# Opis przedmiotu zamówienia.

## Cele wdrożenia:

Celem wdrożenia jest podniesienie bezpieczeństwa i wydajności infrastruktury sieciowo-serwerowej eksploatowanej w ZWiK Sp. z o.o. w Szczecinie, zwaną dalej „Zamawiającym” - poprzez wymianę przełączników rdzeniowych oraz wdrożenie i wykorzystanie technologii xWDM do transmisji danych między oddziałami Zamawiającego.

Wdrożenie obejmuje wykonanie analizy oraz dokumentacji przedwdrożeniowej dla całości projektu (sieci xWDM, przełączników rdzeniowych, przełączników dostępowych, oprogramowania klasy NAC oraz NMS) wraz z harmonogramem prowadzonych prac.

Wdrożenie obejmuje dostawę, konfigurację oraz wymianę przełączników rdzeniowych w lokalizacjach Golisza (DC1) oraz Pomorzany (DC2), dostawę, konfigurację oraz wymianę przełączników dystrybucyjnych w lokalizacjach: Golisza 8 (budynek AB oraz C) – 2 sztuki, OS Zdroje (2 sztuki) i przełączników dostępowych w lokalizacji Golisza 10 – 9 sztuk.

Wymiana przełączników rdzeniowych i dystrybucyjnych ma odbywać się z zachowaniem ciągłości pracy infrastruktury zamawiającego - ewentualne przerwy związane z przełączeniami mogą odbywać się we wcześniej ustalonych oknach serwisowych (od poniedziałku do piątku w godzinach 16-20 lub sobota – niedziela).

Wszelkie prace prowadzone na traktach sieci światłowodowej należy uzgodnić z Zamawiającym co najmniej 7 dni wcześniej.

Wykonanie poszczególnych etapów realizacji wdrożenia (np. instalacja xWDM) nie może powodować braku działania, awarii lub przestoju działania (nie dotyczy uzgodnionego pisemnie czasu okna serwisowego) obecnie eksploatowanych usług oraz sieci komputerowej Zamawiającego.

## Rozbudowa sieci światłowodowej:

W ramach rozbudowy sieci światłowodowej należy wykorzystać istniejące trakty światłowodowe oraz technologię xWDM w celu zmultiplikowania transmisji na różnych kanałach pomiędzy oddziałami Zamawiającego a DC1 i DC2. Rozbudowa sieci światłowodowej obejmuje DC1 (serwerownia główna ul. Golisza 10), DC2 (serwerownia zapasowa OŚK Pomorzany) oraz oddziały Zamawiającego - OŚK Zdroje, 1Maja – TK-I, Golisza 8AB oraz Golisza 8C zgodnie ze schematem sieci światłowodowej w załączniku nr 1 od OPZ. Zamawiający zastrzega, że znajdujące się w załączniku wyniki pomiarów zostały wykonane za pomocą reflektometru przez pracowników Zamawiającego i należy je traktować jako pomiary orientacyjne.

Proponowane rozwiązanie musi spełniać poniższe kryteria:

* Proponowane rozwiązanie musi pracować w technologii xWDM.
* Proponowane rozwiązanie musi umożliwić przynajmniej 20 transmisji pomiędzy skrajnymi lokalizacjami DC1 i DC2 z wykorzystaniem 2J.
* Proponowane rozwiązanie musi umożliwić przynajmniej po 2 transmisje do DC1 i DC2 z każdej lokalizacji pośredniej z wykorzystaniem tych samych włókien na odcinku do DC1 i DC2 :
	+ DC1 – Golisza 8AB 2x 10Gb
	+ DC1 – Golisza 8C 2x 10Gb
	+ DC1 – 1Maja (TK-I) 2x10Gb
	+ DC1 – OŚK Zdroje 2x10Gb
	+ DC2 – Golisza 8AB 2x 10Gb
	+ DC2 – Golisza 8C 2x 10Gb
	+ DC2 – 1Maja (TK-I) 2x10Gb
	+ DC2 – OŚK Zdroje 2x10Gb

**Pasywna platforma xWDM**

* Każda półka platformy pasywnej musi mieć wysokość 1U
* urządzenie musi mieć głębokość nie większa niż 200mm
* urządzenie musi posiadać 4 poziomie sloty umożliwiające instalację do 4 niezależnych modułów xWDM
* urządzenie musi mieć możliwość regulacji głębokości montażu w szafie 19”, od 0 do 5 cm
* wszystkie elementy pasywnej platformy muszą wykorzystywać włókna G657A1
* platforma pasywna xWDM musi posiadać moduły oraz umożliwiać wykorzystanie ich na potrzeby rozbudowy:
	+ multiplexera/demultiplexera, OADM xWDM w wykonaniu do pracy na jednym włóknie optycznym 1J jak również na dwóch włóknach 2J
	+ kompensatora dyspersji chromatycznej DCF od 5 do 120km
	+ kompensatora dyspersji chromatycznej FBG od 40 do 120km
	+ cyrkulatora dla długości fali 1310 i/lub 1550nm
	+ łączników światłowodowe 12/24J typu plug-and-play
	+ łączników miedziane 6xRJ45 typu plug-and-play

**Multiplekser/demultiplekser DWDM**

* Pasywne urządzenie optyczne pracujące w paśmie C,
* Musi obsługiwać kanały zgodne z ITU-T G694.1 w siatce 100GHz,
* Wszystkie złącza optyczne w urządzeniu muszą być w standardzie LC/UPC,
* urządzenie musi mieć głębokość nie większa niż 200mm
* Izolacja dla kanałów przyległych musi być większa bądź równa 25dB,
* Izolacja dla kanałów nie-przyległych musi być większa bądź równa 29dB,
* Maksymalne straty wtrąceniowe nie mogą przekraczać 3,5 dB,
* Urządzenie musi być przystosowane do montażu w szafie rack 19” i a jego wysokość nie może przekraczać 1U,
* Urządzenie musi posiadać dedykowany port do monitoringu mocy sygnału zarówno na wejściu jak i wyjściu sygnału zbiorczego,

**Platforma Aktywna (jeżeli wymagana)**

Wymiary:

* 1U, 19”
* Głębokość półki nie większa niż 250mm

Parametry fizyczne:

* Dwa redundantne zasilacze typu hot-swap pracujących w dowolnej konfiguracji 2xAC, 2xDC oraz AC+DC
* Przycisk umożliwiający reset półki do ustawień fabrycznych.
* Zarządzenie WEB, SNMP, SSH
* Porty komunikacyjne 1xUSB typ B oraz 1xRJ45 10/100/1000M
* Wszystkie sloty, porty, zasilanie muszą być dostępne z frontu urządzenia
* Wentylatory zabudowane w formie wymiennej karty “Hot-swap”
* Dostępne 3 sloty na karty rozszerzeń
* Pobór mocy nie może przekraczać 110W

Zarządzanie:

* Zarządzanie z poziomu przeglądarki WEB za pomocą protokołu HTTPS
* Obsługa protokołów SNMPv1 i SNMPv2C
* Możliwość update’u oprogramowania z poziomu przeglądarki
* Logowanie do półki za pomocą nazwy użytkownika i hasła

Platforma musi posiadać możliwość rozbudowy o karty rozszerzeń:

* Transpondery dla usług 4/8/16/32G FC, 1/10/25/100GE
* Wzmacniacze optyczne typu Booster, In-Line oraz Preamplifier
* Karta przełącznika optycznego
* Kompensator tunowalny
* Karta analizatora optycznego OSA

## Rozbudowa sieci światłowodowej w budynkach Golisza 8 AB, Golisza 8 C oraz Golisza 10.

* 1. Modyfikacja relacji DC1-DC2.

Zamawiający zakłada konieczność wykonania modyfikacji istniejącego światłowodu pomiędzy DC1 (Golisza 10 – oznaczony w Załączniku nr …. jako Budynek Administracyjny) a Przepompownią Ścieków P17 (ul. Ludowa) polegająca na wykonaniu połączeń międzybudynkowych do budynków Golisza 8AB oraz Golisza 8C poprzez wspawanie w studni kablowej SK2 splitera oraz ułożenie kabli światłowodowych do budynków przy ul. Golisza 8AB pok. B123 oraz Golisza 8C pok. C108. Kable światłowodowe wewnątrz budynków należy poprowadzić w korytkach plastikowych lub w przestrzeni ponad sufitem podwieszanym, przy czym w miarę możliwości należy wykorzystać istniejące przepusty, korytka itp. – każdorazowo w uzgodnieniu z Zamawiającym.

Zakres prac obejmuje co najmniej:

* Wycofanie zapasu kabla 24J ze studni kablowej oznaczonej na rysunku jako SK1 do studni kablowej oznaczonej SK2
* Dostawa i instalacja kabla 4J ze studni kablowej SK2 do obiektu „AB”
* Dostawa i instalacja kabla 4J ze studni kablowej SK2 do obiektu „C”
* Należy pozostawić odpowiedni zapas kabla światłowodowego.
* Zakończenie kabla 4J w obiekcie „AB” na panelu 19” złączami LCPC
* Zakończenie kabla 4J w obiekcie „C” na panelu 19” złączami LCPC
* W studni SK2 wykorzystując przeciągnięty zapas kabla należy wykonać wzdłużne nacięcie aby nie przecinać wszystkich tub z włóknami.
* W odpowiednie włókna kabla 24J należy wspawać dostarczane splitery.
* Do wyjść spliterów należy dospawać włókna kabli 4J prowadzące do obiektów „AB” oraz „C”.
* Wykonać reflektometryczne pomiary sprawdzające oraz dokumentację powykonawczą.
* Wykonawca zobowiązany jest do usunięcia wszelkich szkód powstałych z winy Wykonawcy.

3.2 Wykonanie okablowania pomiędzy punktami dystrybucyjnymi a serwerownią

Wykonanie połączenia wewnątrz budynku przy ul. Golisza 10 pomiędzy GPD (Główny Punkt Dystrybucyjny – DC1) a PPD (Pośredni Punkt Dystrybucyjny) na piętrach. Wszystkie pomieszczenia znajdują się w jednym pionie i są wyposażone w szafy RACK. Kable światłowodowe wewnątrz budynku należy poprowadzić w korytkach plastikowych.

Zakres prac obejmuje co najmniej:

* Udrożnienie przejść pomiędzy stropami w budynku.
* Dostawa i instalacja kabli 6G OM4 pomiędzy szafą GPD a szafami PPD na poziomach -1, 0, 2 i 3.
* Dostawa i instalacja kabla 6J pomiędzy szafą GPD a szafami PPD na poziomie 0.
* Zakończenie kabli 6G OM4 w panelach 19” w poszczególnych szafach
* Wykonanie przejść pożarowych w przepustach pomiędzy piętrami w budynku.
* Wykonanie reflektometrycznych pomiarów sprawdzających zainstalowanych kabli światłowodowych i dokumentacji powykonawczej.
* Wykonawca zobowiązany jest do usunięcia wszelkich szkód powstałych z winy Wykonawcy.

## Dostawa urządzeń aktywnych sieci komputerowej – przełączniki.

Wymagania w zakresie dostawy przełączników rdzeniowych (2 szt.):

1. Przełącznik o budowie modularnej pozwalającej na instalację minimum 240 portów gigabitowych z obsługą PoE++ (802.3bt Class 6 – 60W), 240 portów 10-gigabitowych SFP+, 240 portów miedzianych 1/2,5/5-gigabitowych z negocjacją prędkości oraz obsługą standardu PoE++ (802.3bt Class 6 – 60W), 60 portów 100-gigabitowych, 240 portów 25-gigabitowych, 20 portów 50-gigabitowych lub ich kombinacji.
2. Przełącznik musi posiadać redundantne moduły zarządzające wyposażone w minimum 32GB pamięci stałej (typu Flash) oraz minimum 16GB pamięci operacyjnej (typu RAM) na każdym z modułów.
3. Przełącznik wyposażony w:

- Minimum 96 portów 1000BaseT/2.5GBaseT/5GBaseT ze wsparciem dla standardu 802.3bt (PoE+ 60W)

- Minimum 72 porty 10-gigabitowymi SFP+. Dla zapewnienia redundancji porty SFP+ muszą być rozdzielone na co najmniej dwa różne moduły.

- Minimum 20 portów 10/25/50-gigabitowych SFP56. Dla zapewnienia redundancji porty SFP56 muszą być rozdzielone na co najmniej dwa różne moduły.

- Redundantne, wewnętrzne, modularne, zasilacze wspierające standard 802.3bt zapewniające minimum 2500W dla PoE oraz zapewniające redundancję zasilania i budżetu mocy w trybie N+N.

1. Wbudowany, dodatkowy, dedykowany port Ethernet do zarządzania poza pasmem - out of band management
2. Port konsoli RS232 ze złączem DB9 lub RJ45
3. Port konsoli USB ze złączem USB-C lub miroUSB
4. Port USB 2.0, niezależny od portu konsoli
5. Funkcja podłączenia i obsługi interfejsu Bluetooth
6. Przepustowość: minimum 14 Tbps
7. Wydajność: minimum 5 Bp/s
8. Przełączanie w warstwie 2 i 3 modelu OSI
9. Wielkość bufora pakietów (packet buffer): minimum 8MB na każdej karcie liniowej
10. Modularny system operacyjny bazujący na jądrze Linux
11. Przełącznik wyposażony w redundantne, modularne wentylatory (minimum dwa niezależne moduły wentylatorów)
12. Przepływ powietrza w przełączniku musi odbywać się w kierunku z przodu przełącznika do tyłu przełącznika. Niedopuszczalne są rozwiązania, z mieszanym przepływem powietrza.
13. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
14. Funkcja łączenia przełączników w grupy co najmniej 2 urządzeń, w sposób ciągły synchronizujących ze sobą konfiguracje przy zachowaniu niezależnych płaszczyzn zarządzani (control plane). Przełączniki połączone w grupę muszą zapewnić co najmniej: realizację łączy agregowanych w ramach różnych przełączników będących w grupie, architekturę, w której oba przełączniki są aktywne dla funkcji L2 i L3, funkcje typu ISSU lub Live Upgrade.
15. Obsługa Microsoft Network Load Balancer (NLB)
16. Tablica adresów MAC o wielkości minimum 32000 pozycji
17. Obsługa ramek Jumbo o wielkości co najmniej 9198B
18. Obsługa Quality of Service
19. Obsługa mechanizmów, co najmniej: strict priority (SP) queuing, Deficit weighted round robin (DWRR) queuing oraz SP+DWRR
20. Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol
21. Obsługa sieci IEEE 802.1Q VLAN – 4000 jednoczesnych sieci VLAN
22. Obsługa IGMP v2/v3, IGMP Snooping, PIM SM i PIM DM
23. Routing IPv4 – statyczny i dynamiczny (min. OSPF, BGP)
24. Routing IPv6 – statyczny i dynamiczny (min. OSPFv3, MP-BGP)
25. Obsługa ECMP (Equal Cost Multi Path)
26. Obsługa VRRP
27. Obsługa Ethernet Ring Protection Switching (ERPS)
28. Wsparcie dla VXLAN
29. Obsługa tunelowania GRE
30. Obsługa Virtual Routing and Forwarding (VRF) – co najmniej 250
31. Tablica routingu o pojemności co najmniej 60000 wpisów dla IPv4 oraz co najmniej 60000 wpisów dla IPv6
32. Obsługa list ACL na bazie informacji z warstw 2 i 3 modelu OSI.

Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia

1. Obsługa standardu 802.1p
2. Funkcja ograniczania ruchu typu multicast, broadcast i nieznany unicast z opcją definiowania poziomów
3. Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p
4. Funkcja kopiowania ruchu wejściowego i wyjściowego (port mirroring) lokalnego (w obrębie urządzenia) i zdalnego (na porty znajdujące się na innym urządzeniu)
5. Funkcja centralnego uwierzytelniania administratorów na serwerze RADIUS oraz TACACS+
6. Zarządzanie poprzez port konsoli (CLI), SNMP 2c, SNMP 3, interfejs graficzny (WebGUI) znajdujący się bezpośrednio na urządzaniu oraz SSH v2
7. Obsługa Syslog
8. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
9. Obsługa sFlow
10. Obsługa Network Time Protocol (NTP)
11. Obsługa Secure FTP (SFTP) oraz TFTP
12. Obsługa skryptów w języku Python
13. Obsługa REST API
14. Obsługa RMON (minimum grupy 1, 2, 3 i 9)
15. Obsługa funkcji diagnostycznych ping i traceroute dla IPv4 i IPv6
16. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
17. Przechowywanie co najmniej dwóch wersji oprogramowania na przełączniku
18. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
19. Przełącznik musi posiadać mechanizm (automatycznego i ręcznego) tworzenia punktów szybkiego odtwarzania konfiguracji. Punkty szybkiego odtwarzania muszą zawierać aktualne zrzuty działającej konfiguracji oraz informacje dodatkowe (co najmniej: typ punktu, datę utworzenia, wersję oprogramowania, dane sprzętu, dane zapisującego punkt przywracania, opis). System musi umożliwiać ich kopiowanie i uruchamianie na innych urządzeniach tego samego typu. W urządzeniu musi być przechowywanych nie mniej niż 60 punktów przywracania konfiguracji. Przełącznik musi posiadać funkcję porównywania ze sobą (oraz prezentacji różnic) dwóch punktów odtwarzania konfiguracji oraz punktu odtwarzania konfiguracji z konfiguracją aktualnie działającą i konfiguracją zapisaną jako bieżąca.
20. Wysokość w szafie 19” – nie większa niż 8U o głębokości maksymalnie 50 cm
21. Minimalny zakres temperatur pracy od 0°C do 45°C
22. Minimum 5 letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na wymianę na maksymalnie następny dzień roboczy. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego z czasem reakcji nie dłuższym niż 2 godziny od momentu zgłoszenia problemu z oprogramowaniem. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

W zakresie parametrów, które muszą spełniać przełączniki dystrybucyjne (3 szt.) zamawiający wymaga:

1. Minimum 48 portów 1000BaseT z wsparciem dla standardów PoE (standardy 802.3af i 802.3at), umieszczone z przodu obudowy
2. Minimum 4 porty 1/10/25/50-gigabitowe SFP56 umieszczone z przodu obudowy
3. Przepustowość: minimum 496 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 360 Mp/s
5. Bufor pakietów: minimum 7.5 MB
6. Minimum 8GB pamięci operacyjnej
7. Minimum 30GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9. Dedykowany port konsoli USB
10. Port USB 2.0 (niezależny od portu konsoli USB)
11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)
12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 10 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania.
13. Łączenie w stos z wykorzystaniem portów 10Gb, 25Gb, 50Gb i agregowanych portów 10Gb, 25Gb i 50Gb (w celu zwiększenia przepustowości w stosie). Musi być możliwe stworzenie stosu z urządzeń oddalonych od siebie o co najmniej 1000 metrów.
14. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie
15. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.
16. Budżet mocy PoE przy zastosowaniu dwóch zasilaczy co najmniej 740W
17. Modularne, redundantne wentylatory, podzielone na co najmniej dwa niezależne moduły. Moduły wentylatorów musi mieć możliwość wymiany „na gorąco” (na działającym urządzeniu)
18. Wielkość tablicy routingu: minimum 60000 wpisów IPv4, 60000 wpisów IPv6
19. Tablica adresów MAC o wielkości minimum 32000 pozycji
20. Obsługa Jumbo Frames
21. Obsługa sFlow lub Netflow
22. Obsługa skryptów w języku Python
23. Obsługa REST API
24. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.
25. Obsługa RMON (minimum grupy 1,2,3 i 9)
26. Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN
27. Obsługa standardu 802.1v
28. Obsługa protokołu MVRP
29. Obsługa Ethernet Ring Protection Switching (ERPS)
30. Wsparcie dla VXLAN
31. Obsługa Microsoft Network Load Balancer (NLB)
32. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
33. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
34. Obsługa Secure FTP lub SCP
35. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
36. Obsługa SNTPv4 lub NTP
37. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
38. Obsługa protokołów rutingu: ruting statyczny, OSPF, OSPFv3, BGP, MP-BGP,
39. Obsłyga ruchu multicast: IGMPv1/v2/v3, PIM-SM, PIM-DM, MSDP
40. Obsługa VRRP
41. Obsługa ECMP
42. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
43. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
44. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
45. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
46. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW
47. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
48. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
49. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
50. Wbudowany serwer DHCP
51. Obsługa funkcji User Datagram Protocol (UDP) helper
52. Obsługa blokowania nieautoryzowanych serwerów DHCP
53. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
54. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
55. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP
56. Zakres pracy od 0 do 45°C
57. Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 40 cm.
58. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
59. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
60. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.

**W zakresie parametrów, które muszą spełniać przełączniki dystrybucyjne SFP+ (1 szt.) zamawiający wymaga:**

1. Minimum 24 porty 1/10-gigabitowe SFP+ umieszczone z przodu obudowy
2. Minimum 4 porty 1/10/25/50-gigabitowe SFP56 umieszczone z przodu obudowy
3. Przepustowość: minimum 880 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 650 Mp/s
5. Bufor pakietów: minimum 7.5 MB
6. Minimum 8GB pamięci operacyjnej
7. Minimum 30GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9. Dedykowany port konsoli USB
10. Port USB 2.0 (niezależny od portu konsoli USB)
11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)
12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 10 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania.
13. Łączenie w stos z wykorzystaniem portów 10Gb, 25Gb, 50Gb i agregowanych portów 10Gb, 25Gb i 50Gb (w celu zwiększenia przepustowości w stosie). Musi być możliwe stworzenie stosu z urządzeń oddalonych od siebie o co najmniej 1000 metrów.
14. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie
15. Dwa wbudowane (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.
16. Modularne, redundantne wentylatory, podzielone na co najmniej dwa niezależne moduły. Moduły wentylatorów musi mieć możliwość wymiany „na gorąco” (na działającym urządzeniu)
17. Wielkość tablicy routingu: minimum 60000 wpisów IPv4, 60000 wpisów IPv6
18. Tablica routingu multicast o pojemności co najmniej 8000 wpisów dla IPv4 oraz co najmniej 8000 wpisów dla IPv6
19. Tablica adresów MAC o wielkości minimum 32000 pozycji
20. Obsługa Jumbo Frames o wielkości co najmniej 9198B
21. Obsługa sFlow lub Netflow
22. Obsługa skryptów w języku Python
23. Obsługa REST API
24. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.
25. Obsługa RMON (minimum grupy 1,2,3 i 9)
26. Obsługa 4000 jednoczesnych sieci VLAN 802.1Q
27. Obsługa standardu 802.1v
28. Obsługa protokołu MVRP
29. Obsługa Ethernet Ring Protection Switching (ERPS)
30. Wsparcie dla VXLAN
31. Obsługa Microsoft Network Load Balancer (NLB)
32. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
33. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
34. Obsługa Secure FTP lub SCP
35. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
36. Obsługa SNTPv4 lub NTP
37. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
38. Obsługa protokołów rutingu: ruting statyczny, RIPv2, RIPng, OSPF, OSPFv3, BGP, MP-BGP,
39. Obsłyga ruchu multicast: IGMPv1/v2/v3, PIM-SM, PIM-DM, MSDP
40. Obsługa VRRP
41. Obsługa ECMP
42. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
43. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
44. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
45. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
46. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW
47. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
48. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
49. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
50. Wbudowany serwer DHCP
51. Obsługa funkcji User Datagram Protocol (UDP) helper
52. Obsługa blokowania nieautoryzowanych serwerów DHCP
53. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
54. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
55. Obsługa list kontroli dostępu (ACL) bazujących na porcie oraz na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Musi być możliwe utworzenie minimum 20000 wpisów ACL typu ingress opartych o IPv4 oraz minimum 20000 wpisów ACL typu ingress opartych o MAC.
56. Zakres pracy od 0 do 45°C
57. Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 40 cm.
58. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
59. Wszystkie dostępne na przełączniku funkcje muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
60. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek, pomocy technicznej i aktualizacji oprogramowania przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.

**W zakresie parametrów, które muszą spełniać przełączniki dostępowe (9 szt.) zamawiający wymaga:**

1. Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy ze wsparciem dla protokołu 802.3at (PoE+)
2. Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy
3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 130 Mp/s
5. Bufor pakietów: minimum 7.5 MB
6. Minimum 8GB pamięci operacyjnej
7. Minimum 15GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9. Dedykowany port konsoli USB
10. Port USB 2.0 (niezależny od portu konsoli USB)
11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)
12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Dostępne metody łączenia przełączników muszą umożliwiać realizację stosów na odległość co najmniej 300m.
13. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie
14. Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W. Pobór mocy (bez PoE) nie może być większy niż 80W.
15. Wielkość tablicy routingu: minimum 2000 wpisów IPv4, 1000 wpisów IPv6
16. Wielkość tablicy ARP co najmniej 8000 wpisów, wielkość tablicy ND co najmniej 8000 wpisów
17. Tablica adresów MAC o wielkości minimum 16000 pozycji
18. Obsługa Jumbo Frames
19. Obsługa sFlow lub Netflow
20. Obsługa skryptów w języku Python
21. Obsługa REST API
22. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.
23. Obsługa RMON (minimum grupy 1,2,3 i 9)
24. Obsługa 4094 tagów IEEE 802.1Q oraz 2000 jednoczesnych sieci VLAN
25. Obsługa standardu 802.1v
26. Obsługa protokołu MVRP
27. Wsparcie dla VXLAN
28. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
29. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
30. Obsługa Secure FTP lub SCP
31. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
32. Obsługa SNTPv4 lub NTP
33. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
34. Obsługa protokołów rutingu: ruting statyczny, OSPF, OSPFv3
35. Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 1000 grup), MLD (co najmniej 1000 grup)
36. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
37. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
38. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
39. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
40. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
41. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera
42. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
43. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
44. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
45. Wbudowany serwer DHCP
46. Obsługa blokowania nieautoryzowanych serwerów DHCP
47. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
48. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
49. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Co najmniej 5000 wpisów typu ingress i 2000 wpisów typu egress dla IPv4 i MAC
50. Wbudowana sonda IP SLA
51. Zakres pracy od 0 do 45°C
52. Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 35 cm.
53. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
54. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
55. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.

## Wdrożenie urządzeń aktywnych sieci komputerowej oraz systemów klasy NAC oraz NMS.

**W zakresie wdrożenia przełączników rdzeniowych zamawiający wymaga:**

* aktualizację przełączników do najnowszej zalecanej wersji;
* instalację przełączników we wskazanym przez zamawiającego miejscu;
* stworzenie klastra niezawodnościowego pomiędzy DC1 i DC2 (klaster ma umożliwiać aktualizację pojedynczego przełącznika rdzeniowego bez wpływu na pracę drugiego z przełączników);
* połączenie elementów klastra z istniejącą infrastrukturą;
* przeniesienie kluczowych usług z istniejących przełączników rdzeniowych;
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L1 (m. in. UDLD, opis portów);
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L2 (m. in. VLANy, MC-LACP);
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L3 (m. in. DHCP spoofing, ARP protect, STP);
* migracja routingu w sieci LAN z obecnych przełączników rdzeniowych na urządzenia Fortigate,
* przełączenie połączeń z istniejącego CORE na nowy;
* integracja z oprogramowaniem klasy NMS;
* integracja z oprogramowaniem klasy NAC;

**W zakresie wdrożenia przełączników dystrybucyjnych zamawiający wymaga:**

* aktualizację przełączników do najnowszej zalecanej wersji
* instalację przełączników we wskazanym przez zamawiającego miejscu
* połączenie z istniejącą infrastrukturą z zapewnieniem redundancji
* przeniesienie kluczowych usług z istniejących przełączników dystrybucyjnych
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L1 (m. in. UDLD)
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L2 (m. in. VLANy, LACP)
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L3 (m. in. DHCP spoofing, ARP protect, STP)
* przełączenie połączeń z istniejącego CORE na nowy
* integracja z oprogramowaniem klasy NMS (dostawa, konfiguracja i wdrożenie)
* integracja z oprogramowaniem klasy NAC (dostawa, konfiguracja i wdrożenie)

**W zakresie wdrożenia przełączników dostępowych zamawiający wymaga:**

* aktualizację przełączników do najnowszej zalecanej wersji
* instalację przełączników we wskazanym przez zamawiającego miejscu
* stworzenie stosu przełączników
* połączenie elementów stosu z infrastrukturą z wykorzystaniem redundantnych połączeń wykluczających pojedynczy punkt awarii
* przeniesienie kluczowych usług z istniejących przełączników dostępowych
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L1 (m. in. UDLD)
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L2 (m. in. VLANy)
* konfigurację mechanizmów bezpieczeństwa i wydajności warstwy L3 (m. in. DHCP spoofing, ARP protect, STP)
* przełączenie połączeń z istniejącego przełącznika na nowy
* integracja z oprogramowaniem klasy NMS (dostawa, konfiguracja i wdrożenie)
* integracja z oprogramowaniem klasy NAC (dostawa, konfiguracja i wdrożenie)

**Dostawa, instalacja, konfiguracja i wdrożenie oprogramowania klasy NMS (Network Management Software) :**

* instalacja oprogramowania w najnowszej zalecanej wersji
* podłączenie do oprogramowania dostarczonych elementów infrastruktury, oraz pozostałych przełączników sieciowych w ilości 18 szt.
* konfiguracja planów backupu
* przeprowadzenie szkolenia z obsługi oprogramowania dla pracowników Działu Informatyki

Wymagania oprogramowania klasy NMS:

* System musi być zbudowany w architekturze klient – serwer
* Licencja na system powinna umożliwiać zarządzanie minimum 50 urządzeniami sieciowymi różnych producentów z możliwością rozbudowy do przynajmniej 5000 urządzeń sieciowych.
* System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych w celu uzyskania redundancji. System dostarczony musi być systemem redundantnym możliwym do zainstalowania na minimum 2 serwerach
* System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułów dających dodatkową funkcjonalność, minimalnie:
	+ Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA
	+ Zarządzanie siecią bezprzewodową WLAN
	+ Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych sFlow, NetSream v5 oraz analizy zawartości pakietów SMTP, FTP, http
	+ Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS
	+ Zarządzanie dostępem zdalnym IPsec/VPN
	+ Wbudowany serwer TACACS
	+ Funkcja monitorowania wydajności aplikacji
* System musi zostać dostarczony w najnowszej dostępnej na rynku wersji na dzień ostatecznego odbioru Systemu
* Licencja na System musi umożliwiać zarządzanie wszystkimi urządzeniami sieciowymi różnych producentów
* System musi posiadać funkcje umożliwiać automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet
* System musi posiadać funkcje monitorowania stanu urządzeń po protokole SNMP i wyświetlania informacji co najmniej o:
	+ Średnim wykorzystaniu CPU i pamięci RAM
	+ Średnim czasie odpowiedzi urządzenia
	+ Obciążeniu interfejsów (dla ruchu wchodzącego i wychodzącego)
	+ Ilość błędnych lub odrzuconych pakietów na interfejsie
* System musi posiadać funkcje konfiguracji urządzeń po protokole SNMP i SSH
* System musi posiadać funkcje zarządzania konfiguracją urządzeń, tworzenia backup’ów (ręcznie oraz automatycznie w określonych odstępach czasu) oraz grupowego implementowania konfiguracji na zarządzane urządzenia. System musi zachowywać historię tworzenia backup’ów (minimum 30 dni) wraz z informacją czy przebiegł on pomyślnie, a w przypadku, jeżeli nie, powinien także poinformować o przyczynie niepowodzenia
* System musi pozwalać na tworzenie szablonów konfiguracji co najmniej w oparciu o cały plik konfiguracyjny, fragment konfiguracji, skrypt CLI, skrypt TCL.
* System musi posiadać funkcje archiwizacji konfiguracji i zarządzania obrazami oprogramowania urządzeń, w tym możliwość przechowywania kilku wersji oprogramowania dla jednego modelu urządzenia, możliwość importowania obrazu z komputera do Systemu (tzw. Offline), możliwość pobrania obrazu do Systemu bezpośrednio z Internetu (tzw. Online/LiveUpdate)
* System musi pozwalać na globalne zarządzanie VLAN, tzn. na tworzenie, modyfikowanie oraz usuwanie VLAN jednocześnie ze wszystkich lub wybranych przełączników zarządzanych przez System. Musi istnieć także możliwość automatycznego generowania map logicznej topologii sieci obrazującej konkretny VLAN a zarządzanych urządzeniach.
* System musi posiadać funkcję zarządzania listami kontroli dostępu (ACL), w tym: możliwość importowania ACL z urządzeń i tworzenie na ich podstawie szablonu, tworzenie ACL w systemie zarządzania, możliwość pojedynczej lub grupowej implementacji przechowywanych w systemie ACL na urządzeniach
* System musi posiadać możliwość wyświetlania zbiorczej tablicy routingu zbudowanej w oparciu o tablice zarządzanych urządzeń
* System musi posiadać zcentralizowany mechanizm przeglądania zdarzeń w sieci, tzw. Dashboard (skonsolidowany, syslog, trapy snmp, zdarzenia i alarmy)
* System musi generować alarmy na podstawie takich parametrów jak: wykorzystanie CPU, wykorzystanie RAM, temperatura urządzenia, obciążenie interfejsów fizycznych na wejściu i wyjściu, ilość odrzuconych pakietów; Muszą być dostępne co najmniej dwa poziomy alarmu dla pojedynczego parametru oraz muszą być one możliwe do zmiany.
* System musi posiadać funkcje wysyłania alarmów np. e-mailem lub SMS’em wraz z możliwością konfiguracji konkretnego zakresu czasowego i dnia tygodnia, w którym wiadomości będą wysyłane.
* System musi pozwalać na budowanie widoków przez administratora
* System musi posiadać funkcje generowania raportów (co najmniej w formatach PDF, CSV, Excel, XLSX, Docx) w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta. Generowanie raportów musi się odbywać na życzenie (on demand) i w regularnych odstępach czasowych (scheduled, np. codziennie, raz w tygodniu, raz na kwartał itp.)
* System musi posiadać narzędzia graficznej prezentacji topologii sieciowej wraz z dynamiczną prezentacją zmian stanu urządzeń oraz poziomem występujących na nich alarmów. Musi być też możliwość zmiany ikony reprezentującej urządzenie na topologii sieci wraz z możliwością wykorzystania różnych ikon dla różnych poziomów alarmów na urządzeniu.
* System musi posiadać wbudowane narzędzie do przeprowadzenia inwentaryzacji sprzętu używanego w sieci.
* System musi posiadać funkcje lokalizowania użytkowników przewodowych po adresie IP lub MAC. Wynikiem musi być wskazanie konkretnego portu zarządzanego urządzenia sieciowego, do którego podłączony jest użytkownik
* System musi posiadać funkcję powiązywania konkretnego interfejsu fizycznego zarządzanego urządzenia z adresem MAC urządzenia końcowego, które będzie miało dostęp do sieci tylko na tym interfejsie. Po wykryciu nieautoryzowanej próby połączenia musi być możliwość wygenerowania alarmu, wyłączenia interfejsu po określonym czasie od zaistnienia zdarzenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) oraz ponownego włączenia interfejsu po określonym czasie od wyłączenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund)
* System musi posiadać predefiniowaną bazę zakresów adresów MAC dla urządzeń sieciowych oraz biurowych wiodących producentów. Baza musi być zbudowana co najmniej dla takich producentów jak: Cisco, Epson, Toshiba, NEC, Nortel, Canon, Sony, Samsung, 3Com, Siemens, Nokia, Apple, Lexmark, Xerox, Avaya, D-Link, LG, Dell, Alcatel, Netgear, HPE, TP-Link, Ruckus oraz Huawei. Musi istnieć możliwość ręcznego dodania wpisu do tej bazy.
* System musi posiadać wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie
* System musi posiadać funkcje tworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym, w tym:
	+ Wykrywanie ataków między innymi takich jak: Duplicate ARP Address, ICMP Flood, TCP Port Scan, WinNuke, IP Spoofing, ICMP Redirect, Source Route, SYN Flood, UDP Port Scan, UDP Flood, Ping of Death, DHCP Server Detect
	+ Stworzenie topologii obrazującej logiczne połączenia między urządzeniami objętymi jednym lub kilkoma atakami sieciowymi, tzn. pokazuje urządzenie/urządzenia będące źródłem ataku i łączy je z urządzeniem/urządzeniami będącymi celem ataku.
	+ Stworzenie topologii obrazującej fizyczne połączenie między urządzeniami objętymi pojedynczym atakiem sieciowym, tzn. pokazuje całą ścieżkę fizyczną między źródłem, a celem ataku.
* System musi posiadać funkcję Telnet/SSH oraz GUI proxy umożliwiającą zarządzanie CLI/Web przez przeglądarkę Internetową
* System musi posiadać funkcje zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android
* System musi posiada funkcje dostępu do sytemu zarządzania realizowaną przez przeglądarkę internetową (min. Chrome i Firefox)
* System musi posiadać funkcje zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, e-mail
* System musi posiadać funkcje tworzenia kont administratorskich z różnymi poziomami uprawnień oraz z możliwością przypisywania administratorów do grup urządzeń. Dodatkowo musi być możliwość stworzenia kont jedynie z uprawnieniami do podglądu – bez możliwości dokonywania zmian w systemie ani na urządzenia.
* System musi posiadać funkcję zarządzania VXLAN – tworzenie listy urządzeń wspierających VXLAN, tworzenie tuneli, tworzenie topologii sieci VXLAN, wyświetlanie informacji o statystykach ruchu w tunelach
* System musi posiadać funkcje zarządzania siecią wirtualną poprzez integrację z VMware (minimum wersja 6.0) i Microsoft Hyper-V(minimum w wersji 2012). Między innymi musi pozwalać na:
	+ Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem VMware ESX z wykorzystaniem protokołu SOAP.
	+ Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Virtual Machine Manager z wykorzystaniem Windows PowerShell.
	+ Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Hyper-V z wykorzystaniem protokołu WMI.
	+ Zarządzanie siecią wirtualną, w tym serwerami VMware vCenter Server oraz Microsoft Virtual Machine Manager, wirtualnymi maszynami oraz wirtualnymi przełącznikami.
	+ Migrację wirtualnych maszyn pomiędzy fizycznymi serwerami.
	+ Przedstawienie wszystkich zasobów, szczegółowych informacji o nich oraz ich wzajemnych relacji w środowisku wirtualnym. Wymaga się, aby był wgląd minimum w:
		- Listę wszystkich fizycznych serwerów VMware ESX oraz Microsoft Hyper-V dostępnych w sieci. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: producent, model, nazwa serwera, adres IP, informacje na temat Managera sieci wirtualnej, ilość pamięci RAM (wraz z poziomem wykorzystania), CPU (wraz z poziomem wykorzystania) oraz informację czy dany serwer wspiera funkcję migracji maszyn wirtualnych.
		- Listę wirtualnych przełączników przyporządkowanych do konkretnych serwerów VMware ESX oraz Microsoft Hyper-V. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa przełącznika, ilość wirtualnych portów.
		- Listę wirtualnych maszyn przyporządkowanych do konkretnych przełączników wirtualnych. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa wirtualnej maszyny, adres IP, stan maszyny (Running, Stopped, Suspended).
	+ Zmianę stanu (minimum: Start VM, Stop VM, Suspend VM, Reset VM) i parametrów wirtualnej maszyny takich jak: zasoby CPU, ilość pamięci RAM, ilość przestrzeni dyskowej.
	+ Dodawanie, klonowanie i usuwanie wirtualnych masz.
	+ Kreowanie szablonów służących do tworzenia nowych wirtualnych maszyn, gdzie można zdefiniować parametry początkowe takie jak: nazwę VMware ESX/Microsoft Hyper-V, zasoby CPU, ilość pamięci RAM, przestrzeń dyskową, system operacyjny wirtualnej maszyny.
	+ Dodawanie wirtualnych przełączników wraz z możliwością wyboru konkretnych kart sieciowych fizycznego serwera, do których będzie połączony wirtualny przełącznik. Dodatkowo musi istnieć możliwość „load balancingu” pomiędzy kartami sieciowymi co najmniej w oparciu o: IP hash, MAC hash, port fizyczny ruchu przychodzącego. Musi być także możliwość ustawienia kart sieciowych w trybie Active-Standby.
* System musi posiadać funkcje zarządzania co najmniej dla 2000 predefiniowanych modeli urządzeń. Oprócz tego musi być możliwość wgrania dowolnej bazy MIB dla urządzeń sieciowych nie obsługiwanych domyślnie przez System
* System musi posiadać funkcję automatycznej aktualizacji przez Internet.
* System musi posiadać funkcje implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów.
* System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled)
* System musi pozwalać na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy
* Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
* Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

**Dostawa, instalacja, wdrożenie i konfiguracja oprogramowania klasy NAC (Network Access Control):**

* instalacja oprogramowania w najnowszej zalecanej wersji
* stworzenie serwisów dostępowych dla urządzeń końcowych z wykorzystaniem 802.1x
* stworzenie serwisów dostępowych dla urządzeń końcowych z wykorzystaniem MAC i DHCP fingerprint
* stworzenie serwisów dostępowych dla administratorów z wykorzystaniem TACACS+
* przeprowadzenie szkolenia z obsługi oprogramowania dla pracowników Działu Informatyki

System do kontroli dostępu musi charakteryzować się następującymi cechami (oprogramowanie klasy NAC):

* Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor)
* System musi odsługiwać minimum 1000 urządzeń klienckich (w tym gości) w trybie HA – klaster dwóch maszyn wirtualnych pracujący w trybie wysokiej dostępności (redundancja). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia
* Musi posiadać wbudowany serwer Radius oraz TACACS +
* Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:
	+ Cisco Systems
	+ Fortinet
	+ Microsoft
	+ Alcatel-lucent Enterprise
	+ HPE
	+ Huawei Networks
	+ Extreme Networks
	+ PaloAlto Networks
	+ Producenta urządzeń opisanych w tym dokumencie
* System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.
* System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.
* Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
* Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych
	+ Microsoft Active Directory
	+ Radius
	+ Kerberos
	+ LDAP
	+ ODBC
	+ Współpraca z serwerami tokenów
* Musi obsługiwać metody profilowania
	+ DHCP
	+ TCP
	+ MAC OUI
	+ SNMP
	+ Cisco device sensor
* Wspierać protokoły
	+ Radius, Radius CoA, TACACS +, web authentication, SAML v2.0
	+ EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
	+ PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD)
	+ TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
	+ EAP-TLS
	+ PAP, CHAP, MSCHAPv1 i v2, EAP-MD5
	+ NAC, Microsoft NAP
	+ Windows machine authentication
	+ MAC Auth
	+ Audit (role oparte na porcie oraz skanowanie podatności)
	+ OCSP (Online Certificate Status Protocol)
	+ SNMP generic MIB, SNMP private MIB
	+ CEF (Common Event Format), LEEF (Log Event Extended Format)
	+ TLS 1.2
* Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami
* Maszyna wirtualna musi mieć możliwość uruchomienia na platformach witalizacyjnych:
	+ Co najmniej ESX 4.0, ESXi 4.1 do 6.0
	+ Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise
* Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (1000). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.
* System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności:
* Samodzielna rejestracja klientów gościnnych w oparciu o:
	+ Adres e-mail
	+ Numer telefonu (wiadomość SMS)
	+ Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link)
* Logowanie w oparciu o portale społecznościowe
* Funkcja integracji z systemami trzecimi poprzez API
* Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do płatności systemy płatności karta kredytową
* Wbudowany system reklamowy umożliwiający integrację z zewnętrznymi serwisami umożliwiającymi w prosty sposób promowanie ofert promocyjnych, materiałów multimedialnych oraz aplikacji mobilnych.
* Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
* Funkcja personalizacji strony gościnnej

- Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

* Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działu IT
* System musi wspierać obsługę następujących systemów operacyjnych
	+ MS Windows
	+ Mac OS X
	+ iOS
	+ Android
	+ Chromebook
	+ Ubuntu
* Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci
* Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej
* Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
* Funkcja tworzenia unikalnych certyfikatów dla urządzeń.
* Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń
* Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID

- Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

System kontroli końcówek klienckich musi mieć następujące funkcjonalności

* System musi wspierać następujące systemy operacyjne
	+ Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis)
	+ Apple Mac OS X 10.7 i nowsze
	+ Red HAT Enterprise Linux 4 i nowsze
	+ CentOS 4 (Community Enterprise Operating System) i nowsze
	+ Fedora Core 5 i nowsze
	+ SUSE linux 10.x i nowsze
* Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall
* Wyświetlanie informacji on-line o statusie monitorowanych końcówek
* System powinien obsługiwać agenta w formie
	+ Stałej (Presistent Agent)
	+ Tymczasowej (Dissolvabe Agent)
	+ Agenta NAP

Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

- Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.

- Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu

- Wszystkie elementy tworzące spójny ekosystem opisane w tym dokumencie (to jest: przełączniki, punkty dostępowe, kontrolery i system kontroli dostępu) muszą posiadać jeden, wspólny punkt kontaktu serwisowego w celu wspólnej diagnozy i pomocy technicznej dla całego środowiska a nie dla pojedynczych jego elementów.

- Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w niemniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.

Dostawa, instalacja i wdrożenie system zarządzania i konfiguracji przełączników sieciowych, który musi charakteryzować się następującymi cechami:

1. System musi być zbudowany w architekturze klient – serwer. Serwer działający w środowisku wirtualnym VMware i Hyper-V, dostarczony w formie Open Virtual Appliance (OVA). Klient oparty o przeglądarkę internetową, muszą być wspierane co najmniej przeglądarki Firefox i Chrome.
2. System musi zarządzać przełącznikami z wykorzystaniem REST API oraz monitorować urządzenia różnych dostawców z wykorzystaniem co najmniej SNMP.
3. System musi być wyposażony w licencje umożliwiające zarządzanie co najmniej 15 urządzeniami oraz monitoring co najmniej 1000 urządzeń.
4. System musi zapewniać graficzną prezentację topologii sieci
5. System musi zapewniać wgląd w czasie rzeczywistym w stan (health) zarządzanych urządzeń, łącznie z prezentacją nieścisłości, błędów i naruszeń polityk bezpieczeństwa
6. System musi zapewniać możliwość zamiany konfiguracji na wielu urządzeniach na raz
7. System musi zapewniać możliwość cofnięcia zmian w konfiguracji zarządzanych urządzeń (rollback)
8. System musi zapewniać funkcje audytu zarządzanych urządzeń
9. System musi śledzić zmiany sprzętowe, softwarowe i konfiguracyjne zarządzanych urządzeń. Musi być możliwe filtrowanie i prezentacja zmian dokonanych w określonym czasie
10. Dopuszcza się licencje czasowe na okres co najmniej 5 lat
11. Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

## Instalacja w szafach RACK

Dostawa i instalacja w DC1 oraz w DC2 systemu okablowania i prowadzenia kabli UTP typu „patchbox”.

Wymagania systemu okablowania i prowadzenia kabli UTP (DC1 – 2szt. , DC2 – 2 szt):

* Montaż w szafie rack 19”, wysokość 1U
* 24 zwijane kable UTP Cat.6a, długość 1,8m
* Złącze RJ45

Wymagania systemu okablowania i prowadzenia kabli światłowodowych jednomodowych (DC1 – 1 szt.):

* Montaż w szafie rack 19”, wysokość 1U
* 24 zwijane kable OS2 Single-Mode,
* Złącze LC Duplex-LC Duplex

Wymagania systemu okablowania i prowadzenia kabli światłowodowych wielomodowych (DC1 – 1 szt.):

* Montaż w szafie rack 19”, wysokość 1U
* 24 zwijane kable OM4 Multi-Mode,
* Złącze LC Duplex-LC Duplex

Dostawa i instalacja kabli 50GbE DAC SFP56 o długości co najmniej 0,5 metra – 2 sztuki. Kable DAC SFP56 muszą być w pełni kompatybilne z dostarczanymi przełącznikami. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełączników oraz muszą być serwisowane przez serwis producentów przełączników.

Dostawa i instalacja kabli 10GbE DAC SFP+ o długości co najmniej 1 metr – 6 sztuk. Kable DAC SFP+ muszą być w pełni kompatybilne z dostarczanymi przełącznikami. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełączników oraz muszą być serwisowane przez serwis producentów przełączników.

Dostawa modułów światłowodowych w technologii xWDM dostarczanego rozwiązania:

* Moduły SFP+ LC xWDM 8Gb/s FC kompatybilnych z przełącznikami FibreChannel Broacade 300 80km - 8szt.
* Moduły SFP+ LC xWDM 10Gb/s 80km – kompatybilne z dostarczanymi przełącznikami – 48szt.
* Moduły SFP LC xWDM 1,25Gb/s 80km - kompatybilne z dostarczanymi przełącznikami – 4szt.
* Moduły SFP+ 10Gbs 850nm LC MMF 300m - kompatybilne z dostarczanymi przełącznikami – 8 szt.
* Moduły SFP+ LC DualRate 10/25Gbs Single Mode EML 10km – 8 szt.

## Wymagania ogólne:

Wszystkie przełączniki i systemy zarządzania muszą tworzyć spójny ekosystem i posiadać wspólny, autoryzowany przez ich producenta punkt serwisowy.

Producent sprzętu musi być sklasyfikowany w raporcie Gartnera „ Magic Quadrant for the Wired and Wireless LAN Access Infrastructure” i znajdować się w kwadracie liderów (Leaders). Dane z najnowszego raportu aktualne na dzień ogłoszenia postępowania.

Oferta musi zawierać kompletne zestawianie numerów katalogowych produktów i wszystkich jego dodatkowych składników (licencje, zasilacze, wkładki SFP, etc.) umożliwiających ich jednoznaczną identyfikację u producenta sprzętu.

Zamawiający może zażądać przed dostawą przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w nieniejszym postępowaniu. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużyszym niż 2 tygodnie od chwili zażądania przez Zamawiającego ich przeprowadzenia. Nieprzystąpienie do testów lub nieskuteczne ich przeprowadzenie (brak potwierdzenia przez Zamawiającego, że testy zostały zakończone pomyślnie) skutkować będzie odrzuceniem oferty.

Sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.

Zamawiający zastrzega sobie prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.

Wszystkie urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta, bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy.

Zamawiający może zażądać przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych. Zamawiający sprawdzi spełnienie powyższych warunków w polskim biurze producenta na podstawie numeru seryjnego urządzenia – w przypadku niezgodności deklaracji Wykonawcy z opinią producenta - Zamawiający odmówi odbioru przedmiotu zamówienia, jako niezgodnego ze specyfikacją istotnych warunków zamówienia.