IT.262.1.2026

Załącznik nr 2 do SWZ

Szczegółowy opis przedmiotu zamówienia

1. Przedmiot zamówienia

Przedmiotem zamówienia jest zakup trzech routerów rdzeniowych miejskiej sieci światłowodowej oraz integracja nowych urządzeń z istniejącą infrastrukturą sieciową Zamawiającego. Wraz z urządzeniami należy dostarczyć odpowiednie licencje systemu zarządzania.

Celem zakupu jest zapewnienie dalszego rozwoju sieci MAN, zwiększenie efektywności energetycznej infrastruktury, ograniczenie zajmowanej przestrzeni w szafach telekomunikacyjnych oraz przygotowanie środowiska do dalszej sukcesywnej wymiany urządzeń, które zakończyły swój cykl życia.

Dostarczone urządzania i oprogramowanie muszą pochodzić od jednego producenta.

1.1 Zakres rzeczowy zamówienia

Zakres zamówienia obejmuje:

1) Dostawę 3 sztuk jednakowych urządzeń szkieletowych spełniających wymagania techniczne określone w Tabeli 1.
2) Dostawę licencji dla Systemu Zarządzania, spełniającego wymagania określone w Tabeli 2.
3) Dostawę wkładek światłowodowych, kompatybilnych zarówno z nowo dostarczanymi urządzeniami, jak i urządzeniami Juniper Networks pracującymi w sieci Zamawiającego, określonych w Tabeli 3.
4) Przeprowadzenie analizy przedwdrożeniowej w celu znalezienia optymalnego wariantu instalacji dostarczonych urządzeń, z założeniem osiągniecia wymaganych w przedmiocie zamówienia celów oraz utrzymaniem istniejącej funkcjonalności sieci oraz jakości usług.
5) Opracowanie projektu technicznego.
6) Opracowanie dokumentacji wdrożeniowej.
7) Demontaż istniejących urządzeń tych, których konieczność wymiany wyniknie z przeprowadzonej analizy .
8) Instalację, montaż oraz uruchomienie dostarczonych urządzeń w zamian za urządzenia zdemontowane.
9) Wykonanie niezbędnych prac rekonfiguracyjnych związanych z migracją usług z urządzeń istniejących na urządzenia dostarczane.
10) Integrację nowych urządzeń z istniejącą infrastrukturą IP/MPLS Zamawiającego.
11) Opracowanie dokumentacji powykonawczej.
12) Wykonanie testów odbiorowych.
13) Przeprowadzenie migracji usług produkcyjnych.
14) Przeprowadzenie szkoleń i warsztatów technicznych dla administratorów Zamawiającego.
15) Zapewnienie wsparcia technicznego i gwarancyjnego.

Wszystkie czynności niezbędne do osiągnięcia pełnej funkcjonalności rozwiązania należy traktować jako objęte zakresem zamówienia, nawet jeżeli nie zostały wymienione wprost w niniejszym dokumencie.

Dodatkowo Zamawiający wymaga przeprowadzenia testów POC (Proof of Concept) w celu potwierdzenia spełnienia wszelkich wymogów opisanych w niniejszym postępowaniu.

2. Stan obecny

Zamawiający eksploatuje sieć MAN opartą o rozwiązania firmy Juniper Networks.

Sieć MAN pracuje w topologii pierścienia łączącego 5 węzłów szkieletowych typu P wyposażonych w urządzenia Juniper serii MX, do których podłączone są urządzenia dostępowo-dystrybucyjne PE Juniper serii ACX. Zamawiający, w niedalekiej przyszłości, planuje zredukować liczbę węzłów P do 3 sztuk.

Sieć stanowi wielousługową infrastrukturę IP/MPLS wykorzystywaną do świadczenia usług transmisji danych oraz usług głosowych.

W sieci wykorzystywane są następujące technologie:
- protokół routingu OSPF jako protokół IGP,
- MPLS,
- LDP jako protokół dystrybucji etykiet MPLS,
- RSVP-TE,
- BGP jako protokół realizujący usługi VPN,
- Route Reflection dla protokołu BGP.

Podstawowymi usługami realizowanymi w sieci są:
- L2VPN,
- L3VPN,
- usługi transmisji danych,
- usługi telefonii IP pomiędzy jednostkami samorządu terytorialnego.

Dwa routery szkieletowe pełnią funkcję Route Reflectorów dla protokołu BGP.
Na urządzeniach szkieletowych P oraz dystrybucyjnych PE wdrożone są mechanizmy ochrony płaszczyzny sterowania (Control Plane Protection) ograniczające możliwość przeciążenia urządzeń oraz umożliwiające dostęp do usług zarządzających wyłącznie z zaufanych sieci.

Jedną z kluczowych usług realizowanych z wykorzystaniem sieci MAN jest łączność telefoniczna VoIP pomiędzy jednostkami samorządowymi. Zapewnienie ciągłości działania tej usługi stanowi jeden z podstawowych wymogów stawianych modernizowanej infrastrukturze.

3. Stan docelowy

Zamawiający planuje wymianę urządzeń w wybranych, w analizie przedwdrożeniowej, węzłach szkieletowych.

Urządzenia eksploatowane obecnie zakończyły lub w najbliższym czasie zakończą swój cykl życia producenta (EOL/EOS), co uzasadnia konieczność ich sukcesywnej wymiany.

Nowa infrastruktura powinna zapewnić:
- pełną funkcjonalność istniejącej sieci IP/MPLS,
- możliwość dalszej rozbudowy sieci,
- ograniczenie poboru energii elektrycznej,
- zmniejszenie zajmowanej przestrzeni montażowej,
- co najmniej utrzymanie obecnego poziomu niezawodności, oraz wydajności.

4. Wymagania funkcjonalne

Wszystkie wymagania Zamawiającego jakie musi spełniać oferowane rozwiązanie zawarte są w Tabeli 1, Tabeli 2 i Tabeli 3. Oferowane rozwiązanie musi umożliwiać realizację wszystkich funkcjonalności wykorzystywanych obecnie przez Zamawiającego oraz zapewnić pełną interoperacyjność pomiędzy dostarczonymi urządzeniami, a obecnie używanymi urządzeniami Juniper Networks.

5. Wymagania dotyczące interoperacyjności

Zamawiający zakłada, że po realizacji tego projektu sieć będzie funkcjonowała jako środowisko składające się z działających urządzeń Juniper Networks oraz urządzeń dostarczonych w ramach niniejszego postępowania. W związku z tym należy zapewnić pełną interoperacyjność pomiędzy dostarczonymi urządzeniami, a obecnie używanymi urządzeniami Juniper Networks.

Przez pełną interoperacyjność Zamawiający rozumie możliwość zestawienia, utrzymania oraz eksploatacji wszystkich wymaganych protokołów, usług oraz mechanizmów ochronnych pomiędzy urządzeniami dostarczanymi i obecnie używanymi bez ograniczenia funkcjonalności oraz pogorszenia parametrów pracy.

Wykonawca zobowiązany jest zapewnić pełną współpracę oferowanego rozwiązania z istniejącą infrastrukturą Zamawiającego bez konieczności:

- zmiany planu adresacji IP,
- zmiany numeracji ASN,
- zmiany modelu świadczenia usług,
- zmiany parametrów usług VPN,
- rekonfiguracji urządzeń klienckich,
- przebudowy istniejących usług MPLS.

Wszelkie koszty związane z identyfikacją, analizą oraz usunięciem problemów interoperacyjności ponosi Wykonawca.

Współpraca oferowanego rozwiązania z infrastrukturą klienta (interoperacyjność) musi zostać poparta wykonaniem POC, zgodnie z wymaganiami zawartymi w punkcie 7.

Wykonawca zobowiązany jest dostarczyć raport interoperacyjności obejmujący:

- opis wykonanych testów,
- scenariusze testowe,
- wyniki testów,
- rekomendacje producenta.

Raport musi zostać przekazany Zamawiającemu przed rozpoczęciem migracji produkcyjnej.

Za spełnienie wymagań interoperacyjności Zamawiający uzna wyłącznie rozwiązanie, dla którego wykazano poprawną współpracę ze wszystkimi eksploatowanymi elementami infrastruktury Juniper Networks w zakresie protokołów, usług oraz mechanizmów określonych w niniejszym dokumencie.

W przypadku niewykazania interoperacyjności w trakcie testów POC Zamawiający zastrzega sobie prawo do odrzucenia rozwiązania na etapie PoC.

6. Wymagania dotyczące migracji

Migracja musi zostać przeprowadzona w sposób zapewniający ciągłość działania wszystkich usług produkcyjnych.

W szczególności niedopuszczalne jest:

- zmiana funkcjonalności i zakresu istniejących usług IP/MPLS oraz dostępu do Internetu,
- zmiana planu adresacji IP,
- zmiana numeracji ASN,
- zmiana architektury routingu i MPLS,
- pogorszenie parametrów jakościowych usług głosowych i transmisji danych, utrata separacji tablic routingu w obecnie uruchomionych usługach L3VPN pomiędzy punktami dostępu do usług na urządzeniach PE,

Wykonawca zobowiązany jest przygotować szczegółowy plan migracji zawierający:

- harmonogram prac,
- analizę ryzyka,
- plan wycofania zmian (rollback),
- procedury testowe.

Procedura rollback musi umożliwiać przywrócenie stanu sprzed migracji bez utraty konfiguracji oraz usług produkcyjnych.

Zachowanie usług końcowych

Migracja nie może powodować konieczności rekonfiguracji usług po stronie użytkowników końcowych ani urządzeń przyłączonych do sieci MAN.

W szczególności niedopuszczalne jest wymaganie:
- zmiany planu adresacji IP użytkowników,
- zmiany konfiguracji urządzeń klienta końcowego CPE,
- zmiany konfiguracji systemu telefonii IP,
- zmiany konfiguracji systemów transmisyjnych korzystających z usług VPN np. zmiana parametrów pracy interfejsów podłączonych do urządzeń CPE,
- zmiany parametrów routingu po stronie klientów usług VPN,
- zmiany konfiguracji urządzeń przyłączonych do usług VPWS, VPLS lub L3VPN.

Proces migracji musi pozostać transparentny dla użytkowników końcowych oraz systemów korzystających z infrastruktury MAN bez wpływu na jakość dostarczanych usług.

Zachowanie numeracji i identyfikatorów usług

Migracja nie może wymagać zmiany :

- identyfikatorów VRF:
  - Identyfikatorów Route Distinguisher (RD),
  - Identyfikatorów Route Target (RT),
- numeracji VLAN wykorzystywanej przez istniejące usługi,
- numeracji ASN,
- adresacji IP wykorzystywanej przez usługi produkcyjne.

Wszelkie odstępstwa od powyższych wymagań wymagają uprzedniej pisemnej zgody Zamawiającego.

W trakcie realizacji migracji oraz po jej zakończeniu musi zostać zachowana pełna funkcjonalność istniejących usług świadczonych przez sieć MAN.

Migracja nie może wymagać zmiany modelu świadczenia usług oraz rekonfiguracji urządzeń pozostających w eksploatacji poza zakresem niezbędnym do przyłączenia nowych urządzeń, np. urządzeń CPE.

W szczególności musi zostać zachowane działanie:
- Protokołu MPLS jako transportu dla ruchu w poszczególnych L2VPN oraz L3VPN,
- OSPF jako protokołu IGP,
- LDP jako protokołu dystrybucji etykiet MPLS w sieci dostępowej,
- RSVP-TE, jako protokołu dystrybucji etykiet MPLS w sieci szkieletowej,
- BGP Labeled Unicast jako protokołu dystrybucji etykiet MPLS dla tras do interfejsów, loopback routerów P/PE,
- LDP/IGP Synchronization,
- Fast Reroute,
- BFD dla usług IP i MPLS.
- L3VPN IPv4,
- L2VPN standard Martini lub Compella,
- VPWS,
- Route Reflection
- Targeted LDP session.

Musi zostać zachowana obsługa:
- BGP Community,
- BGP Extended Community,

- BGP Local Preference,
- BGP MED,
- BGP AS-Path Prepending,
- Już działających w sieci parametrów Route Targets,
- Już działających w sieci parametrów Route Distinguishers.

Migracja nie może powodować utraty funkcjonalności mechanizmów QoS.
W szczególności wymagane jest zachowanie:
- klasyfikacji ruchu,
- oznaczeń DSCP,
- oznaczeń MPLS EXP/TC,
- kolejkowania ruchu,
- priorytetyzacji ruchu głosowego,
- mechanizmów ograniczania i kształtowania ruchu.

Migracja nie może powodować pogorszenia parametrów transmisyjnych usług telefonii IP.
Musi zostać zachowana:
- ciągłość połączeń głosowych,
- priorytetyzacja ruchu głosowego,
- zgodność z istniejącymi politykami QoS.

Migracja nie może wymagać:
- zmiany planu adresacji IP,
- zmiany numeracji ASN,
- zmiany numeracji VRF,
- zmiany parametrów Route Distinguisher,
- zmiany parametrów Route Target,
- zmiany modelu realizacji usług VPN.

7. Proof of Concept (PoC)

Wykonawca przeprowadzi testy PoC oferowanych urządzeń połączone z testami interoperacyjności z obecnie użytkowanymi urządzaniami Zamawiającego. Na każdym etapie przeprowadzanych testów Zamawiający zastrzega sobie prawo do udziału w nich.

PoC musi obejmować co najmniej:
Routing
- sąsiedztwo OSPF,
- wymianę tras IPv4 i IPv6,
- rekonwergencję po awarii łącza,
- rekonwergencję po awarii urządzenia.

MPLS
- zestawienie sesji LDP,
- dystrybucję etykiet MPLS,
- przełączanie ruchu MPLS,
- LDP/IGP Synchronization.

RSVP-TE
- ustanawianie ścieżek,
- rekonwergencję po awarii,
- odtworzenie ścieżek.

BGP

- peering z Route Reflectorem,
- wymianę tras VPNv4,
- obsługę Community,
- obsługę Extended Community,
- Graceful Restart.

VPN

- L3VPN,
- L2VPN,
- QoS,
- zachowanie oznaczeń DSCP,
- zachowanie oznaczeń MPLS EXP/TC,
- poprawność działania polityk QoS.

BFD

- współpracę z OSPF,
- współpracę z BGP,
- współpracę z RSVP-TE.

Testy interoperacyjności

Wykonawca zobowiązany jest przeprowadzić testy współpracy dostarczonych urządzeń z istniejącymi routerami Juniper MX oraz wykazać poprawne działanie następujących usług w następującej konfiguracji:

- Utworzenie testowego węzła MPLS typu P z użyciem testowanego (dostarczanego) urządzenia. Węzeł będzie podłączony do istniejących węzłów, tj. routerów Juniper MX-480, za pomocą minimum 2 interfejsów 100 Gigabit/s, każdy do innego węzła sieci,

- Podłączenie urządzeń PE Zamawiającego do testowego węzła P sieci MPLS w trybie L3 VPN:

    - Urządzenie Juniper ACX 2100 ma zostać podłączone do testowego węzła sieci MPLS dwoma interfejsami SFP+ 10Gbit, zagregowanymi protokołem LACP. Na punkcie styku P-PE zastosowana sygnalizacja LDP, protokół IGP: OSPF, Sygnalizacja BGP family L3VPN, BGP-LU,

    - Urządzenie Juniper ACX 1100 ma zostać podłączony do testowego węzła sieci MPLS dwoma interfejsami SFP 1Gbit, zagregowanymi protokołem LACP. Na punkcie styku P-PE zastosowana sygnalizacja LDP, protokół IGP: OSPF, Sygnalizacja BGP family L3VPN, BGP-LU,

- Wymagane testy:

    - Weryfikacja protokołów sygnalizacji na styku P-PE i P-P: RSVP, LDP, BGP-LU (labeled unicast), BGP, BGP family L3VPN oraz OSPF. Należy udowodnić brak problemów z kompatybilnością tych protokołów pomiędzy oferowanymi urządzeniami i użytkowanymi urządzeniami Juniper MX480, ACX 2100, ACX 1100,

    - Testy transmisji danych dla usługi L3VPN. Układ testowy powinien być podłączony do urządzenia PE interfejsem 1G. Test będzie polegał na porównaniu transmisji z urządzenia PE Juniper ACX podłączonego do istniejącego węzła P z transmisją z urządzenia PE Juniper ACX podłączonego do testowego węzła P. Dla wariantu z użyciem testowego węzła P, przepustowość oraz utrata pakietów nie powinny być gorsza niż 3%,

- Testy transmisji danych dla usługi L2VPN. Układ testowy powinien być podłączony do urządzenia PE interfejsem 1G. Test będzie polegał na porównaniu transmisji z urządzenia PE Juniper ACX podłączonego do istniejącego węzła P z transmisją z urządzenia PE Juniper ACX podłączonego do testowego węzła P. Dla wariantu z użyciem testowego węzła P, przepustowość oraz utrata pakietów nie powinny być gorsza niż 3%,

Testy aktualizacji oprogramowania

Wykonawca przedstawi procedurę aktualizacji oprogramowania oraz jej wpływ na świadczone usługi.
Pozytywne zakończenie PoC stanowi warunek rozpoczęcia migracji produkcyjnej.
Zamawiający zastrzega sobie prawo do odrzucenia rozwiązania na etapie PoC w przypadku niewykazania pełnej interoperacyjności z eksploatowaną infrastrukturą.

8. Testy odbiorowe

Po zakończeniu wdrożenia Wykonawca zaproponuje scenariusze testów odbiorowych i zrealizuje je w następującym zakresie:

- poprawność działania routingu,
- poprawność działania MPLS,
- poprawność działania usług L2VPN,
- poprawność działania usług L3VPN,
- poprawność działania telefonii IP,
- poprawność działania QoS,
- poprawność działania telemetrii.

Testy awaryjne:

- awaria pojedynczego łącza,
- awaria urządzenia szkieletowego,
- awaria urządzenia brzegowego,
- awaria zasilania,
- odtworzenie działania po usunięciu awarii.

Testy usług głosowych
Testy muszą potwierdzić brak negatywnego wpływu wdrożonego rozwiązania na usługi telefonii IP.

9. Zarządzanie i monitoring

Zamysłem Zamawiającego jest budowa homogenicznej sieci zarządzanej i monitorowanej przez nowoczesny system zarzadzania / monitoringu. Przez nowoczesny Zamawiający rozumie brak wykorzystywania przestarzałego protokołu SNMP na rzecz telemetrii pracującej w czasie rzeczywistym wykorzystującym takie funkcjonalności jak:

- Sreaming Telemetry - eksport danych telemetrycznych w czasie rzeczywistym,
- gNMI,
- OpenConfig,
- NETCONF,
- REST API,
- eksport danych telemetrycznych w czasie rzeczywistym,
- automatyzację konfiguracji z wykorzystaniem API.

Protokół SNMP może być wykorzystywany wyłącznie jako mechanizm pomocniczy do integracji z zewnętrznymi systemami monitoringu (np. Zabbix) i nie stanowi podstawowego mechanizmu komunikacji pomiędzy systemem zarządzania a zarządzanymi urządzeniami.

Szczegółowe wymagania dotyczące systemu zarządzania i monitoringu dostarczanego sprzętu zawarto w Tabeli 2.

10. Wsparcie techniczne i transfer wiedzy

Wykonawca zapewni opiekę techniczną i wsparcie producenta przez okres minimum 36 miesięcy od daty odbioru końcowego.

Wsparcie musi obejmować:
- dostęp do aktualizacji oprogramowania,
- dostęp do poprawek bezpieczeństwa,
- dostęp do dokumentacji technicznej,
- możliwość zgłaszania incydentów technicznych.

Wykonawca przeprowadzi warsztaty techniczne obejmujące:
- architekturę rozwiązania,
- konfigurację usług IP/MPLS,
- diagnostykę i troubleshooting,
- obsługę telemetrii,
- procedury aktualizacji,
- procedury odtworzeniowe.

Warsztaty techniczne powinny trwać minimum 16 godzin.

11. Dokumentacja powykonawcza

Wykonawca dostarczy:
- dokumentację projektową,
- dokumentację wdrożeniową,
- dokumentację powykonawczą,
- schemat logiczny rozwiązania,
- schemat fizyczny rozwiązania,
- konfigurację wszystkich urządzeń,
- plan adresacji,
- zestawienie interfejsów,
- zestawienie usług VPN,
- opis polityk routingu,
- opis polityk QoS,
- raport z PoC,
- raport z testów odbiorowych,
- procedury eksploatacyjne,
- procedury odtworzeniowe,
- procedury aktualizacji oprogramowania.

Dokumentacja musi zostać przekazana w wersji elektronicznej edytowalnej oraz w formacie PDF.

Dokumentacja powykonawcza podlega odbiorowi i zatwierdzeniu przez Zamawiającego.

12. Warunkiem odbioru końcowego jest pisemna akceptacja dokumentacji powykonawczej przez Zamawiającego.

13. Gwarancja

a. Warunki gwarancji i wsparcia serwisowego

- okres gwarancji: minimum 36 miesięcy,
- wsparcie producenta 24x7,
- dostęp do aktualizacji oprogramowania,
- dostęp do poprawek bezpieczeństwa,
- dostęp do bazy wiedzy producenta,
- możliwość eskalacji zgłoszeń do producenta.

b. SLA:

- przyjmowanie zgłoszeń 24x7x365,
- kanały zgłoszeń: portal WWW, e-mail, telefon,
- czasy reakcji: maksymalnie 1 godzina. Czas reakcji rozumiany jest jako czas na potwierdzenie zgłoszenia oraz wyznaczenie terminu naprawy
- czas usunięcia awarii krytycznej: maksymalnie następny dzień roboczy. Przez awarię krytyczną rozumie się taką awarię, której wystąpienie powoduje brak dostępu do sieci teleinformatycznej (włączając w to sieć telefonii VOIP) jakiejkolwiek z przyłączonych do sieci jednostek (obiektów). Pozostałe awarie określane są jako niekrytyczne.
- Zamawiający dopuszcza tryb naprawy tymczasowej polegający na instalacji tymczasowych (a nie docelowych) urządzeń lub modułów/części urządzeń o identycznych parametrach w celu zapewnienia normalnej pracy sieci teleinformatycznej. W razie wykonania naprawy poprzez podstawienia urządzeń lub modułów/części urządzeń o identycznych parametrach, ale nie docelowych, czas wymiany urządzeń lub modułów/części urządzeń zastępczych na docelowe wynosi maksymalnie 7 dni roboczych liczone od momentu pierwotnego zgłoszenia przez Zamawiającego awarii sprzętu.
- Usługi serwisu i wsparcia technicznego muszą być świadczone przez Wykonawcę na miejscu, w siedzibie Zamawiającego. Zamawiający dopuszcza możliwość prowadzenia przez Wykonawcę zdalnego serwisu konfiguracyjnego z zastrzeżeniem, że każdy taki serwis zdalny musi zostać uprzednio (przed jego dokonaniem) zgłoszony Zamawiającemu oraz musi uzyskać aprobatę Zamawiającego co do proponowanego terminu wykonywania prac serwisowych oraz co do ich zakresu.
- Uszkodzony sprzęt może być odbierany od Zamawiającego tylko osobiście przez Wykonawcę – nie dopuszcza się odbioru sprzętu przez podwykonawców, włączając w to firmy kurierskie. Naprawiony sprzęt lub nowy sprzęt (sprowadzany w miejsce uszkodzonego) może być przekazywany Zamawiającemu tylko osobiście przez Wykonawcę – nie dopuszcza się przekazywania Zamawiającemu sprzętu przez podwykonawców, włączając w to firmy kurierskie. W przypadku korzystania przez Wykonawcę (po osobistym odbiorze przez Wykonawcę uszkodzonego sprzętu od Zamawiającego i przed osobistym przekazaniem Zamawiającemu nowego lub naprawionego sprzętu przez Wykonawcę) z pośrednictwa podwykonawców, w tym usług kurierskich, Wykonawca ponosi pełny koszt zabezpieczenia sprzętu podczas całej drogi transportu sprzętu i ubezpieczenia sprzętu na czas transportu i jego naprawy.
- W każdym przypadku dostarczenia przez Wykonawcę naprawionego sprzętu lub części/modułu/sprzętu a także w każdym przypadku wymiany przez Wykonawcę uszkodzonego sprzętu lub części/modułu sprzętu na nowy sprzęt lub nową część/moduł sprzętu, Wykonawca dokona na własny koszt konfiguracji naprawionego lub nowego sprzętu i naprawionej lub nowej części/modułu sprzętu do ustawień jakie posiadał uszkodzony sprzęt lub uszkodzona część/moduł sprzętu przed wystąpieniem awarii. W przypadkach, kiedy podłączenie nowego

lub naprawionego urządzenia a także nowej lub naprawionej części/modułu urządzenia wymaga rekonfiguracji sieci oraz towarzyszącej infrastruktury pasywnej (np. okablowanie), Wykonawca dokona na własny koszt niezbędnej rekonfiguracji sieci oraz zmodyfikuje na własny koszt infrastrukturę pasywną w zakresie uzgodnionym z Zamawiającym, tak, by zapewnić funkcjonowanie sieci w zakresie odpowiadającym stanowi funkcjonowania sprzed wystąpienia awarii sprzętu.

14. Warunki odbioru

Warunkiem odbioru końcowego będzie:

- dostarczenie wszystkich urządzeń objętych zamówieniem,
- wykonanie migracji zgodnie z zaakceptowanym planem,
- pozytywne zakończenie testów PoC,
- pozytywne zakończenie testów interoperacyjności,
- pozytywne zakończenie testów odbiorowych,
- pozytywne zakończenie testów awaryjnych,
- dostarczenie kompletnej dokumentacji powykonawczej,
- potwierdzenie zachowania ciągłości działania wszystkich usług produkcyjnych,
- dostarczenie dokumentu wystawionego przez producenta potwierdzającego, że oferowane urządzenia i oprogramowanie pochodzą z oficjalnego kanału sprzedaży producenta na terenie Polski i są objęte gwarancją na okres minimum 36 miesięcy.

Zamawiający zastrzega sobie prawo do odmowy odbioru rozwiązania w przypadku niewykazania pełnej interoperacyjności z istniejącą infrastrukturą Juniper Networks lub niespełnienia któregokolwiek z wymagań określonych w niniejszym dokumencie.

Tabela 1

MINIMALNE WYMAGANIA SPRZĘTOWE	
Konfiguracja Urządzenia	
1.	Minimalna ilość portów QSFP 1x100GE - 8 sztuk
2.	Minimalna ilość portów SFP+ obsługujących 1GE/10GE/25GE – 48 sztuk
3.	Urządzenie musi być wyposażone w zasilacze zmiennoprądowe i wentylatory pracujące w konfiguracji redundantnej. W celu zachowania redundancji zasilania, każde urządzenie musi poprawnie działać po awarii jednego zasilacza. Zanik napięcia na jednym z obwodów zasilających, nie może spowodować przerwy w działaniu urządzenia.
4.	Urządzenie musi umożliwiać instalację, wymianę lub zamianę zasilaczy w trakcie pracy urządzenia (ang. hot-swap).
5.	Urządzenie musi umożliwiać instalację, wymianę lub zamianę wentylatorów w trakcie pracy urządzenia (ang. hot-swap).
6.	Urządzenie musi umożliwiać instalację, wymianę lub zamianę poszczególnych modułów (takich jak karty z interfejsami sieciowymi, moduły optyczne) w trakcie pracy urządzenia (ang. hot-swap).
7.	Obudowa przeznaczona do montażu w szafie rack 19, maksymalny rozmiar w jednostkach RackUnit (wysokość) 2U
8.	Maksymalna głębokość obudowy Urządzenia 65 [cm]
9.	Wymagany kierunek przepływu powietrza (front określony jako lokalizacja portów we/wy): front - tył
10.	Urządzenie musi poprawnie pracować w zakresie temperatur: 0-40 ^{O}C
11.	Urządzenie musi poprawnie pracować przy względnej wilgotności powietrza co najmniej w zakresie od 5% do 90% zakładając brak występowania zjawiska kondensacji pary wodnej.
12.	Urządzenia muszą mieć odblokowane wszystkie wymagane funkcjonalności, a jeśli potrzebne są do tego licencje dostawca musi je dostarczyć wraz z urządzeniami. Licencje nie mogą być czasowe. Restart Elementów nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych potrzebnych do odblokowania wszystkich wymaganych funkcjonalności. Licencje powinny być lokalne dla każdego urządzenia - nie dopuszcza się komunikacji z systemami trzecimi w celu utrzymywania/weryfikacji licencji.
13.	Wszystkie interfejsy liniowe urządzeń muszą być bezterminowo odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanych urządzeniach
14.	Urządzenie musi posiadać wsparcie techniczne producenta oraz być w komercyjnie dostępnej wersji, tj. wersji oferowanej wszystkim klientom i widoczne publicznie na stronie producenta. Niedopuszczalne jest wykorzystanie urządzeń prototypowych.
15.	Oprogramowanie musi posiadać wsparcie techniczne producenta oraz być w komercyjnie dostępnej wersji, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wykorzystanie oprogramowania prototypowego, wytwarzanie wersji oprogramowania wyłącznie na potrzeby projektu - nieoferowanej innym klientom.
16.	Wszystkie urządzenia oraz elementy współpracujące z nimi (np. moduły optyczne) muszą być fabrycznie nowe (tj. nieużywane za wyjątkiem wykonania testów potrzebnych do sprawdzenia ich poprawnego działania). Na dzień złożenia oferty żadne z oferowanych urządzeń nie może być przeznaczone do wycofania ze sprzedaży przez producenta (ang. end of sale) ani nie może być wiadomym, że urządzenia te nie będą objęte pomocą techniczną producenta (ang. end of life).
17.	Usługi wsparcia muszą obejmować dostęp do wszelkich aktualizacji, łat i poprawek (w tym możliwość podniesienia wersji oprogramowania systemowego i zarządzającego do najnowszej wersji udostępnianej przez producenta) bez dodatkowych opłat.
18.	Usługi wsparcia muszą być dostarczane i gwarantowane bezpośrednio przez producenta.
19.	Sprzętowa obsługa szyfrowania MACsec na wszystkich wymaganych portach (włączając breakout), jeżeli do uruchomienia tej funkcjonalności potrzebna jest licencja - nie jest wymagana do dostarczenia w niniejszym postępowaniu
Parametry wydajnościowe	
20.	Minimalna wydajność przełączania sprzętowego - 2 Tbps
21.	Minimalna ilość przetwarzanych pakietów na sekundę 1 Bpps
22.	Maksymalna moc pobierana przez urządzenie 2500 W
Funkcjonalność dla warstwy L2	
23.	Trunking IEEE 802.1Q VLAN;
24.	Minimalny rozmiar ramki Jumbo dla wszystkich portów (Jumbo Frame) - 9 216
25.	Minimalna ilość obsługiwanych VLANów dostępna dla użytkowników - 4096
26.	Minimalna ilość obsługiwanych adresów MAC - 32k
27.	Możliwość limitowania adresów MAC dla określonych VLANów
28.	Minimalna ilość grup Link Aggregation Control Protocol (LACP): IEEE 802.3ad - 128
29.	Minimalna ilość portów w grupie LACP IEEE 802.3ad - 64
30.	IEEE 802.1s Multiple Spanning Tree (MST)
31.	Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
32.	Urządzenie musi umożliwiać stworzenie protekcji terminującej zagregowane interfejsy (LAG) na dwu Elementach przełączających (ang. Dual Homing) - odpowiednik rozwiązania vPC, Multichasis LAG. W ramach takiej protekcji wszystkie porty zagregowanego połączenia LAG muszą aktywnie przenosić dane (ang. Active/Active). Awaria jednego Elementu nie może wpływać na status połączenia zagregowanego.

33.	Wsparcie sprzętowe dla tunelowania QinQ
34.	Obsługa Selective QinQ
35.	Wsparcie sprzętowe dla VLAN translation
36.	Wsparcie dla IGMPv2, IGMPv3, MLDv2
37.	Wsparcie dla IGMP snooping i MLDv2 snooping
Funkcjonalność zapewnienia jakości obsługi w sieci	
38.	Layer 2 IEEE 802.1p (CoS) oraz DSCP
39.	Minimalna ilość kolejek QoS na port – 8
40.	Klasyfikacja QoS w oparciu o listy ACL (Access control list)
41.	Kolejkowanie bezwzględne (strict-priority)
42.	Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych.
43.	Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
44.	Obsługa ECN (Explicit Congestion Notification)
45.	Obsługa Pause Flow Control 802.3x
Funkcjonalność dla warstwy L3	
46.	Sprzętowe przełączanie pakietów w warstwie L3 dla IPv4 i IPv6
47.	Routing w oparciu o trasy statyczne
48.	Minimalna ilość wpisów IPv4 LPM (lub prefix) obsługiwanych sprzętowo 1.2M
49.	Minimalna ilość obsługiwanych jednoczesnych ścieżek o równej metryce (ECMP) 128
50.	Protekcja VRRP i VRRPv3
51.	Wsparcie dla BFD (Bidirectional Forwarding Protocol)
52.	Wsparcie dla wirtualnych tablic routingu VRF
53.	Routing w oparciu o OSPF dla protokołów IPv4 oraz IPv6.
54.	Routing w oparciu o ISIS dla protokołów IPv4 oraz IPv6. Obsługa wielu instancji ISIS
55.	Routing w oparciu o BGP dla protokołów IPv4 oraz IPv6.
56.	Obsługa BGP graceful restart
57.	Obsługa BGP IPv4 routes with IPv6 nexthops (RFC 5549)
58.	Obsługa BGP LS producer, BGP LS route reflector
59.	Możliwość przesyłania Accumulated IGP Metric (AIGP) poprzez BGP w celu wybierania optymalnej ścieżki routingu
60.	Możliwość zmian routingu poprzez zdefiniowane polityki (PBR Policy-based routing)
61.	Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
62.	Obsługa sprzętowego tunelowania IP poprzez GRE.
Funkcjonalność MPLS i SR	
63.	Obsługa transportu MPLS z sygnalizacją LDP
64.	Obsługa transportu MPLS z sygnalizacją RSVP
65.	Obsługa transportu Segment Routing z sygnalizacją ISIS-SR, TI-LFA
66.	Obsługa transportu Segment Routing wersji 6 (SRv6)
67.	Obsługa MPLS ping / traceroute
68.	Obsługa PseudoWire z sygnalizacją LDP i transportem MPLS
69.	Obsługa L3 EVPN z transportem MPLS
70.	Obsługa L3 IPVPNs (RFC 4364) z transportem MPLS
71.	Obsługa L3 IPVPNs (RFC 4364) z transportem Segment Routing
72.	Obsługa zarzadzania ruchem RSVP LSR/LER
73.	Obsługa zarzadzania ruchem Flex algo
74.	Obsługa zarzadzania ruchem SR-TE
75.	Obsługa protekcji TI-LFA
Funkcjonalność zarządzania i zabezpieczeń	
76.	Dedykowany port zarządzający 10/100/1000 Baste-T (out-of-band)
77.	Dedykowany port konsoli
78.	Zarządzanie In-band
79.	Obsługa SSHv2, Telnet
80.	Obsługa RADIUS; Radius over TLS (szyfrowanie), TACACS+, Radsec (RFC6614)
81.	Obsługa Syslog; Syslog z możliwością szyfrowania TLS

82.	Obsługa Syslog; Syslog z możliwością zmiany i dodawania własnych komentarzy do komunikatów Syslog
83.	Wymagana obsługa SNMP v1, v2c, v3;
84.	Wymagana obsługa sFlow
85.	Obsługa IEEE 802.1ab LLDP
86.	Network Time Protocol (NTP, NTPv6).
87.	Monitorowanie parametrów optycznych DOM (Digital Optical Monitoring)
88.	Możliwość modyfikacji konfiguracji z potwierdzeniem zmian (commit), konfiguracja nie jest aktywna dopóki nie zostanie wydana komenda potwierdzenie. Musi istnieć możliwość wskazania czasu, po którym wymagane jest dodatkowe potwierdzenie poprawności zmian konfiguracji, w przeciwnym wypadku system musi wrócić automatycznie do poprzedniego stanu (rollback).
89.	Możliwość diagnostyki wykorzystując podstawowe narzędzia Ping i Traceroute
90.	Możliwość rozszerzonej diagnostyki wykorzystując narzędzie typu ICMP Probe (RFC8335) które nie tylko dostarcza potwierdzenia możliwości komunikacji (typ Ping) ale również dostarcza informacji o interfejsie oraz zdalnym sąsiedztwie.
91.	Telemetria w oparciu o mechanizm strumieniowania, zapewniający (alternatywnie do SNMP) wysyłanie danych o stanie urządzenia poprzez protokoły gRPC lub Netconf.
92.	Precision Time Protocol IEEE1588 Boundary Clock, Transparent Clock. Jeżeli do uruchomienia tej funkcjonalności potrzebna jest licencja - nie jest wymagana do dostarczenia w niniejszym postępowaniu.

Tabela 2

Wymagania ogólne Systemu Zarządzania	
1.	System Zarządzania musi umożliwiać zarządzanie infrastrukturą sieciową złożoną z przełączników i routerów, zorganizowanych w dowolnej topologii.
2.	Interfejs użytkownika systemu zarządzania musi być dostępny z poziomu przeglądarki WWW bez konieczności instalowania dedykowanego oprogramowania klienta/administratora. Musi być zapewniona prawidłowa obsługa co najmniej następujących przeglądarek: Microsoft, Mozilla Firefox, Google Chrome.
3.	System Zarządzania musi obsługiwać jednoczesną pracę wielu użytkowników.
4.	System Zarządzania musi zapewniać możliwość zdalnego aktualizowania firmware'u (oprogramowania) dla zarządzanych Elementów, z możliwością wycofania i przywrócenia poprzedniej wersji firmware. Musi być możliwość przeprowadzenia procesu aktualizacji dla wielu Elementów jednocześnie, proces może rozpocząć się natychmiast lub w zaplanowanym czasie. System Zarządzania musi zapewnić weryfikację nowo dodanego firmware pod kątem jego poprawności i integralności.
5.	System Zarządzania musi zapewniać możliwość wykorzystania interfejsu programistycznego (REST API) do wykonywania typowych operacji konfigurowania takich jak tworzenie, dodawanie i implementowanie Modułów Konfiguracyjnych (ang configlet)
6.	Niedostępność Systemu Zarządzania nie może mieć jakiegokolwiek wpływu na zarządzane Elementy. W szczególności nie może uniemożliwiać lub ograniczać możliwością konfigurowania urządzeń za pomocą interfejsu CLI
7.	System Zarządzania musi być dostarczony z odpowiednimi licencjami umożliwiającymi zarządzanie i monitorowanie dostarczonego sprzętu przez okres minimum 36 miesięcy.
8.	System Zarządzania musi umożliwiać zarządzanie do 500 urządzeń.
9.	System Zarządzania musi posiadać możliwość realizacji funkcji AAA poprzez integrację z zewnętrznym serwerem Radius oraz z zewnętrznym serwerem TACACS (przy czym nie jest wymagana integracja z dwoma tymi serwerami jednocześnie).
10.	Jeśli licencja dostarczona wraz z systemem zarządzania będzie w formie obrazu maszyny wirtualnej, musi umożliwić stworzenie klastra zapewniającego tryb wysokiej dostępności tak, aby awaria sprzętowa wyłączająca jedną z instancji nie powodowała przerwy w działaniu całego Systemu Zarządzania.
Wymagania dla funkcjonalności monitorowania i wizualizacji	
11.	System Zarządzania musi umożliwiać zbieranie i wizualizację w postaci tabel i wykresów następujących parametrów: - Parametry urządzenia: nazwa, model, numer seryjny, wersja firmware, wykorzystanie CPU i pamięci RAM, temperatura pracy. - Interfejsy: stan administracyjny (aktywny, wyłączony, itp.), prędkość pracy, adres IP, statystyki ruchowe dla transmisji i odbioru, statystyki błędów, wartość MTU . - Synchronizacji czasu: PTP (status i parametry). - Ethernet: tablica MAC, wpisy ARP. - IP routing: zbudowana tablica routingu IPv4 i IPv6, (wliczając wirtualne tablice routingu VRF). - BGP: numery AS, zestawione sąsiedztwa.
12.	System Zarządzania musi zapewniać wizualizację topologii połączeń zarządzanych Elementów. Topologia połączeń musi być automatycznie wykrywana i budowana.
13.	Na planie topologii połączeń, System Zarządzania musi wizualizować: - wydarzenia i alarmy, - szybkości interfejsów, - wykorzystanie pasma, - błędy w postaci utraconych pakietów, - przepływy pakietów dla wskazanych par IP i protokołów, - rozkład dystrybucji VLAN oraz VXLAN VNI.
14.	Wszystkie parametry muszą być wizualizowane w czasie rzeczywistym (odpowiadającym zmianom w urządzeniach sieciowych) oraz historycznie z możliwością wyboru dowolnego przedziału czasowego z ostatniego miesiąca zbieranych danych. System Zarządzania musi umożliwiać budowanie i komponowanie własnych zestawień parametrów do obserwacji.
15.	System Zarządzania musi zbierać i prezentować parametry jakości transmisji pomiędzy Elementami przełączającymi. Parametry określone są jako Opóźnienie (ang. Latency), Zmiany Opóźnień (ang. Jitter), Straty pakietów (ang. Packet Loss).

16.	System Zarządzania musi zbierać i prezentować informację o przepływach pakietów danych w postaci par IP i protokołów w postaci wykresów oraz wizualizować na topologii sieci. Dane zbierane są poprzez otwarte protokoły typu sFlow lub IPFIX.
17.	System Zarządzania musi umożliwiać definiowanie i budowanie własnych widoków (ang Dashboad), na których mogą być prezentowane dane dotyczące: - interfejsów (status, szybkość pracy, opis, błędy, itp.), - stanu protokołów (BGP, PTP, NTP, itp.)
Wymagania dla funkcjonalności obsługi alarmów	
18.	System Zarządzania musi zbierać i prezentować alarmy generowane przez zarządzane Elementy. Alarmy muszą obejmować zdarzenia generowane przez syslog, zmiany stanu interfejsów, przekroczenia progów błędów na interfejsach wejściowych (CRC), przeciążenia ruchowe interfejsów wejściowych i wyjściowych.
19.	System Zarządzania musi zapewnić mechanizm potwierdzania alarmów i dodawania komentarzy.
20.	System Zarządzania musi zapewnić mechanizm wyróżniania ważności alarmów i zdarzeń oraz możliwość ich modyfikacji. Przy wyświetlaniu alarmów powinna być możliwość filtrowania alarmów pod kątem ważności.
21.	System Zarządzania musi umożliwiać definiowanie progów po których przekroczeniu generowany jest alarm. Dotyczy to takich parametrów jak Obciążenia CPU, problemów z PTP, temperatur wkładek optycznych.
22.	System Zarządzania musi umożliwiać przekierowywanie alarmów do innych platform takich jak e-mail (SMTP), narzędzi analizujących logi i alarmy typu SIEM (np. Slack), klientów komunikatorów chat.
Wymagania dla funkcjonalności wyszukiwania i analizy anomalii	
23.	System Zarządzania musi zapewnić możliwość dodawania identyfikatorów Elementów oraz interfejsów, które następnie wspomagają proces wyszukiwania.
24.	System Zarządzania musi umożliwiać wyszukiwanie adresów IP oraz MAC widocznych z poziomu zarządzanych Elementów. Możliwość wyszukiwania dotyczy adresów w statycznych i dynamicznych tablicach poszczególnych Elementów. Odnalezione adresy powinny być prezentowane wraz z kontekstem opisującym Elementy oraz interfejsy/tablice związane z danym adresem.
25.	System Zarządzania musi umożliwiać porównywanie i wizualizację różnic pomiędzy parametrami dla dwu dowolnych zarządzanych Elementów we wskazanych momentach czasowych. Parametrami podlegającymi porównaniu muszą być konfiguracje urządzeń, podstawowe tablice danych sieciowych (adresy IP, adresy MAC, wpisy ARP, sąsiedztwa sieciowe na bazie LLDP, tablice VXLAN, tablice NDP, tablice routingu IPv4, tablice routingu IPv6, tablice multicast IPv4). System musi umożliwiać równoczesne porównywanie stanu wymienionych metryk dwóch różnych urządzeń w niezależnych punktach czasu dla każdego z urządzeń. Np. Porównanie tablicy routingu IPv4 urządzenia A z godziny X z tablicą routingu urządzenia B z godziny Y.
26.	System Zarządzania musi na bieżąco (bez wymuszenia) sygnalizować modyfikację konfiguracji wykonaną z poziomu konsoli Elementów, która wprowadza różnicę pomiędzy konfiguracją budowaną przez System Zarządzania a wprowadzoną na urządzeniu. Administrator Systemu Zarządzania powinien mieć możliwość przywrócenia poprzedniej konfiguracji lub akceptacji zmian dokonanych na poziomie konsoli.
27.	System Zarządzania musi prezentować informację o podatnościach bezpieczeństwa i wykrytych błędach dla zarządzanych Elementów. Jednocześnie sugerując właściwe wersje oprogramowania.
Wymagania dla funkcjonalności zestawiania i konfigurowania usług (ang. provisioning)	
28.	Za pomocą Systemu Zarządzania musi istnieć możliwość skonfigurowania wszystkich parametrów zarządzanych Elementów.
29.	System Zarządzania musi umożliwiać budowanie konfiguracji Elementów. Konfiguracja musi być zgodna z konfiguracją tworzoną z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface / CLI).
30.	Zintegrowanie Elementów z systemem zarządzania nie może wykluczać bezpośredniej pracy z interfejsami administracyjnymi Elementów. Rozwiązanie musi umożliwiać wymienną konfigurację Elementów: poprzez System Zarządzania lub bezpośrednio z wykorzystaniem interfejsu tekstowego (ang. CLI).
31.	System Zarządzania musi wykrywać i wizualizować rozbieżności pomiędzy konfiguracją wynikającą z parametrów zdefiniowanych na systemie zarządzania oraz parametrów skonfigurowanych bezpośrednio na Elementach.
32.	System Zarządzania musi dostarczyć mechanizm budowania konfiguracji Elementów z wykorzystywaniem Modułów Konfiguracyjnych (części konfiguracji CLI, ang configlet). Musi istnieć możliwość wykorzystania Modułów Konfiguracyjnych w trybie hierarchicznym, to znaczy że Moduł Konfiguracji jest dziedziczony przez wszystkie Elementy znajdujące się w danej hierarchii. Modyfikacja Modułu Konfiguracji musi powodować odpowiednią zmianę konfiguracji wszystkich Elementów znajdujących się w danej hierarchii.
33.	System musi umożliwiać budowanie hierarchii Modułów Konfiguracyjnych dla jednego i kilku obszarów lub lokalizacji.
34.	System Zarządzania musi dostarczyć mechanizm weryfikacji oczekiwanych wyników przed implementacją Modułów Konfiguracyjnych na zarządzanych Elementach. Po implementacji zmian konfiguracyjnych opisanych w Modułach Konfiguracyjnych musi istnieć mechanizm wycofania tych zmian.

35.	System Zarządzania musi zapewnić funkcjonalność „Nadzoru Nad Zmianami” (ang. Change Control). W ramach tej funkcjonalności administrator musi mieć możliwość: a) weryfikacji zmiany konfiguracji przed implementacją, b) implementację zmiany, c) możliwość wycofania zmiany.
36.	System Zarządzania musi umożliwiać proces automatyzacji wielu zmian konfiguracyjnych i grupowania ich w pakiety (obejmujące wiele Elementów). System musi umożliwiać wykonywanie niestandardowych akcji (np. wykonania skryptu) jako jeden z elementów pakietów zamian. System musi umożliwiać zatrzymanie wykonywania kolejnych zmian w sekwencji, jeżeli zamiany je poprzedzające się nie powiodą. System musi umożliwiać zatwierdzanie pakietu zmian przez upoważnionego użytkownika zanim możliwe będzie uruchomienie pakietu.
37.	System Zarządzania musi zapewniać możliwość zapisania i odtworzenia kopi zapasowej Modułów Konfiguracyjnych.
38.	System Zarządzania musi umożliwić wykorzystanie prostych schematów i formatek (ang. Wizzard) do automatycznego budowania konfiguracji usług i portów.
Wymagania dla funkcjonalności zarządzania bezpieczeństwem i segmentacją	
39.	System Zarządzania musi dostarczać architekturę segmentacji, w której możliwe jest zdefiniowanie grup zabezpieczeń (security group) i przydział punktów końcowych (endpoits) do tych grup. Możliwość tworzenia grup zabezpieczeń musi być niezależna od topologii, logicznej konfiguracji sieci i użytych enkapsulacji (routing, switching, VXLAN). System Zarządzania musi mieć możliwość dynamicznego programowania punktów końcowych na kontrolowanych urządzeniach.
40.	System Zarządzania musi mieć możliwość tworzenia grup zabezpieczeń (security group) lokalnie oraz wykorzystując źródła zewnętrzne.
41.	System Zarządzania musi mieć możliwość dynamicznego dodawania punktów końcowych do grup zabezpieczeń (security group) wykorzystując źródła zewnętrzne.
42.	System Zarządzania musi dostarczać architekturę segmentacji, w której możliwe jest przydzielenie jednego punktu końcowego (endpoint) do wielu grup zabezpieczeń. Na przykład, punkt końcowy należy jednocześnie do grup „Drukarka” i „Budynek-A” i „Administracja”. Innym przykładem może być maszyna wirtualna należąca jednocześnie do grup: „Accounting” i „Web-Serwer”, i „Development”.
43.	System Zarządzania musi umożliwiać sterowanie Urządzeniami tak że polityki bezpieczeństwa są egzekwowane (segmentacja) również w przypadku przemieszczania się punktów końcowych pomiędzy urządzeniami.
44.	System Zarządzania musi mieć możliwość sterowania egzekwowaniem zasad segmentacji w odniesieniu do określonej grupy urządzeń sieciowych, bez konieczności uczestnictwa wszystkich przełączników w sieci w obszarze sterowania segmentacją. Przykład: segmentacja stosowana wyłącznie w przełącznikach agregacyjnych, podczas gdy przełączniki dostępowe działają jako standardowe urządzenia L2.
45.	System Zarządzania musi dostarczać architekturę segmentacji, w której możliwe jest stopniowe wprowadzanie segmentacji poprzez sukcesywne ‘uszczelnianie’ komunikacji oraz schemat „Zero Trust”, w którym komunikacja domyślnie jest zablokowana natomiast sukcesywnie odblokowywane są tylko pożądane przepływy pakietów. Musi być możliwość równoczesnego implementowania obu tych podejść jednocześnie dla różnych grup bezpieczeństwa. W szczególności część grup bezpieczeństwa może opierać się na podejściu „Zero Trust” a część na sukcesywnym „uszczelnianiu”.
46.	System Zarządzania musi dostarczać architekturę segmentacji, w której polityki bezpieczeństwa zdefiniowane są w postaci sekwencji reguł identyfikujących przepływy pakietów. Reguły muszą umożliwiać co najmniej identyfikację na warstwie L3 (adresacja IP, typ transmisji UDP/TCP/ICMP) i warstwie L4 (aplikacje/porty). System Zarządzania musi umożliwiać tworzenie standardowych „bibliotek” polityk bezpieczeństwa.
47.	System Zarządzania musi umożliwiać skonfigurowanie segmentacji poprzez zdefiniowanie polityk bezpieczeństwa pomiędzy grupami zabezpieczeń (security group) w formie następujących akcji: blokowania (drop), przepuszczania (forward), przekierowania (redirect) i monitorowania/inspekcji.
48.	System Zarządzania musi umożliwiać monitorowanie segmentacji poprzez raportowanie wykorzystania polityk, grup i reguł.

Tabela 3

Rodzaj wkładki	**Ilość**
100GBASE-ER QSFP 40km	6
SFP+ 10G WDM 20km (1310/1550 nm)	40
SFP+ 10G WDM 20km (1550/1310 nm)	40
1000BASE 1G WDM 20km (1310/1550 nm)	105
1000BASE 1G WDM 20km (1550/1310 nm)	105