przez producenta (lub zespół producentów) na etapie procesu produkcyjnego. Pod pojęciem walidacji Zamawiający rozumie zaprojektowanie, wykonanie i testy wszystkich elementów do wzajemnej prawidłowej współpracy.
14. Wymagane jest, aby Infrastruktura serwerowa była gotowym produktem posiadającym nazwę handlową i złożonym z zamkniętej, ściśle zdefiniowanej listy komponentów posiadających odpowiednie numery katalogowe.
15. Dostarczane oprogramowanie musi zostać dostarczonej w najnowszej stabilnej wersji chyba, że Zamawiający wyrazi zgodę na instalację starszej wersji.
16. Wykonawca jest zobowiązany do doboru odpowiednich, do przewidywanych odległości pomiędzy poszczególnymi urządzeniami, typów wkładek do interfejsów komunikacyjnych. Dobór zostanie zrealizowany na etapie analizy przedwykonawczej.

Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

4.1 Specyfikacja ilościowa Zamówienia podstawowego

Zamawiający w ramach realizacji Przedmiotu Zamówienia wymaga dostarczenia poniższych elementów infrastruktury:

Tabela 2 Specyfikacja ilościowa

Lp.	Nazwa	Liczba kompletów
1.	Przełącznik sieciowy Typ A	4
2.	Przełącznik sieciowy Typ B	2
3.	Przełącznik sieciowy Typ C	2
4.	Przełącznik sieciowy Typ D	2
5.	Przełącznik sieciowy Typ E	4
6.	Urządzenie ochrony przed rozproszonymi atakami sieciowymi	2
7.	Systemy analizy i zarządzania	1
8.	Serwer RACK	10
9.	Przełącznik SAN	4
10.	Macierz typ 1	1
11.	Macierz typ 2	1

4.2 Specyfikacja techniczna Infrastruktury sieciowej

4.2.1 Przełącznik sieciowy Typ A

Tabela 3 Opis parametrów Przełącznik sieciowy Typ A – Rozbudowa obecnej infrastruktury sieciowej

Lp.	Nazwa parametru	Opis parametru
1.	Przełącznik musi posiadać	a. Min. 48 portów 1/10/25G definiowanych za pomocą wkładek SFP/SFP+ b. Min. 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m).
2.	Parametry wydajnościowe	a. Prędkość przełączania wirespeed dla wszystkich portów b. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3.	Przełącznik musi posiadać następującą funkcjonalność dla warstwy L2:	a. Trunking IEEE 802.1Q VLAN; b. Wsparcie dla 3000 sieci VLAN; c. Wsparcie sprzętowe dla 90 tysięcy adresów MAC; d. IEEE 802.1w Rapid Spanning Tree (RST); e. IEEE 802.1s Multiple Spanning Tree (MST); f. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU); g. Internet Group Management Protocol (IGMP) Versions 2, 3; h. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach; i. Link Aggregation Control Protocol (LACP): IEEE 802.3ad; j. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów); k. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN; l. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI;
4.	Przełącznik musi posiadać następującą funkcjonalność dla warstwy L3:	a. Sprzętowe przełączanie pakietów w warstwie L3 b. Routing w oparciu o trasy statyczne c. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. d. Policy Based Routing (PBR)

		e. VRRP lub HSRP f. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6 g. Wsparcie sprzętowe dla minimum 750 tyś prefixów LPM/ wpisów hosta w tablicy routingu IP h. Wsparcie dla min. 32 VRF i. Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP) j. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast) k. Wsparcie dla IGMPv3 oraz MSDP l. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych m. Obsługa minimum 5000 wpisów dla ACL (access control list)
5.	Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN	a. Zintegrowany, sprzętowy VXLAN Bridging/Routing b. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) c. Implementacja VXLAN BGP EVPN (Ethernet VPN) d. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN) e. Mechanizm wykrywania i zapobiegania efektom pętli w podłączone infrastrukturze L2 poprzez mechanizm VXLAN OAM
6.	Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:	a. Layer 2 IEEE 802.1p (CoS) oraz DSCP b. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6) c. Kolejkowanie bezwzględne (strict-priority) d. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection) e. Ograniczanie ruchu (policing) do zadanej przepływności f. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych g. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb h. Protokół RDMA/RoCE oraz ECN

7.	Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:	a. Obsługa list kontroli dostępu (ACL) i. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu; ii. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); iii. ACL oparte o porty (PACL); b. DHCP Snooping c. ARP Inspection d. IP Source Guard e. Unicast reverse path forwarding (uRPF) f. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast g. Wsparcie dla MACSEC na wszystkich portach. Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie na obecnym etapie. h. Wsparcie dla szyfrowania AES 256 w warstwie overlay (VTEP do VTEP - tunel VXLAN). Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie na obecnym etapie
8.	Przełącznik musi wspierać następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:	a. Port zarządzający 100/1000 Mbps; b. Port konsoli CLI; c. Zarządzanie In-band; d. SSHv2; e. Authentication, authorization, and accounting (AAA); f. RADIUS; g. TACACS+ h. Syslog; i. SNMP v1, v2c, v3; j. Role-Based Access Control RBAC; k. IEEE 802.1ab LLDP l. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) m. 802.1x

		n. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) o. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring) p. Pełen Netflow v9 q. Network Time Protocol (NTP); r. Precision Time Protocol IEEE 1588 s. Diagnostyka procesu BOOT; t. Ping u. Traceroute
9.	Telemetria z control/data plane eksportowana w interwałach co najmniej 100 milisekund bezpośrednio z układu ASIC przełącznika. Wsparcie dla narzędzi programistycznych w standardzie „OpenTelemetry”. Eksportowane dane w formacie gRPC lub GPB dostarczają następujące informacje (dla każdego przepływu/flow	a. Informacji o przepływie (flow), zawierają dane o adresach IP, protokołach, portach, kiedy przepływ się rozpoczął, jak długo przepływ był aktywny , ile było w nim sumarycznie danych itp. b. Zmienność między pakietami, daje wgląd w zmiany pomiędzy pakietami w danym przepływie. Przykłady obejmują zmiany czasu życia (TTL), flagi IP i TCP, długość payload itp. c. Szczegóły kontekstu przepływu, informacje te są uzyskiwane poza nagłówkiem pakietu, w tym zmiany w wykorzystaniu bufora kolejki, powód odrzucania pakietów w przepływie (bufor, routing, ACL), powiązanie z końcami tunelu VXLAN (VTEP) itp. d. Dodatkowo funkcjonalność telemetrii pozwalająca na pozyskanie metadanych o każdym przepływie, który spełnia określone kryteria (np. odrzucenie, opóźnienie, microburst) z dodatkowymi informacjami identyfikującymi przyczynę (np. ACL/routing/bufor drop, opóźnienie dla scieżki, wystąpienie microburst itp.) e. Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie
10.	Narzędzia programowania i	a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API

	zarządzania przełącznikiem	b. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika c. Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. d. Interfejs programistyczny REST API wraz z upublicznionym SDK e. Możliwość zainstalowania klienta Chef f. Możliwość zainstalowania agenta Puppet
11.	Zasilacze	Przełącznik musi być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej, wyrzut powietrza od strony portów liniowych. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania
12.	Obudowa	Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19
13.	Tryb pracy	Urządzenie ma mieć możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym (kontrolerem sieci SDN).
14.	Wyposażenie przełącznika musi obejmować	a. wkładki QSFP 100/40GE umożliwiające połączenie 100GE lub 40GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional) b. wkładki SFP+ typu 10GBASE-SR
15.	Gwarancja	a. Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); b. Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii.
16.	Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą	a. Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej

	przez cały okres gwarancji i obejmuje	b. Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji.
17.	Wyposażenie przełącznika	a) Wkładki QSFP 100/40GE umożliwiające połączenie 100GE lub 40GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional) b) Wkładki SFP+ typu 10GBASE-SR

Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

4.2.2 Przełącznik sieciowy Typ B

Tabela 4 Wymagania dla przełącznika sieciowego Typ B

Lp.	Nazwa parametru	Opis parametru
1.	Typ i liczba portów	48 portów 10/100/1000BaseT RJ-45 + uplink 4x10G SFP+
2.	Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:	• Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet typu twinax (SFP+ - SFP+) • 10Gigabit Ethernet typu twinax (SFP+ - SFP+), • 25Gigabit Ethernet 25GBASE-SR, • 25Gigabit Ethernet typu twinax (SFP28 – SFP28), • 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF), • 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)
3.	Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:	• Przepustowość w ramach stosu - 80Gb/s, • 8 urządzeń w stosie, • Zarządzanie poprzez jeden adres IP, • Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
4.	Zasilanie i chłodzenie:	• Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), • Redundantne wentylatory,
5.	Parametry wydajnościowe:	• Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 256 Gb/s (z podłączeniem do stosu) • Prędkość przesyłania (forwarding rate): 130.95 Mpps • Bufor pakietów – 6MB • Pamięć DRAM – 2GB • Pamięć flash – 4GB

		• Obsługa: ○ 500 aktywnych sieci VLAN ○ 16000 adresów MAC ○ 3000 tras IPv4 ○ 1500 tras IPv6 ○ Ilość wpisów w listach kontroli dostępu Security ACL – 1000 ○ ilość wpisów w listach kontroli dostępu QoS ACL – 1000 ○ 512 interfejsów SVI L3 ○ 48 połączeń zagregowanych typu „port channel” ○ 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP ○ Jumbo frame 9198B
6.	Protokoły	• Obsługa protokołu NTP • Obsługa IGMPv1/2/3 i MLDv1/2 Snooping • Obsługa protokołu LLDP i LLDP-MED
7.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:	• IEEE 802.1w Rapid Spanning Tree • Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1s Multi-Instance Spanning Tree • Obsługa 64 instancji protokołu STP • Wsparcie dla protokołu REP (Resilient Ethernet Protocol) • Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku podstawowego
8.	Możliwość uruchomienia funkcji serwera DHCP 14. Mechanizmy związane z	• Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, • Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, • Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,

	bezpieczeństwem sieci: Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilegelevel),	• Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, • Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, • Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, • Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – • 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), • Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, • Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), • Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, • Obsługa list kontroli dostępu (ACL) następujących typów: • Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, • VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, • Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); • Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA), • Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), • Funkcja Private VLAN z obsługą dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej

		prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS, • Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci,
9.	Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:	• sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, • sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
10.	Mechanizmy związane z zapewnieniem jakości usług w sieci:	• Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, • Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do • innych (Strict Priority), • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: • źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), • Kontrola sztormów dla ruchu broadcast/multicast/unicast, • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
11.	Obsługa protokołów i mechanizmów routingu:	• Routing statyczny dla IPv4 i IPv6, • Routing dynamiczny – RIP, OSPF do 1000 routes • Policy-based routing (PBR), • Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup, • Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
12.	Dodatkowe wymagania	• Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na

		nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, • RSPAN, • Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego, • Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane • zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), • Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ) • Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
13.	Funkcjonalność sondy IP SLA Responder, 22. Zarządzanie	• Port konsoli, • Dedykowany port Ethernet do zarządzania out-of-band, • Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA, • Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, • Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog, • Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania

		zdefiniowanych według potrzeb danych do zewnętrznych systemów, • Wsparcie dla protokoły RESTCONF, Wsparcie dla protokołu gNMI, • Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych, • Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą, • Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB, • Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym • (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne • bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,
14.	Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający	a) Monitoring pracy przełącznika w zakresie: a. Użycie CPU, użycie pamięci, temperatura pracy, b. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny, c. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, d. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router) E. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, e. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,

f. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
g. Protokół REP (Resilient Ethernet Protocol),
h. Protokół STP (Spanning Tree Protocol),
i. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),

b) Konfigurację przełącznika w zakresie:
a. Konfiguracja interfejsów:
i. Fizycznych:

- - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
- - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),
- - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,
- - przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

ii. ogicznych typu „port channel":

- opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,
- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla
- portu dostępowego, natywna sieć VLAN,
- przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla

		kontroli sztormów braodcastowych, multicastowych i unicastowych) iii. Wirtualnych typu SVI: • opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP) • Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN, • Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), • Konfiguracja mechanizmów SPAN i RSPAN, • Konfiguracja protokołu STP, ⍰⍰ Konfiguracja protokołu REP, • Konfiguracja routingu statycznego i dynamicznego, • Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów, • Tworzenie i przypisanie list kontroli dostępu ACL, • Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, • Konfiguracja i uruchomienie NetFlow, • Konfiguracja polityk QoS, • Administracja przełącznika w zakresie: • Zdalne uruchamianie komend linii poleceń, • Nazwa przełącznika, • Tryb pracy L2/L3, • Adres IP przełącznika do celów zarządzania zdalnego, • Konfiguracja serwera DHCP, • Konfiguracja DNS, • Czas systemowy w tym protokół NTP, • Konta administracyjne, • Upgrade oprogramowania, ⍰⍰ Backup konfiguracji,

		• Zdalny restart urządzenia, Konfiguracja i dostęp przez SNMP, Diagnostyka urządzenia: • Narzędzie PING i TRACEROUTE, • Przeglądanie logów systemowych, • Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
15.	Parametry fizyczne	• Przystosowany do montażu w szafie rack 19”, • Wysokość urządzenia 1 RU, • Głębokość chassis urządzenia bez wentylatorów i zasilaczy: mniejsza niż 30 cm Głębokość chassis urządzenia z wentylatorami i zasilaczami: mniejsza niż 33 cm
16.	Ukompletowanie urządzenia	• Przełącznik wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania, • Przełącznik wyposażony w moduł do łączenia w stos wraz z kablem stakującym o długości 3m, • Przełącznik wyposażony w następujące wkładki interfejsowe: 10Gigabit Ethernet 10GBase-SR, • Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat
17.	Gwarancja i wsparcie techniczne	• Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); • Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii. • Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą przez cały okres gwarancji i obejmuje:

		○ Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej ○ Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji

4.2.3 Przełącznik sieciowy Typ C

4.2.4 Tabela 5 Wymagania dla przełącznika sieciowego Typ C

Lp.	Nazwa parametru	Opis parametru
1.	Typ i liczba portów:	48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP
2.	Moc dostępna dla PoE:	740W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie redundantnym),
3.	Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:	• Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
4.	Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:	• Przepustowość w ramach stosu - 80Gb/s, • 8 urządzeń w stosie, • Zarządzanie poprzez jeden adres IP, • Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
5.	Zasilanie i chłodzenie:	• Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap),

		• W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika), • Redundantne wentylatory,
6.	Parametry wydajnościowe:	• Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 256 Gb/s (z podłączeniem do stosu) • Prędkość przesyłania (forwarding rate): 130.95 Mpps • Bufor pakietów – 6MB • Pamięć DRAM – 2GB • Pamięć flash – 4GB • Obsługa: o 500 aktywnych sieci VLAN o 16000 adresów MAC o 3000 tras IPv4 o 1500 tras IPv6 o Ilość wpisów w listach kontroli dostępu Security ACL – 1000 o ilość wpisów w listach kontroli dostępu QoS ACL – 1000 o 512 interfejsów SVI L3 o Jumbo frame 9198B o 48 połączeń zagregowanych typu „port channel” o 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
7.	Obsługa protokołów	• Obsługa protokołu NTP • Obsługa IGMPv1/2/3 i MLDv1/2 Snooping • Obsługa protokołu LLDP i LLDP-MED
8.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci	• IEEE 802.1w Rapid Spanning Tree • Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1s Multi-Instance Spanning Tree • Obsługa 64 instancji protokołu STP • Wsparcie dla protokołu REP (Resilient Ethernet Protocol) • Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem

		podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku podstawowego
9.	Dodatkowe funkcje	• Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ) • Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego • Możliwość uruchomienia funkcji serwera DHCP • Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN, • Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego, • Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
10.	Mechanizmy związane z bezpieczeństwem sieci:	• Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), • ·Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, • Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

		• · Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, • Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, • ·Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, • ·Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, • Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – • 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), • Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, • Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), • Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, Obsługa list kontroli dostępu (ACL) następujących typów: o Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, o VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, o Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, o Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); • Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika(dla połączeń switch-switch)

		kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA), • Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), • Funkcja Private VLAN z obsługą dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS, • Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci,
11.	Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:	• sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, • bezpieczna sekwencja uruchamiania, • sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
12.	Mechanizmy związane z zapewnieniem jakości usług w sieci:	• Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, • Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), • Kontrola sztormów dla ruchu broadcast/multicast/unicast, • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

13.	Obsługa protokołów i mechanizmów routingu:	• Routing statyczny dla IPv4 i IPv6, • Routing dynamiczny – RIP, OSPF do 1000 routes, • Policy-based routing (PBR), • Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup, • Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
14.	Funkcjonalność sondy IP SLA Responder, 23. Zarządzanie	• Port konsoli, • Dedykowany port Ethernet do zarządzania out-of-band, • Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA, • Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, • Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog, • Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, • Wsparcie dla protokoły RESTCONF, • Wsparcie dla protokołu gNMI, • Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych, • Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą, • Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB • Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki

		• logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące, • wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: a. Monitoring pracy przełącznika w zakresie: i. Użycie CPU, użycie pamięci, temperatura pracy, ii. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny, iii. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, iv. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router) v. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, vi. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, vii. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik, Protokół REP (Resilient Ethernet Protocol), viii. IProtokół STP (Spanning Tree Protocol), ix. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy), b. Konfigurację przełącznika w zakresie: i. Konfiguracja interfejsów:

		1. Fizycznych: • - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, • - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP), • - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy • MAC przełącznika), konfiguracja 802.1x, • - przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) 2. Logicznych typu „port channel”: • opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, • w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, • w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) 3. Wirtualnych typu SVI: • opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do” oraz „z”, parametry protokołu DHCP Relay (adres IP serwera DHCP) Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,

		• Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu • (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), • Konfiguracja mechanizmów SPAN i RSPAN, • Konfiguracja protokołu STP, • Konfiguracja protokołu REP, Konfiguracja routingu statycznego i dynamicznego, Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów, Tworzenie i przypisanie list kontroli dostępu ACL, • Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, • Konfiguracja i uruchomienie NetFlow, • Konfiguracja polityk QoS, • Administracja przełącznika w zakresie: • Zdalne uruchamianie komend linii poleceń, • Nazwa przełącznika, • Tryb pracy L2/L3, • Adres IP przełącznika do celów zarządzania zdalnego, • Konfiguracja serwera DHCP, • Konfiguracja DNS, • Czas systemowy w tym protokół NTP, • Konta administracyjne, • Upgrade oprogramowania, • Backup konfiguracji, • Zdalny restart urządzenia, • Konfiguracja i dostęp przez SNMP, • Diagnostyka urządzenia: • Narzędzie PING i TRACEROUTE, • Przeglądanie logów systemowych, • Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
15.	Parametry fizyczne:	• Możliwość montażu w szafie rack 19”,

		• Wysokość urządzenia 1 RU, • Głębokość chassis urządzenia bez wentylatorów i zasilaczy: mniejsza niż 30 cm • Głębokość chassis urządzenia z wentylatorami i zasilaczami: mniejsza niż 33 cm
16.	Ukompletowanie urządzenia	• Przełącznik wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania, • Przełącznik wyposażony jest w moduł do łączenia w stos wraz z kablem stakującym o długości 1m, · Przełącznik wyposażony jest w następujące wkładki interfejsowe: 10Gigabit Ethernet 10GBase-SR, • Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat,
17.	Gwarancja i wsparcie techniczne	• Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); • Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii. Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą przez cały okres gwarancji i obejmuje: o Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej o Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji.

Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

4.2.5 Przełącznik sieciowy Typ D

4.2.6 Tabela 6 Wymagania dla przełącznika sieciowego Typ D

Lp.	Nazwa parametru	Opis parametru
1.	Przełącznik musi posiadać:	• 48 portów 1000BaseT lub 1/10GBASE-T • 6 portów uplink, w tym min. 2 porty 40/100GE definiowane za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m).
2.	Parametry wydajnościowe:	• Prędkość przełączania 348Gbps full duplex • Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3.	Przełącznik posiada następującą funkcjonalność dla warstwy L2:	a) Trunking IEEE 802.1Q VLAN; b) Wsparcie dla 3000 sieci VLAN; c) Wsparcie sprzętowe dla 90 tysięcy adresów MAC d) IEEE 802.1w Rapid Spanning Tree (RST) e) IEEE 802.1s Multiple Spanning Tree (MST) f) Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU) g) Internet Group Management Protocol (IGMP) Versions 2, 3; h) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach i) Link Aggregation Control Protocol (LACP): IEEE 802.3ad j) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów); k) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN l) Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4.	Przełącznik posiada następującą funkcjonalność dla warstwy L3:	a) Sprzętowe przełączanie pakietów w warstwie L3 b) Routing w oparciu o trasy statyczne c) Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. d) Policy Based Routing (PBR) e) VRRP f) Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6 g. Tunele GRE g) Wsparcie sprzętowe dla minimum 750 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP i. Wsparcie dla min. 32 VRF

		h) Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP) i) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast) j) Wsparcie dla IGMPv3 oraz MSDP k) Wsparcie sprzętowe dla minimum 32,000 tras multicastowych l) Obsługa minimum 5000 wpisów dla ACL (access control list)
5.	Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:	a) Zintegrowany, sprzętowy VXLAN Bridging/Routing b) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) c) Implementacja VXLAN BGP EVPN (Ethernet VPN) d) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności e) Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN) f) Mechanizm wykrywania i zapobiegania efektom pętli w podłączone infrastrukturze L2 poprzez mechanizm VXLAN OAM
6.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:	a) Layer 2 IEEE 802.1p (CoS) oraz DSCP b) Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6) c) Kolejkowanie bezwzględne (strict-priority) d) Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection) e) Ograniczanie ruchu (policing) do zadanej przepływności f) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych g) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb h) Protokół RDMA/RoCE, DCBX oraz ECN
7.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci	a) Obsługa list kontroli dostępu (ACL) b) ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu; c) ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), d) TCP, User Datagram Protocol (UDP); e) ACL oparte o porty (PACL); f) DHCP Snooping g) ARP Inspection h) IP Source Guard

		i) Unicast reverse path forwarding (uRPF) j) Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast k) MacSec na portach SFP+ i QSFP28. Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie
8.	Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:	a) Port zarządzający 100/1000 Mbps; b) Port konsoli CLI; c) Zarządzanie In-band; d) SSHv2; e) Authentication, authorization, and accounting (AAA); f) RADIUS; g) TACACS+ h) Syslog; i) SNMP v1, v2c, v3; j) Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB. k. Role-Based Access Control RBAC; k) IEEE 802.1ab LLDP l) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) n. 802.1x m) Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) n) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring) o) Network Time Protocol (NTP); p) Precision Time Protocol IEEE 1588 q) Diagnostyka procesu BOOT; r) Ping s) Traceroute
9.	Telemetria z control/data plane eksportowana w interwałach co najmniej 100 milisekund bezpośrednio z	a) Informacji o przepływie (flow), zawierają dane o adresach IP, protokołach, portach, kiedy przepływ się rozpoczął, jak długo przepływ był aktywny , ile było w nim sumarycznie danych itp. b) Zmienność między pakietami, daje wgląd w zmiany pomiędzy pakietami w danym przepływie. Przykłady obejmują zmiany czasu życia (TTL), flagi IP i TCP, długość payload itp.

	układu ASIC przełącznika. Wsparcie dla narzędzi programistycznych w standardzie „OpenTelemetry". Eksportowane dane w formacie gRPC lub GPB dostarczają następujące informacje (dla każdego przepływu/flow	Szczegóły kontekstu przepływu, informacje te są uzyskiwane poza nagłówkiem pakietu, w tym zmiany w wykorzystaniu bufora kolejki, powód odrzucania pakietów w przepływie (bufor, routing, ACL), powiązanie z końcami tunelu VXLAN (VTEP) itp. c) Dodatkowo funkcjonalność telemetrii pozwalająca na pozyskanie metadanych o każdym przepływie, który spełnia określone kryteria (np. odrzucenie, opóźnienie, microburst) z dodatkowymi informacjami identyfikującymi przyczynę (np. ACL/routing/bufor drop, opóźnienie dla scieżki, wystąpienie microburst itp.) d) Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie na tym etapie
10.	Narzędzia programowania i zarządzania przełącznikiem:	a) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API b) Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika c) Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. d) Interfejs programistyczny REST API wraz z upublicznionym SDK e) Możliwość zainstalowania klienta Chef f) Możliwość zainstalowania agenta Puppet g) Wsparcie dla OpenStack Neutron plugin
11.	Ogólne parametry	a) Przełącznik jest wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz b) wentylatory w konfiguracji zapewniającej, wyrzut powietrza od strony portów liniowych; c) bud owa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19". d) Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym (kontrolerem sieci SDN).

12.	Wyposażenie przełącznika musi obejmować:	a) wkładki QSFP 100/40GE umożliwiające połączenie 100GE lub 40GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional) wkładki SFP+ typu 10GBASE-SR
13.	Gwarancja	b) Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); c) Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii. d) Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą przez cały okres gwarancji i obejmuje: Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej e) Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji.

4.2.7 Przełącznik sieciowy Typ E

Tabela 7 Opis parametrów Przełącznik sieciowy Typ E

Lp.	Nazwa parametru	Opis parametru
1.	Wymagania dotyczące portów	a) min. 32 porty 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m). b) min. 2 porty 10GE definiowane za pomocą wkładek SFP+
2.	Parametry wydajnościowe:	a) Prędkość przełączania 3.2Tbps full duplex b) Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3.	Przełącznik posiada następującą funkcjonalność dla warstwy L2:	a) Trunking IEEE 802.1Q VLAN; b) Wsparcie dla 3000 sieci VLAN; c) Wsparcie sprzętowe dla 90 tysięcy adresów MAC d) IEEE 802.1w Rapid Spanning Tree (RST) e) IEEE 802.1s Multiple Spanning Tree (MST) f) Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU) g) Internet Group Management Protocol (IGMP) Versions 2, 3; h) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach i) Link Aggregation Control Protocol (LACP): IEEE 802.3ad; j) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów); k) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN l) Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4.	Przełącznik posiada następującą funkcjonalność dla warstwy L3:	a) Sprzętowe przełączanie pakietów w warstwie L3 b) Routing w oparciu o trasy statyczne c) Umożliwia rozbudowę poprzez licencje o funkcjonalności warstwy L3 – OSPF, BGP, IS-IS dla protokołów IPv4 oraz IPv6 d) Policy Based Routing (PBR)

		e) VRRP f) Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6 g) Tunele GRE h) Wsparcie sprzętowe dla minimum 250 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP i) Wsparcie dla min. 32 VRF j) Wybór do 16-tu jednoczesnych ścieżek o równej metryce (ECMP) k) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast) l) Wsparcie dla IGMPv3 oraz MSDP m) Wsparcie sprzętowe dla minimum 32,000 tras multicast n) Obsługa minimum 5000 wpisów dla ACL (access control list) o)
5.	Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN	a) Zintegrowany, sprzętowy VXLAN Bridging/Routing b) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) c) Implementacja VXLAN BGP EVPN (Ethernet VPN) d) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN
6.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci	a) Layer 2 IEEE 802.1p (CoS) oraz DSCP b) Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6) c) Kolejkowanie bezwzględne (strict-priority) d) Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection) e) Ograniczanie ruchu (policing) do zadanej przepływności f) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych g) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
7.	Przełącznik wspiera następujące mechanizmy	a) Obsługa list kontroli dostępu (ACL) 1. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;

	związane z zapewnieniem bezpieczeństwa w sieci	2. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); 3. ACL oparte o porty (PACL); b) DHCP Snooping c) ARP Inspection d) IP Source Guard e) Unicast reverse path forwarding (uRPF) f) Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast g) Wsparcie dla MACSEC na co najmniej 4 portach 100G
8.	Urządzenie realizuje następujące funkcjonalności dotyczące zarządzania i zabezpieczenia:	a) Port zarządzający 100/1000 Mbps; b) Port konsoli CLI; c) Zarządzanie In-band; d) SSHv2; e) Authentication, authorization, and accounting (AAA); f) RADIUS; g) TACACS h) Syslog; i) SNMP v1, v2, v3; j) Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB. k) Role-Based Access Control RBAC; l) IEEE 802.1ab LLDP m) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) n) 802.1x o) Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) p) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring) q) Network Time Protocol (NTP); r) Precision Time Protocol IEEE 1588

		s) Diagnostyka procesu BOOT; t) Ping u) Traceroute
9.	Narzędzia programowania i zarzadzania przełącznikiem:	a) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API b) Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika c) Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. d) Interfejs programistyczny REST API wraz z upublicznionym SDK e) Możliwość zainstalowania klienta Chef f) Możliwość zainstalowania agenta Puppet
10.	Zasilanie i wentylacja	Przełącznik jest wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych
11.	Obudowa	Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
12.	Tryb pracy	Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym (kontrolerem sieci SDN).
13.	Wyposażenie przełącznika	c) **W**kładki QSFP 100/40GE umożliwiające połączenie 100GE lub 40GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional) d) Wkładki SFP+ typu 10GBASE-SR
14.	Gwarancja	a) Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); **b)** Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii.

15.	Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą przez cały okres gwarancji i obejmuje:	a) Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej b) Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji.

Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

4.2.8 Urządzenie ochrony przed rozproszonymi atakami sieciowymi

Tabela 8 Wymagania dla Urządzenia ochrony przed rozproszonymi atakami sieciowymi

Lp.	Opis parametru
1.	System musi realizować co najmniej następujące funkcje: a. Rozkład ruchu pomiędzy serwerami aplikacji Web b. Selektywny http caching c. Selektywna kompresja danych d. Terminowanie sesji SSL e. Filtrowanie pakietów f. Optymalizacja i akceleracja aplikacji
2.	Wszystkie wymienione w niniejszym dokumencie funkcje muszą być dostępne w obrębie jednego urządzenia.
3.	Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.
4.	System musi posiadać co najmniej następujące metody równoważenia obciążenia: a. Cykliczna b. Ważona c. Najmniejsza liczba połączeń d. Najszybsza odpowiedź serwera e. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera f. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie g. Dynamicznie ważona oparta na SNMP/WMI h. Definiowana na podstawie grupy priorytetów dla serwerów
5.	Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy: a. Analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów b. Obsługa protokołów: http, tcp, xml, rtsp, sip c. Musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS
6.	Język skryptowy musi bazować na języku programowania Tool Command Language lub równoważnym, z własnymi komendami.

7.	Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego.
8.	Producent systemu musi dostarczyć darmową, specjalizowaną aplikację do analizy poprawności składni skryptów pisanych przy wykorzystaniu języka skryptowego opisanego w punkcie 6. Aplikacja musi posiadać wbudowane szablony skryptów oraz funkcję automatycznego uzupełniania wpisywanych komend.
9.	Rozwiązanie musi pracować w trybie pełnego proxy.
10.	Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.
11.	Rozwiązanie musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji.
12.	Funkcjonalność lokalnego równoważenia obciążenia a. Wspierane mechanizmy równoważenia obciążenia: round robin, ważona, dynamicznie ważona (na podstawie SNMP/WMI), najmniejsza liczba połączeń, najszybsza odpowiedź, observed, predictive, grupy priorytetów, możliwość modyfikacji za pomocą języka skryptowego b. Buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera c. Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług d. Obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert, passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID e. Wsparcie dla usług warstw 4-7: inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, ochrona przed atakami DoS/DDoS i SYN Flood, multipleksacja zapytań HTTP, kompresja i cache'owanie HTTP
13.	Optymalizacja i akceleracja aplikacji: a. Urządzenie musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci: I. LAN II. WAN III. CELL (komórkowy)

	b. Urządzenie powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta. c. Urządzenie musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control) d. Urządzenie musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP e. Urządzenie musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od: I. Listy dozwolonych URI II. Listy wykluczonych URI III. Listy kompresowalnych Content-Type IV. Listy wykluczonych Content-Type
14.	System musi posiadać co najmniej następujące interfejsy administracyjne: a. GUI przy wykorzystaniu protokołu https b. Zarządzanie poprzez SSH c. Zarządzanie poprzez SOAP-SSL d. Zarządzanie poprzez API REST
15.	Autoryzacja administratorów systemu musi bazować na rolach użytkowników
16.	System musi posiadać funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu co najmniej następujących atrybutów:Cookie (hash, rewrite, custom, insert, passive) a. Adres źródła b. SIP call ID c. Identyfikator sesji SSL d. Microsoft Terminal Services (RDP) – nazwa użytkownika e. Adres docelowy f. Tworzone przez administratora systemu przy wykorzystaniu języka skryptowego z punktu 5
17.	System musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.
18.	System musi zapewniać możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS.
19.	System musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów.
20.	Sprzętowe wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy.

21.	Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów.
22.	System musi zawierać wsparcie dla TLS 1.3, HTTP2.0, QUICK, DoT, DoH.
23.	System musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów.
24.	System musi obsługiwać sieci VLAN w standardzie IEEE 802.1q..
25.	System musi obsługiwać agregację linków w standardzie IEEE 802.3ad (LACP).
26.	System musi obsługiwać Jumbo Frames.
27.	System musi umożliwiać weryfikację działającego na urządzeniu firmware, czy nie uległ on modyfikacji (TPM Chain of Custody).
28.	System musi świadczyć, co najmniej następujące usługi w warstwach 4-7: a. Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http b. Ukrywanie zasobów c. Zmiana odpowiedzi serwera d. Przepisywanie odpowiedzi (response rewriting) e. Ochrona przed atakami typu SYN Flood f. Multipleksowanie połączeń http
29.	System musi posiadać następujące funkcje zarządzania siecią: a. Obsługa protokołu SNMP v1/v2c/v3 b. Zewnętrzny syslog c. Zbieranie danych i ich wyświetlanie d. Zbieranie danych zgodnie z ustawieniami administratora e. Osobna brama domyślna dla interfejsu zarządzającego f. Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot) g. Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy) h. Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.
30.	System musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.
31.	System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablonypowinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.

32.	System musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki: a. Czas odpowiedzi per serwer b. Czas odpowiedzi per URI c. Ilość sesji użytkownika d. Przepustowość e. Adres źródła f. Kraj g. User Agent (wykorzystywana przez klienta aplikacja) h. Metoda dostępu
33.	System musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL.
34.	Rozwiązanie musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji.
35.	Rozwiązanie musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. Musi umożliwiać poprawnie działanie rozwiązania, kiedy podłączone VLANy do urządzenia mają takie same podsieci i adresy IP.
36.	Rozwiązanie musi oferować stworzenie wielu partycji administracyjnych oraz wielu jednoczesnych domen routingu. Partycje administracyjne i domeny routingu muszą być dostępne również, jeżeli urządzenie pracuje w formie klastra.
37.	Rozwiązania musi być dostarczone w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń sprzętowych tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1.
38.	38. Urządzenie musi umożliwiać podział urządzenia na wirtualne części, przy czym każda taka część musi pracować logicznie jako niezależne urządzenie z niezależnym oprogramowaniem(każda cześć może posiadać inną wersję oprogramowania oraz osobną tablice routingu). Urządzenie musi umożliwić podział na minimum 8 wirtualnych części.
39.	W ramach klastra musi istnieć możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych.
40.	Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu
41.	Klaster wysokiej dostępności musi zapewniać synchronizację:

	a. Konfiguracji b. Stanu połączeń c. Przywiązywania sesji (Session persistence)
42.	Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu, co najmniej następujących metod: a. Weryfikacja stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover)
43.	43. Urządzenia muszą być objęte min. 12 miesięczną gwarancją producenta. W ramach gwarancji Zamawiający nabywa prawo do: a. Dostępu do aktualnych wersji oprogramowania, różnego rodzaju poprawek oraz dokumentacji producenta b. Sposobu obsługi zgłoszeń gwarancyjnych w trybie 5x10 c. Wymiany uszkodzonego sprzętu lub kluczowych elementów warunkujących jego pracę w miejscu instalacji (on-site) nie później niż następnego dnia roboczego po identyfikacji usterki (tryb 8x5xNBD). d. W przypadku wymiany dysku twardego, uszkodzony dysk pozostaje w dyspozycji Zamawiającego.
44.	System w postaci jednego urządzenia musi spełniać wymogi przedstawione w tabeli poniżej.
45.	System musi mieć możliwość licencyjnej rozbudowy do obsługi przepustowości nie mniejszej niż 95 Gbps w warstwie 7

Tabela 9 Wymagania dla jednego urządzenia ochrony przed rozproszonymi atakami sieciowymi

Lp.	Nazwa parametru	Opis parametru
1.	Pamięć	Nie mniej niż 128 GB
2.	Dysk Twardy	Jeden dysk SSD o pojemności nie mniejszej niż 1 TB
3.	Przepływność dla warstwy 4	Nie mniej niż 95 Gbps
4.	Przepływność dla warstwy 7	Nie mniej niż 60 Gbps
5.	Ilość połączeń na sekundę w warstwie 7	Nie mniej niż 350 tysięcy

6.	Ilość jednocześnie obsługiwanych połączeń	Nie mniej niż 75 milionów
7.	Ilość transakcji SSL na sekundę dla klucza o długości 2048	Nie mniej niż 60 tysięcy
8.	Ilość transakcji SSL na sekundę dla szyfrowania ECC (ECDHE-ECDSA-AES128-SHA256)	Nie mniej niż 30 tysięcy
9.	Przepływność ruchu szyfrowanego	Nie mniej niż 35 Gbps
10.	Ilość połączeń na sekundę w warstwie 4	Nie mniej niż 1 milion
11.	Kompresja sprzętowa	Nie mniej niż 35 Gbps
12.	Sprzętowa ochrona DDoS	Nie mniej niż 80 milionów SYN cookies na sekundę
13.	Gęstość interfejsów	Nie mniej niż dwa interfejsy z możliwością obsadzenia wkładkami SFP28/QSFP+ 100Gb/40Gb i nie mniej niż 8 interfejsów z możliwością obsadzenia wkładkami SFP28/SFP+ 25Gb/10 Gb, oddzielny interfejs zarządzania, port konsolowy, port USB 3.0 Należy zapewnić wkładki 40Gb QSFP+ SR oraz wkładki 10Gb SFP+ SR. Dopuszcza się tylko moduły w pełni wspierane przez producenta tego urządzenia.
14.	Zarządzanie	Panel i wyświetlacz LCD (dotykowy) z funkcjami: ustawienia adresu IP na potrzeby zarządzania, ustawienia parametrów portu szeregowego, wyświetlania podstawowych alarmów, możliwości restartu urządzenia, wyświetlania informacji o systemie Funkcjonalność „Always On Management”. Dopuszczane

		równoważne rozwiązania realizujące powyższe wymagania bez zastosowania wyświetlacza LCD lub bez wyświetlacza dotykowego.
15.	Obudowa	Przeznaczona do montażu w szafie rack 19”, wysokość nie większa niż 1 U
16.	Zasilanie	Nie mniej niż dwa redundantne zasilacze - prąd zmienny 230V AC
17.	Wymagana certyfikacja	FCC Class A (Part 15), IC Class A; VCCI Class A EN 55032:2012/AC:2013 Class A EN 55035:2017 EN 300 386 V1.6.1 (2012)

4.3.1 Systemy analizy, zarządzania i monitorowania

Tabela 10 Opis parametrów Systemów analizy i zarządzania

Lp.	Nazwa parametru	Opis parametru
1.	Ogólny opis	Rozwiązanie składa się z redundantnych i uzupełniających się komponentów sprzętowych i programowych tworzących wspólną całość: • Centralny komponent zarządzający - zarządzający siecią fizyczną, wirtualną, kontenerową oraz warstwą logiczną i zapewniający uruchamianie usług w oparciu o modelowanie polityk dla aplikacji. • Centralny systemu analityczny wspierający zarządzanie i diagnostykę, dbający o poprawność implementacji polityk oraz zawierający moduły audytu bezpieczeństwa. • Systemu monitoringu – system monitorowania baz danych i aplikacji
2.	Centralnego komponent zarządzający	1. Zarządza infrastrukturą sieciową złożoną z przełączników 10/25/40/100 GigabitEthernet, zorganizowanych w dwustopniowej nieblokowalnej architekturze rdzeń-brzeg (spine-leaf) określanej jako „IP Fabric”. Opisanych jako Typ-A, Typ-E, oraz posiadanych przez zamawiającego przełączników Nexus N9K-C93360, jeśli dla posiadanych przez zamawiającego przełączników wymagane jest rozszerzenie o dodatkowe licencje należy dostarczyć je w ramach rozwiązania. 2. Jest zrealizowany w oparciu o dedykowaną warstwę sprzętową i programową. Zasoby sprzętowe (CPU, pamięć, dyski, porty sieciowe) są w pełni dedykowane dla oprogramowania zarządzającego. 3. Zrealizowany jest redundantnie (np. w formie klastra kilku instancji) zarówno w warstwie sprzętowej, jak i programowej tak, aby zapewnić spójne działanie środowiska i możliwość modyfikacji konfiguracji po ewentualnej utracie jednej z instancji. 4. Utrata wszystkich instancji klastra nie wpływa na działanie infrastruktury sieciowej w zakresie istniejącej konfiguracji (może wpływać na wprowadzanie do niej zmian). 5. Obsługuje wyłącznie ruch związany z zarządzaniem i monitorowaniem infrastruktury sieciowej (tzw. „control plane”), nie zajmuje się przełączaniem ruchu (tzw. „data plane”).

		6. Umożliwia zarządzanie infrastrukturą sieciową złożoną z 1200 portów i dołączonych do niej 600 fizycznych serwerów dwuprocesorowych w ramach dostarczanych licencji. 7. Umożliwia automatyzację konfiguracji zarządzanej sieci w oparciu o model sieciowych polityk grupowych powiązanych z aplikacjami. 8. Umożliwia wydzielanie izolowanych wirtualnych środowisk sieciowych wraz z dedykowanymi zespołami administratorów i prawami dostępu dla 100 takich środowisk (tzw. „multi-tenant"). 9. Dla izolowanych środowisk sieciowych umożliwia implementację funkcjonalności dedykowanej bramy wyjściowej L2/L3 oraz dedykowanych usług zewnętrznych realizowanych dla warstw 4-7. 10. Umożliwia tworzenie wirtualnych instancji sieciowych umożliwiających nakładanie się adresacji IP w wielu zaimplementowanych równocześnie instancjach (VRF) w liczbie 10 instancji VRF na wirtualne środowisko. 11. Umożliwia jednoczesne konfigurowanie sieci dla środowisk złożonych z: a. Serwerów fizycznych; b. Serwerów wirtualnych realizowanych w oparciu o VMWare vSphere i VMware vCenter; c. Serwerów wirtualnych realizowanych w oparciu o Microsoft HyperV; d. Serwerów wirtualnych realizowanych w oparciu o RedHat KVM i OVS (Open vSwitch) w środowisku OpenStack; e. Kontenerów wirtualnych realizowanych w oparciu o Kubernetes i Openshift. 12. Umożliwia zintegrowanie usług zewnętrznych poprzez zapewnienie szczegółowej konfiguracji i mechanizmu przekierowania ruchu dla warstw 4-7 dla urządzeń Firewall i Loadbalancer posiadanych obecnie: a. Loadbalancer F5; b. Firewall FortiGate; c. Firewall CheckPoint. 13. Umożliwia monitorowanie i diagnostykę sieciową dla uruchamianych środowisk:

		a. Prezentację sprawności bieżącej i historycznej środowiska w formie SLA dla danego środowiska sieciowego oraz modelu polityk aplikacyjnych; b. Prezentowanie bieżącej i historycznej statystyki ruchu dla danego środowiska sieciowego, zdefiniowanych warstw aplikacji oraz interfejsów fizycznych; c. Pomiar ruchu na portach wejściowych i wyjściowych infrastruktury sieciowej dla środowisk uruchamianych w oparciu o model polityk aplikacyjnych; d. Diagnostykę ścieżki (traceroute) między dowolną parą portów fizycznych bądź wirtualnych wchodzących w skład infrastruktury; e. Monitorowanie i raportowanie ilości wykorzystanych i dostępnych zasobów wchodzących w skład infrastruktury; f. Zbieranie, agregowanie i interpretowanie zdarzeń (events) i problemów (faults) w ramach infrastruktury sieciowej; g. Monitorowanie ruchu poprzez kopiowanie (mirroring) ruchu dla wybranych warstw aplikacyjnych. 14. Umożliwia automatyczną detekcję topologii oraz inwentarza infrastruktury sieciowej. 15. Implementuje centralne repozytorium oprogramowania (firmware) dla infrastruktury sieciowej. 16. Implementuje centralny mechanizm aktualizacji oprogramowania (firmware) dla infrastruktury sieciowej. 17. Umożliwia zachowywanie (snapshot) i odtwarzanie (rollback) dla całości konfiguracji infrastruktury sieciowej. 18. Udostępnia następujące interfejsy zarządzające: a. GUI (http/https); b. CLI (linia komend konsoli); c. Plugin dla OpenStack umożliwiający integrację na poziomie Neutron ML2. 19. Udostępnia następujące mechanizmy programowania/API: a. REST API ze wsparciem dla formatu XML; b. Możliwość konfiguracji infrastruktury bezpośrednio poprzez http, np. z wykorzystaniem Postman REST Client; c. Python SDK;

		d. Udostępnione przez producenta playbooki dla Ansible i Terraform e. Powszechnie dostępna dokumentacja dla REST API. 20. Udostępnia autoryzację dostępu użytkowników w oparciu o mechanizmy: a. Lokalną definicję; b. RADIUS; c. TACACS+; d. LDAP. 21. Umożliwia synchronizację całej infrastruktury sieciowej w oparciu o protokół NTP. 22. Implementuje następujące protokoły i mechanizmy L2 na zarządzanej infrastrukturze sieciowej: 23. Sprzętowe wsparcie dla VXLAN Bridging i VXLAN Routing w oparciu o sprzętowy VTEP; a. Umożliwia tworzenie segmentów sieci L2 w oparciu o technologię VXLAN; b. Definiowanie domen rozgłoszeniowych L2 z opcjonalną możliwością eliminacji ruchu rozgłoszeniowego dla mechanizmów ARP/GARP, Unknown Unicast; c. Eliminacja ruchu rozgłoszeniowego dla mechanizmów ARP i Unknown Unicast poprzez lokalizację w oparciu o bazę adresową L2/L3; d. Dołączanie urządzeń zewnętrznych (serwerów, modułów, przełączników) poprzez zagregowaną wiązkę połączeń LACP 802.3ad do dwóch przełączników brzegowych (multi link aggregation, virtual port channel, itp.); e. Pełna mobilność serwera fizycznego i wirtualnego w domenie L2; f. Definiowanie zewnętrznych połączeń w domenie L2; g. Mechanizm eliminacji pętli na przełącznikach brzegowych w fabric. 24. Implementuje następujące protokoły i mechanizmy L3 na zarządzanej infrastrukturze sieciowej: a. IPv4 Unicast i Multicast; b. Przesyłanie IPv6 Unicast; c. Niezależne sieci prywatne (VRF) z duplikacją adresacji IP;

		d. Protokoły routingu eBGP, iBGP, OSPF dla IPv4 i IPv6; e. Routing statyczny dla IPv4 i IPv6; f. Przełączanie ruchu pomiędzy parą podsieci IP (SVI) realizowane sprzętowo w modelu IP Anycast w ramach fabric, tj. na każdym przełączniku brzegowym, niezależnie od ilości przełączników brzegowych w fabric; g. Pełna mobilność serwera fizycznego i wirtualnego w domenie L3; h. Interfejsy i subinterfejsy L3 (per VLAN) na portach fizycznych przełączników brzegowych; i. Definiowanie zewnętrznych połączeń w domenie L3; 25. Implementuje następujące mechanizmy optymalizacji ruchu: Load-balancing pakietów dostosowany się do różnych warunków przesyłania (natłoku) w ramach środowiska i priorytezacja połączeń. 26. Umożliwia wyniesienie dowolnej pary urządzeń typu leaf do lokalizacji zdalnej przy zachowaniu przynależności do centralnej IP Fabric 27. Komunikacja pomiędzy oprogramowaniem zarządzającym a zarządzanymi urządzeniami sieciowymi odbywa się w sposób spójny dla wszystkich funkcjonalności (jeden protokół komunikacji) i w sposób zaszyfrowany.
3.	Centralny system analityczny	1. Narzędzie lub zespół narzędzi analitycznych zawierających zestaw zaawansowanych algorytmów powiadamiania, ustalania wartości bazowych, korelacji i prognoz/trendów. 2. Narzędzie(a) mają zapewnić wgląd w zachowanie/stan sieci przy wykorzystaniu danych telemetrycznych z komponentów sieciowych i zarządzających. 3. Rozwiązanie ma pomagać w szybkim znajdowaniu przyczyn problemów, wspierać ich rozwiązywanie poprzez wizualizacje oraz rekomendacje w zakresie działań naprawczych. Wymagane jest wsparcie dla „IP Fabric” (topologii sieciowych spine-leaf). 4. Funkcjonalności w zakresie weryfikacji bieżącego stanu sieci(IP Fabric) z bazami online producenta: a. Analiza na bieżąco zdarzeń i logów celem identyfikacji znanych ostrzeżeń, ich wpływu na określone przełączniki urządzenia, oraz zalecenia dotyczące działań naprawczych,

		b. Informacje o błędach, podatnościach (PSIRT/CVE), zaleceniach producenta, poprawkach, EOL / EOS oprogramowania i sprzętu, c. Anomalie w konfiguracji – informacje o przekroczeniu przez konfiguracje zweryfikowanej skali dla danego urządzenia i użytkowanej wersji oprogramowania, d. Informacje o problemach w procesie utwardzania (zabezpieczania) platformy, niezgodnościach w warstwie zarządzania e. Informacja o wpływie poprawek na dostępność systemu, np. czy aktualizacja oprogramowania będzie bezprzerwowa, czy (nowy) sprzęt może obsługiwać istniejący zestaw funkcji i skalę, f. Otwieranie zgłoszeń u producenta wraz ze wsparciem przygotowania i dostarczenia wymaganych logów, g. Wsparcie wysyłania powiadomień o powyższych problemach i rekomendacjach poprzez email i Kafka (szyna danych); 5. Analiza warstwy zarządzania (control plane) Fabryki IP z następującymi funkcjonalnościami: a. Zbieranie danych: zmiany konfiguracji, zdarzenia i błędy w warstwie zarządzania, b. Analiza z wykorzystaniem AI/ML (uczenie maszynowe) celem określenia korelacji między wszystkimi zmianami, zdarzeniami i błędami, c. Wykrywanie anomalii: z wykorzystaniem AI/ML detekcja nieoczekiwanych zdarzeń, w tym tych mających wpływ na przestoje; d. Analiza protokołów multicast i ich stanu (PIM/IGMP oraz IGMP snooping), e. Co najmniej 30 dniowa retencja danych; 6. Wizualizacja wykorzystania zasobów, z podziałem na następujące kategorie a. Zasoby operacyjne: wyświetla pojemność zasobów, które mają charakter dynamiczny i oczekuje się ich zmiany w krótkich odstępach czasu. Przykładami są trasy LPM, adresy MAC, tablice zabezpieczeń (ACL TCAM), itp. Predykcja przekroczenia na bazie trendu,

		b. Zasoby konfiguracyjne: Wyświetla wykorzystanie pojemności zasobów zależnych od konfiguracji, takich jak liczba VRF, VLAN, (mikro)segmentów, itp., c. Zasoby sprzętowe: wykorzystanie ilości portów i przepustowość, d. Środowiskowe (temperatura, utylizacja CPU, RAM, prędkości wentylatorów, itp.), e. Co najmniej 30 dniowa retencja danych; 7. Analityka przepływów w sieci (flow)– celem identyfikacji anomalii sieciowych i ich źródeł w warstwie transmisji (data plane). Wspierane anomalie/funkcjonalności: a. odrzucone pakiety, b. opóźnienia, c. ruchy, przemieszczenia workload (MAC flapping, itp) dla vm i bare metal wraz z ich lokalizacją, d. problemy z routingiem, e. odrzucone pakiety/ramki przez ACL, f. Co najmniej 7 dniowa retencja danych o wszystkich przepływach i związanych z nimi anomaliach zebranych ze wszystkich urządzeń Fabryki IP. 8. Silnik analityczny, który po analizie konfiguracji i weryfikacji stanu sieci zapewnia zabezpieczenie poprawności działania i konfiguracji w sieci opartej o architekturę IP Fabric. Przeprowadzona analiza zawiera opis zdarzenia, obiekty, których dotyczy (jak urządzenia końcowe, segment/VLAN/VRF itp.) oraz rekomendację co działań naprawczych. 9. Wspomaganie zarządzania zmianami konfiguracji i predykcji ich wpływu na usługi sieciowe a. Analiza wpływu dokonanych zmian w konfiguracji w określonym przedziale czasu, z wyszczególnieniem zlikwidowanych oraz nowych zdarzeń/alertów z podziałem na ważność problemu. b. Analiza porównawczej pomiędzy dwoma stanami sieci, np. sprzed i po oknie serwisowym ze szczegółowym wykazaniem wszystkich zmian, wskazaniem ich wpływu na poszczególne części sieci (obiekty sieciowe jak segment/VRF, itp.) oraz osób odpowiedzialnych za wdrożenie tych zmian.

		c. Przewidywanie wpływu zmiany – analiza zmiany zdefiniowanej jako plik konfiguracyjny (typu JSON/XML, itp.) w stosunku do aktualnej konfiguracji w szczególności z wyszczególnieniem zdarzeń/alertów z podziałem na nowe, zachowane, usunięte oraz na ważność problemu. d. Możliwość automatycznego testowania (poprawności) zmiany. 10. Weryfikacja stanu sieci - zapewnienie komunikacji i eliminacja potencjalnych awarii/luk w konfiguracji przed wystąpieniem jakiegokolwiek wpływu na produkcję, np. pętli routingowych oraz zduplikowanych sieci w tym samym VRF; 11. Weryfikacja zgodności konfiguracji z ustalonymi regułami polityki bezpieczeństwa i polityki dostępności. a. Bieżąca analiza i weryfikacja dynamicznego stanu całej sieci pod kątem ustalonych reguł dotyczących: komunikacji lub jej braku, realizacji polityki ruchu i bezpieczeństwa. b. Generowanie alertów dla administratora w przypadku wystąpienia naruszeń, np. ACL dopuszczająca ruch pomiędzy dwoma segmentami, kiedy jest to zabronione odpowiednią regułą polityki bezpieczeństwa. 12. Analiza problemów z łącznością dla urządzeń końcowych z klasyfikacją ich ważności; 13. Graficzna analiza zasad polityki ruchu (z uwzględnieniem obiekty typu segment, urządzenie końcowe, VRF, tenant). Możliwość weryfikacji łączności pod kątem komunikacji oraz zasad bezpieczeństwa (ACL) i segmentacji między obiektami sieciowymi. 14. Zestaw narzędzi jest dostarczony na platformie sprzętowej rekomendowanej przez producenta, zwymiarowanej zgodnie z wymaganiami oraz odpornej na wystąpienie pojedynczej awarii (dysk, CPU, węzeł). 15. Kompatybilność pomiędzy oprogramowaniem zarządzającym, analitycznym a urządzeniami sieciowymi jest potwierdzona dokumentacją producenta.
4.	System monitoringu	**System zarządzania- moduł zarządzania wydajnością** W ramach dostawy urządzeń Wykonawca zapewni system zarządzania wydajnością oraz korelacjami wydajności infrastruktury serwerowej z

		wydajnością aplikacji oraz wydajnością baz danych. Wykonawca zapewni monitorowanie min. 24 logicznych serwerów aplikacyjnych (rozwiązanie musi wspierać technologie min. Java. .NET, Python, PHP) oraz 8 instancji baz danych (rozwiązanie musi wspierać monitorowanie baz danych Oracle, MS SQL, NoSQL, Postgress) 1. Monitorowanie aplikacji ma odbywać się w sposób ciągły, z wykorzystaniem oprogramowania monitorującego. Część centralna oprogramowania może być udostępniona w modelu SaaS. 2. Rozwiązanie oparte o model SaaS musi zapewniać poziom bezpieczeństwa potwierdzony min. Certyfikatem SOC-2 lub równoważnym. Rozwiązanie powinno być zgodne z zasadami dyrektywy GDPR oraz zapewniać, że dane w SaaS będą przechowywane oraz przetwarzane na terenie Unii Europejskiej. Komunikacja pomiędzy komponentami rozwiązania w SaaS a komponentami w infrastrukturze Zamawiającego musi być szyfrowana z wykorzystaniem min. AES-256 lub równoważnym, komunikacja może się odbywać jedynie jednokierunkowo – od strony komponentów zlokalizowanych w infrastrukturze Zamawiającego do SaaS. 3. Interfejs zarządzania musi być dostępny w postaci interfejsu graficznego z poziomu przeglądarki internetowej. 4. Dostęp musi był zabezpieczony hasłem. Autentykacja i autoryzacja w usłudze umożliwiać kontrolę dostępu opartą na rolach (RBAC) 5. Oprogramowanie zarządzające musi umożliwiać integrację bazy użytkowników z LDAP. 6. Oprogramowanie musi zapewniać zabezpieczenie dostępu z poziomu operatora i użytkownika oprogramowania za pomocą protokołu HTTPS. 7. Elementy oferowanego rozwiązania muszą w zakresie komunikacji (wewnętrznej i zewnętrznej) umożliwiać wykorzystywanie protokołów bezpieczeństwa, przynajmniej SSL. 8. Oprogramowanie monitorowania musi zapewniać: a. możliwość uruchomienia monitoringu dla aplikacji pracujących przynajmniej na następujących systemach operacyjnych: • AIX

- Linux:
  - Debian
  - Fedora
  - openSUSE Leap
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise
  - Ubuntu

b. Windows:
  - 2012
  - 2012 R2
  - 2016
  - 2019
  - 2022

9. Oprogramowanie zarządzające musi zapewniać możliwość monitorowania wielowarstwowych aplikacji wykonanych w następujących technologiach:
   a. Java
   b. .Net
   c. PHP
   d. Python
10. Na podstawie wykrytych przepływów, oprogramowanie w sposób automatyczny pozwala odwzorować w formie graficznej monitorowany system obrazując powiązania i zależności monitorowanych komponentów i procesów oraz ich wzajemną komunikację, w szczególności uwzględniając takie warstwy jak serwery aplikacyjne, bazy danych, zewnętrzne serwisy i kolejki. W przypadku wykrycia odstępstwa od normy skutkującej wygenerowaniem alertu, monitorowany komponent, musi zostać

		oznaczony na wizualizacji w sposób jednoznacznie wskazujący na wystąpienie problemu w danym miejscu. 11. Wykrywa i monitoruje przebieg wszystkich transakcji przepływających przez aplikację w sposób automatyczny oraz oferuje możliwość ręcznego dostosowania sposobów wykrywania i monitoringu transakcji. Oprogramowanie musi wspierać definiowanie własnych transakcji biznesowych na podstawie spersonalizowanych reguł dopasowania, opartych o: a. URL b. wartość parametru z nagłówka HTTP, c. wartość parametru z zapytania GET lub POST, d. wykonanie konkretnej metody w kodzie Java lub .NET, e. wywołanie konkretnej usługi WebService. 12. Automatycznie wykrywa rodzaje komunikacji pomiędzy wykrytymi komponentami monitorowanych aplikacji, a w tym wspiera śledzenie transakcji wykorzystujących co najmniej następujące technologie synchroniczne i asynchroniczne: a. HTTP b. REST c. SOAP/XML d. JMS 13. Oferuje możliwość uzyskania następujących informacji o wybranych transakcjach: a. drzewo wywołania kodu oprogramowania w ramach transakcji uwzględniając nazwy wywoływanych metod, zarówno dla wątków wywoływanych synchronicznie jak i asynchronicznie wraz z czasem wykonania pojedynczych metod b. czasach odpowiedzi serwera do aplikacji klienckiej jak i całkowitym czasie wykonania transakcji po stronie serwera (wątków synchronicznych oraz asynchronicznych) c. zapytaniach SQL wykonanych w ramach transakcji z możliwością uzyskania informacji o użytych w nich zmiennych lub celowego ich maskowania, d. wartościach parametrów wywołania wskazanych metod, e. wartościach zwracanych przez wskazane metody.

		14. Usługa musi umożliwiać korelację transakcji realizowanych przez monitorowane komponenty z odpowiadającymi im danymi infrastrukturalnymi, bazodanowymi i sesją użytkownika końcowego. 15. Umożliwia automatyczne wytwarzanie linii bazowych dla wszystkich metryk kolekcjonowanych przez oprogramowanie, które są wyliczane z uwzględnieniem sezonowości w charakterystyce zapytań przepływających przez aplikację, z uwzględnieniem dni, tygodni i miesięcy (z rozdzielczością godzinną). Zamawiający musi mieć możliwość definiowania własnych linii bazowych, budowanych na podstawie kroczącego okresu czasu i na podstawie danych pobieranych w odstępach dziennych, tygodniowych lub miesięcznych. 16. Usługa musi udostępniać reguły powiadamiania w przypadku wykrycia problemów z wydajnością w aplikacji lub innych anomalii w oparciu o automatycznie wygenerowane linie bazowe lub statyczne wartości. 17. Oferowana usługa musi automatycznie, na podstawie danych bazowych/wzorcowych wykrywać problemy związane co najmniej z: a. wydłużeniem czasów odpowiedzi poszczególnych usług po stronie serwerowej, b. zwiększeniem poziomu problemów dla poszczególnych usług po stronie serwerowej, c. wydłużeniem czasów odpowiedzi dla poszczególnych akcji wykonywanych przez użytkownika końcowego na aplikacji WWW lub aplikacji mobilnej, zwiększeniem poziomu problemów dla poszczególnych akcji wykonywanych przez użytkownika końcowego na aplikacji WWW lub aplikacji mobilnej, d. przeciążeniem CPU, nadmiernym wykorzystaniem pamięci, e. spadkiem wydajności dysków, f. brakiem dostępności aplikacji. 18. Umożliwia definiowanie, konfigurację i modyfikację reguł, na podstawie których oprogramowanie generuje alerty. Oprogramowanie musi mieć możliwość wygenerowania alertu na podstawie zadanego odchylenia danej metryki od wyżej wspomnianej linii bazowej lub na podstawie statycznego progu. Funkcjonalność ta

		musi umożliwiać tworzenie złożonych warunków generowania tych alertów przy użyciu wyrażeń logicznych. 19. Na podstawie wygenerowanego alertu, musi umożliwiać wykonanie automatycznie następujących akcji: a. wysłanie powiadomienia do konkretnych użytkowników za pomocą wiadomości SMS lub e-mail b. uruchomienie dokładnej diagnostyki dla monitorowanych transakcji biznesowych, dla których został wygenerowany alert automatyczne wykonanie zrzutu wątku dla technologii Java (ang. thread dump) c. wykonać dowolny skrypt na monitorowanym serwerze aplikacyjnym d. wysłać zapytanie HTTP o dowolnej treści na dowolny URL 20. W opcji instalowania części centralnej Oprogramowania w infrastrukturze Zamawiającego, pozwala definiować własne spersonalizowane akcje, które mogą być uruchamiane jako efekt wygenerowania przez Oprogramowanie alertu, które pozwalają na integrację z zewnętrznymi narzędziami używanymi przez Zamawiającego takimi jak systemy do śledzenia problemów i projektów. 21. Usługa musi posiadać mechanizm przeciwdziałania generowania fałszywych alertów. 22. Pozwala zbierać i monitorować najbardziej wpływające na wydajność monitorowanej aplikacji zapytania SQL wykonywane z poziomu monitorowanej aplikacji z możliwością ich powiązania z transakcjami, które dane zapytania wykonują. 23. Ogranicza swój wpływ na monitorowane platformy i aplikacje m.in poprzez inteligentne zbieranie informacji celem uniknięcia zbędnego zużywania zasobów. Dodatkowo rozwiązanie musi oferować możliwość zbierania zwiększonego zakresu informacji poprzez manualne wyłączanie mechanizmu ograniczania narzutu na zasoby monitorowanego serwera dla wybranych transakcji biznesowych lub serwerów aplikacyjnych, np. w celach diagnostycznych lub testowych. Posiada możliwość prezentowania na wykresach dowolnych metryk gromadzonych przez oprogramowanie

		24. Pozwala na tworzenie dowolnych niestandardowych pulpitów prezentujących gromadzone w ramach usługi dane, z poziomu interfejsu graficznego. Usługa musi umożliwiać nadawanie użytkownikom uprawnień wyświetlania lub edycji poszczególnych pulpitów. 25. Oprogramowanie w przypadku wykrycia problemu automatycznie wskazauje możliwe przyczyny wystąpienia problemu. 26. Musi gwarantować odpowiedni poziom dostępu do danych definiowany na poziomie nadawania uprawnień do świadczonej usługi oparty o system ról i grup użytkowników (ang. Role-Based Access Control). Mechanizm konfiguracji uprawnień musi być dostępny w interfejsu graficznego jak i z poziomu interfejsu API oprogramowania, służącego wykonywaniu usługi 27. musi umożliwiać porównywanie działania aplikacji w różnych przedziałach czasowych na poziomie czasów odpowiedzi, liczby błędów, poziomu ruchu i tym podobnych. 28. Oprogramowanie musi zbierać informacje o wszystkich o błędach i wyjątkach. Musi istnieć możliwość zobaczenia szczegółowych informacji na temat transakcji, w których wystąpił błąd bądź został wygenerowany wyjątek. 29. Oprogramowanie, poza domyślnym mechanizmem detekcji problemów, musi oferować możliwość konfiguracji tzw. wyjątków – odstępstwa od reguły, pozwalające na odrzucenie błędów technicznych, które nie mają wpływu na biznesowe działanie aplikacji. 30. Oprogramowanie musi posiadać możliwość tworzenia lub konfigurowania definiowanych przez Administratora lub użytkownika aplikacji dodatkowych niestandardowych wtyczek monitorujących. Dla metryk dostarczanych przez te dodatkowe wtyczki, Oprogramowanie musi automatycznie wygenerować linie bazowe. 31. Usługa musi logować wszystkie aktywności użytkowników związane ze zmianami konfiguracji. Logowanie musi umożliwiać jednoznaczne wskazanie osoby, która wykonała zmianę. 32. Oprogramowanie musi oferować także udokumentowany interfejs programistyczny (API) służący do konfiguracji Oprogramowania, pobierania danych, a w tym metryk historycznych.

		33. Pozwala analizować wpływ zmian wersji oprogramowania na wydajność procesów, transakcji oraz wartość metryk związanych z obsługą użytkowników aplikacji, celem wskazania czy wprowadzane zmiany prowadzą do pożądanego stanu funkcjonowania aplikacji. Usługa musi oferować możliwość rejestracji zdarzenia wgrania nowej wersji aplikacji. 34. W zakresie monitorowania baz danych, oprogramowanie musi spełniać poniższe wymagania techniczne i posiadać niżej wymienione funkcje: a. Umożliwia monitorowanie następujących baz danych: i. Apache Cassandra ii. Datastax Enterprise (DSE) Cassandra iii. IBM DB2 (instalowanych na OS Linux, Ubuntu oraz Windows) iv. MongoDB v. MySQL vi. Microsoft SQL Server vii. Oracle viii. PostgreSQL 35. Umożliwia monitorowanie baz danych będących częścią monitorowanego środowiska, celem wykrycia źródeł problemów wydajnościowych, zarówno z punktu widzenia wykonywania zapytań i procedur zainicjowanych przez monitorowane aplikacje jak i przez inne podmioty nieobjęte monitoringiem. 36. Monitoruje bazy danych w sposób nie wymagający instalacji agenta na hoście bazy danych. 37. Zapewnia informacje dotyczące zużycia zasobów serwera bazy danych takich jak CPU, Pamięć, I/O dysku i I/O sieci. 38. Zapewnia ogólne informacje dotyczące ilości zapytań wykonywanych w bazie w zadanym okresie czasu wraz z czasem spędzonym na ich wykonywaniu. 39. Zapewnia informacje dotyczące stanów oczekiwania (ang. Wait States) wraz z dystrybucją czasu spędzonego w każdym ze stanów oczekiwania. 40. Zapewnia informacje na temat zapytań i procedur, które zajmują najwięcej czasu w bazie danych przedstawiając ich składnie, ilość wykonań lub ilość wykonywujących je sesji oraz czas spędzony na

		wykonywaniu, jednocześnie pozwalając na grupowanie zapytań i procedur o tej samej lub zbliżonej składni. 41. Zapewnia informacje o nazwach hostów i adresach IP klientów korzystających z baz danych. 42. Zapewnia informacje o identyfikatorach sesji korzystających z bazy danych wraz z informacją o czasie spędzonym w bazie danych. 43. Pozwala na uzyskanie informacji dotyczących blokujących się wzajemnie sesji celem zbadania powodów występowania deadlock'ów. Pozwala na generację i analizę planów zapytań SQL do bazy danych. 44. Umożliwia definiowanie niestandardowych metryk tworzonych na podstawie zapytań bazodanowych definiowanych przez Administratora lub użytkownika oprogramowania. Dla tych niestandardowych metryk, Oprogramowanie również musi automatycznie wygenerować linie bazowe. 45. Dostarczone oprogramowanie musi zapewnić monitoring bezpieczeństwa aplikacji 46. Dla aplikacji opartych o Java oraz .Net oprogramowanie zapewni także możliwość monitoringu w czasie rzeczywistym istniejących, znanych podatności, istniejących lub takich, które pojawią się w czasie świadczenia wsparcia i zostaną sklasyfikowane za pomocą sygnatur podatności takich jak CVE, SNYK itd. 47. Dostarczone oprogramowanie, oprócz analizy sygnatur CVE w oparciu o punktację CVSS musi wykorzystywać metryki czasowe oraz kontekstowe (związane z konkretną aplikacją) prezentując informację opartą o aktywnym wykorzystywaniu podatności w Internet, łatwość wykonania ataku (exploitacji), podatności na ataki malware, popularność danej podatności jako celu ataku. 48. Oprogramowanie w sposób ciągły, w czasie rzeczywistym musi raportować wzrost zagrozenia atakiem dla danej podatności. 49. Zamawiający uzyska ciągły (24/7h) dostęp do bazy informacji na temat podatności w monitorowanych aplikacjach w taki sposób aby mógł uzyskać informację o: a. stosowanych bibliotekach programistycznych, w których występują znane podatności b. powiązaniu bibliotek z konkretnymi procesami aplikacyjnymi i wykonywanymi metodami

		c. poziomie krytyczności wykrytych podatności ze wskazaniem, które z podatności mają charakter krytyczny, wysoki, średni oraz niski d. wadze punktowej, określającej poziom zagrożenia związanego z wykrytą podatnością e. czy dla wykrytych podatności istnieją metody ich wykorzystania, f. czy dana podatność jest aktywnie wykorzystywana g. krótki opis wykrytej podatności wraz z sugerowanym sposobem jej usunięcia jeśli taki istnieje h. poziomie bezpieczeństwa zapytań API do monitorowanej aplikacji 50. Dostarczone oprogramowanie musi być oparte o dane z min. jednej organizacji Threat Intelligence, dostępna w sposób ciągły bez konieczności instalowania żadnych komponentów sprzętowych w infrastrukturze Zamawiającego
5.	Gwarancja	Wszystkie dostarczone systemy muszą zostać objęte 36 miesięczną gwarancja

4.3 Specyfikacja techniczna Infrastruktury serwerowej

4.3.2 Serwer Rack

Tabela 11 Opis wymagań Serwer RACK

Lp.	Nazwa parametru	Opis parametru
1.	Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
2.	Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3.	Procesor	Zainstalowane dwa procesory min. 26-rdzeniowe, min. 2.2GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 357 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Możliwość obsługi procesorów 32 rdzeniowych
4.	RAM	Minimum 768GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci.
5.	Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing. Zamawiający dopuszcza rozwiązania równoważne.
6.	Gniazda PCI	- minimum trzy loty PCIe generacji 4
7.	Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) na minimum 2 kartach rozszerzeń oraz min 2 interfejsy Fiber Channel min. 16 Gb na minimum 2 kartach rozszerzeń. Dopuszcza się wykorzystanie interfejsów wbudowanych na stałe.
8.	Dyski twarde	Zainstalowane 2 dyski SATA o pojemności min. 480GB, SSD przeznaczone do pracy w serwerze. Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1 oparte na kontrolerze BOSS lub równoważnym Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 32GB, z możliwością konfiguracji zabezpieczenia synchronizacji

		pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
9.	Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10.
10.	Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim. Możliwa realizacja funkcjonalności oparta o rozwiązanie DVI lub DisplayPort
11.	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
12.	Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
13.	Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0
14.	Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera Dopuszcza się rozwiązanie równoważnego, które realizowanu powyższe funkcje

		przez dołączone oprogramowanie do zarządzania, a nie bezpośrednio z karty zarządzającej.
15.	Oprogramowanie do zarządzania	Zainstalowane oprogramowanie producenta, do zarządzania, spełniającego poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Opis wykrytych systemów oraz ich komponentów przedstawiający co najmniej podstawowy zakres informacji w tym nazwę i producenta • Możliwość eksportu raportu do CSV, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera w tym co najmniej: Nazwa, lokalizacja, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)

		• Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Możliwość wygenerowania następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera • Wdrażanie serwerów w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
16.	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” minimum dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
17.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
18.	Warunki gwarancji	Należy zapewnić min. 36 miesięcy gwarancji producenta. Wykonawca w ramach gwarancji producenta zapewni również min. 36 miesięcy

		wsparcia technicznego producenta, z czasem reakcji do 4h od zakończenia zdalnej diagnostyki. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

4.3.3 Przełącznik SAN

Tabela 12 Opis wymagań Przełącznik sieciowy SAN

Lp.	Nazwa parametru	Opis parametru
1.	Wymagania dotyczące portów	Nie mniej niż 48 fizycznych i aktywnych portów Fibre Channel w standardzie SFP pracujących w trybie 4/8/16/32 Gbps z pełną przepustowością dla prędkości 32G FC.
2.	Parametry wydajnościowe:	a) Obsługa wszystkich portów równocześnie z pełną wydajnością 32G, b) Każdy port jest wyposażony w 500 kredytów bufora, c) Dwa porty posiadają co najmniej 6000 kredytów/ duże bufory i wspierają pracę na dystansie do 500km bez spadku wydajności dla prędkości 16 Gbps.
3.	Przełącznik musi posiadać następujące podstawowe funkcjonalności:	a) Obsługa co najmniej 4 wirtualnych sieci (fabryk) SAN, b) Routing między VSAN (Inter VSAN Routing), c) Agregację nie mniej niż 16 portów fizycznych w jedno połączenie logiczne („trunk", „channel"). W skład zagregowanego połączenia logicznego („trunk", „channel") jest możliwe włączenie dowolnego aktywnego portu przełącznika d) Urządzenie wspiera wymiane oprogramowania bez przerwy w działaniu urządzenia (tzw. nondisruptive software upgrades), e) Redundantny system plików do startu systemu, f) Mechanizmy gwarancji jakości usług (QoS), g) Sprzętowo implementowany zoning ze wsparciem dla list kontroli dostępu, h) N-Port ID Virtualization (NPIV), i) Protokołu NVMe (NVMeOF).
4.	Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa:	a) Protokół FC-SP (Fibre Channel Security Protocol) ze wsparciem dla uwierzytelnienia host-switch oraz switch-switch, b) Mechanizmy ochrony warstwy control plane, c) Sprzętowe szyfrowania danych z wykorzystaniem kluczy AES co najmniej 128 bit, d) Bezpieczne boot-owanie (wykrywanie nieautoryzownaych zmian oprogramowania i firmware).
5.	Przełącznik musi posiadać następujące mechanizmy	a) czas wykonania operacji (ECT - exchange completion time) b) opóźnienie dostępu do danych

	sprzętowe analityki, które w czasie rzeczywistym, sumarycznie i per flow IT (Initiator-Target) zbierają z ramek FC/NVMe takie dane jak	c) maksymalna liczba niezakończonych transakcji (maximum number of outstanding exchanges) d) ilość operacji I/O na sekundę (IOPS)
6.	Przełącznik musi wspierać następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia urządzenia	a) Zarządzanie/monitorowanie SNMPv3, b) Dostęp administracyjny SSHv2, c) Transfer za pomocą SFTP, d) Rejestrowanie zdarzeń poprzez mechanizm „syslog”, e) Możliwość bezzakłóceniowego monitorowania ruchu na portach przez kopiowanie ruchu z określonego portu na wybrany port monitorujący (z dołączonym zewnętrznym analizatorem), f) Narzędzia dla Fibre Channel odpowiadające fukcjonalnie poleceniom sieciowym „ping” i „traceroute”, g) Autoryzacja dostępu administracyjnego do przełącznika za pomocą RADIUS i TACACS+, LDAP, Microsoft Active Directory, h) RESTful-API do skryptowania/programowania, i) Wsparcie sprzętowe dla pokazywania statystyk ruchu dla poszczególnych vm, j) Konfiguracja poprzez terminal i linię komend CLI, interfejs graficzny GUI oraz RESTful API, k) Szeregowy port konsoli oraz port USB.
7.	Oprogramowanie do konfiguracji i monitorowania przełącznika musi posiadać graficzny interfejs użytkownika oparty o HTML i realizować następujące funkcjonalności	a) Konfiguracja parametrów pracy w wielu urządzeniach jednocześnie w obrębie pojedynczej sieci SAN, b) Konfiguracja zoningu, c) Wyświetlanie stanu i statystyk poszczególnych portów i modułów, d) Wizualizacja fizycznych połączeń miedzy urządzeniami z podaniem informacji o łączach (przynajmniej stan, prędkość, typ), e) Wizualizacja statystyk poszczególnych portów i modułów, f) integracja z VMWare vCenter wraz z wizualizacją ścieżek SAN dla maszyn VM g) Gromadzenie i analizowanie danych historycznych (performance trending), h) Archiwizacja konfiguracji,

		i) Raportowanie mechanizmu Slow Drain (wraz ze statystyka reagowania na nie). j) Kolektor i wizualizacja analityki z punktu 5)
8.	Zasilanie i wentylacja	a) Urządzenie musi posiadać redundantne zasilacze i wentylatory z możliwością ich wymiany w czasie pracy. b) Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. c) Przepływ powietrza w kierunku portów przełącznika (wlot na zasilaczach, wylot na portach)
9.	Obudowa	Urządzenie musi posiadać obudowę o wysokości maksymalnie 2RU (rack unit), przystosowaną do montażu w szafie 19” i wykonaną z metalu. Wraz z przełącznikiem należy dostarczyć niezbędny zestaw montażowy.
10.	Wyposażenie przełącznika	a) 48 aktywnych portów FC 32G b) 48 modułów optycznych SFP z optyką 32G SW FC (short wave).
11.	Gwarancja	Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miej scu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii. Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą przez cały okres gwarancji i obejmuje: Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji.

4.3.4 Macierz typ 1

Tabela 13 Opis wymagań Macierz typ 1

Lp.	Nazwa parametru	Opis parametru
1.	Obudowa i komponenty	Rozbudowa do nowego systemu musi być dostarczona ze wszystkimi komponentami do instalacji w szafie rack 19''. Podzespoły macierzy tj. wentylatory, zasilacze muszą być w pełni redundantne żeby zapewnić odpowiedni poziom bezpieczeństwa.
2.	Pojemność	System musi zostać dostarczony w konfiguracji zawierającej minimum: 120 dysków 3800GB SSD w półkach oraz posiadać możliwość rozbudowy o kolejne dyski. System musi wspierać dyski o wielkościach: • SSD od 960GB do co najmniej 15300GB • NVMe od 1900GB do 15 300GB • oraz wszystkie zasoby obecnie podłączone do systemu AFF A300 SN: 211818000138;211814000060 (do rozbudowanego nowego systemu Zamawiający wymaga podłączenia wszystkich zasobów z AFF A300)
3.	Kontroler	Dwa kontrolery wyposażone w przynajmniej 128GB cache każdy. W przypadku awarii zasilania dane nie zapisane na dyskach, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub za pomocą zrzutu danych na pamięć nieulotną. Procesory macierzy powinny być wykonane w technologii INTEL lub AMD wielordzeniowej z przynajmniej 12 rdzeniami na każdy kontroler. Zamawiający dopuszcza alternatywne procesory z min 64 rdzeniami. Macierz musi pozwalać na rozbudowę do klastra 24 kontrolerów lub musi pozwalać na obsługę przynajmniej 1500 dysków w obrębie pary kontrolerów lub klastra.

		Rozwiązanie musi pozwalać także na rozbudowę kontrolerów w technologii NVMe z obsługą do min 560 dysków w technologii NVMe. Macierz musi pozwalać na zbudowanie klastra z rozwiązaniami hybrydowymi, tj. macierzami które wspierają dyski: zarówno Flash (SSD lub NVMe oraz dyski SAS, NL-SAS
4.	Interfejsy	Oferowana macierz musi posiadać minimum: • 8 portów 25GbE (SFP28) • 8 portów 32Gb (SFP+) • 4 porty 10Gb (2 szt. kabla typu DAC lub twinax długości min. 0,5m) 4 porty 1Gb RJ45 • 8 portów 12Gb SAS, • 4 porty 100GbE Macierz musi wspierać rozbudowę o porty: • 32Gb FC o min. 8 szt. • 100GbE o min. 4 szt. Jeśli skorzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+) short vawe, Zamawiający wymaga ich dostarczenia wraz z urządzeniem. Rodzaj wkładek zostanie dobrany na etapie analizy przed wykonawczej.
5.	RAID	System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii jednego i dwóch dysków w grupie RAID.
6.	Obsługiwane protokoły	Macierz musi obsługiwać jednocześnie protokoły FC, iSCSI; NFS; CIFS/SMB, S3 Zamawiający w tym postępowaniu wymaga dostarczenia licencji na wszystkie protokoły.
7.	Obsługiwane protokoły	Macierz musi obsługiwać jednocześnie protokoły FC; iSCSI; NFS; CIFS/SMB, S3 Zamawiający w tym postępowaniu wymaga dostarczenia licencji na wszystkie protokoły.
8.	Inne wymagania	Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych in-line. Macierz musi posiadać także funkcjonalność kompresji danych in-line.

		Jeżeli oferowane rozwiązanie nie pozwala na deduplikację i kompresję w locie lub nie posiada możliwości deduplikacji i kompresji Zamawiający wymaga dostarczenia 4 krotnej pojemności wyspecyfikowanej w punkcie 2. Macierz musi umożliwiać budowę wielowęzłowego klastra z istniejącym systemem AFF A400/FAS 8700 . Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Windows Server 2008, Vmware ESXi, Red Hat Linux, FreeBSD Macierz musi posiadać funkcjonalność priorytetyzacji zadań w tym ustawienie max parametrów (I/Ops i Mbps) dla poszczególnych LUN. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. Macierz musi posiadać funkcjonalność replikacji danych z istniejącą macierzą AFF A400 w trybie synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych i kompresji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub Zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości zasobów. Macierz musi posiadać funkcjonalność klonowania danych bez potrzeby fizycznego kopiowania danych na nośnikach. Macierz musi posiadać funkcjonalność wykonania spójnego snapshotu dla następujących aplikacji: • Vmware ESXi • SAP • Oracle Database • MS Exchange Server oraz MS SQL • Veeam Backup Oferowana konfiguracja macierzy musi pozwalać na osiągnięcie wydajności do 250 000IOPS przy 8Kb bloku i stosunku 70/30% odczyt/zapis.

		Zamawiający wraz z ofertą wymaga dostarczenia oficjalnego dokumentu producenta z wymiarowaniem wydajności oraz dopuszcza możliwość sprawdzenia wydajności macierzy przy odbiorze. Macierz musi posiadać narzędzie umożliwiające generowanie raportu o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy. Macierz musi być wyposażona w oprogramowanie do audytu zasobów plikowych w szczególności pozwalać na: • blokowanie zapisywania plików z określonym (do zdefiniowania przez administratora) rozszerzeniem monitorowaniu operacji wykonywanych na plikach • Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na: • monitoring wykorzystania przestrzeni na macierzy • monitoring grup RAIDowych • monitoring wykonywanych backupów/replikacji danych między macierzami • monitoring wydajności macierzy • analizę i diagnozę spadku wydajności Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną maksymalną pojemność systemu. Macierz musi posiadać funkcjonalność „Tieringu" zimnych danych na: • inną macierz tego samego producenta (z wolnymi dyskami np. NL-SAS) • inną macierz dowolnego producenta z protokołem S3 Tiering musi być natywnym narzędziem macierzy i wykonywać się automatycznie. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność urządzenia i pozwalać na wspólne działanie (żadna funkcjonalność nie może wykluczać działania innej funkcjonalności).
9.	Gwarancja i serwis	36 miesięcy gwarancji producenta. Przez cały okres gwarancji Wykonawca zapewni również wsparcie techniczne producenta, z 2 godzinnym

		czasem odpowiedzi i wymianą części na następny dzień roboczy po diagnozie problemu. Dostarczony serwis musi umożliwiać zgłaszanie awarii w trybie 24x7. Dostarczony system musi posiadać również 36 miesięcy subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. Uszkodzone nośniki (dyski) pozostają u Zamawiającego

4.3.5 Macierz typ 2

Tabela 14 Opis wymagań Macierz typ 2

Lp.	Nazwa parametru	Opis parametru
1.	Obudowa	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19'' oraz szafą rack o wysokości 42U.
2.	Pojemność:	System musi zostać dostarczony w konfiguracji zawierającej minimum: 60 dysków 10TB NL-SAS oraz posiadać możliwość rozbudowy o kolejne dyski. System musi wspierać dyski: • SAS 10k: od 900GB do 1800GB • SATA/NL-SAS: od 4TB do 16TB • SSD: od 960GB do 30 000GB System musi mieć możliwość rozbudowy do 12PB przestrzeni użytkowej. Jeżeli istnieje model wyższy od zaoferowanego w portfolio producenta w tej samej linii produktowej, budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby migracji danych. (przez rozbudowę do wyższego modelu zamawiający rozumie rozbudowę do modelu macierzy z większą ilością Cache, większą skalowalnością i mocniejszymi procesorami) .
3.	Kontroler	Minimum dwa kontrolery wyposażone w sumie przynajmniej w 4TB cache oparte o RAM Zamawiający dopuszcza alternatywnie rozwiązanie posiadające co najmniej 512GB cache oparte o RAM jeżeli dodatkowo zostanie dostarczona z macierzą dodatkowa pamięć Flash NVMe minimum 4TB pamięci (wbudowana w kontrolery lub formie dodatkowych dysków Flash skonfigurowanych w RAID 10 jako SSD Cache) W przypadku awarii zasilania dane nie zapisane na dyskach, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub za pomocą zrzutu danych na pamięć nieulotną. Oferowane rozwiązanie musi ponadto pozwalać na rozbudowę cache (odczyt i zapis) za pomocą dysków SSD do min 40TB, zamawiający nie dopuszcza

		zastosowania dysków SSD w formie Tieringu dla w/w funkcjonalności. Jeżeli oferowane rozwiązanie nie pozwala na rozbudowę do 40TB zamawiający wymaga by cała wymagana przestrzeń była zaoferowana na szybkich dyskach SSD. Macierz musi pozwalać na rozbudowę do klastra 12 kontrolerów udostępniających (każdy) zarówno dane blokowe jak i plikowe.
4.	Interfejsy	Oferowane rozwiązanie musi posiadać minimum: • 8 portów 25GbE SFP28 • 8 portów 32Gb FC • 8 portów 12Gb SAS do podłączenia zewnętrznych półek dyskowych Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), zamawiający wymaga ich dostarczenia wraz z urządzeniem. Rodzaj wkładek zostanie dobrany na etapie Analizy przedwykonawczej. System musi pozwalać na podwojenie liczby istniejących portów.
5.	RAID	System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii jednego i dwóch dysków w grupie RAID.
6.	Kopie Migawkowe	Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy większego niż 5% System musi pozwalać na rozbudowę o specjalny moduł do zabezpieczenia przez atakiem Ransomware w szczególności: • musi informować administratora w przypadku nie standardowego zachowania systemu oraz danych • wykonywać prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware • wykonywać kopię migawkową „snapshot” z zastosowaniem zabezpieczenia WORM dla pojedynczego wolumenu/LUNu.
7.	Obsługiwane protokoły	Rozwiązanie musi obsługiwać jednocześnie protokoły FC, iSCSI, CIFS i NFS, RoCE, S3. Zamawiający w tym postępowaniu wymaga dostarczenia wszystkich w/w licencji
8.	Inne wymagania	Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych którą można stosować na macierzy/danych produkcyjnej

		dla wszystkich rodzajów danych. Macierz powinna mieć możliwość czynności odwrotnej tzn. Cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie Natywna replikacja z istniejącą macierzą NetApp FAS 8700 posiadaną przez Zamawiającego. Macierz musi umożliwiać budowę wielowęzłowy klastra z istniejącym systemem FAS 8700/AFF A400 Macierz musi posiadać funkcjonalność kompresji danych w trybie off-line oraz in-line. Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów • Windows server 2008 • Red Hat Linux • Vmware Vsphere • FreeBSD Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. Macierz musi pozwalać na stworzenie dla zasobów plikowych zasób o pojemności niemniejszej niż 256TB oraz 128TB dla zasobów blokowych. Macierz musi posiadać funkcjonalność replikacji danych w trybie asynchronicznym oraz synchronicznym. Funkcjonalność replikacji danych musi być natywnym rozwiązaniem macierzy dyskowej. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza oraz skrócenia czasu backupu dla replikowanych zasobów. Jeżeli oferowane rozwiązanie nie pozwala na deduplikację replikowanych zasobów zamawiający wymaga dostarczenia zewnętrznego urządzenia do deduplikowania replikowanych danych. W przypadku zastosowania zewnętrznych urządzeń do deduplikacji replikowanych danych, Zamawiający wymaga zastosowania ich w formie redundantnej tj. po 2 szt. na macierz. Rozwiązanie ponadto musi być skonfigurowane w trybie klastra geograficznego pozwalającego na przełączenie wszystkich

		zasobów między macierzami bez interwencji człowieka w sposób automatyczny. Zamawiający wymaga dostarczenia wszystkich niezbędnych elementów do poprawnego skonfigurowania i działania klastra geograficznego. Macierz musi posiadać funkcjonalność priorytetyzacji zadań w tym ustawienie maksymalnych parametrów (I/Ops i Mbps) na Lunach. System operacyjny kontrolerów musi natywnie obsługiwać automatyczny tiering bloków danych pomiędzy minimalnie trzema rodzajami pamięci SSD, SAS 10k i NL-SAS lub pamięcią główną RAM, pamięcią NVMe i SSD. Tiering musi odbywać się w czasie rzeczywistym i dla wszystkich rodzajów danych obsługiwanych przez system. Wymaga się granularności tieriengu na poziomie bloków danych o wielkości 4kB. Macierz musi być wyposażona oprogramowanie do audytu zasobów plikowych w szczególności pozwalać na: • blokowanie zapisywania plików z określonym (do zdefiniowania przez administratora) rozszerzeniem • monitorowaniu operacji wykonywanych na plikach Oprogramowanie do audytu zasobów plikowych może pochodzić od innego producenta niż producent macierzy. Zamawiający wymaga dostarczenia licencji na maksymalną pojemność macierzy. Macierz musi pozwalać na wykonanie spójnego snapshotu dla Vmware, Oracle oraz Microsoft MSSQL i Exchange. Macierz musi posiadać funkcjonalność wykonania wirtualnych klonów, które nie wymagają kopiowania bloków danych. Macierz musi posiadać możliwość automatycznego informowania przez macierz i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na: • monitoring wykorzystania przestrzeni na macierzy

		• monitoring grup RAIDowych • monitoring wykonywanych backupów/replikacji danych między macierzami • monitoring wydajności macierzy • analizę i diagnozę spadku wydajności Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność macierzy. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy Producent musi dostarczyć usługę w postaci portalu WWW lub dodatkowego oprogramowania umożliwiającą następujące funkcjonalności: a) Narzędzie do tworzenia procedury aktualizacji oprogramowania macierzowego. • procedura musi opierać się na aktualnych danych pochodzących z macierzy oraz najlepszych praktykach producenta. • procedura musi uwzględniać systemy zależne tj. macierze replikujące • procedura musi umożliwiać generowanie planu cofnięcia aktualizacji. b) Wyświetlanie statystyk dotyczących wydajności, wykorzystanie zasobów, oszczędności wykorzystania zasobów uzyskanych dzięki funkcjonalnościom macierzy (deduplikacja, kompresja). c) Wyświetlanie konfiguracji macierzy oraz porównywanie jej z najlepszymi praktykami producenta w celu usunięcia błędów konfiguracji. Portal może pochodzić od innego producenta niż producent macierzy. Zamawiający wymaga by wszystkie funkcjonalności działały jednocześnie. Włączenie jednej funkcjonalności nie może eliminować działania innej. Macierz musi posiadać funkcjonalność „Tieringu” zimnych danych na: • inną macierz tego samego producenta (z wolnymi dyskami lub dyskami innego typu) • inną macierz dowolnego producenta z protokołem S3 • Tiering musi być natywnym narzędziem macierzy i wykonywać się automatycznie.

		Opis przedmiotu zamówienia w sposób jednoznaczny musi określać stawiane wymogi, w związku z powyższym niedopuszczalne jest używanie sformułowań „np.”.
9.	Gwarancja i serwis	36 miesięcy gwarancji producenta na Macierz oraz na półki dyskowe obecnie podpięte do macierzy. Przez cały okres gwarancji Wykonawca zapewni również wsparcie techniczne producenta, z 2 godzinnym czasem odpowiedzi (reakcji na zgłoszenie) i wymianą części (naprawy) na następny dzień roboczy po diagnozie problemu w miejscu instalacji Macierzy. Dostarczony serwis musi umożliwiać zgłaszanie awarii w trybie 24x7. Dostarczony serwis musi posiadać również 36 miesięcy subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. Uszkodzone nośniki (dyski) pozostają u Zamawiającego.

4.4 Specyfikacja techniczna Infrastruktury wskazanej w prawie opcji

4.4.1 Serwer Rack – Prawo Opcji

Tabela 15 Opis wymagań Serwer RACK – Prawo opcji

Lp.	Nazwa parametru	Opis parametru
1.	Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2,5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
2.	Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3.	Procesor	Zainstalowane dwa procesory min. 26-rdzeniowe, min. 2.2GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 357 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. Możliwość obsługi procesorów 32 rdzeniowych
4.	RAM	Minimum 768GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci.
5.	Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing. Zamawiający dopuszcza rozwiązania równoważne.
6.	Gniazda PCI	minimum trzy loty PCIe generacji 4
7.	Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) na minimum 2 kartach rozszerzeń oraz min 2 interfejsy Fiber Channel min. 16 Gb na minimum 2 kartach rozszerzeń. Dopuszcza się wykorzystanie interfejsów wbudowanych na stałe.
8.	Dyski twarde	Zainstalowane 2 dyski SATA o pojemności min. 480GB, SSD przeznaczone do pracy w serwerze.

		Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1 oparte na kontrolerze BOSS lub równoważnym Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 32GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
9.	Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 5, 10.
10.	Wbudowane porty	4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim. Możliwa realizacja funkcjonalności oparta o rozwiązanie DVI lub DisplayPort
11.	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
12.	Zasilacze	Redundantne, Hot-Plug min. 800W każdy.
13.	Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0
14.	Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

		• integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera Dopuszcza się rozwiązanie równoważnego, które realizowaniu powyższe funkcje przez dołączone oprogramowanie do zarządzania, a nie bezpośrednio z karty zarządzającej.
15.	Oprogramowanie do zarządzania	Zainstalowane oprogramowanie producenta, do zarządzania, spełniającego poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Opis wykrytych systemów oraz ich komponentów przedstawiający co najmniej podstawowy zakres informacji w tym nazwę i producenta • Możliwość eksportu raportu do CSV, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera w tym co najmniej: Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej

		• Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Przesyłanie alertów „as-is" do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
16.	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 Serwer musi posiadać deklaracja CE. Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych

		plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.
17.	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
18.	Warunki gwarancji	Należy zapewnić min. 36 miesięcy gwarancji producenta. Wykonawca w ramach gwarancji producenta zapewni również min. 36 miesięcy wsparcia technicznego producenta, z czasem reakcji do 4h od zakończenia zdalnej diagnostyki. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

		Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

4.4.2 Przełącznik sieciowy Typ B – Prawo Opcji

Tabela 168 Wymagania dla przełącznika sieciowego Typ B

Lp.	Nazwa parametru	Opis parametru
1.	Typ i liczba portów	48 portów 10/100/1000BaseT RJ-45 + uplink 4x10G SFP+
2.	Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:	• Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet typu twinax (SFP+ - SFP+) • 10Gigabit Ethernet typu twinax (SFP+ - SFP+), • 25Gigabit Ethernet 25GBASE-SR, • 25Gigabit Ethernet typu twinax (SFP28 – SFP28), • 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF), • 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)
3.	Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:	• Przepustowość w ramach stosu - 80Gb/s, • 8 urządzeń w stosie, • Zarządzanie poprzez jeden adres IP, • Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
4.	Zasilanie i chłodzenie:	• Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), • Redundantne wentylatory,
5.	Parametry wydajnościowe:	• Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 256 Gb/s (z podłączeniem do stosu)

		• Prędkość przesyłania (forwarding rate): 130.95 Mpps • Bufor pakietów – 6MB • Pamięć DRAM – 2GB • Pamięć flash – 4GB • Obsługa: o 500 aktywnych sieci VLAN o 16000 adresów MAC o 3000 tras IPv4 o 1500 tras IPv6 o Ilość wpisów w listach kontroli dostępu Security ACL – 1000 o ilość wpisów w listach kontroli dostępu QoS ACL – 1000 o 512 interfejsów SVI L3 o 48 połączeń zagregowanych typu „port channel” o 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP o Jumbo frame 9198B
6.	Protokoły	• Obsługa protokołu NTP • Obsługa IGMPv1/2/3 i MLDv1/2 Snooping • Obsługa protokołu LLDP i LLDP-MED
7.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:	• IEEE 802.1w Rapid Spanning Tree • Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1s Multi-Instance Spanning Tree • Obsługa 64 instancji protokołu STP • Wsparcie dla protokołu REP (Resilient Ethernet Protocol) • Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku podstawowego
8.	Możliwość uruchomienia funkcji serwera	• Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,

	DHCP 14. Mechanizmy związane z bezpieczeństwem sieci: Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilegelevel),	• Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, • Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, • Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, • Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, • Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, • Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – • 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), • Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, • Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), • Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, • Obsługa list kontroli dostępu (ACL) następujących typów: • Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, • VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, • Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); • Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),

		• Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), • Funkcja Private VLAN z obsługą dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS, • Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci,
9.	Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:	• sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, • sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
10.	Mechanizmy związane z zapewnieniem jakości usług w sieci:	• Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, • Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do • innych (Strict Priority), • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: • źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), • Kontrola sztormów dla ruchu broadcast/multicast/unicast, • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
11.	Obsługa protokołów i mechanizmów routingu:	• Routing statyczny dla IPv4 i IPv6, • Routing dynamiczny – RIP, OSPF do 1000 routes • Policy-based routing (PBR),

		• Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup, • Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
12.	Dodatkowe wymagania	• Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, • RSPAN, • Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego, • Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane • zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), • Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ) • Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
13.	Funkcjonalność sondy IP SLA Responder, 22. Zarządzanie	• Port konsoli, • Dedykowany port Ethernet do zarządzania out-of-band, • Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA, • Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,

		• Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog, • Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, • Wsparcie dla protokoły RESTCONF, Wsparcie dla protokołu gNMI, • Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych, • Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą, • Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB, • Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym • (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne • bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,
14.	Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający	c) Monitoring pracy przełącznika w zakresie: a. Użycie CPU, użycie pamięci, temperatura pracy, b. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny, c. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, d. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router) E. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN,

liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,

e. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
f. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
g. Protokół REP (Resilient Ethernet Protocol),
h. Protokół STP (Spanning Tree Protocol),
i. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),

d) Konfigurację przełącznika w zakresie:
   a. Konfiguracja interfejsów:
      i. Fizycznych:

- - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
- - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),
- - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,
- - przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

      ii. ogicznych typu „port channel":

- opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,

		• w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla • portu dostępowego, natywna sieć VLAN, • przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) iii. Wirtualnych typu SVI: • opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP) • Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN, • Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), • Konfiguracja mechanizmów SPAN i RSPAN, • Konfiguracja protokołu STP, ⍰⍰ Konfiguracja protokołu REP, • Konfiguracja routingu statycznego i dynamicznego, • Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów, • Tworzenie i przypisanie list kontroli dostępu ACL, • Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, • Konfiguracja i uruchomienie NetFlow, • Konfiguracja polityk QoS, • Administracja przełącznika w zakresie: • Zdalne uruchamianie komend linii poleceń, • Nazwa przełącznika, • Tryb pracy L2/L3, • Adres IP przełącznika do celów zarządzania zdalnego, • Konfiguracja serwera DHCP, • Konfiguracja DNS,

		• Czas systemowy w tym protokół NTP, • Konta administracyjne, • Upgrade oprogramowania, Backup konfiguracji, • Zdalny restart urządzenia, Konfiguracja i dostęp przez SNMP, Diagnostyka urządzenia: • Narzędzie PING i TRACEROUTE, • Przeglądanie logów systemowych, • Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
15.	Parametry fizyczne	• Przystosowany do montażu w szafie rack 19", • Wysokość urządzenia 1 RU, • Głębokość chassis urządzenia bez wentylatorów i zasilaczy: mniejsza niż 30 cm Głębokość chassis urządzenia z wentylatorami i zasilaczami: mniejsza niż 33 cm
16.	Ukompletowanie urządzenia	• Przełącznik wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy zasilacza podstawowego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania, • Przełącznik wyposażony w moduł do łączenia w stos wraz z kablem stakującym o długości 3m, • Przełącznik wyposażony w następujące wkładki interfejsowe: 10Gigabit Ethernet 10GBase-SR, • Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat
17.	Gwarancja i wsparcie techniczne	• Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); • Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii.

		• Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą przez cały okres gwarancji i obejmuje: ○ Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej ○ Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji

4.4.3 Przełącznik sieciowy Typ C – Prawo Opcji

Tabela 19 Wymagania dla przełącznika sieciowego Typ C

Lp.	Nazwa parametru	Opis parametru
1.	Typ i liczba portów:	48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP
2.	Moc dostępna dla PoE:	740W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie redundantnym),
3.	Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:	• Gigabit Ethernet 1000Base-T, • Gigabit Ethernet 1000Base-SX, • Gigabit Ethernet 1000Base-LX/LH, • Gigabit Ethernet 1000Base-EX, • Gigabit Ethernet 1000Base-ZX, • Gigabit Ethernet 1000Base-BX-D/U, • 10Gigabit Ethernet 10GBase-SR, • 10Gigabit Ethernet 10GBase-LR, • 10Gigabit Ethernet 10GBase-ER, • 10Gigabit Ethernet 10GBase-ZR, • 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
4.	Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:	• Przepustowość w ramach stosu - 80Gb/s, • 8 urządzeń w stosie, • Zarządzanie poprzez jeden adres IP, • Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
5.	Zasilanie i chłodzenie:	• Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), • W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika), • Redundantne wentylatory,
6.	Parametry wydajnościowe:	• Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 256 Gb/s (z podłączeniem do stosu)

		• Prędkość przesyłania (forwarding rate): 130.95 Mpps
		• Bufor pakietów – 6MB
		• Pamięć DRAM – 2GB
		• Pamięć flash – 4GB
		• Obsługa:
		  ○ 500 aktywnych sieci VLAN
		  ○ 16000 adresów MAC
		  ○ 3000 tras IPv4
		  ○ 1500 tras IPv6
		  ○ Ilość wpisów w listach kontroli dostępu Security ACL – 1000
		  ○ ilość wpisów w listach kontroli dostępu QoS ACL – 1000
		  ○ 512 interfejsów SVI L3
		  ○ Jumbo frame 9198B
		  ○ 48 połączeń zagregowanych typu „port channel”
		  ○ 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP

7.	Obsługa protokołów	• Obsługa protokołu NTP • Obsługa IGMPv1/2/3 i MLDv1/2 Snooping • Obsługa protokołu LLDP i LLDP-MED
8.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci	• IEEE 802.1w Rapid Spanning Tree • Per-VLAN Rapid Spanning Tree (PVRST+) • IEEE 802.1s Multi-Instance Spanning Tree • Obsługa 64 instancji protokołu STP • Wsparcie dla protokołu REP (Resilient Ethernet Protocol) • Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku podstawowego
9.	Dodatkowe funkcje	• Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ)

		• Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego • Możliwość uruchomienia funkcji serwera DHCP • Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN, • Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego, • Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
10.	Mechanizmy związane z bezpieczeństwem sieci:	• Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), • ·Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, • Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, • · Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, • Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, • ·Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, • ·Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

		• Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – • 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), • Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, • Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), • Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, Obsługa list kontroli dostępu (ACL) następujących typów: o Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, o VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, o Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, o Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); • Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika(dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA), • Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing), • Funkcja Private VLAN z obsługą dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS, • Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci,

11.	Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:	• sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, • bezpieczna sekwencja uruchamiania, • sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
12.	Mechanizmy związane z zapewnieniem jakości usług w sieci:	• Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, • Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), • Kontrola sztormów dla ruchu broadcast/multicast/unicast, • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
13.	Obsługa protokołów i mechanizmów routingu:	• Routing statyczny dla IPv4 i IPv6, • Routing dynamiczny – RIP, OSPF do 1000 routes, • Policy-based routing (PBR), • Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup, • Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
14.	Funkcjonalność sondy IP SLA Responder, 23. Zarządzanie	• Port konsoli, • Dedykowany port Ethernet do zarządzania out-of-band, • Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego

		adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA, • Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, • Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog, • Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, • Wsparcie dla protokoły RESTCONF, • Wsparcie dla protokołu gNMI, • Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych, • Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą, • Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB • Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki • logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące, • wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający: c. Monitoring pracy przełącznika w zakresie: i. Użycie CPU, użycie pamięci, temperatura pracy, ii. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,

		iii. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy, iv. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router) v. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, vi. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast, vii. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik, Protokół REP (Resilient Ethernet Protocol), viii. IProtokół STP (Spanning Tree Protocol), ix. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy), d. Konfigurację przełącznika w zakresie: i. Konfiguracja interfejsów: 1. Fizycznych: • - opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, • - w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP), • - w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości

		adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy • MAC przełącznika), konfiguracja 802.1x, • - przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) 2. Logicznych typu „port channel": • opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3, • w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, • w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych) 3. Wirtualnych typu SVI: • opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP) Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN, • Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu • (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.), • Konfiguracja mechanizmów SPAN i RSPAN, • Konfiguracja protokołu STP, • Konfiguracja protokołu REP, Konfiguracja routingu statycznego i dynamicznego,

		Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów, Tworzenie i przypisanie list kontroli dostępu ACL, • Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego, • Konfiguracja i uruchomienie NetFlow, • Konfiguracja polityk QoS, • Administracja przełącznika w zakresie: • Zdalne uruchamianie komend linii poleceń, • Nazwa przełącznika, • Tryb pracy L2/L3, • Adres IP przełącznika do celów zarządzania zdalnego, • Konfiguracja serwera DHCP, • Konfiguracja DNS, • Czas systemowy w tym protokół NTP, • Konta administracyjne, • Upgrade oprogramowania, • Backup konfiguracji, • Zdalny restart urządzenia, • Konfiguracja i dostęp przez SNMP, • Diagnostyka urządzenia: • Narzędzie PING i TRACEROUTE, • Przeglądanie logów systemowych, • Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
15.	Parametry fizyczne:	• Możliwość montażu w szafie rack 19”, • Wysokość urządzenia 1 RU, • Głębokość chassis urządzenia bez wentylatorów i zasilaczy: mniejsza niż 30 cm • Głębokość chassis urządzenia z wentylatorami i zasilaczami: mniejsza niż 33 cm
16.	Ukompletowanie urządzenia	• Przełącznik wyposażony w zasilacz podstawowy oraz dodatkowy zasilacz zapasowy o mocy analogicznej do mocy zasilacza

		podstawowego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania, • Przełącznik wyposażony jest w moduł do łączenia w stos wraz z kablem stakującym o długości 1m, · Przełącznik wyposażony jest w następujące wkładki interfejsowe: 10Gigabit Ethernet 10GBase-SR, • Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat,
17.	Gwarancja i wsparcie techniczne	• Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); • Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii. Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą przez cały okres gwarancji i obejmuje: o Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej o Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji.

4.4.4 Przełącznik sieciowy Typ D – Prawo Opcji

Tabela 20 Wymagania dla przełącznika sieciowego Typ D

Lp.	Nazwa parametru	Opis parametru
1.	Przełącznik musi posiadać:	• 48 portów 1000BaseT lub 1/10GBASE-T • 6 portów uplink, w tym min. 2 porty 40/100GE definiowane za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m).
2.	Parametry wydajnościowe:	• Prędkość przełączania 348Gbps full duplex • Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3.	Przełącznik posiada następującą funkcjonalność dla warstwy L2:	m) Trunking IEEE 802.1Q VLAN; n) Wsparcie dla 3000 sieci VLAN; o) Wsparcie sprzętowe dla 90 tysięcy adresów MAC p) IEEE 802.1w Rapid Spanning Tree (RST) q) IEEE 802.1s Multiple Spanning Tree (MST) r) Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU) s) Internet Group Management Protocol (IGMP) Versions 2, 3; t) Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach u) Link Aggregation Control Protocol (LACP): IEEE 802.3ad v) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów); w) Funkcjonalność izolowania portów znajdujących się w tym samym VLAN x) Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4.	Przełącznik posiada następującą funkcjonalność dla warstwy L3:	m) Sprzętowe przełączanie pakietów w warstwie L3 n) Routing w oparciu o trasy statyczne o) Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. p) Policy Based Routing (PBR) q) VRRP r) Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6 g. Tunele GRE s) Wsparcie sprzętowe dla minimum 750 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP i. Wsparcie dla min. 32 VRF

		t) Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP) u) Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast) v) Wsparcie dla IGMPv3 oraz MSDP w) Wsparcie sprzętowe dla minimum 32,000 tras multicastowych x) Obsługa minimum 5000 wpisów dla ACL (access control list)
5.	Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:	g) Zintegrowany, sprzętowy VXLAN Bridging/Routing h) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) i) Implementacja VXLAN BGP EVPN (Ethernet VPN) j) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności k) Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN) l) Mechanizm wykrywania i zapobiegania efektom pętli w podłączone infrastrukturze L2 poprzez mechanizm VXLAN OAM
6.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:	i) Layer 2 IEEE 802.1p (CoS) oraz DSCP j) Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6) k) Kolejkowanie bezwzględne (strict-priority) l) Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection) m) Ograniczanie ruchu (policing) do zadanej przepływności n) Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych o) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb p) Protokół RDMA/RoCE, DCBX oraz ECN
7.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci	l) Obsługa list kontroli dostępu (ACL) m) ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu; n) ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), o) TCP, User Datagram Protocol (UDP); p) ACL oparte o porty (PACL); q) DHCP Snooping r) ARP Inspection s) IP Source Guard

		t) Unicast reverse path forwarding (uRPF) u) Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast v) MacSec na portach SFP+ i QSFP28. Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie
8.	Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:	t) Port zarządzający 100/1000 Mbps; u) Port konsoli CLI; v) Zarządzanie In-band; w) SSHv2; x) Authentication, authorization, and accounting (AAA); y) RADIUS; z) TACACS+ aa) Syslog; bb) SNMP v1, v2c, v3; cc) Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB. k. Role-Based Access Control RBAC; dd) IEEE 802.1ab LLDP ee) Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) n. 802.1x ff) Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) gg) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring) hh) Network Time Protocol (NTP); ii) Precision Time Protocol IEEE 1588 jj) Diagnostyka procesu BOOT; kk) Ping ll) Traceroute
9.	Telemetria z control/data plane eksportowana w interwałach co najmniej 100 milisekund bezpośrednio z	e) Informacji o przepływie (flow), zawierają dane o adresach IP, protokołach, portach, kiedy przepływ się rozpoczął, jak długo przepływ był aktywny , ile było w nim sumarycznie danych itp. f) Zmienność między pakietami, daje wgląd w zmiany pomiędzy pakietami w danym przepływie. Przykłady obejmują zmiany czasu życia (TTL), flagi IP i TCP, długość payload itp.

	układu ASIC przełącznika. Wsparcie dla narzędzi programistycznych w standardzie „OpenTelemetry". Eksportowane dane w formacie gRPC lub GPB dostarczają następujące informacje (dla każdego przepływu/flow	Szczegóły kontekstu przepływu, informacje te są uzyskiwane poza nagłówkiem pakietu, w tym zmiany w wykorzystaniu bufora kolejki, powód odrzucania pakietów w przepływie (bufor, routing, ACL), powiązanie z końcami tunelu VXLAN (VTEP) itp. g) Dodatkowo funkcjonalność telemetrii pozwalająca na pozyskanie metadanych o każdym przepływie, który spełnia określone kryteria (np. odrzucenie, opóźnienie, microburst) z dodatkowymi informacjami identyfikującymi przyczynę (np. ACL/routing/bufor drop, opóźnienie dla scieżki, wystąpienie microburst itp.) h) Jeśli funkcjonalność ta wymaga dodatkowej licencji nie jest wymagane jej dostarczenie na tym etapie
10.	Narzędzia programowania i zarządzania przełącznikiem:	h) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API i) Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika j) Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. k) Interfejs programistyczny REST API wraz z upublicznionym SDK l) Możliwość zainstalowania klienta Chef m) Możliwość zainstalowania agenta Puppet n) Wsparcie dla OpenStack Neutron plugin
11.	Ogólne parametry	e) Przełącznik jest wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz f) wentylatory w konfiguracji zapewniającej, wyrzut powietrza od strony portów liniowych; g) bud owa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19". h) Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem zarządzającym (kontrolerem sieci SDN).

12.	Wyposażenie przełącznika musi obejmować:	f) wkładki QSFP 100/40GE umożliwiające połączenie 100GE lub 40GE z wykorzystaniem pojedynczej pary światłowodów wielomodowych (bidirectional) wkładki SFP+ typu 10GBASE-SR
13.	Gwarancja	g) Wymagane min. 36 miesięcy gwarancji od momentu podpisania protokołu odbioru realizowane w reżimie 8x5xNBD w godzinach od 8.00 lub wcześniej do godz. 16.00 lub później (co najmniej 8 godzin w każdym dniu); h) Wymiana uszkodzonego urządzenia albo kluczowych elementów warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) w następnym dniu roboczym od zgłoszenia awarii. i) Usługa wsparcia i aktualizacji przez producenta dla przełączników świadczone będą przez cały okres gwarancji i obejmuje: Zgłaszanie błędów i pomoc w rozwiązywaniu problemów przez producenta w dni robocze, świadczoną w ciągu godzin pracy określonych w punkcie powyżej j) Wymagany dostęp do najnowszego oprogramowania oraz oprogramowania typu hotfix i service pack urządzenia w okresie gwarancji.

Projekt jest współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020

Spis tabel

Tabela 1 Harmonogram wdrożenia 13
Tabela 2 Specyfikacja ilościowa 21
Tabela 3 Opis parametrów Przełącznik sieciowy Typ A – Rozbudowa obecnej infrastruktury sieciowej 22
Tabela 4 Wymagania dla przełącznika sieciowego Typ B – Rozbudowa obecnej infrastruktury sieciowej**Błąd! Nie zdefiniowano zakładki.**
Tabela 5 Wymagania dla przełącznika sieciowego Typ C – Rozbudowa obecnej infrastruktury sieciowej**Błąd! Nie zdefiniowano zakładki.**
Tabela 6 Wymagania dla przełącznika sieciowego Typ D – Rozbudowa obecnej infrastruktury sieciowej**Błąd! Nie zdefiniowano zakładki.**
Tabela 7 Opis parametrów Przełącznik sieciowy Typ E – Rozbudowa obecnej infrastruktury sieciowej**Błąd! Nie zdefiniowano zakładki.**
Tabela 8 Wymagania dla Urządzenia ochrony przed rozproszonymi atakami sieciowymi 57
Tabela 9 Wymagania dla jednego urządzenia ochrony przed rozproszonymi atakami sieciowymi 62
Tabela 10 Opis parametrów Systemów analizy i zarządzania ..... **Błąd! Nie zdefiniowano zakładki.**
Tabela 11 Opis wymagań Serwer RACK ..... **Błąd! Nie zdefiniowano zakładki.**
Tabela 12 Opis wymagań Przełącznik sieciowy SAN 87
Tabela 13 Opis wymagań Macierz typ 1 90
Tabela 14 Opis wymagań Macierz typ 2 95
Tabela 16 Opis wymagań Serwer RACK – Prawo opcji 101
Tabela 17 Wymagania dla przełącznika sieciowego Typ B 107
Tabela 18 Wymagania dla przełącznika sieciowego Typ C 117
Tabela 19 Wymagania dla przełącznika sieciowego Typ D 127