Projekt wykonawczy

# Przedmiot zamówienia: Rozbudowa brzegu i szkieletu sieci teleinformatycznej na potrzeby TARR Centrum Innowacyjności Sp. z o.o.

Przygotował: Leszek Wadas  
Toruń, dn. 10 grudnia 2013

Spis treści

[Przedmiot zamówienia: Rozbudowa brzegu i szkieletu sieci teleinformatycznej na potrzeby TARR Centrum Innowacyjności Sp. z o.o. 1](#_Toc381104093)

[1. Część Ogólna 4](#_Toc381104094)

[1.1. Przedmiot opracowania 4](#_Toc381104095)

[1.2. Opis ogólny i zakres rzeczowy inwestycji 4](#_Toc381104096)

[1.2.1. Opis ogólny 4](#_Toc381104097)

[1.2.2. Spis lokalizacji objętych projektem 4](#_Toc381104098)

[1.2.3. Zakres rzeczowy 5](#_Toc381104099)

[2. Charakterystyka techniczna opracowania 7](#_Toc381104100)

[2.1. Symbolika wykorzystana w projekcie 7](#_Toc381104101)

[2.2. Standard i oznaczenia wykorzystane w projekcie 8](#_Toc381104102)

[2.3. Topologia i organizacja logiczna sieci 9](#_Toc381104103)

[2.4. Wymagania w zakresie separacji transmisji danych 9](#_Toc381104104)

[2.4.1. Analiza potrzeb 9](#_Toc381104105)

[2.4.2. Przyjęte rozwiązanie 10](#_Toc381104106)

[2.5. Założenia techniczne 10](#_Toc381104107)

[2.6. Wymagania ogólne dla urządzeń sieciowych podlegających dostawie 13](#_Toc381104108)

[2.6.1. Wymagania w zakresie zarządzania i monitorowania urządzeń sieciowych 13](#_Toc381104109)

[2.6.2. Wymagania ogólne dla urządzeń w W.RDZEN 14](#_Toc381104110)

[2.6.3. Wymagania ogólne dla urządzeń w W.DOSTEP 15](#_Toc381104111)

[2.6.4. Wymagania ogólne dla urządzeń w W.INTERNET 16](#_Toc381104112)

[2.6.5. Wymagania ogólne dla urządzeń w W.SERWIS 17](#_Toc381104113)

[2.6.6. Wymagania ogólne dla urządzeń w W.KAMPUS 18](#_Toc381104114)

[2.6.7. Wymagania w zakresie możliwości rozbudowy DC 18](#_Toc381104115)

[2.7. Bloki fizyczne sieci Data Center 19](#_Toc381104116)

[2.7.1. Główny punkt dystrybucyjny – GPDx 20](#_Toc381104117)

[2.7.1.1. Infrastruktura głównego punktu dystrybucyjnego 20](#_Toc381104118)

[2.7.2. End of Row – EoR 21](#_Toc381104119)

[2.7.3. Top of Rack – ToR 21](#_Toc381104120)

[2.7.4. Szafa serwerowa dla sieci kampusowej – KAMPx 21](#_Toc381104121)

[2.8. Organizacja połączeń między warstwowych 22](#_Toc381104122)

[2.8.1. Organizacja połączeń pomiędzy W.RDZEN a W.INTERNET 22](#_Toc381104123)

[2.8.2. Organizacja połączeń pomiędzy W.RDZEN a W.SERWIS 22](#_Toc381104124)

[2.8.3. Organizacja połączeń pomiędzy W.RDZEN a W.KAMPUS 23](#_Toc381104125)

[2.8.4. Organizacja połączeń pomiędzy W.RDZEN a W.DOSTEP 23](#_Toc381104126)

[2.8.5. Organizacja połączeń wewnątrz W. DOSTEP 23](#_Toc381104127)

[2.9. Charakterystyka techniczna urządzeń 24](#_Toc381104128)

[2.9.1. Wymagania dla urządzeń rdzeniowych 24](#_Toc381104129)

[2.9.2. Wymagania dla przełączników dostępowych 27](#_Toc381104130)

[2.9.3. Wymagania dla urządzeń styku z Internetem 30](#_Toc381104131)

[2.9.4. Wymagania dla zapory ogniowej 31](#_Toc381104132)

[2.9.5. Wymagania dla przełącznika Campus (I) 34](#_Toc381104133)

[2.9.6. Wymagania dla przełącznika Campus (II) 37](#_Toc381104134)

[2.9.7. Wymagania dla przełącznika agregującego sieć zarządzającą 39](#_Toc381104135)

[2.9.8. Wymagania dla przełącznika sieci zarządzającej 42](#_Toc381104136)

[2.9.9. Wymagania dla koncentratora VPN – sieć zarządzająca 42](#_Toc381104137)

[2.9.10. Wymagania dla oprogramowania do monitoringu parametrów sieciowych 43](#_Toc381104138)

[2.9.11. Wymagania dotyczące serwera wspierającego zarządzanie siecią 44](#_Toc381104139)

[2.9.12. Wymagania stawiane systemowi zarządzania i automatyzacji środowiska sieciowego 45](#_Toc381104140)

[2.9.13. Wymagania stawiane platformie usług sieciowych 49](#_Toc381104141)

[2.9.14. Wymagania stawiane przełącznikowi KVM 52](#_Toc381104142)

[2.9.15. Wymagania stawiane serwerowi przełącznika KVM 52](#_Toc381104143)

[2.9.16. Wymagania stawiane patchpanelowi światłowodowemu realizującemu funkcje dystrybucji 52](#_Toc381104144)

[2.9.17. Wymagania stawiane patchpanelowi światłowodowemu realizującemu funkcje agregacji 53](#_Toc381104145)

[2.9.18. Wymagania stawiane patchpanelowi światłowodowemu realizującemu funkcje rdzeniowe 53](#_Toc381104146)

[2.9.19. Wymagania stawiane kablom połączeniowym do patchpaneli światłowodowych 53](#_Toc381104147)

[2.9.20. Wymagania dotyczące patchordów światłowodowych 53](#_Toc381104148)

[2.10. Opis czynności uruchomieniowych i wstępnej konfiguracji sieci 54](#_Toc381104149)

[2.10.1. Przygotowanie Planu Wdrożenia 54](#_Toc381104150)

[2.10.2. Ramowe wymagania odnośnie konfiguracji urządzeń 56](#_Toc381104151)

[2.10.2.1. W.RDZEN 56](#_Toc381104152)

[2.10.2.2. W.DOSTEP 57](#_Toc381104153)

[2.10.2.3. W.INTERNET 57](#_Toc381104154)

[2.10.2.4. W.SERWIS 58](#_Toc381104155)

[2.10.2.5. W.KAMPUS 58](#_Toc381104156)

[2.10.2.6. Dodatkowe 58](#_Toc381104157)

[2.11. Testy akceptacyjne, odbiór i gwarancja 59](#_Toc381104158)

[2.11.1. Testy akceptacyjne 59](#_Toc381104159)

[2.11.2. Odbiór 61](#_Toc381104160)

[2.11.3. Serwis gwarancyjny 62](#_Toc381104161)

[2.12. Wymagania w zakresie szkoleń 64](#_Toc381104162)

[3. Tabele 65](#_Toc381104163)

[3.1. Zestawienie urządzeń podlegających dostawie 65](#_Toc381104164)

[3.2. Zestawienie czynności 65](#_Toc381104165)

[4. Rysunki 66](#_Toc381104166)

# Część Ogólna

## Przedmiot opracowania

Niniejsze opracowanie stanowi załącznik dokumentacji przetargowej: „Rozbudowa brzegu i szkieletu sieci teleinformatycznej na potrzeby TARR Centrum Innowacyjności Sp. z o.o.”. Opracowanie zawiera szczegółowe specyfikacje techniczne wykonania i odbioru, instrukcje oraz przedmiary prac dla elementów będących przedmiotem zamówienia.

## Opis ogólny i zakres rzeczowy inwestycji

### Opis ogólny

Szkielet sieci EXEA oparty jest na warstwach reprezentowanych przez odpowiednie urządzenia sieciowe. Obiekt EXEA zbudowany został z myślą o świadczeniu wysokodostępnych usług cloud computing. Pojemność całkowita obiektu to 320 szaf serwerowych. Zamówienie, którego zakres opisuje niniejsze opracowanie, dotyczy rozbudowy obiektu przez zapewnienie wysoko skalowalnego rozwiązania sieciowego dla 40 szaf przy zachowaniu pełnej możliwości rozbudowy do finalnej liczby 320 szaf. Podstawowym założeniem projektu jest możliwość dalszej rozbudowy bez konieczności zatrzymywania systemu.

### Spis lokalizacji objętych projektem

Realizacja projektu rozbudowy będzie przebiegać w jednej lokalizacji: TARR Centrum Innowacyjności Sp. z o.o., 87-100 Toruń, ul. Włocławska 167.

### Zakres rzeczowy

Opracowanie zawiera projekt części aktywnej sieci Data Center dla TARR Centrum Innowacyjności (w dalszej części używany będzie skrót TARR C.I.). W projekcie opisano wyposażenie punktów sieci w sprzęt aktywny, sposób ich połączenia oraz opis wymagań stawianych tym urządzeniom. Zakres rzeczowy projektu obejmuje wyposażenie:

* Części jednej komory w EXEA Data Center
* Dwóch punktów agregacyjnych sieci kampusowej TARR C.I.

Architektura zaproponowanego rozwiązania musi umożliwiać rozbudowę sieci, w sposób modularny, o dodatkowe 3 komory serwerowe (bez potrzeby dodawania dodatkowych urządzeń w rdzeniu sieci) oraz logicznie o kolejne budynki, które mogą być w przyszłości dołączone do sieci zbudowanej na potrzeby Data Center EXEA.

W ramach realizacji niniejszego projektu należy:

1. Dostarczyć urządzenia aktywne, zamontować i uruchomić je we właściwych szafach telekomunikacyjnych zgodnie z opisem technicznym zamieszczonym w punkcie 2.
2. Dostarczyć przełącznice pasywne, zamontować je we właściwych szafach, umożliwiając tym samym prostą formę łączenia urządzeń wykorzystujących wkładki optyczne w standardzie wielomodowym w obrębie jednej komory, wymienione w Tabeli 3.1.
3. Wykonać niezbędne krosowania pomiędzy portami urządzeń do przełącznic oraz urządzeń do urządzeń, realizując topologię sieci opisaną w punkcie 2.8. Krosowania wykonać poprzez łączenie portów urządzeń aktywnych z odpowiednimi portami przełącznicy za pomocą dostarczonych w zamówieniu patchcordów.
4. Opracować Plan Wdrożenia oraz dokonać konfiguracji urządzeń, zgodnie z wymaganiami zamieszczonymi w punkcie 2.10.1.
5. Przeprowadzić testy akceptacyjne potwierdzające spełnienie opisanych wymagań przez poszczególne urządzenia oraz osiągnięcie zaplanowanych funkcjonalności przez całą budowaną infrastrukturę sieciową, zgodnie z opisem zamieszczonym w punkcie 2.11.1.
6. Zapewnić wsparcie systemu oraz gwarancję opisaną w punkcie 2.11.3.
7. Przeprowadzić szkolenia personelu, zgodnie z opisem zamieszczonym w punkcie 2.12.

Szczegółowe zestawienie urządzeń i elementów objętych dostawą wraz z oprogramowaniem i licencjami niezbędnymi do uzyskania opisanej w projekcie funkcjonalności zostało ujęte w Tabeli 3.1.

Szczegółowe zestawienie prac objętych niniejszym projektem, wraz z podaniem zakresu wymagań dla tych prac, zostało ujęte w Tabeli 3.2.

# Charakterystyka techniczna opracowania

## Symbolika wykorzystana w projekcie

|  |  |
| --- | --- |
|  | Cx - urządzenie warstwy sieci rdzeniowej |
|  | AKxyyz - przełącznik warstwy sieci dostępowej |
|  | AKxyyvvv - moduł wyniesiony przełącznika warstwy sieci dostępowej |
|  | FWx - zapora ogniowa w warstwie serwisowej |
|  | INTx – urządzenie w warstwie dostępu do Internetu |
|  | SWx – przełącznik w warstwie sieci kampusowej |

## Standard i oznaczenia wykorzystane w projekcie

* DC – DataCenter, określające zespół komór i pomieszczeń dodatkowych, służących do świadczenia usług klientom zewnętrznym, usługom wewnętrznym oraz usługom Cloud.
* Kx – Komora serwerowa (gdzie x dotyczy numeru komory). K1 określa pierwszą komorę, której wyposażeniem jest cel tego projektu
* W.RDZEN – Warstwa sieci rdzeniowej
* Cx – Urządzenie w W.RDZEN (gdzie x oznacza numer urządzenia)
* W.DOSTEP – Warstwa sieci dostępowej
* AKxyyz – Przełącznik w W.DOSTEP (gdzie x oznacza numer komory, yy oznacza numer pary urządzeń, z oznacza numer urządzenia w danej parze y)
* AKxyyvvv – Moduł wyniesiony urządzenia AKxyyz (gdzie vvv oznacza numer modułu wyniesionego dla danej pary urządzeń AKxyyz)
* W.SERWIS – Warstwa serwisowa
* FWx – Zapora ogniowa w W.SERWIS (gdzie x oznacza numer urządzenia)
* W.INTERNET – Warstwa styku z Internetem
* INTx – Urządzenie w W.INTERNET (gdzie x oznacza numer urządzenia)
* W.KAMPUS – Warstwa sieci kampusowej
* SWx – Przełącznik w W.KAMPUS (gdzie x oznacza numer urządzenia)
* SRVMGMTxx – Serwer przeznaczony do systemów zarządzania siecią DC (gdzie xx oznacza numer serwera)
* MGMTAUT – System zarządzania i automatyzacji środowiska sieciowego
* MGMTUSx - Platforma usług sieciowych (gdzie x oznacza numer urządzenia)
* GPDx – Główny Punkt Dystrybucyjny (x oznacza numer punktu dystrybucyjnego w komorze K1. Punkt dystrybucyjny będzie zawierał w dwóch szafach serwerowych urządzenia wykorzystywane w W.RDZEN, W.INTERNET i W.SERWIS.
* EoR – Szafa serwerowa, w której znajdować się będą przełączniki dostępowe AKxyyz wykorzystywane w W.DOSTEP (EoR = End of Row)
* ToR – Szafa serwerowa, w której znajdować się będą moduły wyniesione przełączników dostępowych AKxyyvvv wykorzystywane w W.DOSTEP (ToR = Top of Rack)
* KAMPx – Szafa serwerowa przeznaczona do instalacji SWx.
* KVMx – Przełącznik KVM instalowany w GPDx (gdzie x oznacza numer urządzenia)
* SRVKVMx – Serwer przełącznika KVMx (gdzie x oznacza numer urządzenia)
* PPD – Patchpanel światłowodowy (włókna wielomodowe) realizujący funkcję dystrybucji. Instalowany w ToR oraz GPDx
* PPA – Patchpanel światłowodowy (włókna wielomodowe) realizujący funkcję agregacji. Instalowany w EoR.
* PPR – Patchpanel światłowodowy (włókna wielomodowe) realizujący funkcje rdzeniowe. Instalowany w GPDx.
* PPINT –Patchpanel światłowodowy (włókna jednomodowe) realizujący funkcję połączenia łącz operatorskich. Instalowany w GPDx.
* SWMGMTx – Urządzenie agregujące przełączniki zarządzające sieci OOB - Out of Band Management (gdzie x oznacza numer urządzenia)
* SWMGMTKxyy – Przełącznik zarządzający OOB – Out of Band Management (gdzie x oznacza numer komory, yy oznacza numer urządzenia)

## Topologia i organizacja logiczna sieci

Architektura zaprojektowanej sieci dla TARR C.I. bazuje na czytelnym podziale sieci na warstwy funkcjonalne. Schemat podziału sieci wg warstw przedstawiono na Rysunku nr 1. Zastosowanie takiego podziału pozwala w prosty i czytelny sposób zorganizować ruch w sieci, sprawnie monitorować jej działanie oraz skutecznie nią zarządzać. Dlatego też, w opisywanej sieci wyodrębnia się:

* Warstwę sieci rdzeniowej (W.RDZEN)
* Warstwę sieci dostępowej (W.DOSTEP)
* Warstwę serwisową (W.SERWIS)
* Warstwę styku z Internetem (W.INTERNET)
* Warstwę sieci kampusowej (W.KAMPUS)

W wyniku zastosowania takiego podziału funkcjonalnego oraz po przeanalizowaniu potrzeb zaprojektowano sieć, która składa się z 2 urządzeń w W.RDZEN, 4 przełączników w W.DOSTEP wraz z 40 kartami wyniesionymi (AKxyyzz), 2 ścian ogniowych w W.SERWIS, 2 urządzeń w W.INTERNET oraz 2 urządzeń w W.KAMPUS. Schemat ogólny sieci przedstawiono na Rysunku nr 1.

Obecna część projektu dotyczy budowy sieci w komorze K1 z możliwością rozbudowy o kolejne 3 komory. Istotnym punktem są dwa główne punkty dystrybucyjne (GPD1 i GPD2), umieszczone w przeciwległych punktach komory. Dodatkowymi punktami będą punkty KAMPx, EoR oraz ToR. Rozmieszczenie fizyczne urządzeń w punktach GPDx, KAMPx, EoR i ToR przestawiono na Rysunkach nr 7, 8, 9, 10, 11, 12.

## Wymagania w zakresie separacji transmisji danych

Wykonana w ramach zamówienia sieć musi obsługiwać co najmniej następujące technologie:

* MPLS (Multiprotocol Label Switching) wraz z odpowiednimi protokołami warstwy trzeciej w rdzeniu sieci,
* VLAN,
* Wirtualne tablice routingowe dla usług w warstwie trzeciej.

Użyte w projekcie rodzaje urządzeń aktywnych oraz zastosowane rozwiązania dla sieci bazują na tych technologiach.

### Analiza potrzeb

Rozbudowa sieci będąca przedmiotem projektu musi uwzględniać kwestie bezpieczeństwa oraz zarządzania transmisjami sieciowymi i usługami w strukturze całej sieci. Są to zagadnienia związane z tworzeniem i konfiguracją wirtualnych podsieci grupujących poszczególnych klientów i usługi, czyli możliwości kreowania niezależnych wirtualnych usług sieciowych w obrębie wspólnej fizycznej infrastruktury. W wyniku realizacji projektu wykonane rozwiązanie sieciowe musi umożliwiać implementację kilku różnych technologii, umożliwiających realizację logicznej separacji transmisji danych:

* VLAN,
* QinQ,
* VRF,
* MPLS L2/L3 VPN.

Należy przewidzieć i zaimplementować możliwość wydzielenia wirtualnych segmentów wg. poszczególnych usług. W szczególności przewidzieć należy wydzielenie podsieci wirtualnych dla:

* Sieci kampusowej rozproszonej w wielu miejscach DC,
* Klientów Inkubatora EXEA Smartspace,
* Sieci klienckich realizowanych w trzech formach,
  + Kompletna sieć klienta umiejscowiona w szafach serwerowych będąca na wyposażeniu Zamawiającego,
  + Serwery klienta umiejscowione w szafach serwerowych będących na wyposażeniu Zamawiającego,
  + Kompletna sieć klienta umiejscowiona w szafach klienta, umiejscowionych w komorach serwerowych (Kx),
* Usług cloud computing dostarczanych przez TARR C.I. wliczając w to usługi SaaS (Software as a Service), IaaS (Infrastructure as a Service) oraz PaaS (Platform as a Service).

### Przyjęte rozwiązanie

Przyjęta w projekcie architektura sieci będąca przedmiotem projektu została oparta o technologię MPLS w rdzeniu sieci. Technologia ta musi umożliwiać, w zależności od potrzeb, realizację usług separacji logicznej (VPN) w oparciu o MPLS L2/L3 VPN. Ponadto, w zależności od potrzeb architektura sieci musi umożliwiać użycie dodatkowych technologii separacji ruchu: technologii VLAN (802.1Q), QinQ i wirtualnych tablic routingu.

Dzięki zastosowaniu przyjętej architektury sieci musi być możliwa:

* Klasyfikacja ruchu na podstawie tagów VLAN,
* Elastyczne mapowanie ruchu do zdefiniowanych usług transportowych w W.RDZEN i W.INTERNET za pomocą takich technologii, jak: EoMPLS, MPLS VPN, VPLS, VRF,
* Definiowanie polityk QoS dla zdefiniowanych usług transportowych (hierarchiczne polityki, duża liczba kolejek).

## Założenia techniczne

Celem projektu jest zbudowanie wysokowydajnej i redundantnej sieci rdzeniowej i dostępowej, w której W.RDZEN i W.DOSTEP połączone są ze sobą łączami o przepustowości 10 Gbps i wielokrotności 10 Gbps. Podłączanie urządzeń końcowych do sieci dostępowej odbywać się może za pomocą łącz 1 Gbps lub 10 Gbps. Projekt rozbudowy infrastruktury zakłada wykonanie w ramach projektu redundancję połączeń między wszystkimi warstwami, co zostało opisane na Rysunkach 2, 3, 4, 5, 6.

Na etapie doboru urządzeń aktywnych przyjęto następujące założenia techniczne, które muszą zostać spełnione po realizacji projektu:

* Konieczne jest zastosowanie redundancji typu in-chassis, redundancji matryc przełączających oraz zasilaczy dla wszystkich urządzeń w W.RDZEN.
* Konieczne jest zastosowanie redundancji zasilaczy dla wszystkich urządzeń W.DOSTEP.
* Konieczne jest umiejscowienie w każdej z szaf rack (w której znajdować się będą serwery, lub usługi klientów zewnętrzny lub usługi wewnętrzne) dwóch wyniesionych modułów przełączników W.DOSTEP, co zapewni szybką konfigurację oraz pełną redundancję.
* Należy przewidzieć zapas portów na urządzeniach w W.RDZEN, umożliwiający szybką rozbudowę sieci i dołączanie kolejnych węzłów dostępowych, możliwość instalacji dodatkowych kart liniowych oraz migracje do prędkości powyżej 10 Gbps per port (40 Gbps/100 Gbps). Zapas portów powinien umożliwić dalszą rozbudowę sieci opisaną w punkcie 2.6.7, bez konieczności dodawania nowych urządzeń w W.RDZEN.
* Należy przewidzieć zapas portów na urządzeniach w W.DOSTEP poprzez dołączanie kolejnych wyniesionych modułów w formie zewnętrznych przełączników instalowanych w szafach serwerowych.
* Ruch pomiędzy W.RDZEN, W.INTERNET oraz W.DOSTEP musi być zabezpieczony poprzez ścianę ogniową (Firewall – FWx) z możliwością kontroli ruchu na poziomie warstwy aplikacyjnej. Ściana ogniowa powinna znajdować się w W.SERWIS. Ruch pomiędzy poszczególnymi warstwami powinien być przekierowywany za pomocą konfiguracji logicznej na urządzeniach w W.RDZEN. Warstwa W.SERWIS musi pozwolić na dodawanie kolejnych usług w miarę rozbudowy sieci DC, takich jak IPS albo Load Balancing.
* Urządzenia w W.SERWIS muszą umożliwiać wydzielanie wirtualnych urządzeń, które mogą być używane do filtracji odpowiednich usług klientów, albo wewnętrznych usług.
* Warstwa W.INTERNET musi mieć możliwość terminowania szyfrowanych tuneli oraz charakteryzować się redundancją urządzeń. Warstwa W.INTERNET musi być zaprojektowana w ten sposób, aby możliwa była rozbudowa dostępnych urządzeń o dodatkowe interfejsy (w tym również 10 Gbps) oraz rozbudowa o kolejne urządzenia sieciowe dowolnego producenta, bez potrzeby przeprojektowywania obecnej architektury sieci. Ma to na celu możliwość łączenia sieci EXEA z operatorami, punktami wymiany ruchu (IX) oraz z sieciami klienckimi podłączonymi bezpośrednio do W.INETERNET.
* Użycie protokołów MPLS oraz 802.1Q musi umożliwić przekazanie dowolnych usług L2 lub L3 do dowolnej szafy serwerowej, jako logicznie odseparowanego połączenia lub jako połączenia dostępnego dla więcej niż jednej szafy serwerowej.
* Sieć musi być przygotowana do obsługi protokołu IPv6 w celu zapewnienia sprzętowej realizacji usług wykorzystujących zarówno IPv4 i IPv6.
* W celu eliminacji protokołu Spanning-Tree pomiędzy W.RDZEN a W.DOSTEP, sieć ma mieć możliwość uruchomienia tychże urządzeń jako jednej fabryki. Fabryka powinna umożliwiać podłączanie dodatkowych urządzeń do W.RDZEN i W.DOSTEP, w dowolnym miejscu bez potrzeby stosowania protokołu Spanning-Tree jako głównego protokołu do zapobiegania pętlom L2. Rozwiązanie ma na celu umożliwienie rozbudowy sieci w warstwie drugiej modelu OSI, zmniejszając do minimum możliwość wystąpienia pętli.
* Urządzenia w W.RDZEN oraz W.DOSTEP muszą umożliwiać wdrożenie rozwiązania Multi-Chassis Link Aggregation.
* Sieć musi być przygotowana do obsługi aplikacji, takich jak wideo oraz usługi voice over IP, a także do wykorzystania sieci i jej urządzeń do np. rozsyłania treści za pomocą multicast.
* Funkcjonalność urządzeń musi umożliwiać wirtualizację i separację wielu sieci LAN w DC na współdzielonej infrastrukturze. Urządzenia użyte do budowy infrastruktury w W.RDZEN oraz W.INTERNET muszą sprzętowo wpierać funkcje MPLS, a także umożliwiać uruchomienie usług MPLS w warstwie drugiej (L2), bądź trzeciej (L3) bez konieczności zmian sprzętowej konfiguracji urządzeń oraz zapewniać właściwy poziomu jakości usług (Quality of Service). Urządzenia W.DOSTEP muszą wspierać separację ruchu w oparciu o VLAN-y.
* System połączeń pomiędzy szafami serwerowymi dostarczony wraz z urządzeniami sieciowymi musi umożliwić proste łączenie urządzeń pomiędzy punktami EoR, ToR, GPDx, przy wykorzystaniu światłowodów wielomodowych. Tym samym system musi pozwolić na szybkie przenoszenie dowolnego bloku bez konieczności używania spawarek światłowodowych. Wykonany w ramach zamówienia system połączeń musi ograniczyć ilość fizycznych kabli biegnących pod podłogą w K1 do minimum.

Ponadto przy doborze urządzeń kierowano się następującymi wskazówkami technicznoinwestycyjnymi:

* **Unifikacja urządzeń** - należy ograniczyć liczbę rodzajów (rodzin) produktów do niezbędnego minimum w celu ograniczenia kosztów szkolenia kadr i utrzymania sieci. W przypadku warstw W.RDZEN, W.DOSTEP konieczne jest zastosowanie jednej rodziny produktów.
* **Skalowalność urządzeń** - urządzenia modularne muszą umożliwić zwiększenie przepływności na przykład poprzez dołożenie kolejnych interfejsów lub ich wymianę na inne o większej przepustowości. Warstwa W.RDZEN powinna umożliwić przyłączanie takiej ilości urządzeń w W.DOSTEP, aby umożliwić podłączenie sumarycznie 4 komór serwerowych (każda z komór zawierać będzie 80 szaf serwerowych, gdzie w każdej z szaf powinny się znajdować minimum dwa urządzenia AKxyyvvv). W urządzeniach w W.RDZEN, W.INTERNET, W.KAMPUS należy przewidzieć wolne słoty na rozbudowę o kolejne porty. Ilość wymagań dotyczących ilości wolnych slotów wymaganych do rozbudowy opisana została w punkcie 2.9.

Realizacja powyższych zaleceń jest krytyczna i stanowi wymogi minimalne realizacji projektu. Wymogi te spełniają ogólne trendy światowe w budowie sieci Data Center, zalecenia Unii Europejskiej dotyczące stosowania technologii telekomunikacyjnych zakładających dalszą rozbudowę i pełne wykorzystanie rozbudowanej sieci w przyszłości z możliwością skalowania rozwiązań sieciowych według potrzeb.

W celu zapewnienia wysokiego bezpieczeństwa oraz dostępności całej zaprojektowanej infrastruktury przyjęto rozwiązania stosowane jako najlepsze praktyki w budowaniu sieci klasy Data Center. Wysoka dostępność będzie realizowana poprzez duplikację kluczowych elementów infrastruktury oraz zapewnienie zapasowych połączeń pomiędzy nimi. Urządzenia w W.RDZEN będą posiadały redundantne moduły zarządzająco-przełączające i zasilacze; a urządzenia w W.DOSTEP będą wyposażone tylko w nadmiarowe zasilacze. Elementy W.DOSTEP będą zduplikowane w celu zapewnienia wysokiej dostępności, jakim jest możliwość podłączenia serwerów i innych urządzeń do dwóch oddzielnych wyniesionych modułów przełączników dostępowych (w obrębie jednej szafy) za pomocą interfejsów 1 Gbps. Musi być możliwe jednoczesne podłączenie serwerów za pomocą interfejsów 10 Gbps do dwóch niezależnych przełączników dostępowych, które pracują jako urządzenia nadrzędne dla wyniesionych modułów w szafach serwerowych. W celu zwiększenia niezawodności i bezpieczeństwa pary urządzeń W.RDZEN, W.SERWIS oraz W.INTERNET muszą zostać umieszone w przeciwległych punktach K1.

## Wymagania ogólne dla urządzeń sieciowych podlegających dostawie

Wymagania ogólne dotyczące urządzeń:

* Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży,
* Dostarczone urządzenia muszą być nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem), nieużywane (przy czym dopuszcza się, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia. W takim przypadku wykonawca będzie zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo do inspekcji sprzętu przed jego rozpakowaniem).
* Całość dostarczonego sprzętu musi być objęta serwisem gwarancyjnym opartym o świadczenia gwarancyjne producenta w okresie co najmniej 12 miesięcy.
* Zamawiający może zażądać testów poszczególnych funkcjonalności przed dokonaniem wyboru oferty.
* Konieczne jest by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy) na dzień poprzedzający złożenie oferty.
* Oferowane urządzenia w dniu składania oferty nie mogą być ogłoszone przez producenta do wycofania z produkcji lub sprzedaży.

### Wymagania w zakresie zarządzania i monitorowania urządzeń sieciowych

Zarządzanie jest bardzo ważnym elementem składającym się na działanie sieci, jako całości. Aby nowoczesne rozwiązanie sieciowe mogło działać efektywnie musi posiadać mechanizmy zapewniające sprawną i szybką reakcję na zaistniałe problemy oraz pozwalające szybko ocenić stan sieci, bez konieczności przeglądania stanu każdego urządzenia z osobna. Również zmiany konfiguracji urządzeń, szczególnie związanych z zapewnieniem, uzgodnionego z klientem SLA, poziomu usług, wymaga narzędzi pozwalających przeprowadzać je globalnie dla dużej liczby urządzeń jednocześnie.

Wymagania stawiane urządzeniom w W.RDZEN i W.DOSTEP w zakresie zarządzania są następujące:

Urządzenia muszą wspierać standardowe mechanizmy monitoringu stanu połączeń tj:

* Umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu – funkcja SPAN.
* Umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN – Remote SPAN.
* Urządzenia muszą być zarządzane poprzez:
  + Interfejs CLI (konsolę)
  + SNMP v1, SNMP v2, SNMP v3
* Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Oznacza to, iż konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
* Plik konfiguracyjny urządzenia musi być zabezpieczony przed niepowołanym dostępem oraz zmianami – tylko osoby uwierzytelnione powinny posiadać dostęp do pliku konfiguracyjnego.
* Zarządzanie urządzeniami odbywać się będzie z wydzielonej podsieci, niedostępnej dla innych urządzeń sieciowych. Jedynym stykiem sieci będzie podłączenie do jednego z przełączników KAMPx. W przyszłości sieć do zarządzania urządzeniami w 100% zostanie odizolowana od sieci produkcyjnej. Celem jest przejrzysty podział zakresu odpowiedzialności oraz szybkie i skuteczne rozwiązywanie problemów. Dodatkowo zabezpiecza system przed nieautoryzowanymi zmianami konfiguracji urządzeń sieciowych.
* Wraz z urządzeniami sieciowymi muszą być dostarczone dwa serwery wraz z odpowiednimi systemami operacyjnymi, które będą służyły do instalacji na nich aplikacji wspierających działanie sieci, opisane w punkcie 2.9.
* Dodatkowym elementem będzie platforma usług sieciowych, takich jak DHCP oraz DNS wraz z systemem umożliwiającym proste, graficzne zarządzanie wyżej wymienionymi usługami oraz zarządzanie adresacją IP.
* Dodatkowym elementem będzie system zarządzania i automatyzacji środowiska sieciowego, ułatwiający pracę Administratorom oraz zapewniający spójny interfejs do zarządzania siecią DC.
* Dodatkowym elementem będzie system monitoringu sieci oparty o protokół SNMP, przedstawiający w szczególności obciążenia danych linków, wykorzystaną pamięć RAM urządzeń oraz błędy na interfejsach urządzeń.

### Wymagania ogólne dla urządzeń w W.RDZEN

Urządzenia w rdzeniu sieci odpowiadają za zapewnienie stabilnych połączeń pomiędzy W.DOSTEP, W.SERWIS, W.INTERNET oraz W.KAMPUS. Dlatego najważniejsze cechy, jakie muszą charakteryzować takie urządzenia to wydajność i niezawodność.

Wymagania ogólne stawiane urządzeniom szkieletu sieci to:

* Wysoka wydajność (line-rate na wszystkich portach) potrzebna do obsłużenia połączeń 1 Gbps, 10 Gbps, uzyskana poprzez zastosowanie urządzeń pozycjonowanych przez producenta urządzenia jako przełączniki rdzeniowe do Data Center. Urządzenia powinny umożliwić prostą rozbudowę (polegająca na wymianie lub dołożeniu kart liniowych), umożliwiającą uruchomienie portów 40 Gbps i 100 Gbps.
* Konieczność uruchomienia wirtualnych kontekstów, w celu użycia przełączników rdzeniowych w formie wirtualnych urządzeń oraz zapewnienia w przyszłości ich rozbudowy o kolejne wirtualne konteksty. Konteksty powinny zapewnić pełną izolację procesów przełączania oraz routingu tak, aby przełączniki, z logicznego punktu widzenia, były widziane jako niezależne jednostki. Jest to niezwykle ważne, gdyż standardowa ilość sieci VLAN, wynikająca ze specyfikacji standardu 802.1Q, zezwala na używanie 4095 wirtualnych sieci. Z racji na planowany rozwój sieci, w przyszłości wymagane będzie uruchomienie większej ilości sieci VLAN (ponad 10000) na jednym urządzeniu fizycznym w W.RDZEN, co może być zrealizowane jedynie przez wirtualizacje urządzenia.
* Funkcjonalność MPLS pomiędzy jednym z wirtualnych kontekstów na urządzeniach w W.RDZEN a urządzeniami W.INTERNET. Funkcjonalność umożliwiająca tworzenie wirtualnych sieci LAN w warstwie drugiej (L2) oraz trzeciej (L3), budowanie logicznych sieci (sieci klientów, sieć kampusowej, sieć dla inkubatora technologicznego). Funkcjonalność MPLS ma w prosty sposób zapewnić transport ruchu z połączeń wchodzących do urządzeń w W.INTERNET do poszczególnych wirtualnych tablic routingu na urządzeniach W.RDZEN, lub VLANów na urządzeniach W.DOSTEP.
* Obsługa mechanizmów: MPLS Fast Reroute oraz Traffic Engineering, celem zminimalizowania czasu konwergencji sieci w przypadku przerwy w transmisji (np. w momencie awarii jednego z urządzeń wspierających MPLS).
* Możliwość realizacji zaawansowanych polityk dotyczących jakości świadczonych usług (Quality of Service), w szczególności poprzez budowanie hierarchicznych polityk.

Urządzenia W.RDZEN, W.SERWIS oraz W.INTERNET (dostarczane parami) muszą być zainstalowane w przeciwległych rogach K1, w celu zapewnienia dodatkowej redundancji i uniezależnienia od lokalnych (w obrębie komory K1) problemów.

### Wymagania ogólne dla urządzeń w W.DOSTEP

Urządzenia W.DOSTEP odpowiadają za przekazywanie pakietów z urządzeń końcowych znajdujących się w szafach serwerowych do innych szaf serwerowych, albo do W.RDZEN. W celu zapewnienia wysokiego poziomu redundancji zaprojektowano dołączenie urządzeń W.DOSTEP do W.RDZEN w topologii podwójnej gwiazdy na dwóch poziomach:

1. Podwójna gwiazda pomiędzy przełącznikami dostępowymi a wyniesionymi modułami przełączników dostępowych. Każdy z wyniesionych modułów jest podłączony do dwóch przełączników dostępowych.
2. Podwójna gwiazda pomiędzy przełącznikami dostępowymi a urządzeniami W.RDZEN. Każdy z przełączników dostępowych jest podłączony do każdego z urządzeń W.RDZEN.
3. Urządzenia W.DOSTEP muszą mieć możliwość instalacji modułów wyniesionych do chassis blade różnych producentów. Musi być możliwość podłączenia tych modułów bezpośrednio do W.RDZEN.

Urządzenia W.DOSTEP muszą umożliwiać:

* Realizację architektury w formie modularnej:
  + Agregacja W.DOSTEP w wirtualnych kontekstach lub wirtualnych tablicach routingu realizowanych na urządzeniach W.RDZEN.
  + Przełączniki dostępowe pracujące, jako urządzenia End of Row (EoR), agregujące połączenia z wyniesionych modułów instalowanych w szafach serwerowych.
  + Równoczesne działanie wszystkich używanych łączy przy zastosowaniu protokołu LACP, bez konieczności stosowania protokołu Spanning Tree do wyłączania poszczególnych łącz (w celu zapobiegania pętlom).
  + Wykorzystanie protokołu LACP powinno umożliwiać uruchomienie rozwiązania w formie Multichassis LACP pomiędzy W.DOSTEP a W.RDZEN.

Z racji potrzeby rozbudowania sieci, bezpieczeństwa oraz zarządzania wymaga się, aby:

* Administratorzy mieli dostęp do zarządzanych urządzeń warstwy dostępowej poprzez wydzieloną sieć. Celem jest przejrzysty podział zakresu odpowiedzialności i tym samym w niezawodny sposób dostarczyć usługi sieciowe.
* Wyniesione moduły kart liniowych nie powinny umożliwiać aktywnego zarządzania. Całość zarządzania musi się odbywać z poziomu przełączników dostępowych ułatwiając architekturę i zmiany konfiguracyjne.
* Wszystkie porty użytkowników muszą być standardowo wyłączone i umożliwiać skonfigurowanie ignorowania ruchu kontrolnego (dla różnych protokołów). Dzięki temu można uniknąć nieoczekiwanych zmian w sieci DC spowodowanych przez błędny lub złośliwy ruch kontrolny spoza sieci.
* Na portach dostępowych niezbędna jest także możliwość weryfikacji za pomocą odpowiednich mechanizmów czy adresy IP i adresy MAC zawarte w pakietach i ramkach odpowiadają tym, które powinny się na tych portach pojawiać. W przypadku wykrycia wrogich działań, przełączniki powinny blokować możliwość lokalnego dostępu urządzeń klienckich do siebie nawzajem.
* Urządzenia w W.DOSTEP muszą posiadać mechanizmy ochrony warstwy kontrolnej przed atakami oraz możliwość filtracji zalewów ramek poprzez wspieranie: DHCP Snooping, Dynamic ARP Inspection, IP Source, Control Plane Security, Storm Control, Port Security, ACLs, 802.1X lub mechanizmy równoważne. Poszczególni użytkownicy sieci powinni być przyłączeni z limitem przepustowości przyjętym przez Administratorów Sieci, zależnym od aktualnego zapotrzebowania klienta lub usługi.
* Przełączniki muszą zapewniać narzędzia typu Quality of Service, co pozwoli na zapewnienie aplikacjom odpowiedniego pasma, opóźnienia oraz jitter-u.
* Przełączniki muszą umożliwiać odseparowanie ruchu różnych aplikacji i użytkowników od siebie poprzez zastosowanie osobnych, wirtualnych sieci (VLAN).

### Wymagania ogólne dla urządzeń w W.INTERNET

Warstwa W.INTERNET zapewniająca dostęp do Internetu powinna zapewniać redundantny i bezpieczny dostęp do światowych zasobów sieciowych. Protokołem routingu wymaganym do użycia na styku z dostawcami łączy do Internetu jest BGP. Ze względu na dużą liczbę wpisów do tablicy routingu BGP, styk musi zapewniać odpowiednią skalowalność i wsparcie protokołu IPv6 oraz mechanizmy umożliwiające świadczenie usług w sposób niezawodny i bezpieczny charakteryzującymi się wysokimi parametrami jakościowych. W przypadku urządzeń w W.INTERNET istotnymi, wymaganymi właściwościami są:

* Wysoka niezawodność i ciągłość świadczenia usług osiągnięta przez redundancję połączeń, urządzeń i oprogramowania zarządzającego routerami.
* Wysoka wydajność umożliwiająca realizację wymaganych usług (peering BGP, Quality of Service).
* Zawansowanie mechanizmy Quality of Service umożliwiające elastyczną konfigurację wielu usług i polityk. Punkt styku z operatorami będzie zawsze wąskim gardłem w porównaniu z przepustowością uzyskiwaną w sieci DC z tego też względu parametry takie jak ilość kolejek, polityk, hierarchiczny QoS będą niezwykle istotne.
* Wsparcie dla tunelowania GRE i szyfrowania IPSec, które umożliwi bezpieczny dostęp do zasobów znajdujących się poza obszarem sieci miejskiej (mogą być to różnego rodzaju aplikacje zewnętrzne posadowione na serwerach obsługiwanych przez zewnętrznych operatorów, w zewnętrznych Centrach Przetwarzania Danych).
* Wsparcie dla MPLS i MPLS VPN L2 i L3 w celu elastycznej współpracy z W.RDZEN.
* Wsparcie dla IPv6.

Podłączenie do Internetu musi być zrealizowane w oparciu o usługi, co najmniej dwóch dostawców oraz za pomocą co najmniej dwóch identycznych urządzeń sieciowych. Całość podłączona zostanie w sposób redundantny do W.RDZEN. Zdublowanie urządzeń W.INTERNET pozwala na rozłożenie obciążenia związanego z obsługą ruchu Internetowego, a w przypadku awarii jednego z nich zapewnia ciągłość działania usługi dostępu do Internetu jak i innych usług terminowanych na urządzeniach W.INTERNET.

Uruchomienie funkcjonalności MPLS pomiędzy urządzeniami W.INTERNET a W.RDZEN, pozwoli na proste rozbudowanie systemu o kolejne routery wspierające większe przepustowości i większą ilość interfejsów sieciowych, jeżeli takie zapotrzebowanie nastąpi.

### Wymagania ogólne dla urządzeń w W.SERWIS

W.SERWIS musi zapewnić spójny i prosty w rozbudowie punkt oferowania serwisów dla usług wewnętrznych Zamawiającego i klientów zewnętrznych. Głównym elementem W.SERWIS są zapory ogniowe (firewall). Musza oferować usługi filtracji ruchu z możliwością wydzielenia wirtualnych zapór ogniowych dla klientów zewnętrznych lub usług Zamawiającego w formie usługi dodatkowej. Architektura rozwiązania powinna umożliwić w przyszłości jego rozbudowę o kolejne zapory ogniowe (minimum 4 w klastrze), które pracowałyby jako jedno logiczne urządzenie, zapewniające dodatkową przepustowość przesyłanych danych. Architektura W.SERWIS powinna również umożliwić dodawanie innych serwisów, takich jak system balansowania ruchem (Load Balancer), system wykrywania i zapobiegania atakom (IPS), etc.

W przypadku zapór ogniowych istotnymi, wymaganymi właściwościami są:

* Wysoka niezawodność i ciągłość świadczenia usług osiągnięta przez redundancję urządzeń pracujących logicznie jako jedno urządzenie.
* Możliwość zwiększenia przepustowości rozwiązania poprzez dołączanie kolejnych par identycznych zapór ogniowych, które pracują logicznie jako jedno urządzenie.
* Wsparcie dla interfejsów 10 Gbps, które zostaną wykorzystane do podłączenia do W.RDZEN oraz połączeń klastra.
* Obsługę przynajmniej 50 wirtualnych kontekstów, które charakteryzują się oddzielnymi konfiguracjami.
* Możliwość przyłączania fizycznych, bądź logicznych interfejsów na każdy wirtualny kontekst.

### Wymagania ogólne dla urządzeń w W.KAMPUS

W.KAMPUS zapewnia miejsce do podłączenia pracowników DC, TARR oraz klientów EXEA Smartspace. Dostarczone urządzenia znajdować się będą w przeznaczonych do tego pomieszczeniach, a ich podłączenie jest przedstawione na rysunku 4. Umiejscowienie urządzeń w szafach zostało przedstawione na rysunku 11.

Z racji na potrzebę dalszej rozbudowy sieci, bezpieczeństwa oraz zarządzania siecią wymaga się, aby:

* Przełączniki były modularnymi urządzeniami, aby zapewnić prosty sposób na zwiększenie portów poprzez dołożenie kart liniowych do urządzenia.
* Przełączniki były urządzeniami z jednej rodziny produktowej, celem łatwości zarządzania tymi urządzeniami.
* Każde z urządzeń powinno posiadać możliwość dodawania kart liniowych wspierających standardy Power over Ethernet.
* Każdy z przełączników powinien posiadać dwa moduły zarządzające oraz minimum dwa zasilacze, aby zapewnić redundancję wewnątrz jednego urządzenia.
* Z racji na plany rozwojowe DC EXEA, przełączniki powinny mieć opcje uruchomienia kontrolera sieci bezprzewodowej wewnątrz przełącznika jako karty liniowej, albo wbudowanego systemu kontrolera na karcie zarządzającej.

### Wymagania w zakresie możliwości rozbudowy DC

Obecny projekt ma na celu dostarczenie urządzeń (mowa tu w szczególności o urządzeniach W.RDZEN), które będą w stanie realizować usługi sieciowe dla DC w pełnym obłożeniu. Projekt sieci uwzględnia wydzielenie dwóch punktów GPDx (każdy składający się z 2 szaf). Docelowa wielkość sieci DC zakłada obsługę 320 szaf serwerowych. Wymagane jest więc, aby wielkość i możliwości rozbudowy urządzeń w punktach GPDx umożliwiły obsłużenie ruchu z całego DC, wg. wymagań opisanych w punkcie 2.6.

Na rysunku 12 przedstawione zostało przykładowe rozłożenie urządzeń aktywnych i pasywnych w punktach GPDx, przy pełnym obłożeniu DC, zakładając, że w maksymalnie 320 szafach serwerowych znajdować się będą 2 moduły wyniesione opisane w punkcie 2.9.2. Na rysunkach kolorem różowym zostały zaznaczone planowane umiejscowienia elementów aktywnych i pasywnych (opisanych poniżej). Kolorem szarym zaś zostały oznaczone elementy, które są opisane w tym projekcie. Umiejscowienie i wysokość tychże urządzeń ma duże znaczenie, w aspekcie planowanego rozwoju DC do maksymalnych możliwości.

Zakłada się możliwość rozbudowy każdego z GPDx o:

* Usługi sieciowe dla maksymalnie 320 szaf serwerowych (w każdej z szaf powinny się znaleźć 2 moduły wyniesione przełączników dostępowych), ilość urządzeń rdzeniowych nie może ulec zmianie.
* Połączenie 40 Gbps (migracja z 10 Gbps do 40 Gbps) przez wymianę/dołożenie określonych kart liniowych, bez potrzeby dodawania kolejnych urządzeń rdzeniowych.
* 10 patchpaneli światłowodowych (włókna wielomodowe) realizujących funkcję dystrybucji, służącej do podłączenia wszystkich urządzeń z punktów EoR.
* Minimum 1 patchpanel światłowodowy (włókna wielomodowe) realizującego funkcje rdzeniowe, służącego do połączenia urządzeń pomiędzy GPDx.
* Minimum 2 dodatkowe zapory sieciowe (W.SERWIS), o parametrach nie gorszych niż urządzenia opisane w punkcie 2.9.4.
* Minimum 5 urządzeń W.INTERNET o parametrach nie gorszych niż urządzenia opisane w punkcie 2.9.3.
* Dodatkowe systemy zarządzania. W celu zapewnienia planów dotyczących możliwości systemów zarządzania, założono 16-17 RU (Rack Units) wolnego miejsca w szafie GPDx.
* Dodatkowe urządzenia W.SERWIS (w szczególności load balancer oraz IPS).

## Bloki fizyczne sieci Data Center

Sieć DC zbudowana jest z określonych warstw, przedstawionych na Rysunku 1. Zastosowanie warstw oraz wymagań z punktu 2.6. wymagają zastosowania bloków fizycznych w zakresie danej komory DC, gdzie znajdować się będą urządzenia opisane w punkcie 2.9.

Pod względem funkcjonalności wyodrębnić można 4 bloki fizyczne:

* GPDx – blok fizyczny składający się z dwóch szaf serwerowych. W obrębie DC znajdują się dwa takie bloki, które zostaną usytuowane w przeciwległych punktach K1. Każdy z bloków będzie zawierał identyczną ilość urządzeń W.RDZEN, W.SERWIS oraz W.INTERNET. W momencie zapotrzebowania, w bloku GPDx mogą być w niej umieszczone również moduły wyniesione AKxyyvvv. Szczegółowy opis bloków GPDx przedstawiony został na Rysunku 7,8.
* EoR – szafa serwerowa, w której znajdują się dwa przełączniki AKxyyz, do którego podłączane będą wyniesione moduły AKxyyvvv. W obrębie jednej komory planuje się umieszczenie 8 bloków EoR, przy czym w obrębie całego DC planuje się umieszczenie 32 bloków EoR. Obecny projekt przewiduje dostarczenie urządzeń do 2 bloków EoR. Wolne miejsce w szafach wykorzystanych do bloków EoR będzie używane do umiejscowienia serwerów, lub innych urządzeń. W momencie zapotrzebowania, mogą być w niej umieszczone również wyniesione moduły AKxyyvvv. Blok EoR w szczególnych przypadkach może zostać umieszczony w bloku GPDx. Szczegółowy opis bloku EoR przedstawiony został na Rysunku 9.
* ToR –szafa serwerowa, w której znajdują się dwa wyniesione moduły AKxyyvvv, do których podłączone są serwery, bądź inne urządzenia sieciowe należące do zasobów DC, lub do klientów zewnętrznych. W obrębie jednej komory planuje się umieszczenie 70-80 bloków ToR, przy czym w obrębie całego DC planuje się umieszczenie 280-320 bloków ToR. Obecny projekt przewiduje dostarczenie urządzeń do 20 bloków ToR. Szczegółowy opis bloku ToR przedstawiony został na Rysunku 10.
* KAMx – KAM1 oraz KAM2 są szafami serwerowymi, w których zostaną zainstalowane SW1 oraz SW2. KAM1 oraz KAM2 mieszczą się w dwóch niezależnych pomieszczeniach. W szafach przylegających do KAMx umiejscowione są istniejące już patchpanele, służące do podłączania pracowników DC, Inkubatora technologicznego oraz innych podmiotów. Szczegółowy opis bloku KAMx przedstawiony został na Rysunku 11.

### Główny punkt dystrybucyjny – GPDx

W obrębie DC umieszczone zostaną dwa punkty GPDx, które stanowić będą centralną część sieci. W celu zapewnienia ochrony przed lokalnymi awariami, punkty te zostaną umiejscowione w przeciwległych rogach K1, z możliwością ewentualnego przeniesienia jednego z punktów GPDx do innej komory (Kx). Z racji na plany rozwoju DC, wymaga się, aby dostarczane urządzenie nie przekraczały wysokości, określonych w pkt. 2.9 oraz tabeli 3.2. Plan rozwoju punktów GPDx opisany został w pkt. 2.6.7 oraz został zobrazowany na rysunku 12.

### Infrastruktura głównego punktu dystrybucyjnego

Blok GPDx (widoczny na rysunku 7,8) musi składać się co najmniej z:

* Dwóch szaf serwerowych z systemem zasilania oraz systemem chłodzenia dostarczonym przez Zamawiającego
* Urządzenia rdzeniowego warstwy W.RDZEN - Cx, pełniącego funkcje agregacji urządzeń dostępowych oraz sterowania ruchem pomiędzy poszczególnymi warstwami opisanymi na rysunku 1.
* Dwóch patchpaneli światłowodowych (włókna wielomodowe) PPA i PPR. Jeden pełnić będzie funkcję połączenia przełączników dostępowych z bloków EoR z GPDx, drugi pełnić będzie funkcje połączenia obu bloków GPDx.
* Jednego patchpanelu światłowodowego (włókna jednomodowe) – PPINT - dostarczonego przez Zamawiającego, pełniącego funkcje agregacji połączeń z KAMx, jak również połączeń od operatorów.
* Jednego urządzenia styku z Internetem - INTx, do którego podłączane będą łącza operatorów terminowane w K1 na patchpanelu światłowodowym PPINT.
* Zapory ogniowej (FWx) podłączanej do urządzeń W.RDZEN.
* Serwera realizującego funkcję wsparcia systemów zarządzających SRVMGMTx.
* Serwera realizującego funkcję platformy usług sieciowych MGMTUSx.
* Przełącznika sieci zarządzającej – SWMGMTKxyy, do którego podłączane będą systemy zarządzające siecią DC oraz porty zarządzające urządzeń sieciowych.
* Przełącznika KVM – KVMx
* Serwera przełącznika KVM – SRVKVMx

Dodatkowo w GPD1 dodany zostanie:

* Przełącznik agregujący (SWMGMTx) połączenia z przełączników SWMGMTKxyy.

Dodatkowo w GPD2 dodany zostanie:

* Serwer realizujący funkcję systemu zarządzania i automatyzacji środowiska sieciowego – MGMTAUT.

### End of Row – EoR

Blok EoR (widoczny na rysunku 9) musi składać się co najmniej z:

* Jednej szafy serwerowej z systemem zasilania oraz systemem chłodzenia dostarczonym przez Zamawiającego
* Dwóch przełączników dostępowych AKxyyz
* Czterech patchpaneli światłowodowych (włókna wielomodowe) PPA. Panele pełnić będą funkcję połączenia przełączników dostępowych AKxyyz z wyniesionymi kartami przełączników dostępowych AKxyyvvv oraz z urządzeniami rdzeniowymi Cx.
* Przełącznika sieci zarządzającej – SWMGMTKxyy, do którego podłączane będą systemy zarządzające siecią DC oraz porty zarządzające urządzeń sieciowych.

### Top of Rack – ToR

Blok ToR (widoczny na rysunku 10) musi składać się co najmniej z:

* Jednej szafy serwerowej z systemem zasilania oraz systemem chłodzenia dostarczonym przez Zamawiającego
* Dwóch modułów wyniesionych przełączników dostępowych AKxxyyvvv.
* Jednego patchpanela światłowodowego (włókna wielomodowe) PPA. Panel pełnić będzie funkcję połączenia AKxxyyvvv do przełączników dostępowych AKxxyyz.

### Szafa serwerowa dla sieci kampusowej – KAMPx

Blok KAMx (widoczny na rysunku 11) musi składać się co najmniej z:

* Jednej szafy serwerowej z systemem zasilania oraz systemem chłodzenia dostarczonym przez Zamawiającego
* Jednego patchpanelu światłowodowego (włókna jednomodowe) - dostarczonego przez Zamawiającego, pełniącego funkcję połączeń do GPDx.
* Systemu patchpaneli RJ45 dostarczonego przez Zamawiającego, terminującego w szczególności połączenia pracowników DC, EXEA Smartspace.

Dodatkowo w każdym z bloków zainstalowany zostanie przełącznik realizujący funkcje W.KAMPUS: SW1, albo SW2.

## Organizacja połączeń między warstwowych

Opis organizacji połączeń między warstwowych ma na celu określenie sposobu łączenia określonych urządzeń z określonych warstw. W celu zachowania zasady konkurencyjności projekt nie określa producenta poszczególnych urządzeń. W związku z tym, projekt nie określa dokładnie które porty danych urządzeń mają być połączone. Dokładne ustalenia dotyczące połączeń są przedmiotem Planu Wdrożenia, który zostanie opracowany po wyborze oferty przez Zamawiającego.

### Organizacja połączeń pomiędzy W.RDZEN a W.INTERNET

Organizacja połączeń pomiędzy W.RDZEN a W.INTERNET została przedstawiona na rysunku 3.

* Urządzenia C1 i C2 zostaną połączone odpowiednią ilością łączy 10 Gbps (lub szybszych) w celu zapewnienia odpowiednich przepustowości dla ruchu pomiędzy urządzeniami Cx oraz innymi urządzeniami realizujących połączenia tą drogą, np. FWx. Połączenia będą również realizować funkcje synchronizacji protokołów używanych m.in. do funkcjonalności Multi-Chassis Link Aggregation.
* Każde z urządzeń INTx podłączone będzie za pomocą linków 10 Gbps (lub szybszych) do każdego z urządzeń Cx w celu zapewniania pełnej redundancji, a tym samym umożliwić wystarczające pasmo dla przyszłych usług realizowanych na łączach operatorskich dołączanych do portów 1 Gbps, albo 10 Gbps na urządzeniach INTx.
* Z racji na brak ruchu tranzytowego pomiędzy urządzeniami INTx oraz na potrzebę uniezależnienia urządzeń INT1 od INT2, nie planowane jest podłączanie urządzeń podłączonych do INT1 bezpośrednio do INT2.

### Organizacja połączeń pomiędzy W.RDZEN a W.SERWIS

Organizacja połączeń pomiędzy W.RDZEN a W.SERWIS została przedstawiona na rysunku 5.

* Każda z zapór ogniowych (FWx) podłączona zostanie do każdego z przełączników Cx co najmniej dwoma linkami 10 Gbps (lub szybszych). Ma to na celu zapewnienie odpowiedniej przepustowości, ale również możliwość wykorzystania funkcjonalności klastrowania urządzeń. Przy usłudze klastrowania wymagane są połączenia do synchronizacji stanów sesji oraz wymiany informacji o ruchu symetrycznym, które powinny mieć tą samą przepustowość co łącza realizujące przesył danych.

### Organizacja połączeń pomiędzy W.RDZEN a W.KAMPUS

Organizacja połączeń pomiędzy W.RDZEN a W.KAMPUS została przedstawiona na rysunku 4.

* Każde z urządzeń SWx umiejscowione jest w osobnym pomieszczeniu. Z racji potrzeby agregacji połączeń od klientów podłączonych do SWx, konieczne jest podłączenie każdego z SWx do każdego z urządzeń Cx. Realizowane to będzie poprzez połączenie każdego z SWx do każdego Cx przynajmniej jednym połączeniem 10 Gbps (lub szybszym).
* W celu zapewnienia redundancji z poziomu przełącznika SWx oraz ochrony przed pętlami L2, zdecydowano na użycie dwóch kart zarządzających w przełącznikach SWx oraz na rezygnację z połączenia pomiędzy SW1 i SW2, stosując przy tym samym połącznie L3 pomiędzy Cx i SWx.

### Organizacja połączeń pomiędzy W.RDZEN a W.DOSTEP

Organizacja połączeń pomiędzy W.RDZEN a W.DOSTEP została przedstawiona na rysunku 2.

* Urządzenia AKxyy1 i AKxyy2, reprezentujące jeden blok EoR, połączone będą ze sobą za pomocą odpowiedniej ilością łączy 10 Gbps (lub szybszych) w celu zapewnienia odpowiednich przepustowości dla ruchu pomiędzy przełącznikami dostępowymi AKxyyz oraz do wymiany ruchu synchronizacyjnego.
* Każde z urządzeń AKxyyz połączone będzie do każdego z urządzeń Cx przynajmniej dwoma linkami 10 Gbps (lub szybszymi) w celu zapewnienia odpowiedniej przepustowości oraz możliwości użycia funkcjonalności Multi-Chassis Link Aggregation przy pełnej przepustowości. Zakłada się użycie w sumie 8 łącz (10 Gbps lub szybszych) pomiędzy jedną parą urządzeń AKxxyy1 (reprezentujących blok EoR) z parą urządzeń Cx (W.RDZEN).

### Organizacja połączeń wewnątrz W. DOSTEP

Organizacja połączeń wewnątrz W.DOSTEP została przedstawiona na rysunku 6.

* Para modułów wyniesionych przełączników dostępowych AKxyyvvv reprezentuje jeden blok ToR.
* Każdy z modułów podłączony będzie do dwóch przełączników dostępowych AKxyy1 i AKxyy2 jednym łączem 10 Gbps (lub szybszym). Opcja podłączenia każdego z modułów AKxyyvvv do każdego z przełączników dostępowych AKxyyz została wybrana, ponieważ oczekuje się, że sieć DC będzie redundantna w każdym elemencie. Zamawiający nie dopuszcza podłączenia jednego modułu wyniesionego do tylko jednego przełącznika, które wprowadza możliwość odcięcia modułów AKxyyvvv (w 10+ szafach serwerowych) w momencie awarii dowolnego przełącznika dostępowego AKxyyz.

## Charakterystyka techniczna urządzeń

Wskazane poniżej wymagania zostały określone w celu sprecyzowania parametrów i warunków techniczno-użytkowych. Dopuszcza się zastosowanie urządzeń o parametrach nie gorszych od podanych w projekcie oraz spełniających wymagania norm mających zastosowanie do budowy systemu. Wszelkie zmiany należy uzgodnić z Zamawiającym.

### Wymagania dla urządzeń rdzeniowych

1. Urządzenie musi być modularne, min. 10 gniazd na moduły, z czego min. 8 gniazd dostępnych dla modułów z interfejsami liniowymi.
2. Urządzenie musi być oparte o w pełni rozdzielną i niezależną od warstwy przesyłania danych warstwę kontrolno-zarządzającą. Moduły kontrolno-zarządzające nie mogą zajmować się przesyłaniem ramek/pakietów między modułami liniowymi.
3. Urządzenie w pełni musi wspierać rozproszone przełączanie ramek/pakietów tzn. każdy z modułów liniowych musi posiadać lokalną tablice przełączania i na jej podstawie kierować ramki/pakiety do innych modułów liniowych.
4. Urządzenie musi posiadać architekturę opartą o modularne matryce przełączające
5. Urządzenie musi zapewniać równoległy dostęp każdego z modułów liniowych do każdej matrycy przełączającej, niezależnie od liczby zainstalowanych matryc.
6. Urządzenie musi być oparte o niezawodny i modularny system operacyjny umożliwiający m.in. izolację poszczególnych procesów od siebie, ich bezpieczne i indywidualne restartowanie.
7. Należy wyposażyć urządzenia w ilość matryc gwarantującą pracę z pełną wydajnością wszystkich modułów.
8. Urządzenie zapewnia możliwość podziału na minimum 4 logiczne przełączniki (wirtualne konteksty), z których każdy posiada własne zarządzanie z osobnym adresem IP. Konteksty muszą być w pełni odizolowane od innych i posiadające dedykowane i niezależne zasoby takie jak fizyczne porty, sieci VLAN, tablice routingu oraz zarządzanie. Dostęp do każdego z wirtualnych kontekstów musi być oparty o niezależnie definiowanych użytkowników/administratorów mających prawa dostępu tylko do danego kontekstu. Awaria czy też restart procesu (np. związanego z routingiem OSPF czy też z Spanning Tree) w danym kontekście nie może powodować zakłócenia działania podobnego procesu w innym kontekście. Jeżeli dana funkcjonalność wymaga dostarczenia licencji, należy ją dostarczyć.
9. Urządzenie zapewnia możliwość rozbudowy do 8 logicznych przełączników. Jeżeli dana funkcjonalność wymaga dostarczenia licencji, nie jest ona wymagana w zakresie tego postępowania.
10. Zainstalowane minimum dwa niezależne zasilacze, przy czym musi być zagwarantowana redundancja zasilania i źródeł zasilania oraz wymagana jest redundancja modułów wentylatorów.
11. Musi mieć zainstalowane co najmniej dwa moduły zarządzające .
12. Wymagana jest funkcjonalność umożliwiająca aktualizację firmware (systemu operacyjnego) bez przerywania pracy urządzenia, w szczególności bez przerwania transmisji ramek/pakietów („zero packet loss”).
13. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem zarządzania urządzeniami:
    1. Port konsoli CLI,
    2. SSHv2,
    3. Authentication, authorization, and accounting (AAA),
    4. RADIUS,
    5. Syslog,
    6. SNMP v2, v3,
    7. Enhanced SNMP MIB,
    8. Remote monitoring (RMON),
    9. Role-Based Access Control RBAC,
    10. Network Time Protocol (NTP).
14. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    1. port security,
    2. ochrona struktur sterujących urządzenia przed atakami DoS (Control Plane Policing),
    3. wejściowe filtry ACL (standardowe oraz rozszerzone),
    4. standardowe oraz rozszerzone ACL dla warstwy 2 w szczególności oparciu o adresy MAC i typ protokołu,
    5. standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w szczególności w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP).
15. Urządzenie musi wspierać następujące mechanizmy związane z Quality of Service:
    1. Layer 2 IEEE 802.1p (CoS),
    2. Dedykowana konfiguracja QoS dla każdego portu,
    3. Kolejkowanie na wyjściu w oparciu o CoS,
    4. Bezwzględne (strict-priority) kolejkowanie na wyjściu,
    5. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu.
16. Urządzenie musi umożliwiać bezpłatną aktualizację oprogramowania przez okres wsparcia.
17. Oprogramowanie urządzenia spełniające warunki specyfikacji musi być oficjalnie dostępną wersją możliwą do pobrania ze strony producenta dla każdego posiadacza produktu danego producenta. Nie dopuszczalne jest oferowanie oprogramowania pisanego na potrzeby tego zamówienia specjalnie dla Zamawiającego.
18. Musi istnieć polskojęzyczna linia wsparcia technicznego producenta urządzeń dla oferowanych produktów.
19. Każdy z przełączników musi mieć możliwość dołączania zewnętrznych, wyniesionych modułów liniowych posiadających 48 portów 100/1000BaseT, 32x1/10G, 48x1/10G dołączanych do jednostki centralnej pasmem odpowiednio 10-40 Gbps, 10-80 Gbps oraz 10-160-Gbps. Przełącznik musi umożliwiać dołączenie przynajmniej 32 takich modułów. Zarządzanie modułami musi odbywać się wyłącznie z jednostki centralnej. Dołączenie modułów nie może być zrealizowane z wykorzystaniem mechanizmów L2 (Spanning Tree). Dołączenie musi stanowić rozszerzenie w domenie warstwy L1.
20. Przełącznik musi mieć opcję instalacji modułu wyniesionego do chassis blade różnych producentów.
21. Urządzenie musi umożliwiać obsadzenie co najmniej 384 portów optycznych 10GE pracujących z pełną wydajnością (wirespeed) w warstwie 2 (L2) i w konfiguracji opartej wyłącznie o porty 10GE lub szybsze.
22. Urządzenie musi być wyposażone w minimum 72 porty 10GE obsługującymi wkładki typu X2, XENPAK, XFP lub równoważne.
23. Urządzenie musi być dostarczone z min. 30 wkładkami umożliwiającymi pracę na dystansie minimum 100 metrów po światłowodzie wielomodowym (standard 10G-SR).
24. Urządzenie musi być dostarczone z min. 4 wkładkami umożliwiającymi pracę na dystansie minimum 100 metrów po światłowodzie jednomodowym (standard 10G-LRM).
25. Wkładki muszą pochodzić od tego samego dostawcy co oferowane urządzenia celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.
26. Urządzenie musi zapewniać obsługę min. 4,000 sieci VLAN dla pracy w warstwie L2, z możliwością rozszerzenia do 10,000 poprzez wykorzystanie kontekstów.
27. Urządzenie musi zapewniać min. 16,000 wpisów MAC dla działania w trybie L2.
28. Urządzenie musi wspierać sprzętowe uczenie się adresów MAC.
29. Urządzenie musi oferować wydajność wirespeed dla przełączania w warstwie L2 /L3 dla ramek/pakietów o minimalnej wielkości 64bajtów.
30. Urządzenie musi wspierać następujące funkcjonalności Ethernet dla warstwy 2:
    1. Trunking IEEE 802.1Q VLAN,
    2. Rapid Per-VLAN Spanning Tree Plus (PVRST+) (IEEE 802.1w),
    3. Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s),
    4. Internet Group Management Protocol (IGMP) Versions 2, 3 snooping,
    5. UDLD lub mechanizm odpowiadający,
    6. Grupowanie portów Ethernet (do 8 portów per wiązka),
    7. MultiChassis Channel, czyli terminowanie pojedynczej wiązki Ethernet na 2 niezależnych przełącznikach,
    8. Link Aggregation Control Protocol (LACP): IEEE 802.3ad,
    9. Ramki Jumbo dla wszystkich portów (do 9000 bajtów),
    10. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.
31. Urządzenie musi umożliwiać implementację mechanizmu FabricPath lub równoważnego (TRILL) pozwalającego na budowę sieci bez wykorzystania mechanizmów Spanning Tree. Jeżeli wymagana jest licencja, nie wymaga się dostarczenia jej w ramach zamówienia.
32. Urządzenie dla portów L2 musi spełniać następujące zalecenia IEEE związane z Data Center Bridging:
    1. IEEE 802.1Qbb PFC (per-priority pause frame support),
    2. Wsparcie dla DCBX Protocol,
    3. IEEE 802.1Qaz Enhanced Transmission Selection.
33. Urządzenie musi umożliwiać obsadzenie minimum 384 interfejsów optycznych 10 GigabitEthernet pracujących w warstwie L3 w konfiguracji wyłącznie z portami 10 GE pracujących z pełną wydajnością (wirespeed).
34. Wymagane jest, aby decyzja o przełączeniu pakietu odebranego na porcie wejściowym w warstwie L3, łącznie z wyznaczeniem docelowego adresu MAC i portu wyjściowego została podjęta na poziomie karty liniowej, na której znajduje się dany port wejściowy (tzw. rozproszone przełączanie L3).
35. Urządzenie musi zapewniać min. 16,000 wpisów MAC dla działania w trybie L3.
36. Urządzenie musi zapewniać min. 30 000 wpisów w tablicy routingu IPv4.
37. Urządzenie musi zapewniać min. 1000 pozycji filtrujących typu „ACL” na poziomie warstwy L3.
38. Urządzenie musi oferować wydajność wirespeed dla przełączania IPv4 dla oraz dla IPv6, lokalnie dla każdego modułu.
39. Urządzenie musi wspierać następujące protokoły routingu:
    1. IPv4: OSPF, BGP, IS-IS,
    2. IPv6: OSPFv3, BGP, IS-ISv6,
    3. W przypadku gdyby obsługa powyższych protokołów wymagała dostarczenia licencji z urządzeniem licencja ta musi zostać dostarczona,
    4. Wsparcie dla Gracefull Restart i NSF.
40. Urządzenie musi wspierać następujące protokoły multicast:
    1. IGMPv2/v3, IGMP snooping,
    2. PIMv2 Sparse, SSM, Bidirectional dla IPv4 oraz IPv6,
    3. MLDv2 dla IPv6.
41. Urządzenie musi wspierać następujące aplikacje protokołu MPLS
    1. Funkcjonalność MPLS VPN warstwy trzeciej,
    2. Funkcjonalność MPLS VPN warstwy drugiej (AToM, VPLS),
    3. MPLS Traffic Engineering oraz Fast Reroute (FRR),
    4. Multicast VPNs,
    5. Jeśli urządzenie wymaga licencji do uruchomienia powyższych funkcjonalności wymagane jest dostarczenie jej dla minimum 24 portów.
42. Urządzenie musi dodatkowo wspierać następujące protokoły:
    1. Bidirectonal Forwarding Detection z klientem ISISv6, PIMv6, BGPv6, OSPFv3,
    2. HSRP (Hot-Standby Routing Protocol) dla IPv4 I IPv6 lub odpowiadający (VRRP).
43. Urządzenie musi posiadać funkcjonalność umożliwiającą dołączanie zewnętrznych przełączników do pary urządzeń będących przedmiotem specyfikacji. Zewnętrzny przełącznik, niezależnie od jego typu i producenta, musi mieć możliwość dołączenia poprzez zagregowany kanał (LACP, EtherChannel) złożony z min. 2 fizycznych interfejsów w taki sposób, że jeden interfejs zewnętrznego przełącznika dołączony jest do jednego z opisywanych urządzeń, drugi zaś do innego, niezależnego (tzw. MultiChassis Channel).

### Wymagania dla przełączników dostępowych

1. Przełącznik musi być wyposażony w co najmniej 48 portów 10G i 4 porty 40G pracujące zamiennie jako 16 portów 10G, definiowanych za pomocą wkładek SFP, SFP+, QSFP lub równoważnych. Wymagana jest obsługa wkładek interfejsowych typu 10GE-SR, 10GE-LR, 10G-ER, 40G-SR4. Wymagane jest, aby wszystkie porty z pośród w/w umożliwiały pracę w trybie GigabitEthernet (1GE) z możliwością instalacji wkładki interfejsowej SFP lub równoważnej typu 1000BaseT, ZX, LX oraz SX; Wymagana jest obsługa kabli typu 10GE Twinax o długości 1, 3, 5, 7 oraz 10 metrów.
2. Każdy z przełączników musi mieć możliwość dołączania zewnętrznych, wyniesionych modułów posiadających 48x portów 100/1000BaseT dołączanych pasmem 10-40G, 32x 1/10G dołączanych pasmem 10-80G, 48x 1/10G dołączanych pasmem 10-160G.
3. Moduły 1/10G muszą być definiowane za pomocą wymiennych wkładek/modułów. Moduły te muszą obsługiwać standardy 1G, 10GE oraz FCoE na portach 10G.
4. Przełącznik musi umożliwiać dołączenie przynajmniej 24 takich modułów.
5. Przełącznik musi mieć opcję modułu wyniesionego do chassis blade różnych producentów.
6. Zarządzanie modułami musi odbywać się wyłącznie z jednostki centralnej. Dołączenie modułów nie może być zrealizowane z wykorzystaniem mechanizmów L2 (Spanning Tree). Dołączenie musi stanowić rozszerzenie w domenie warstwy L1;
7. Przełącznik musi wspierać integrację z VMware 5.x, KVM oraz Hyper-V 3.0 w oparciu o technologie VM-FEX/VN-TAG lub odpowiadająca funkcjonalnie (np. VEPA)
8. Wymagane jest opóźnienie przełączania pakietów nie większe niż 1 µs przy 10 Gbps (L2/L3);
9. Wymagana jest prędkość przełączania L2/L3„wirespeed” dla każdego portu 10GE/40GE;
10. Wymagany jest rozmiar tabeli adresów MAC min. 128 000;
11. 19 cali – do montażu w szafie rakowej, wysokość max 1 RU
12. Urządzenie musi umożliwiać uruchomienie na wszystkich portach 10GE przełącznika implementacji FCoE zgodnie z ANSI T11 (FC-BB-5), w szczególności FCoE Initialization Protocol (FIP); Jeżeli wymagana jest licencja, nie wymaga się dostarczenia jej w ramach zamówienia.
13. Urządzenie musi umożliwiać implementację mechanizmu FabricPath lub równoważnego (TRILL) pozwalającego na budowę sieci bez wykorzystania mechanizmów Spanning Tree. Jeżeli wymagana jest licencja, nie wymaga się dostarczenia jej w ramach zamówienia.
14. Urządzenie musi mieć możliwość wsparcia następujących standardów:
    1. IEEE 802.1Qbb PFC (per-priority pause frame support),
    2. IEEE 802.1AB DCBX Protocol,
    3. IEEE 802.1Qaz Enhanced Transmission Selection.
15. Urządzenie musi wspierać następujące funkcjonalności Ethernet dla warstwy 2:
    1. Trunking IEEE 802.1Q VLAN,
    2. Wsparcie dla 4000 sieci VLAN,
    3. Rapid Per-VLAN Spanning Tree Plus (PVRST+) (IEEE 802.1w),
    4. Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s): minimum 64 instancje,
    5. Spanning Tree PortFast,
    6. Spanning Tree Root Guard,
    7. Spanning Tree Bridge Assurance,
    8. Internet Group Management Protocol (IGMP) Versions 2, 3,
    9. Grupowanie EtherChannel (do 16 portów per wiązka EtherChannel),
    10. Grupowanie virtual PortChannel (vPC) polegające na terminowaniu pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach,
    11. Link Aggregation Control Protocol (LACP): IEEE 802.3ad,
    12. Ramki Jumbo dla wszystkich portów (do 9216 bajtów),
    13. Ramki Pause (IEEE 802.3x),
    14. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast,
    15. Implementacja mechanizmu Private VLAN lub równoważnego.
16. Urządzenie musi wspierać następujące funkcjonalności warstwy L3:
    1. Przełączanie pakietów w warstwie L3,
    2. Obsługa interfejsów warstwy 3 - portów routowalnych, svi, subinterfejsów PortChannel minimum 4000,
    3. Minimum 32000 prefixów oraz 128000 wpisów hosta w tablicy routingu,
    4. Wsparcie dla 32000 tras multicastowych,
    5. Wsparcie dla 4000 VRF,
    6. Wybór do 16-tu jednoczesnych ścieżek o równej metryce (ECMP),
    7. 2000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list,
    8. Obsługa protokołów routing dla IPv4: Routing Statyczny, Routing Information Protocol Version2 (RIPv2), Open Shortest Path First Version 2 (OSPFv2) oraz Border Gateway Protocol (BGP),
    9. Obsługa protokołów routing dla IPv6: Routing Statyczny, Open Shortest Path First Version 3 (OSPFv3) oraz Border Gateway Protocol (BGP),
    10. Obsługa Hot-Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP, także VRRPv3) lub mechanizmów odpowiadających im funkcjonalnie,
    11. Obsługa protokołów Multicastowych: Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol V2, 3 (IGMP v2, v3),
    12. Wsparcie dla mechanizmów Virtual Route Forwarding (VRF): VRF-lite (IP VPN),
    13. VRF-aware unicast; BGP-, OSPF-, RIP-, oraz VRF-aware multicast,
    14. Mechanizm Unicast Reverse Path Forwarding (uRFP) lub odpowiadający,
    15. Obsługa ramek Jumbo do 9216 byte-ów.
17. Urządzenie musi wspierać następujące funkcjonalności QoS:
    1. Layer 2 IEEE 802.1p (CoS),
    2. 8 sprzętowych kolejek per port,
    3. Dedykowana konfiguracja QoS dla każdego portu,
    4. Przypisanie CoS na każdym porcie,
    5. Klasyfikacja QoS w oparciu o listy ACL (Access control list) – w warstwach 2, 3, 4,
    6. Virtual output queuing dla każdego portu,
    7. Kolejkowanie na wyjściu w oparciu o CoS,
    8. Bezwzględne (strict-priority) kolejkowanie na wyjściu,
    9. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu.
18. Urządzenie musi wspierać następujące funkcjonalności bezpieczeństwa:
    1. Wejściowe ACL (standardowe oraz rozszerzone),
    2. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC, typ protokołu,
    3. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i v6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP),
    4. ACL oparte o VLAN-y (VACL),
    5. ACL oparte o porty (PACL),
    6. Logowanie i statystyka dla ACL.
19. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem zarządzania urządzeniami
    1. Port zarządzający 10/100/1000 Mbps,
    2. Port konsoli CLI,
    3. Zarządzanie In-band switch,
    4. SSHv2,
    5. Telnet,
    6. Authentication, authorization, and accounting (AAA),
    7. RADIUS,
    8. Syslog,
    9. SNMP v1, v2, v3,
    10. Wsparcie dla mechanizmów Enhanced SNMP MIB,
    11. Remote monitoring (RMON),
    12. Advanced Encryption Standard (AES) dla ruchu zarządzającego,
    13. Microsoft Challenge Handshake Authentication Protocol (MS-CHAP),
    14. Role-Based Access Control RBAC,
    15. Kopiowanie ruchu za pośrednictwem mechanizmu Switched Port Analyzer (SPAN/ERSPAN) dla fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN,
    16. Kopiowanie ruchu za pośrednictwem mechanizmu Switched Port Analyzer (SPAN/ERSPAN) dla pakietów przekraczających określone opóźnienie w przełączaniu,
    17. Kopiowanie ruchu za pośrednictwem mechanizmu Switched Port Analyzer (SPAN/ERSPAN) dla pakietów odrzucanych przez switch (SPAN on drop),
    18. Liczniki pakietów wchodzących/wychodzących per każdy port,
    19. Network Time Protocol (NTP),
    20. Diagnostyka procesu BOOT.
20. Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.
21. Chłodzenie musi być realizowane przód - tył, przy czym wylot ciepłego powietrza musi być skierowany w kierunku portów GE służących do dołączania serwerów przełączników oraz modułów wyniesionych.
22. Dla każdego z przełączników należy dostarczyć:
    1. 4 moduły SFP+ 10Gb SR na każdy z przełączników,
    2. 10 modułów wyniesionych posiadające 48 x portów 100/1000BaseT, gdzie każdy będzie dołączany sumarycznym pasmem 20G do minimum dwóch przełączników,
    3. Odpowiednią ilość modułów 10Gb umożliwiających połączenie przełączników oraz modułów wyniesionych opisanych w podpunkcie b.,
    4. 4 kable typu 10GE Twinax o długości 1m,
    5. Wkładki muszą pochodzić od tego samego dostawcy co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.

### Wymagania dla urządzeń styku z Internetem

1. Urządzenie o wysokości maksymalnie 2U z możliwością montażu w szafie 19”
2. Wyposażone w co najmniej 6 portów Gigabit Ethernet typu SFP lub równoważnych, pracujących bez nadsubskrypcji.
3. Wyposażone w co najmniej 2 porty 10GE obsługującymi wkładki typu X2, XENPAK, XFP lub równoważne.
4. Możliwość zainstalowania interfejsów ATM (jeżeli wymagana jest dodatkowa karta, nie jest wymagane dostarczenie jej w tej części postępowania).
5. Zapewnia redundancję procesów routingowych poprzez redundancję modułów zarządzających lub poprzez uruchomienie dwóch kopii systemu operacyjnego.
6. Zapewnia wydajność systemu na poziomie 5 Gbps z możliwością rozbudowy do min. 30 Gbps.
7. Zapewnia sprzętowe wsparcie dla protokołu IPSec na poziomie minimum 2 Gbps (minimum 3500 tuneli). W przypadku gdyby obsługa powyższego wsparcia wymagała dostarczenia licencji z urządzeniem licencja ta musi zostać dostarczona.
8. Obsługuje co najmniej 1.000.000 prefiksów w tablicach routing IPv4 albo 1.000.000 prefiksów w tablicach routing IPv6.
9. Obsługuje routing dynamiczny: RIP, OSPF, BGP.
10. Wspiera IPv4 oraz IPv6, w szczególności protokoły routingu RIPng oraz OSPFv3.
11. Wspiera MPLS i MPLS VPN.
12. Obsługuje co najmniej 100 instancji wirtualnych tablic routingu.
13. Posiada możliwość aktywacji funkcjonalności bezpieczeństwa o następujących parametrach:
    1. Zapora ogniowa typu statefull (ang. statefull firewall),
    2. Analiza i klasyfikacja pakietów w warstwie 2-7 polegająca na przeszukiwania pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków,
    3. Funkcjonalność Firewall/NAT z obsługą 2.000.000 sesji (200.000 nowych sesji Firewall/NAT na sekundę),
    4. Jeżeli powyższe funkcjonalności wymagają dostarczenia licencji, nie jest to wymagana w tym postępowaniu.
14. Obsługuje tunele GRE.
15. Sprzętowa ochrona warstwy zarządzającej (Control Plane Policing)
16. Wspiera multicast w szczególności: PIM sparse/dense/SSM, IGMP, MLD
17. Obsługuje RPF (Reverse Path Forwarding)
18. Obsługuje zarządzanie ruchem (QoS)
    1. Kolejka priorytetowa,
    2. 120,000 dynamicznych kolejek,
    3. Bufory przeznaczone do kolejkowania pakietów min. 500 MB.
19. Obsługuje SFlow lub odpowiednik (J-Flow, Net-Flow)
20. Ma funkcjonalność VRRP lub odpowiednika.
21. Umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3
22. Porty umożliwiające zarządzanie: port konsoli, port Ethernet.
23. Posiada redundantne zasilacze - 230V
24. Posiada pamięć RAM, minimum: 8GB DRAM
25. Wsparcie dla RADIUS.
26. Dla każdego z urządzeń należy dostarczyć:
    1. 2 wkładki umożliwiającymi pracę na dystansie minimum 100 metrów po światłowodzie wielomodowym (standard 10G-SR),
    2. 2 wkładki umożliwiające podłączenie operatorów po światłowodzie jednomodowym (standard 1000BASE-LX/LH),
    3. 2 wkładki umożliwiające podłączenie operatorów w standardzie 1000BASE-T,
    4. Wkładki muszą pochodzić od tego samego dostawcy co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.

### Wymagania dla zapory ogniowej

1. Urządzenie musi zapewniać wydajność 2 Gbps dla ruchu IPv4 i IPv6.
2. Musi zapewniać wydajność nie mniejszą niż 1 200 000 pakietów na sekundę (dla pakietów o wielkości 64B).
3. Musi zapewniać co najmniej 1Gbps dla szyfrowania VPN algorytmami 3DES/AES.
4. Urządzenie musi pozwalać na obsługę jednocześnie 5 000 tuneli IPSec.
5. Urządzenie musi być przygotowane dla obsługi SSL/VPN z podaną wydajnością bez konieczności doposażenia go w jakiekolwiek komponenty sprzętowe, jeżeli takowe są niezbędne, należy je uwzględnić w ofercie. W momencie dostawy i uruchomienia projektu wymaga się dostarczenia licencji na zestawienie 2 tuneli SSL/VPN.
6. Urządzenie musi pozwalać na zestawienie co najmniej 40 000 nowych połączeń na sekundę.
7. Urządzenie musi posiadać do najmniej 8 interfejsów Gigabit Ethernet 10/100/1000Base-T i 6 interfejsów10 Gigabit Ethernet definiowane przez SFP+ (lub inny standard np. XFP).
8. Urządzenie musi poprawnie obsługiwać ramki Jumbo (9216 bajtów).
9. Urządzenie musi poprawnie obsłużyć minimum 1000 VLANów.
10. Urządzenie musi umożliwiać grupowanie VLANów w trybie pracy jako transparent firewall (Firewall warstwy 2) – minimum 8 grup po 4 VLANy. Funkcjonalność powinna być możliwa do uruchomienia dla IPv4 i IPv6.
11. Urządzenie musi posiadać co najmniej 6 GB pamięci RAM i 2 GB pamięci Flash.
12. Urządzenie musi umożliwiać dostęp administracyjny do interfejsu zarządzania w oparciu o role (RBAC).
13. Urządzenie musi posiadać dedykowany interfejs zarządzający GigabitEthernet do wprowadzania zmian konfiguracyjnych w trybie Out-of-Band (OOB).
14. Urządzenie musi posiadać co najmniej 2 porty USB z możliwością obsługi systemu plików na kluczach USB.
15. Urządzenie musi posiadać port konsoli dla realizacji lokalnego dostępu do urządzenia, może być on realizowany przez port szeregowy lub inne rozwiązanie spełniające wskazaną funkcjonalność. Port ten powinien być portem dedykowanym tzn. nie może do tego celu być wykorzystany żaden z portów wyspecyfikowanych powyżej.
16. Urządzenie musi pozwalać na realizację modelu wdrożenia w wysokiej dostępności dla IPv4 i IPv6 w trybach
    1. Active-Standby,
    2. Active-Active,
    3. Klaster – z opcją rozbudowy do więcej niż 4 urządzeń,
    4. Urządzenie musi posiadać mechanizmy pozwalające na obsługę ruchu asymetrycznego w modelu Active-Active.
17. Urządzenie musi być zasilane prądem zmiennym 230V, należy zastosować właściwy zasilacz.
18. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego.
19. Urządzenie musi zapewniać niski pobór mocy – poniżej 400W.
20. Urządzenie musi mieć możliwość montażu w szafie Rack 19”. Jeżeli uchwyty są dostępne jako akcesoria to należy uwzględnić je w ofercie i dostarczyć w projekcie.
21. Rozwiązanie oparte o dedykowany system operacyjny – 64 bitowy. Nie dopuszcza się rozwiązań gdzie platformą systemową jest system operacyjny ogólnego zastosowania, a na nim posadowione oprogramowanie firewall (jako aplikacja).
22. Rozwiązanie powinno posiadać funkcjonalność ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji.
23. Rozwiązanie nieposiadające ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
24. Rozwiązanie pozwalające na definiowanie firewalli w trybie warstwy 3 (routed) i warstwy 2 transparentnym (w warstwie L2 OSI).
25. Rozwiązanie musi posiadać możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory.
26. Rozwiązanie pozwalające na wirtualizację konfiguracji poprzez wirtualne firewalle/konteksty/domeny. Wymagana jest obsługa co najmniej 50 wirtualnych kontekstów Firewall. Jeżeli wymagane jest dostarczenie licencji do uzyskania opisanej funkcjonalności, należy ją dostarczyć w ramach tego postępowania.
27. Urządzenie powinno umożliwiać rozszerzenia ilości obsługiwanych wirtualnych kontekstów Firewall, do co najmniej 200. Jeżeli wymagane jest dostarczenie licencji do uzyskania opisanej funkcjonalności, nie jest to wymagane w ramach tego projektu.
28. Rozwiązanie musi zapewniać mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
    1. Hypertext Transfer Protocol (HTTP),
    2. File Transfer Protocol (FTP),
    3. Simple Mail Transfer Protocol (SMTP),
    4. Domain Name System (DNS),
    5. H.323,
    6. Session Initiation Protocol (SIP),
    7. Lightweight Directory Access Protocol (LDAP),
    8. Internet Control Message Protocol (ICMP),
    9. Network File System (NFS).
29. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego OSPF oraz RIPv2
30. Rozwiązanie musi zapewniać obsługę ruchu multicast w tym
    1. Protokoły routingu multicast (PIM),
    2. IGMP,
    3. Definiowanie list kontroli dostępu dla ruchu multicast.
31. Rozwiązanie musi zapewniać obsługę ruchu z adresacją IPv6
    1. Pracę w sieci z adresacją IPv6,
    2. Definiowanie list kontroli dostępu dla ruchu IPv6,
    3. Inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń,
    4. Hop-by-Hop Options,
    5. Routing (Type 0),
    6. Fragment,
    7. Destination Options,
    8. Authentication,
    9. Encapsulating Security Payload,
    10. Zarządzanie urządzeniem poprzez SSHv2, HTTPS w sieci IPv6.
32. Rozwiązanie musi umożliwiać zestawienie sesji IPSec VPN i WebVPN.
33. Rozwiązanie musi obsługiwać IKE i IKEv2.
34. Rozwiązanie musi wspierać funkcję Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPSec z IKEv2 dla dostępu zdalnego w oparciu o Klienta VPN (w tym z uwierzytelnianiem wykorzystującym certyfikat).
35. Rozwiązanie musi obsługiwać współpracę z serwerami certyfikatów (CA).
36. Rozwiązanie musi posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji co najmniej z wykorzystaniem protokołu RADIUS.
37. Rozwiązanie musi posiadać możliwość wyeksportowania konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline .
38. Rozwiązanie powinno być zarządzane przy wykorzystaniu dedykowanej aplikacji umożliwiającej płynną (z użyciem kreatorów) konfigurację poszczególnych funkcji urządzenia.
39. Dla każdego z urządzeń należy dostarczyć:
    1. 4 wkładki umożliwiającymi pracę na dystansie minimum 100 metrów po światłowodzie wielomodowym (standard 10G-SR),
    2. Wkładki muszą pochodzić od tego samego dostawcy co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.

### Wymagania dla przełącznika Campus (I)

1. Przełącznik o konstrukcji modularnej min. 7-slotowy, w tym min. 5 slotów na karty liniowe
2. Wymagane jest, aby w momencie dostawy przełącznik był wyposażony w:
   1. Dwa moduły zarządzające (switch fabric),
   2. 48-portów 10/100/1000BaseT pracujących bez nadsubskrypcji względem matrycy przełączającej,
   3. 48-portów 10/100/1000BaseT pracujących bez nadsubskrypcji względem matrycy przełączającej, wspierających standard PoE - 802.3at,
   4. Min. 8 portów 10Gigabit Ethernet SFP+ (przy czym wymaga się, aby przy użyciu dwóch modułów zarządzających 4 pory na każdym z modułów, mogło pracować jednocześnie bez nadsubskrypcji),
   5. 2 zasilacze redundantne zapewniające poprawną pracę urządzenia,
   6. Minimum 2 sloty na karty liniowe muszą pozostać wolne celem zapewnienia przyszłej możliwości rozbudowy.
3. Porty SFP+ urządzenia muszą umożliwiać instalacje zarówno transceiverów 10GE jak i GE.
4. Urządzenie musi zapewniać pasmo minimum 48Gb/s per slot. Szybkość przełączania/routingu min. 250Mp/s dla IPv4 i 125Mp/s dla IPv6.
5. Urządzenie musi zapewniać obsługę:
   1. Min. 4 000 sieci VLAN, interfejsów SVI, instancji Spanning Tree,
   2. Min. 50 000 adresów MAC,
   3. Sprzętową dla QoS i ACL - minimum 64 000 wpisów sprzętowych.
6. Urządzenie musi posiadać min. 4GB pamięci DRAM.
7. Przełącznik musi obsługiwać ramki Jumbo (do min. 9216 bajtów).
8. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 128.000 (wymagane jest wsparcie sprzętowe).
9. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   1. 802.1w Rapid Spanning Tree,
   2. 802.1s Multi-Instance Spanning Tree,
   3. Możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP) z wykorzystaniem portów pochodzących z różnych kart liniowych,
   4. Możliwość instalacji “na gorąco” zasilaczy oraz kart liniowych.
10. Urządzenie musi umożliwiać przełączanie w warstwie 2 i 3. Wymagane jest wsparcie dla routingu statycznego i dynamicznego (min. dla protokołu RIPv2 i RIPng), routingu multicast IPv4 i IPv6 (PIM-SM, PIM-SSM) i protokołu redundancji bramy VRRP lub równoważnego. Urządzenie musi umożliwiać rozszerzenie funkcjonalności (poprzez upgrade oprogramowania lub zakup odpowiedniej licencji) o zaawansowane protokoły routingu warstwy 3 dla ruchu IPv4 i IPv6 (OSPFv2 i v3, IS-IS dla IPv4 i IPv6, BGPv4, MBGP, Policy Based Routing). Jeżeli oprogramowanie, lub licencja jest wymagana do opisanej funkcjonalności należy ją dostarczyć w ramach tego projektu.
11. Tablica routingu musi posiadać minimum:
    1. 250 000 wpisów dla IPv4,
    2. 125 000 wpisów dla IPv6,
    3. 30 000 wpisów dla ruchu multicast.
12. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Obsługa 8 kolejek sprzętowych dla różnego rodzaju ruchu,
    2. Obsługa co najmniej jednej kolejki ze statusem strict priority,
    3. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    4. Możliwość “re-kolorowania” pakietów przez urządzenie – pakiet przychodzący do urządzenia przed przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS/DSCP.
    5. Kontrola sztormów dla ruchu boradcast i multicast,
    6. Mechanizm AutoQoS lub równoważny.
13. Obsługa protokołu LLDP i LLD-MED.
14. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
15. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    1. Min. 5 poziomów dostępu administracyjnego poprzez konsolę,
    2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL,
    3. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC ,
    5. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    6. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie,
    7. Urządzenie musi umożliwiać wymuszenie ponownego uwierzytelniania portu dostępowego oraz zdalnego restartu portu (zgodnie z RFC 5176),
    8. Wszystkie porty urządzenia muszą zapewniać możliwość szyfrowania ruchu zgodnie ze standardem IEEE 802.1AE (MACSec),
    9. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2,
    10. Obsługa list kontroli dostępu (ACL) dla IPv4 i IPv6,
    11. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard,
    12. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
    13. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1X) do serwerów RADIUS lub TACACS+,
    14. Funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym.
16. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie (mechanizmy SPAN i RSPAN) – wymagana jest obsługa min. 8 sesji SPAN/RSPAN na przełączniku.
17. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.
18. Funkcjonalność traceroute dla warstwy 2 umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
19. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
20. Urządzenie musi posiadać wbudowany analizator pakietów.
21. Urządzenie musi posiadać funkcjonalność umożliwiającą monitorowanie parametrów usług dla ruchu IP (IP SLA), w tym również dla usług wideo (urządzenie musi posiadać wbudowany symulator ruchu wideo). Wymagana jest możliwość monitorowania parametrów takich jak opóźnienie, jitter, utrata pakietów.
22. Obudowa przystosowana do montażu w szafie 19”. Wysokość nie większa niż 11RU.
23. Zamawiający wymaga, aby dostarczone urządzenie zapewniało możliwość stworzenia wirtualnego przełącznika z drugim urządzeniem o analogicznej konfiguracji. Pod pojęciem wirtualnego przełącznika Zamawiający rozumie możliwość:
    1. Konfiguracji obydwu urządzeń z jednego punktu,
    2. Terminowania połączeń link aggregation (z wykorzystaniem protokołu IEEE 802.3ad LACP) z innych urządzeń sieciowych w taki sposób, aby jedno łącze było terminowane na jednym przełączniku, a drugie łącze na drugim przełączniku (tzw. muli-chassis link aggregation).
24. Dodatkowo należy dostarczyć:
    1. 2 wkładki umożliwiającymi pracę na dystansie minimum 100 metrów po światłowodzie jednomodowym (standard 10G-LRM),
    2. 2 wkładki umożliwiającymi pracę na dystansie minimum 100 metrów po światłowodzie jednomodowym (standard 1000BASE-LX/LH),
    3. Wkładki muszą pochodzić od tego samego dostawcy co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.

### Wymagania dla przełącznika Campus (II)

1. Przełącznik o konstrukcji modularnej min. 10-slotowy, w tym min. 8 slotów na karty liniowe
2. Wymagane jest, aby w momencie dostawy przełącznik był wyposażony w:
   1. Dwa moduł zarządzające/switch fabric,
   2. 96-portów 10/100/1000BaseT pracujących bez nadsubskrypcji względem matrycy przełączającej,
   3. 48-portów 10/100/1000BaseT pracujących bez nadsubskrypcji względem matrycy przełączającej, wspierających standard PoE - 802.3at,
   4. Min. 8 portów 10Gigabit Ethernet SFP+ (przy czym wymaga się, aby przy użyciu dwóch modułów zarządzających 4 pory na każdym z modułów, mogło pracować jednocześnie bez nadsubskrypcji),
   5. 2 zasilacze redundantne zapewniające poprawną pracę urządzenia,
   6. Minimum 2 sloty na karty liniowe muszą pozostać wolne celem zapewnienia przyszłych możliwości rozbudowy.
3. Porty SFP+ urządzenia muszą umożliwiać instalacje zarówno transceiverów 10GE jak i GE.
4. Urządzenie musi zapewniać pasmo minimum 48Gb/s per slot. Szybkość przełączania/routingu min. 250Mp/s dla IPv4 i 125Mp/s dla IPv6.
5. Urządzenie musi zapewniać obsługę:
   1. Min. 4 000 sieci VLAN, interfejsów SVI, instancji Spanning Tree,
   2. Min. 50 000 adresów MAC,
   3. Sprzętową dla QoS i ACL - minimum 64 000 wpisów sprzętowych.
6. Urządzenie musi posiadać min. 4GB pamięci DRAM.
7. Przełącznik musi obsługiwać ramki Jumbo (do min. 9216 bajtów).
8. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 128.000 (wymagane wsparcie sprzętowe).
9. Urządzenie musi wspierać następujące mechanizm związane z zapewnieniem ciągłości pracy sieci:
   1. 802.1w Rapid Spanning Tree,
   2. 802.1s Multi-Instance Spanning Tree,
   3. Możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP) z wykorzystaniem portów pochodzących z różnych kart liniowych,
   4. Możliwość instalacji “na gorąco” zasilaczy oraz kart liniowych.
10. Urządzenie musi umożliwiać przełączanie w warstwie 2 i 3. Wymagane jest wsparcie dla routingu statycznego i dynamicznego (min. dla protokołu RIPv2 i RIPng), routingu multicast IPv4 i IPv6 (PIM-SM, PIM-SSM) i protokołu redundancji bramy VRRP lub równoważnego. Urządzenie musi umożliwiać rozszerzenie funkcjonalności (poprzez upgrade oprogramowania lub zakup odpowiedniej licencji) o zaawansowane protokoły routingu warstwy 3 dla ruchu IPv4 i IPv6 (OSPFv2 i v3, IS-IS dla IPv4 i IPv6, BGPv4, MBGP, Policy Based Routing). Jeżeli oprogramowanie, lub licencja jest wymagana do opisanej funkcjonalności należy ją dostarczyć w ramach tego projektu.
11. Tablica routingu musi posiadać minimum:
    1. 250 000 wpisów dla IPv4,
    2. 125 000 wpisów dla IPv6,
    3. 30 000 wpisów dla ruchu multicast.
12. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Obsługa 8 kolejek sprzętowych dla różnego rodzaju ruchu,
    2. Obsługa co najmniej jednej kolejki ze statusem strict priority,
    3. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    4. Możliwość “re-kolorowania” pakietów przez urządzenie – pakiet przychodzący do urządzenia przed przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS/DSCP,
    5. Kontrola sztormów dla ruchu boradcast i multicast,
    6. Mechanizm AutoQoS lub równoważny.
13. Obsługa protokołu LLDP i LLD-MED .
14. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
15. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    1. Min. 5 poziomów dostępu administracyjnego poprzez konsolę,
    2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL,
    3. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    5. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    6. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie,
    7. Urządzenie musi umożliwiać wymuszenie ponownego uwierzytelniania portu dostępowego oraz zdalnego restartu portu (zgodnie z RFC 5176),
    8. Wszystkie porty urządzenia muszą zapewniać możliwość szyfrowania ruchu zgodnie ze standardem IEEE 802.1AE (MACSec),
    9. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2,
    10. Obsługa list kontroli dostępu (ACL) dla IPv4 i IPv6,
    11. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard,
    12. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
    13. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1X) do serwerów RADIUS lub TACACS+,
    14. Funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym.
16. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie (mechanizmy SPAN i RSPAN) – wymagana jest obsługa min. 8 sesji SPAN/RSPAN na przełączniku.
17. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.
18. Funkcjonalność traceroute dla warstwy 2 umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
19. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
20. Urządzenie musi posiadać wbudowany analizator pakietów.
21. Urządzenie musi posiadać funkcjonalność umożliwiającą monitorowanie parametrów usług dla ruchu IP (IP SLA), w tym również dla usług wideo (urządzenie musi posiadać wbudowany symulator ruchu wideo). Wymagana jest możliwość monitorowania parametrów takich jak opóźnienie, jitter, utrata pakietów.
22. Obudowa przystosowana do montażu w szafie 19”. Wysokość nie większa niż 14RU.
23. Zamawiający wymaga, aby dostarczone urządzenie zapewniało możliwość stworzenia wirtualnego przełącznika z drugim urządzeniem o analogicznej konfiguracji. Pod pojęciem wirtualnego przełącznika Zamawiający rozumie możliwość:
    1. Konfiguracji obydwu urządzeń z jednego punktu,
    2. Terminowania połączeń link aggregation (z wykorzystaniem protokołu IEEE 802.3ad LACP) z innych urządzeń sieciowych w taki sposób, aby jedno łącze było terminowane na jednym przełączniku, a drugie łącze na drugim przełączniku (tzw. muli-chassis link aggregation).
24. Dodatkowo należy dostarczyć:
    1. 2 wkładki umożliwiającymi pracę na dystansie minimum 100 metrów po światłowodzie jednomodowym (standard 10G-LRM),
    2. Wkładki muszą pochodzić od tego samego dostawcy, co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.

### Wymagania dla przełącznika agregującego sieć zarządzającą

1. Typ i liczba portów:
   1. Minimum 12 portów 1 Gbps SFP,
   2. Minimum 4 dodatkowe porty uplink 1 Gbps SFP, z możliwością wymiany na 2 uplinki 10 Gbps SFP+, poprzez wymianę/dodanie modułu sprzętowego,
   3. Porty SFP muszą umożliwiać ich obsadzanie wkładkami Gigabit Ethernet – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U oraz modułami CWDM zależnie od potrzeb Zamawiającego.
2. Urządzenie musi obsługiwać minimum 1000 sieci VLAN.
3. Urządzenie musi obsługiwać minimum 16000 adresów MAC.
4. Urządzenie musi posiadać min. 512MB pamięci DRAM i 128MB pamięci flash.
5. Parametry fizyczne – wysokość maksimum 1RU, możliwość montażu w szafie 19”.
6. Zasilanie 230V AC, realizowane przez dwa redundantne zasilacza.
7. Przepustowość przełącznika minimum 20Gb/s (40Gb/s w trybie full duplex).
8. Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność łączenia w stosy z zachowaniem następującej parametrów:
   1. Do min. 8 jednostek w stosie,
   2. Możliwość tworzenia połączeń EtherChannel zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel),
   3. Jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli itp. ich dostarczenie w ramach tego postępowania nie jest wymagane.
9. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów.
10. Wbudowane funkcje zarządzania energią:
    1. Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet),
    2. Możliwość hibernowania przełącznika w określonych godzinach celem dodatkowego oszczędzania energii.
11. Obsługa protokołu NTP.
12. Musi zapewniać obsługę min. 16 statycznych tras dla routingu IPv4 i IPv6.
13. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping.
14. Obsługa protokołów routingu RIP, OSPF.
15. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 128 instancji protokołu STP.
16. Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server.
17. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
18. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów bezpieczeństwa typu Port Security i IP Source Guard na interfejsach link aggregation.
19. Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:
    1. Minimum 5 poziomów dostępu administracyjnego poprzez konsolę,
    2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL,
    3. Obsługa funkcji Guest VLAN,
    4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    5. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    6. Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www,
    7. Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie,
    8. Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6,
    9. Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6,
    10. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard,
    11. Funkcjonalność Protected Port,
    12. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard) oraz ochronę przed fałszowaniem źródłowych adresów IPv6 (IPv6 Source Guard),
    13. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,
    14. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne).
20. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    2. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek,
    3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    4. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi. Wymagana jest możliwość skonfigurowania minimum 256 różnych ograniczeń.
21. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP).
22. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP).
23. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli.
24. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN).
25. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych.
26. Dodatkowo należy dostarczyć:
    1. 10 wkładek umożliwiających pracę na dystansie minimum 100 metrów po światłowodzie wielomodowym (standard 1000BASE-SX),
    2. Wkładki muszą pochodzić od tego samego dostawcy, co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.

### Wymagania dla przełącznika sieci zarządzającej

1. Typ i liczba portów:
   1. Minimum 24 portów 10/100/1000 Ethernet RJ45,
   2. Minimum 2 dodatkowe porty uplink 1 Gigabit Ethernet SFP.
2. Urządzenie musi obsługiwać minimum 60 sieci VLAN.
3. Urządzenie musi posiadać min. 512MB pamięci DRAM i 64MB pamięci flash.
4. Parametry fizyczne – wysokość maksimum 1RU, możliwość montażu w szafie 19”.
5. Wydajność przełączania minimum 64Mpps dla pakietów 64-bajtowych.
6. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów.
7. Obsługa protokołu NTP.
8. Musi zapewniać obsługę min. 16 statycznych tras dla routingu IPv4 i IPv6.
9. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree.
10. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych.
11. Zasilanie 230V AC.

### Wymagania dla koncentratora VPN – sieć zarządzająca

1. Urządzenie musi zapewniać inspekcję ruchu o wydajności m.in. 50 Mbps.
2. Urządzenie musi zapewniać wydajność nie mniejszą niż 50,000 pakietów na sekundę.
3. Urządzenie musi zapewniać co najmniej 50 Mbps dla szyfrowania VPN algorytmami 3DES/AES.
4. Urządzenie musi pozwalać na obsługę jednocześnie 20 tuneli SSL/VPN z użyciem klienta lub w trybie clientless .
5. Urządzenie musi posiadać wbudowany przełącznik, m.in. 4 porty Gigabit Ethernet 10/100/1000Base-T.
6. Urządzenie musi poprawnie obsłużyć minimum 10 VLANów.
7. Urządzenie musi posiadać port konsoli dla realizacji lokalnego dostępu do urządzenia, może być on realizowany przez port szeregowy lub inne rozwiązanie spełniające wskazaną funkcjonalność. Port ten powinien być portem dedykowanym tzn. nie może do tego celu być wykorzystany żaden z portów wyspecyfikowanych powyżej.
8. Urządzenie musi być zasilane prądem zmiennym 230V; możliwe jest użycie zewnętrznego zasilacza.
9. Rozwiązanie musi wspierać funkcję Secure Hash Algorithm SHA-2 o długości 256, 384 i 512 bitów dla połączeń IPSec z IKEv2 dla dostępu zdalnego w oparciu o Klienta VPN (w tym z uwierzytelnianiem wykorzystującym certyfikat).
10. Rozwiązanie musi obsługiwać współpracę z serwerami certyfikatów (CA).
11. Rozwiązanie musi posiadać możliwość współpracy z zewnętrznymi serwerami uwierzytelnienia i autoryzacji, co najmniej z wykorzystaniem protokołu RADIUS.

### Wymagania dla oprogramowania do monitoringu parametrów sieciowych

1. Oprogramowanie powinno umożliwić podłączenie nielimitowanej ilości usług/sensorów oraz nielimitowanej ilości urządzeń;
2. Jako jeden sensor należy liczyć każdą z poniższych pozycji:
   1. Monitorowanie ruchu/obciążenia sieci na jednym porcie urządzenia poprzez SNMP za pomocą standardu MIB2,
   2. Monitorowanie błędów/minimów, pakietów unicast, non-unicast na jednym porcie urządzenia poprzez protokół SNMP za pomocą MIB2,
   3. Monitorowanie innych parametrów systemowych poprzez SNMP (np. procesor, wolne miejsce na dysku), które są dostępne poprzez wartość OID.
3. Wsparcie dla IPv6 i IPv4.
4. Zaimplementowane technologie powiadamiania: wysyłka Email, Syslog, SNMP Trap, żądanie z parametrem http, wpis Event log, odtworzenie pliku dźwiękowego, uruchomienie skryptu.
5. Powiadamianie o stanie (up, down, warning).
6. Alarmy limitów (wartość powyżej/poniżej x).
7. Eskalacja alarmów poprzez dodatkowe powiadomienia co x minut podczas przestoju.
8. Opcja przyjęcia do wiadomości, charakteryzująca się brakiem wysyłanego alarmu.
9. Możliwość instalacji na wszystkich wersjach systemu operacyjnego Windows od 2003 do późniejszych zarówno 32 jak i 64 bitowych.
10. Brak względem dodatkowych modułów do działania systemów (np. .NET, SQL Server, etc.).
11. Interaktywny poradnik w programie.
12. Interfejs użytkownika dostępny przez przeglądarkę internetową.
13. Natywna aplikacja Windows pozwalająca na przeglądanie danych z monitoringu kilku instancji w jednej aplikacji.
14. Możliwość lokalnego i zdalnego dostępu do interfejsu użytkownika poprzez SSL.
15. Obsług wbudowanych typów sensorów, takich jak: SNMP Sensors, Linux Sensors, Bandwidth Monitoring Sensors.
16. Możliwość tworzenia klastrów do 5 instancji w celu stworzenia ubezpieczonego na awarię systemu monitoringu. Nie wymaga się dostarczania licencji obsługujących pracę klastra w tym postępowaniu przetargowym.
17. Aktualizacja oprogramowania nie może powodować przestoju klastra.
18. Możliwość aktualizacji systemu w czasie trwania okresu serwisowego.

### Wymagania dotyczące serwera wspierającego zarządzanie siecią

1. Obudowa typu RACK 19” wraz z zestawem do zamontowania serwerów w szafie teleinformatycznej 19”, umożliwiającej pełne wysunięcie obudowy o wysokości nieprzekraczającej 1 RU.
2. Płyta główna musi posiadać/spełniać warunki:
   1. Musi być zaprojektowana przez producenta serwera i oznaczona trwale jego logo,
   2. Dwa fizyczne gniazda do obsługi procesorów wyspecyfikowanych w następnych punktach,
   3. Co najmniej 16 slotów do obsługi pamięci ECC, pracującej z częstotliwościami 1600 MHz oraz 1866 MHz,
   4. Możliwość wyposażenia serwera w 512GB RAM (16 DIMM ze wsparciem kości 32GB),
   5. Kontroler macierzy SAS umożliwiający obsługę minimum 8-miu dysków w konfiguracjach RAID 0/1/10/5 ze wsparciem dla VMware,
   6. Zintegrowana karta graficzna,
   7. Min. 2 sloty PCI-Express 3-ciej generacji, oba wyprowadzone na zewnątrz serwera, w tym min. 1 dla karty pełnej wysokości, połowy długości z konektorem minimum x16. Jeśli do obsługi slotów PCIe niezbędne są dodatkowe komponenty mechaniczne należy dostarczyć je razem z serwerem,
   8. Wewnętrzny slot USB 2.0 umieszczony na płycie głównej serwera, umożliwiający bootowanie,
   9. Wewnętrzny slot dla dwóch kart SD.
3. Procesor
   1. Dwa procesory 64 bitowe Intel E5-2609 v2 lub równoważne.
4. Pamięć
   1. Pamięć RAM 32 GB pamięci RAM DDR3-1866MHz Registered DIMM w postaci 4 modułów 8GB.
5. Media
   1. Moduł KVM wyprowadzony na przedni panel serwera pozwalający uzyskać dostęp do gniazda monitora, 2xUSB oraz portu szeregowego. Jeżeli w celu wykorzystania funkcjonalności niezbędny jest dodatkowy moduł, należy dostarczyć go razem z serwerem.
6. Dyski twarde
   1. Dyski muszą być wymienne podczas pracy urządzenia - hot swappable,
   2. Dyski twarde 2,5” SAS 6G o pojemności min. 300GB, prędkości obrotowej 10k RPM w ilości 2 sztuk,
   3. Serwer musi umożliwiać instalację w sumie minimum 8-iu dysków twardych 2,5” bez konieczności wymiany komponentów rozwiązania.
7. Interfejsy sieciowe
   1. Min. 2 porty Gigabit Ethernet 10/100/1000 RJ-45,
   2. Min. 2 porty 10 Gigabit Ethernet SFP+ ze wsparciem dla wirtualizacji PCIe (co najmniej 9 interfejsów LAN I 2 SAN widocznych jako osobne urządzenia PCIe),
   3. Min. 4 porty USB (min 2 z przodu oraz min 2 z tyłu serwera),
   4. Min. 2 porty VGA (1 przy wykorzystaniu interfejsu KVM na przednim panelu i 1 z tyłu obudowy serwera),
   5. Min. 1 port RS232,
   6. Min. 1 port RJ-45 10/100/1000 dedykowany dla zarządzania.
8. Zarządzanie. Moduł zdalnego zarządzania (konsoli), który pozwala na
   1. Zdalne włączenie, wyłączenie i restart serwera,
   2. Wykorzystanie zdalnej, graficznej konsoli obsługująca zdalną pracę na serwerze,
   3. Podgląd logów sprzętowych serwera,
   4. Przejęcie pełnej konsoli graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS),
   5. Podłączanie wirtualnych napędów CD i FDD oraz obrazów,
   6. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w slocie PCI,
   7. Konfiguracje parametrów BIOS np. wsparcia dla HT lub NUMA,
   8. Zdalne zarzadzanie poprzez API XML.
9. Zasilanie, chłodzenie.
   1. Minimum dwa zasilacze wymienne podczas pracy serwera,
   2. Redundantne chłodzenie serwera.
10. Serwer musi zawierać szyny montażowe do rack-a 19”.
11. Serwer musi umożliwiać instalację następujących systemów operacyjnych: Microsoft Windows Server 2008 w wersji Standard i Enterprise, RedHat Linux w wersji standardowej oraz Advanced Platform, VMware vSphere w wersji Advanced, Enterprise, Enterprise Plus.
12. Wszystkie komponenty rozwiązania muszą znajdować się na oficjalnej liście wsparcia HCL danego serwera.
13. Cały sprzęt musi być zakupiony bezpośrednio u producenta lub w oficjalnym kanale dystrybucji producenta przeznaczonym na rynek polski z odpowiednim pakietem usług wymaganych przez Zamawiającego.
14. Sprzęt musi być fabrycznie nowy, nieużywany wcześniej w innych projektach, nie dopuszcza się rozwiązań typu „refurbished” itp.
15. Wraz z serwerem zostaną dostarczone dwie (per serwer) licencje VMware vSphere Enterprise Plus w wersji najnowszej na dzień składania oferty, jako rozszerzenie systemu wirtualnego w DC EXEA.
16. Wraz z serwerem zostanie dostarczone dwa systemy operacyjne, które zostaną zainstalowane w wirtualnym środowisku i będą służyły do instalacji/uruchomiania aplikacji i skryptów niezbędnych do prawidłowego funkcjonowania systemów DC:
    1. Windows Server 2012 Standard (z odpowiednią licencją),
    2. CentOS 6.4.
17. Wymagane jest, aby Wykonawca dostarczył również system zarządzania środowiskiem wirtualnym, o którym mowa w punkcie 15.

### Wymagania stawiane systemowi zarządzania i automatyzacji środowiska sieciowego

1. System musi być dostarczony, jako dedykowane rozwiązanie w formie dedykowanego sprzętu i oprogramowania. System musi być dostępny, jako urządzenie fizyczne (tzw. appliance) oraz jako maszyna wirtualna (tzw. Virtual Appliance).
2. Musi być rozwiązaniem, które nie wymaga oddzielnych instalacji systemu operacyjnego, oprogramowania i bazy danych.
3. Zarządzanie systemem musi być wykonywane przez graficzny interfejs użytkownika oraz przez linie poleceń (usługa SSH, port konsolowy).
4. System musi być wyposażony w proces kopii zapasowej (tzw. backup), który umożliwia odtworzenie systemu w pliku kopii na innym urządzeniu w wersji fizycznej (Appliance) jak i wirtualnej (Virtual Appliance). Wykonywanie kopi zapasowej musi być możliwe na lokalny system plików oraz do zdalnego/centralnego punktu składowania w ujęciu co dziennie lub co tydzień.
5. System musi posiadać funkcję licencjonowania ilości obsługiwanych urządzeń sieciowych z możliwością zwiększenia ilości obsługiwanych urządzeń. Należy dostarczyć rozwiązanie do obsługi minimum 100 urządzeń sieciowych z zastosowaniem platformy sprzętowej pozwalającej rozbudować w przyszłości system do obsługi minimum 1400 urządzeń. Urządzenie musi posiadać podwójne (redundantne) zasilacze.
6. System musi obsługiwać urządzenia wielu producentów.
7. System musi obsługiwać urządzenia typu router, przełącznik L2 i przełącznik L3, Firewall, Access Point.
8. System musi być wyposażony w pojedynczy mechanizm API zawarty w cenie rozwiązania. Rozwiązania z wieloma mechanizmami API nie są dozwolone.
9. System musi wspierać przeglądarki IE, Firefox, Safari, Chrome.
10. Możliwość dodawania urządzeń sieciowych za pomocą funkcji automatycznego wykrywania urządzeń sieciowych (tzw. Auto-Discovery) dla protokołów IPv4 i IPv6.
11. Proces wykrywania (Discovery) musi uwzględniać takie informacje jak: TCP discovery, OS fingerprint, Traceroute, Netbios, ARP table, Routing table.
12. Świadomość urządzeń zwirtualizowanych/kontekstowych (np. VDC, context).
13. Możliwość ręcznego dodawania (importowania) urządzeń sieciowych.
14. Zdolność do przechwytywania właściwości urządzeń w wykazie (np. zmiany wersji systemu operacyjnego, adres IP, nazwa hosta, tekstowe pliki konfiguracyjne.
15. Możliwość dodawania i zarządzania dodatkowymi parametrami opisującymi dane urządzenie (np. numer ewidencyjny, rola, lokalizacja, osoba odpowiedzialna itp.).
16. Możliwość przechowywania kopii zapasowych lub archiwizacji wersji konfiguracji urządzeń sieciowych.
17. Możliwość wykrywania sieci dla warstw L2 i L3 prezentacja topologii sieciowych pomiędzy urządzeniami.
18. Możliwość tworzenia raportów inwentaryzacji sprzętu, takie jak wykaz numerów seryjnych, fizyczne wyposażenie, producent, wersja oprogramowania.
19. Zdolność do eksportowania raportów w formatach: PDF, XLS, DOC, HTML
20. System musi wykryć zmiany konfiguracji urządzeń sieciowych w czasie rzeczywistym (na przykład zmiany wersji systemu operacyjnego, adres IP, nazwa hosta, tekstowe pliki konfiguracyjne) dla zarządzanych urządzeń powiadamiających za pomocą komunikatów Syslog.
21. System musi wykrywać zmiany konfiguracji poprzez planowane odpytywania.
22. System musi mieć zdolność do wykrywania zmian w konfiguracji za pomocą ręcznego wywołania.
23. System musi mieć możliwość porównania konfiguracji urządzeń korzystając z dwu częściowego panelu podkreślając różnice między obecnym stanem konfiguracji i ostatnio przechowywanej lub ostatniej znanej dobrej konfiguracji tego urządzenia.
24. System musi mieć możliwość porównania wersji konfiguracji i zaznaczać różnice między obecnym stanem konfiguracji i wcześniejszych wersji lub archiwum konfiguracji tego urządzenia.
25. System musi mieć zdolność do oceny wykrytych zmian w konfiguracji w czasie rzeczywistym, w celu określenia spełnienia polityki zgodności (wzorca).
26. System musi mieć możliwość porównania konfiguracji działającej do konfiguracji startowej dla danego urządzenia.
27. System musi mieć możliwość porównania konfiguracji dwóch różnych urządzeń.
28. System musi mieć możliwość aktualizacji poszczególnych atrybutów konfiguracji (zamiast przesyłania całych plików konfiguracyjnych).
29. System musi mieć możliwość, aby przywrócić urządzenie z powrotem do stanu zgodności automatycznie po naruszeniu zgodności (wzorca).
30. System musi mieć zdolność do planowania zmian (np. uruchomienie zadania w dniu/ o danej godzinie).
31. System musi mieć możliwość wykonywania zmian z poziomu listy linii poleceń urządzenia (tzw. CLI).
32. System musi mieć możliwość wykonywania zmian ze skryptów do obsługi bardziej skomplikowanych zmian na urządzeniach sieciowych.
33. System musi umożliwić wstępne sprawdzenie logiczne przed dokonaniem zmiany (np. sprawdzić, "x" przed wykonaniem zmiany "y" dla danego urządzenia).
34. System musi umożliwiać wybór szablonu, w którym różne wzorce konfiguracyjne są używane w zależności od lokalizacji, urządzenia lub innych kryteriów.
35. System musi obsługiwać wiele urządzeń jednocześnie.
36. System musi posiadać świadomość topologii i pozwalać na wykorzystanie tych informacji w kontekście automatyzacji/zmian (np. konfigurowanie interfejsów na podstawie sąsiedztwa).
37. System musi pozwalać na import istniejących/zapisanych skryptów.
38. System musi posiadać wbudowane tzw. najlepsze praktyki i zalecenia pozwalające mu proaktywnie identyfikować nieoptymalne ustawienia konfiguracyjne. (np. VRRP bez partnera, niedopasowania dupleksu portu, błędów konfiguracji VLAN, niezapisana konfiguracja itp.).
39. Użytkownik musi być w stanie dostosować parametry dobrych praktyk za pomocą szablonów.
40. System musi stale szukać suboptymalnych konfiguracji i generować ostrzeżenia.
41. System musi generować ocenę kondycji stanu systemu sieciowego w trybie ciągłym pozwalając na ocenę zmian oraz jakie zmiany wpłynęły na zmianę oceny.
42. System musi zapewnić ciągłe proaktywne monitorowanie zmian w konfiguracji względem ustalonego wzorca (standardu) konfiguracyjnego.
43. System musi mieć zdolność do ustalania polityki konfiguracji, wyjściowych lub "złoty standard" dla każdego urządzenia do monitorowania zgodności z/lub odstępstw od tej polityki.
44. System musi oferować dostęp użytkowników z kontrolą dostępu do urządzeń. Musi być możliwe wykorzystanie danych logowania do urządzeń na poziomie całego systemu oraz opcjonalnie indywidualnych danych logowania aktualnie zalogowanego użytkownika.
45. System musi mieć zdolność do ustalania poziomu uprawnień do zasobów opartego na rolach (np., kto może zobaczyć / wykonać działanie, na jakiej grupie urządzeń).
46. System musi mieć zdolność do ustalania poziomu uprawnień do funkcji opartego na rolach (np., kto może korzystać z danej części/podsystemu).
47. System musi zapewnić współpracę z systemem centralnego uwierzytelniania AD, RADIUS, TACACS+.
48. System musi mieć zdolność do zgłaszania zmian właściwości urządzenia (na przykład zmiany wersji systemu operacyjnego, adresu IP, nazwa hosta, tekstowego pliku konfiguracyjnego, sprzętu) dla urządzeń w inwentarzu.
49. System musi umożliwiać wyświetlania powiadomienia w momencie gdy zmiany konfiguracji są wykrywane.
50. System musi umożliwiać wyświetlanie wszystkich przypadków zmiany konfiguracji dokonane w danym okresie czasu dla wszystkich urządzeń w inwentarzu.
51. System musi umożliwiać powiadomienie w momencie stwierdzenia naruszenia wzorca (standardu).
52. System powinien mieć możliwość zgłaszania wszelkich naruszeń zasad w określonym okresie czasu.
53. System powinien mieć możliwość zgłaszania wszelkich naruszeń wzorca dla zidentyfikowanej grupy urządzeń.
54. Użytkownicy muszą mieć możliwość aktualizacji lub definicji nowych raportów.
55. Wszystkie raporty muszą być dostępne w czasie rzeczywistym, na żądanie.
56. Raporty muszą być generowane automatycznie na podstawie zaplanowanego harmonogramu.
57. System musi oferować narzędzie do śledzenia wykorzystania portów dostępowych w sieci Ethernet dla użytkowników (ilość portów wolnych i zajętych dla każdej grupy i dla całej sieci) oraz informować o ilości portów z zasilaniem (PoE).
58. System musi wyświetlać historię użycia portu.
59. System musi oferować narzędzie do śledzenia wykorzystania portów dostępowych w sieci Ethernet dla użytkowników w ramach konfigurowalnego okresu czasu wolnego (np. wolne porty Ethernet w ciągu ostatnich 14 dni).
60. System musi wyświetlać nowe oraz nie obecne już urządzenia w sieci.
61. System musi wyświetlać historię obecności IP/MAC na danym porcie oraz historię danego IP/MAC na portach w sieci.
62. System musi mieć możliwość wykonywania tekstowego wyszukiwania danego ciągu znaków (i wyrażeń regularnych tzw. RegEx) w konfiguracji urządzeń w całej sieci.
63. System musi mieć możliwość wyszukiwania według ogólnych właściwości urządzenia i jego stanu oraz niestandardowych atrybutów dodatkowych.
64. System musi zapewniać funkcjonalność wysyłania SNMP trap np. do integracji z systemami nadrzędnymi (np. OSS).
65. System musi oferować przesyłaniem powiadomień SMTP np. w celu powiadamiania lub integracji z systemami typu service desk.
66. System musi oferować przychodzące i wychodzące API.
67. System musi mieć możliwość integracji z zewnętrznymi systemami uwierzytelniania. (Radius, TACACS +, Active Directory).

### Wymagania stawiane platformie usług sieciowych

1. System musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System).
2. System musi być zgodny z wymogami dokumentów RFC 1034, 1035, 1995, 1996, 2136, 2317, 2671, 2782, 3596 (RFC, tj. Request for Commnents http://www.ietf.org/rfc.html).
3. System musi realizować funkcje automatycznej aktualizacji serwisów DNS, zgodne z dokumentem RFC 2136.
4. System musi posiadać wbudowany mechanizm powiadamiania o zmianach stref, zgodne z dokumentem RFC 1996.
5. System musi wspierać protokoły DNS w wersji IPv4 i IPv6.
6. System musi wspierać usługę DNS Anycast dla IPv4 i IPv6 (za pomocą protokołów routingu BGP i OSPF).
7. System musi wspierać usługę DNSSEC z automatycznym aktualizowaniem podpisów przy zmianach dokonywanych w strefach DNS.
8. System musi wspierać przetwarzanie informacji kryptograficznych na potrzeby DNSSEC za pomocą zewnętrznego systemu HSM przynajmniej dwóch różnych producentów.
9. System musi wspierać rozbudowę o usługę DNS dla usług Active Directory.
10. System musi wspierać usługę DDNS.
11. System musi obsługiwać mechanizm IDN (Internationalized Domain Names) – (w tym polskie znaki) i posiadać wbudowany konwerter tzw. punycode.
12. System musi umożliwiać dodanie w przyszłości (licencja i/lub subskrypcja usługi) funkcjonalności filtrowania odpowiedzi DNS na podstawie bazy reputacji domen infekujących Malware/C&C/Botnet. W przypadku braku takiej funkcjonalności w oferowanym systemie IPAM/DNS/DHCP należy dostarczyć dodatkowe urządzenie bezpieczeństwa posiadające taką funkcjonalność z wydajnością minimum 1 Gbps ruchu i 4 interfejsami GE.
13. System musi umożliwiać realizację usług DHCP.
14. System musi umożliwiać aktualizację danych DDNS przez usługę DHCP.
15. Urządzenie musi dostarczać na bieżąco informacje o przyznawaniu adresów IP i urządzeniach, którym dany adres został przypisany (adres MAC, czas i data przyznania adresu, IP).
16. System musi wspierać funkcjonalność DHCP Failover z renegocjacją dostępnych przestrzeni adresowych.
17. Musi istnieć możliwość sprawdzenia dostępności adresu IP przed jego przydzieleniem z czasem ICMP poniżej sekundy.
18. System musi wspierać funkcję rozpoznawania typu urządzenia/systemu stacji, urządzeń mobilnych itp. na podstawie analizy zapytania DHCP. Raportowanie typu urządzenia w historii dzierżaw adresów IP oraz możliwość filtrowania/blokowania przydziału adresu dla wybranych typów urządzeń. (Np. przydziel adres stacji Windows 7/XP, ale nie przydzielaj adresu tabletowi i urządzeniu typu smartphone). W przypadku braku takiej funkcjonalności w oferowanym systemie IPAM/DNS/DHCP należy dostarczyć dodatkowe urządzenie bezpieczeństwa posiadające funkcjonalność profilowania urządzeń dla 2000 portów użytkowników.
19. System musi dostarczać usługę zarządzania adresami IP – IPAM (IP Address Management).
20. System musi zarządzać adresami IPv4 i IPv6 pozwalając na graficzną (mapy sieci) oraz obiektową metodę zarządzania adresacją.
21. System musi pozwalać na integrację z usługami VMware vSphere w celu wykonywania procesu „discovery” maszyn wirtualnych pracujących na infrastrukturze VMware.
22. System musi posiadać mechanizmy kontroli wprowadzania danych (poprawność adresów IP, masek itp.).
23. System musi umożliwiać dodawanie opisów i rozbudowanych atrybutów dla obiektów sieci, adresów IP, domen oraz zakresów DHCP. Atrybuty te muszą umożliwiać definicję typu i rozmiar danego atrybutu. Musi być możliwość stosowania słowników atrybutów z wymuszenie lub proponowaniem danego typu atrybutu dla danego typu obiektu. System atrybutów musi umożliwiać dziedziczenie atrybutów w ramach struktury sieci i podsieci.
24. System musi posiadać mechanizm skanowania sieci i hostów (adresów IP) tzw. discovery. Mechanizm ten musi działać w trybie na żądanie oraz musi pozwalać na planowane powtarzalne rozpoznawania w przyszłości.
25. System musi posiadać mechanizmy typu „znajdź mi 10 nieużywanych adresów z sieci X” oraz „znajdź mi 10 nieużywanych podsieci rozmiaru np. /24 w podsieci np. a.b.c.d/16”.
26. System musi umożliwiać Import danych w formacie CSV bezpośrednio z GUI i posiadać szczegółową dokumentację formatu danych importowanych.
27. Producent rozwiązania musi udostępniać bezpłatnie narzędzie do importu danych z innych systemów DNS/DHCP: Bind 8, Bind 9, Microsoft.
28. System musi umożliwiać rozbudowę w przyszłości o zarządzanie usługami DNS/DHCP na wielu serwerach Microsoft Windows bez potrzeby instalowania oprogramowania po stronie serwerów MS Windows.
29. Wymagane jest wsparcie co najmniej dla:
    1. Microsoft Windows 2003 Standard and Enterprise SP2 32 bits,
    2. Microsoft Windows 2003 R2 Standard and Enterprise Initial Release 32 bits, 64 bits,
    3. Microsoft Windows 2008 Standard and Enterprise SP2 32 bits, 64 bits,
    4. Microsoft Windows 2008 R2 Standard and Enterprise Initial Release 64 bits,
    5. Microsoft Windows 2012 Standard and Enterprise Initial Release 64 bits.
30. Zarządzanie systemem musi odbywać się z jednego miejsca (IP) za pomocą jednolitego systemu graficznego.
31. System musi posiadać mechanizm Workflow do zarządzania procesem potwierdzania i akceptacji zmian.
32. Zarządzanie systemem musi się odbywać przez przeglądarkę WWW bez potrzeby instalacji specjalnego oprogramowania typu agent, klient itp.
33. System musi dostarczać mechanizm API do kontroli systemu, wykonywania i automatyzacji zadań wykonywanych za pomocą GUI. Musi być dostarczona pełna dokumentacja systemu API z przykładami zastosowania itp. Akceptowalne technologie API: Perl (konieczna biblioteka np. CPAN) lub REST.
34. System musi pracować, jako platforma dystrybucji plików za pomocą protokołów TFTP, FTP, HTTP, oraz oferować usługi synchronizacji czasu za pomocą protokołu NTP (Network Time Protocol).
35. System musi umożliwiać integrację z zamawianym w punkcie 2.9.12 systemowi zarządzania i automatyzacji środowiska sieciowego. Integracja ma zezwalać na wykrywanie adresów IP i podsieci IP (ipv4 i ipv6) w sieci i synchronizację danych do systemu IPAM. W drugą stronę system IPAM dla zarządzania siecią powinien być w stanie wykonać automatyczne czynności na przełącznikach (włącz/wyłącz port, zmień VLAN, uruchom nową sieć IP).
36. System musi posiadać funkcję budowy systemu rozproszonego, która pozwoli na zbudowanie systemu rozproszonego z synchronizacją danych poprzez sieć IP z centralnym zarządzaniem całym systemem.
37. System musi dostarczać informacje o wszystkich zmianach wprowadzanych przez administratorów (kto, kiedy, co zostało zmienione).
38. Musi istnieć możliwość wysyłania tych informacji do centralnego repozytorium za pomocą mechanizmu Syslog (TCP i UDP).
39. System musi umożliwiać nadawanie administratorom praw opartych o grupy i role, co pozwala na ograniczenie ich dostępu do wymaganych zasobów. Granulacja uprawnień powinna umożliwiać konfigurowanie uprawnień dla pojedynczych obiektów typu sieć, strefa DNS, rekord DNS, zakres DHCP.
40. Uwierzytelnianie użytkowników musi wspierać: lokalną bazę użytkowników, protokół RADIUS, protokół TACACS+, LDAP oraz Microsoft Active Directory.
41. System musi posiadać wbudowaną bazę danych, przechowującą dane z wszystkich uruchomionych w systemie usług. Baza danych nie może wymagać żadnych czynności administracyjnych związanych z jej konfiguracją.
42. Musi istnieć możliwość prowadzenia statystyk oraz monitorowania parametrów urządzeń przy użyciu protokołu SNMP (Simple Network Management Protocol).
43. Dostęp do konsoli administracyjnej urządzeń systemu powinien być możliwy poprzez:
    1. Interfejs zdalny dostępny poprzez protokół SSH, wsparcie dla wersji SSHv2,
    2. Interfejs znakowy – dostępny poprzez port szeregowy, zabezpieczony hasłem dostępu, które jest powiązane z użytkownikiem.
44. Urządzenie musi wykonywać planowe kopie bezpieczeństwa do zewnętrznego serwera w celu uproszczenia procedur odzyskiwania w razie awarii (TFTP, FTP, SCP).
45. System musi posiadać następujące parametry redundancji:
    1. Usługi IPAM, DNS, DHCP – min. 2 urządzenia pracujące w trybie redundancji HA (High Availability) z czasem przełączenia poniżej 8 sekund.
46. System musi posiadać następujące parametry:
    1. 2 dedykowane urządzenia: Obsługa minimum 30000 zapytań DNS na sekundę. Obsługa minimum 200 zapytań DHCP na sekundę. Urządzenia należy dostarczyć z redundantnymi zasilaczami.
47. System musi być oparty o dedykowaną platformę programową i sprzętową. Nie jest dopuszczalne stosowanie systemów składanych z komponentów typu system operacyjny do tego oddzielnie instalowane komponenty programowe.
48. Urządzenia systemu odpowiedzialne za usługi IPAM/DNS/DHCP muszą posiadać wsparcie dla zapewnienia niezawodności działania (high-availability – HA) na poziomie sieci i na poziomie danych (synchronizacja danych między urządzeniami). Musi funkcjonować za pomocą standardowego protokołu np. VRRP.
49. Urządzenia systemu muszą posiadać następujące ilości portów/interfejsów:
    1. Minimum dwa porty GigabitEthernet do sieci LAN.
    2. Minimum jeden port GigabitEthernet do komunikacji w trybie HA (do synchronizacji danych).
    3. Minimum jeden port GigabitEthernet do sieci zarządzającej.
    4. Minimum jeden port Ethernet do dostępu typu IPMI.

### Wymagania stawiane przełącznikowi KVM

1. Montaż w szafie RACK 19’’, wysokość nie większa niż 1U.
2. Ilość portów 16.
3. Przełącznik KVM musi współpracować z dostarczonymi serwerami i dostarczonym zestawem klawiatury i monitora.
4. Przełącznik KVM musi być dostarczony z minimum 4 kompletami przewodów do połączenia z dostarczonymi serwerami oraz kompletem kabli zasilających.

### Wymagania stawiane serwerowi przełącznika KVM

1. Monitor minimum 17’ LCD.
2. Rozdzielczość co najmniej 1280x1024.
3. Klawiatura - 106 klawisze.
4. Mysz – touchpad.
5. Montaż w szafie RACK 19’’, wysokość nie większa niż 1U.
6. Komplet przewodów umożliwiający połączenie konsoli z dostarczonym przełącznikiem KVM oraz kable zasilające.

### Wymagania stawiane patchpanelowi światłowodowemu realizującemu funkcje dystrybucji

1. Musi posiadać możliwość instalacji w szafie 19”.
2. Głębokość urządzenia nie może przekraczać 250mm.
3. Rozmiar urządzenia nie może przekraczać 1U.
4. Obudowa musi umożliwiać instalację co najmniej 4 niezależnych modułów.
5. Pojedynczy moduł musi umożliwiać instalację na przednim panelu do 11 złączy LC/UPC duplex.
6. Wymaga się dostarczenia minimum 2 modułów dla każdej z obudów
   1. Musi być w postaci modułu pasującego do obudowy modułowej 1U,
   2. Musi posiadać 6 złączy LC/UPC duplex MM,
   3. Musi posiadać 1 złącze umożliwiające terminowanie 12 włókien MM,
   4. Straty wtrąceniowe modułu nie mogą przekraczać 0.8dB.
7. Moduły muszą być instalowane w obudowie poziomo.
8. Zaproponowane rozwiązanie musi dawać możliwość instalacji w obrębie jednego chassis multiplekserów i demultiplekserów CWDM oraz DWDM, urządzeń OADM, cyrkulatorów optycznych oraz łączników światłowodowych.

### Wymagania stawiane patchpanelowi światłowodowemu realizującemu funkcje agregacji

1. Musi posiadać możliwość instalacji w szafie 19”.
2. Głębokość urządzenia nie może przekraczać 250mm.
3. Rozmiar urządzenia nie może przekraczać 1U.
4. Urządzenie musi umożliwiać podłączenie minimum 6 modułów łącznika:
   1. Musi być w postaci modułu pasującego do obudowy modułowej 1U,
   2. Musi posiadać 6 złączy LC/UPC duplex MM,
   3. Musi posiadać 1 złącze umożliwiające terminowanie 12 włókien MM,
   4. Straty wtrąceniowe modułu nie mogą przekraczać 0.8dB.
5. Urządzenie musi posiadać 6 złączy, z których każde umożliwia terminowanie 12 włókien MM.
6. Urządzenie musi posiadać 36 złączy LC/UPC duplex MM.
7. Wszystkie złącza muszą być zlokalizowane na przednim panelu.

### Wymagania stawiane patchpanelowi światłowodowemu realizującemu funkcje rdzeniowe

1. Musi posiadać możliwość instalacji w szafie 19”.
2. Głębokość urządzenia nie może przekraczać 250mm.
3. Rozmiar urządzenia nie może przekraczać 1U.
4. Obudowa musi umożliwiać instalację co najmniej 4 niezależnych modułów.
5. Pojedynczy moduł musi umożliwiać instalację na przednim panelu do 11 złączy LC/UPC duplex.
6. Wymaga się dostarczenia 4 modułów dla każdej z obudów
   1. Musi być w postaci modułu pasującego do obudowy modułowej 1U,
   2. Musi posiadać 6 złączy LC/UPC duplex MM,
   3. Musi posiadać 1 złącze umożliwiające terminowanie 12 włókien MM,
   4. Straty wtrąceniowe modułu nie mogą przekraczać 0.8dB.
7. Moduły muszą być instalowane w obudowie poziomo.

### Wymagania stawiane kablom połączeniowym do patchpaneli światłowodowych

1. Musi posiadać 12J.
2. Średnica kabla nie może przekraczać 4mm.
3. Musi  być zakończony po obu stronach pojedynczym złączem.
4. Każde złącze musi terminować wszystkie 12J.

### Wymagania dotyczące patchcordów światłowodowych

1. Patchcordy typu duplex (kabel stacyjny z dwoma włóknami jednodomowymi, lub wielomodowymi w zależności od zapotrzebowania.
2. Zakończania dopasowane do portów na oferowanych urządzeniach i złączy LC/APC zaprojektowanych na przełącznicach (sugerowane zakończenie na urządzeniach sieciowych - LC/PC).
3. Tłumienność wsteczna (reflektancja) większa od 60dB.

## Opis czynności uruchomieniowych i wstępnej konfiguracji sieci

### Przygotowanie Planu Wdrożenia

W celu uzyskania przez sieć DC właściwej funkcjonalności oraz możliwości wykonania testów odbiorczych niezbędne jest uruchomienie i wstępne skonfigurowanie dostarczonych urządzeń aktywnych. Tryb i szczegółowy zakres konfiguracji zależy w istotny sposób od konkretnej implementacji produktowej (producenta urządzeń), która zostanie ostatecznie wybrana w toku postępowania przetargowego. Dostępne na rynku urządzenia różnych producentów, spełniające wymagania opisane w niniejszej dokumentacji, różnią się pod względem szczegółowej konfiguracji i implementacji różnych technologii.

W związku z powyższym niniejsze opracowanie, jako neutralne technologicznie, definiuje jedynie istotne elementy procesu uruchomienia i konfiguracji (zwanego dalej procesem wdrożenia), które muszą zostać wykonane, niezależnie od ostatecznego wyboru implementacji (producenta urządzeń). Przyjmuje się zatem, że tryb i szczegółowy zakres tych czynności zostanie zaproponowany przez Wykonawcę prac (Dostawcę urządzeń) w niezależnym dokumencie pn. Plan Wdrożenia, stanowiącym integralną część implementacji systemowej (implementacji zespołu urządzeń i oprogramowania). Plan Wdrożenia musi zostać sporządzony przez Wykonawcę przed przystąpieniem do realizacji projektu zgodnie z wymaganiami niniejszej dokumentacji, oraz dostarczony Zamawiającemu w terminie nie późniejszym niż 2 tygodnie od daty podpisania Umowy i zarazem, na co najmniej 4 tygodnie przed planowaną datą rozpoczęcia prac wdrożeniowych przez Wykonawcę. Z uwagi na konieczność zaangażowania personelu Zamawiającego w proces wdrożenia, Plan Wdrożenia podlega sprawdzeniu i akceptacji przez Zamawiającego, który w terminie do 2 tygodni przed planowaną datą rozpoczęcia prac wdrożeniowych może wnieść do niego swoje zastrzeżenia, uwagi lub propozycje korekt.

Plan Wdrożenia winien zawierać w szczególności:

1. Harmonogram wdrożenia.
2. Zdefiniowanie usług świadczonych w sieci dla poszczególnych bloków sieci oraz przypisanie do nich odpowiednich polityk QoS oraz bezpieczeństwa.
3. Schemat przydzielania adresów IP dla urządzeń sieciowych (sposób adresacji urządzeń w DC) i użytkowników sieci (przydział adresów z puli prywatnych i publicznych).
4. Konwencje nazywania urządzeń sieciowych i urządzeń.
5. Szczegóły konfiguracji urządzeń w W.INTERNET.
6. Opis protokołów routingu używanych w sieci i sposobu ich konfiguracji.
7. Opis parametrów i konfiguracji MPLS.
8. Określenie globalnych parametrów QoS (jak będzie obsługiwany ruch w zależności od kodów DSCP, CoS, EXP), propozycję podziału procentowego całego pasma na klasy ruchu.
9. Określenie jak zdefiniowane powyżej usługi będą mapowane na usługi realizowane przez sieć, ze szczególnym uwzględnieniem sposobu konfiguracji MPLS, routingu, VLAN, QoS, bezpieczeństwa.
10. Określenie globalnych parametrów Multicast.
11. Opis mechanizmów równoważenia łączy.
12. Określenie globalnej polityki bezpieczeństwa.
13. Opis wszelkich czynności i szczegółów implementacyjnych pozwalających na osiągnięcie przez oferowany zespół urządzeń funkcjonalności opisanej w niniejszej dokumentacji (w tym treść proponowanych skryptów konfiguracyjnych).
14. Zestawienie parametrów niezbędnych w procesie wdrożenia, których wartości winny być określone przez Zamawiającego przed rozpoczęciem wdrożenia, na podstawie aktualnego w tym okresie planu/polityki świadczenia usług i zarządzania siecią DC przyjętych przez Zamawiającego.
15. Zestawienie i szczegółowy opis testów akceptacyjnych, właściwych dla instalowanych urządzeń, które udokumentują spełnienie przez cały system wymagań odnośnie konfiguracji opisanej w punkcie 2.10.2 oraz jego poszczególne części, dla których wymagania określono w niniejszej dokumentacji w punkcie 2.10.2.
16. Procedury operacyjne dla administratorów.

Ustala się następujące wymagania związane z wdrożeniem i uruchomieniem urządzeń aktywnych sieci DC:

1. Proces wdrożenia winien obejmować następujące etapy:
   1. Przedstawienie harmonogramu prac, zaakceptowanego przez Zamawiającego.
   2. Przeprowadzenia szkoleń pracowników Zamawiającego.
   3. Opracowanie Planu Wdrożenia, w porozumieniu z Zamawiającym, zakończone podpisaniem protokołu akceptacji/odbioru Planu. Odbiór Planu Wdrożenia będzie niezbędnym warunkiem rozpoczęcia prac konfiguracyjnych.
   4. Dostawa i instalacja komponentów całego systemu.
   5. Właściwa konfiguracja i uruchomienie całego systemu - przełączenie ruchu produkcyjnego na nową infrastrukturę - wg. Planu Wdrożenia sporządzonego zgodnie z wymaganiami Zamawiającego i przez niego zaakceptowanego.
   6. Przeprowadzenie testów akceptacyjnych - walidacja rozwiązania (audyt konfiguracji) oraz testów odbiorczych – niezawodnościowych i funkcjonalnych (wymagane dostarczenie zestawienia w postaci tabeli szczegółowo opisującej poszczególne testy wraz z wynikiem pozytywny/negatywny).
   7. Opracowanie dokumentacji powykonawczej i zaleceń powdrożeniowych, obejmującej:
      1. Szczegółowy wykaz komponentów będących przedmiotem zamówienia oraz miejsca i sposobu ich instalacji.
      2. Szczegółowy schemat połączeń poszczególnych urządzeń.
      3. Szczegółową konfigurację poszczególnych urządzeń oraz konfigurację usług.
      4. Procedury operacyjne dla administratorów.
      5. Instrukcje z zadaniami administracyjnymi z wydzieleniem prac codziennych, cotygodniowych, comiesięcznych i ew. innych.
      6. Procedury archiwizacji danych i awaryjne (ratunkowe).
      7. Konfigurację systemów zarządzania.
      8. Wskazanie sposobu rozbudowy poszczególnych urządzeń.
      9. Inne istotne informacje mające wpływ na użytkowanie dostarczonych urządzeń.
2. Szczegółowe informacje o zakresie integracji z istniejącymi sieciami zostaną ustalone z Wykonawcą po podpisaniu umowy.
3. Ogólny opis wdrożenia:
   1. Instalacja, wdrożenie i uruchomienie przełączników kampusowych, rdzeniowych i dostępowych zgodnie z wymaganiami ustalonymi z Zamawiającym.
   2. Instalacja, wdrożenie i uruchomienie routerów realizujących funkcjonalności dostępu do Internetu zgodnie z wymaganiami ustalonymi z Zamawiającym.
   3. Instalacja, wdrożenie i uruchomienie zapór ogniowych oraz rozwiązań bezpieczeństwa zgodnie z wymaganiami ustalonymi z Zamawiającym.
   4. Instalacja, wdrożenie i uruchomienie systemu zarządzania urządzeniami sieci DC, systemu monitorującego sieć oraz platformy usług sieciowych zgodnie z wymaganiami ustalonymi z Zamawiającym.
   5. Instalacja i konfiguracja wszystkich dostarczonych serwerów wraz z systemem operacyjnym i wymaganymi licencjami.

### Ramowe wymagania odnośnie konfiguracji urządzeń

Minimalne niezbędne wymagania dla skonfigurowanych funkcjonalności i parametrów sieci

DC w początkowym okresie jej użytkowania zostały określone poniżej.

### W.RDZEN

* 1. Konfiguracja usług transportowych zgodnie z polityką realizacji usług i zarządzania siecią DC.
  2. Skonfigurowanie elastycznego i wielo-kryterialnego mapowania opartego o VLAN\_ID/inne mapowania ruchu z urządzeń dostępowych na odpowiednie usługi transportowe W.RDZEN, W.SERWIS i W.INTERNET, wraz z przypisanymi im politykami QoS oraz bezpieczeństwa.
  3. Połączenia warstwy trzeciej: protokoły routingu, wirtualne tablice routingu (wraz z przypisanymi odpowiednimi interfejsami) zgodnie z polityką realizacji usług i zarządzania siecią DC.
  4. Konfiguracja mechanizmów niezawodnościowych LACP, MPLS FRR, OSPF BFD i innych zgodnie z Planem Wdrożenia.
  5. Konfiguracja Quality of Service dla W.RDZEN sieci zgodnie z Planem Wdrożenia.
  6. Konfiguracja multicast dla W.RDZEN zgodnie z Planem Wdrożenia.
  7. Konfiguracja wirtualnych kontekstów oraz konfiguracja protokołów wspomagających działanie sieci w środowisku składającym się z wielu kontekstów zgodnie z Planem Wdrożenia.
  8. Konfiguracja ochrony warstwy zarządzającej na urządzeniach.
  9. Skonfigurowanie innych funkcjonalności związanych z bezpieczeństwem (uRPF, ograniczenie ruch określonego typu, uwierzytelnienie protokołu routingu, SSH i inne).
  10. Definicja dostępu administracyjnego.
  11. Skonfigurowanie i zabezpieczenie dostępu do urządzenia poprzez CLI, SSH, SNMP.

### W.DOSTEP

1. Konfiguracji połączenia warstwy trzeciej: protokoły routingu, wirtualne tablice routingu (wraz z przypisanymi odpowiednimi interfejsami) zgodnie z polityką realizacji usług i zarządzania siecią DC.
2. Konfiguracja mechanizmów niezawodnościowych LACP, MPLS FRR, OSPF BFD i innych zgodnie z Planem Wdrożenia.
3. Konfiguracja Quality of Service dla W.RDZEN sieci zgodnie z Planem Wdrożenia.
4. Konfiguracja multicast dla W.RDZEN zgodnie z Planem Wdrożenia.
5. Konfiguracja wirtualnych kontekstów oraz konfiguracja protokołów wspomagających działanie sieci w środowisku składającym się z wielu kontekstów zgodnie z Planem Wdrożenia.
6. Konfiguracja ochrony warstwy zarządzającej na urządzeniach.
7. Skonfigurowanie innych funkcjonalności związanych z bezpieczeństwem (uRPF, ograniczenie ruchu określonego typu, uwierzytelnienie protokołu routingu, SSH i inne).
8. Definicja dostępu administracyjnego.
9. Skonfigurowanie i zabezpieczenie dostępu do urządzenia poprzez CLI, SSH, SNMP.

### W.INTERNET

1. Skonfigurowanie protokołów routingu.
2. Skonfigurowanie peeringu BGP z operatorami wraz z politykami umożliwiającymi elastyczne i efektywne wykorzystywanie łącz do różnych operatorów.
3. Skonfigurowanie polityk QoS związanych z dostępem do Internetu stosownie z wymaganiami usług definiowanych w Planie Wdrożenia.
4. Skonfigurowanie funkcjonalności szyfrowanych sieci prywatnych dla odpowiednich usług.
5. Skonfigurowanie Multicast (PIM, IGMP i inne).
6. Skonfigurowanie list kontroli dostępu filtrujących niepożądanych ruch w ramach poszczególnych usług.
7. Skonfigurowanie innych funkcjonalności związanych z bezpieczeństwem (uRPF, ograniczanie ruchu określonego typu, uwierzytelnianie protokołów routingu, SSH i inne).
8. Ochrona warstwy zarządzającej na urządzeniu.
9. Definicja dostępu administracyjnego (zarówno w oparciu o Radius jak i lokalna).
10. Skonfigurowanie i zabezpieczenie dostępu do urządzenia poprzez CLI, SSH, SNMP.

### W.SERWIS

1. Skonfigurowanie systemu zabezpieczeń opartego o zaporę ogniową oraz system proaktywnej ochrony przed atakami:
   1. Wdrożenie polityk bezpieczeństwa zgodnie z Planem Wdrożenia,
   2. Wdrożenie wirtualnych kontekstów.
2. Skonfigurowanie klastra złożonego z dwóch zapór ogniowych, z możliwością rozszerzenia o kolejne zapory ogniowe.

### W.KAMPUS

1. Odpowiednie zaprojektowanie połączeń pomiędzy W.KAMPUS oraz W.RDZEN.
2. Odpowiednie zaprojektowanie bezpiecznych połączeń dla komputerów podłączonych do W.KAMPUS.
3. Skonfigurowanie odpowiednich protokołów umożliwiających poprawną pracę nawet w przypadku całkowitej awarii jednego z modułów zarządzających.
4. Skonfigurowanie połączenia warstwy trzeciej: protokoły routingu, zgodnie z polityką realizacji usług i zarządzania siecią DC.
5. Konfiguracja ochrony warstwy zarządzającej na urządzeniach.

### Dodatkowe

1. Skonfigurowanie sieci zarządzającej zagregowanej na przełączniku agregacji sieci zarządzającej.
2. Skonfigurowanie połączenia sieci zarządzającej z przełącznikiem SW1.
3. Skonfigurowanie koncentratora VPN sieci zarządzającej zgodnie z Planem Wdrożenia.
4. Skonfigurowanie oraz zainstalowanie środowiska VMware vSphere oraz systemu zarządzającego środowiskiem witalizacyjnym zgodnie z Planem Wdrożenia.
5. Zainstalowanie oraz wstępne skonfigurowanie sytemu operacyjnego wymaganego do zainstalowania oprogramowania do monitoringu parametrów sieciowych.
6. Zainstalowanie oraz skonfigurowanie oprogramowanie do monitoringu parametrów sieciowych zgodnie z Planem Wdrożenia.
7. Skonfigurowanie systemu zarządzania i automatyzacji środowiska sieciowego wraz z podłączeniem pod ten system urządzeń aktywnych wyspecyfikowanych w tabeli 3.1.
8. Skonfigurowanie Platformy usług sieciowych zgodnie z Planem Wdrożenia.

## Testy akceptacyjne, odbiór i gwarancja

### Testy akceptacyjne

Po wykonaniu prac wdrożeniowych wymagane jest przeprowadzenie testów akceptacyjnych i wydajnościowych elementów uruchomionej infrastruktury. Testy te mają na celu zweryfikowanie poprawności wdrożenia i wykazanie spełnienia wszystkich wymagań zawartych w niniejszym projekcie przez dostarczone urządzenia i oprogramowanie. Testy akceptacyjne i wydajnościowe powinny obejmować urządzenia odpowiedzialne za niezawodność oraz ciągłą dostępność urządzeń usług w sieci DC.

W ramach testów akceptacyjnych należy przeprowadzić następujące czynności:

1. Sprawdzenie poprawności instalacji urządzeń, w trakcie tych czynności należy sprawdzić jakość instalacji urządzeń (czytelne i jednoznaczne oznakowanie urządzeń, estetyka montażu).
2. Weryfikację urządzeń i oprogramowania, celem tych czynności jest sprawdzenie zgodności dostarczonych urządzeń i oprogramowania ze specyfikacją projektową, weryfikacja poprawność startu oraz pracy urządzeń, sprawdzenie dostępu do urządzeń i uruchomionych na nich usług.
3. Testy powdrożeniowe obejmujące sprawdzenie poprawności działania skonfigurowanej sieci DC EXEA. Testy te będą obejmować w szczególności:
   1. Testy łączności między urządzeniami w DC,
   2. Testy łączności w styku z Internetem i dostępu do sieci Internet dla użytkowników sieci DC,
   3. Testy awarii urządzeń oraz automatycznego przejęcia pracy przez inne urządzenia,
   4. Testy awarii łącza internetowego,
   5. Testy bezpieczeństwa zapór ogniowych,
   6. Testy konfiguracji i działania VLAN-ów,
   7. Testy konfiguracji protokołów routingu,
   8. Testy konfiguracji i działania MPLS VPN,
   9. Testy poprawnej konfiguracji równoważenia ruchu,
   10. Testy poprawnej konfiguracji polityk QoS.

W ramach testów akceptacyjnych należy także sprawdzić poprawność wykonania czynności wdrożeniowych oraz konfiguracji urządzeń i usług, które zostały opisane w punkcie 2.10.2 niniejszego projektu.

W dalszej kolejności należy sprawdzić poprawność komunikacji pomiędzy dwoma komputerami wpiętymi do różnych przełączników dostępowych za pomocą narzędzi ping lub mtr. Należy sprawdzić maksymalną prędkość transmisji pomiędzy komputerami np. za pomocą narzędzia iperf. Ważne jest także sprawdzenie działania mechanizmu VLAN. W tym celu należy do dwóch różnych przełączników dostępowych podpiąć urządzenia klienckie w różnych VLANach i sprawdzić komunikację pomiędzy tymi urządzeniami.

W ramach testów akceptacyjnych należy sprawdzić jakość usług oferowanych przez sieć DC. Testy te powinny być przeprowadzone dla różnych scenariuszy, określających liczbę użytkowników, obciążenie ruchem oraz typy realizowanych usług. Celem testów jest sprawdzenie, czy wszystkie urządzenia w sieci są dostępne oraz czy komunikacja i wymiana danych pomiędzy tymi urządzeniami jest poprawnie realizowana (drożność systemu) oraz sprawdzenie, czy deklarowane usługi pomiędzy poszczególnymi urządzeniami są realizowane z wymaganym poziomem jakości. W ramach testów jakości usług powinny zostać zmierzone następujące parametry kluczowe:

* Maksymalne opóźnienie przesyłania pakietów dla danego punktu,
* Maksymalne wahanie wartości opóźnienia przesyłania pakietów,
* Maksymalna wartość współczynnika straty pakietów,
* Średnie opóźnienie przesyłania pakietów dla poszczególnych grup/punktów,
* Średnia przepustowość pomiędzy punktami referencyjnymi.

Testy te należy przeprowadzić przy użyciu generatorów ruchu, symulatorów stacji roboczych oraz oprogramowania badającego opóźnienia i straty pakietów.

W czasie testów akceptacyjnych należy także sprawdzić poziom zabezpieczeń ciągłości dostępu

do sieci INTERNET a w szczególności:

* Czy sieć DC jest podłączona łączami od dwóch niezależnych operatorów,
* Czy został uruchomiony protokół routingu BGP (w celu zapewnienia stałej dostępności),
* Czy w przypadku awarii łącza podstawowego nastąpiło poprawne przełączenie na łącze zapasowe i klienci sieci mogą korzystać z niego.

W ramach testów akceptacyjnych należy także sprawdzić zachowanie się urządzeń w czasie awarii oraz czas odtwarzania świadczenia usług po awarii. Celem tych testów jest sprawdzenie czasu, jaki jest wymagany przez urządzenie na odtworzenie oferowanych przez niego usług w przypadku, gdy wystąpiła awaria któregoś, z jego komponentów. Zakres testów wymaga zatem, aby zasymulować różnego rodzaju awarie poszczególnych komponentów urządzenia, następnie przywrócić działanie danego komponentu i oszacować niezbędny czas, jaki jest potrzebny, aby dana funkcjonalność urządzenia została w pełni przywrócona. Następnie należy zweryfikować czy nastąpiło pełne przywrócenie funkcjonalności. W ramach tych testów zostanie zweryfikowane w szczególności:

* Sprawdzić zachowanie sieci po wyłączeniu jednego z punktów GPDx i czasu potrzebnego do poprawnego świadczenia usług klientom sieci. Następnie włączyć ten punkt GPDx i sprawdzić czy sieć powróciła do stanu z przed symulowanej awarii,
* Sprawdzić wpływ awarii łącza podstawowego pomiędzy punktami GPD na funkcjonowanie sieci i czy po naprawie awarii sieć powraca do stanu z przed awarii,
* Sprawdzić wpływ awarii jednego z łączy pomiędzy punktami EoR i GPDx na funkcjonowanie punktu EoR/ToR i czas, jaki jest potrzebny na przełączenie się,
* Sprawdzić wpływ awarii jednego z modułów zarządzających przełącznika w KAMPx na działanie danego przełącznika i dostęp do zasobów sieciowych użytkowników podłączonych do tego przełącznika,
* Sprawdzić wpływ, jaki może wywołać awaria systemu zarządzania lub poszczególnych funkcji przez nierealizowanych (monitoring SNMP, zarządzanie siecią, DHCP, DNS, IPAM) na poprawność działania całej sieci DC,
* Przeprowadzić częściową/kompletną symulację braku zasilania w poszczególnych urządzeniach oraz sprawdzić poprawności przywrócenia konfiguracji/ustawień urządzeń,
* Sprawdzić wpływ awarii sieci jednego z operatorów zapewniających przyłącze sieci DC do sieci Internet na usługę dostępu do Internetu świadczoną w sieci DC,
* Określić/sprawdzić możliwości różnych serwerów i urządzeń sieciowych związane z wymianą poszczególnych ich elementów ‘na gorąco’ podczas normalnej pracy (np. serwery wyposażone w nadmiarowe elementy tj. zasilacze, pamięć, dyski, które można wymieniać ‘na gorąco’ podczas normalnej pracy urządzenia).

Weryfikacja funkcjonalności poszczególnych elementów sieci będzie polegała na zaakceptowaniu przez Zamawiającego każdego z przeprowadzonych testów. Z każdego takiego testu powinien zostać sporządzony raport zawierający wyniki przeprowadzonych procedur testowych wraz z zaszeregowaniem danego wyniku testu, jako testu o wyniku pozytywnym lub negatywnym. W przypadku negatywnego wyniku testu raport powinien zawierać dane dotyczące analizy danego problemu oraz informację o działaniach, jakie należy przeprowadzić w celu wyeliminowania zdiagnozowanych problemów. W takim wypadku testy akceptacyjne i weryfikacyjne po przeprowadzeniu działań naprawczych zostaną prze Wykonawcę powtórzone w celu weryfikacji skutecznego usunięcia nieprawidłowości. Pozytywny wynik testów jest warunkiem koniecznym podpisania przez Zamawiającego protokołu odbioru.

### Odbiór

Po pozytywnym zakończeniu testów akceptacyjnych nastąpi odbiór końcowy. Odbiór systemu będzie przeprowadzony przez komisję techniczną, utworzoną przez wytypowanych przedstawicieli stron. Do protokołu odbioru dołączone powinny być m. in.:

* Dokumentacja opisująca wykonanie testów akceptacyjnych i powdrożeniowych,
* Wykaz urządzeń wraz z numerami seryjnymi,
* Komplet dokumentacji całego systemu w języku polskim oraz procedury eksploatacyjne wraz z instrukcjami,
* Wszystkie wymagane prawem nośniki, licencje i certyfikaty na dostarczony sprzęt i oprogramowanie,
* Wykaz oprogramowania wraz z rodzajem i warunkami licencjonowania,
* Dokumenty potwierdzające przeprowadzenie szkoleń dla pracowników Zamawiającego.

### Serwis gwarancyjny

Opis serwisu gwarancyjnego (jeżeli nie został opisany przy specyfikacji urządzeń w pkt. 2.9) należy przewidzieć tak jak opisano poniżej:

1. Wykonawca udzieli minimum 12 miesięcznego serwisu gwarancyjnego na dostarczone i skonfigurowane komponenty i konfigurację systemu.
2. Okres serwisu gwarancyjnego rozpoczyna się z dniem podpisania przez Zamawiającego protokołu odbioru bez uwag.
3. Serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu;
4. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon, e-mail lub WWW (przez całą dobę, 7 dni w tygodniu);
5. Podjęcie działań zgodnie z odpowiednim poziomem zgłoszonego priorytetu w standardzie:
   1. **Priorytet 1”, „P1”** – oznacza Incydent o charakterze Błędu Krytycznego, incydent spowodowany przez awarię lub dysfunkcję Elementu konfiguracji, które powodują poważne uszkodzenie tego Elementu, nieakceptowane upośledzenie jego funkcjonalności lub niedostępność usług realizowanych przy pomocy tego Elementu konfiguracji. Błędem Krytycznym nie jest awaria redundantnego Elementu konfiguracji.
   2. **„Priorytet 2”, „P2”** – oznacza Incydent o charakterze Awarii, incydent spowodowany przez awarię lub dysfunkcję Elementu konfiguracji, które powodują upośledzenie funkcjonalności albo zmniejszenie wydajności lub niezawodności tego Elementu w stopniu nieakceptowanym dla jego ciągłej pracy lub obniżenie jakości usług realizowanych przy pomocy tego Elementu konfiguracji.
   3. **„Priorytet 3”, „P3”** – oznacza Incydent o charakterze Wady, incydent spowodowany przez wadę lub dysfunkcję Elementu konfiguracji, które powodują nieznaczne upośledzenie funkcjonalności albo zmniejszenie wydajności lub niezawodności tego Elementu, w stopniu pozwalającym na jego dalszą ciągłą pracę lub nieznaczne obniżenie jakości usług realizowanych przy pomocy tego Elementu konfiguracji.
6. Poniższa tabela określa zależności miedzy poziomami SLA Usługi i Priorytetem a maksymalnym czasem reakcji i maksymalnym czasem rozwiązania:

|  |  |  |  |
| --- | --- | --- | --- |
| **Priorytet Incydentu** | **Godziny Obsługi Zgłoszeń** | **Maksymalny Czas reakcji** | **Maksymalny Czas rozwiązania** |
| Priorytet 1 | 7x24 | 2h | 2D |
| Priorytet 2 | 7x24 | NBD | 5D |
| Priorytet 3 | 7x24 | 3D | 14D |

W powyższej tabeli zastosowano następujące skróty:

* 7x24 oznacza: 7 dni w tygodniu, 24 godziny na dobę,
* NBD oznacza: następny dzień roboczy,
* D oznacza ilość dni roboczych,
* 2h oznacza 2 godziny.

1. Wykonawca zapewni poprzez WWW dostęp do systemu, gdzie Zamawiający będzie mógł obserwować stan aktualnych oraz zamkniętych zgłoszeń serwisowych.
2. Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań czynny przez całą dobę 7 dni w tygodniu.
3. Zamawiający wymaga, by serwis Wykonawcy bazował na wykupionym przez Wykonawcę serwisie producenta urządzeń, w celu
   1. zapewnienia naprawy lub wymiany urządzeń lub ich części, na części w pełni sprawne i oryginalne, zgodnie z metodyką i zaleceniami producenta,
   2. zapewnienia możliwości zgłaszania problemów do oficjalnego serwisu producenta w dniach roboczych od poniedziałku do piątku w godzinach 9:00 – 17:00, w przypadku gdy dany problem nie będzie mógł być rozwiązany bezpośrednio przez Wykonawcę. W takim przypadku rozwiązaniem problemu będzie zajmował się inżynier producenta.

1. W ramach serwisu gwarancyjnego Wykonawca zobowiązuje się do:
   1. Udzielania drogą telefoniczną lub mail, przez inżyniera Wykonawcy posiadającego certyfikat producenta ze znajomości danej technologii, 100 godzin konsultacji w zakresie konfiguracji sprzętu, oprogramowania i eksploatacji systemu oraz konfiguracji nowych usług na dostarczonym systemie, w godzinach pracy Zamawiającego;
   2. Udzielenia wsparcia utrzymaniowego polegającego na do 10 wizytach w placówce Zamawiającego w celu konfiguracji i rozwiązywania problemów z siecią, w przypadku jeśli problemu nie uda się rozwiązać zdalnie;
   3. Udostępnienia aktualizacji oprogramowania w ramach posiadanych wersji w porozumieniu z Zamawiającym o ile aktualizacja ta nie wymaga zakupów dodatkowych licencji;
      1. Aktualizacje wykonane zostaną w wcześniej zaplanowanym oknie serwisowym po akceptacji Zamawiającego i Wykonawcy oraz przy zdalnej asyście (mail / telefon ) wyspecjalizowanego inżyniera Wykonawcy.
   4. Usuwania usterek funkcjonalnych sprzętu i oprogramowania wynikających z wad powstałych podczas integracji lub implementacji oraz aktualizacji tego oprogramowania;

W przypadku awarii sprzętowych dostarczonych urządzeń, Wykonawca zobowiązuje się do bezpłatnej dostawy sprawnego urządzenia najpóźniej:

* do końca następnego dnia roboczego - w przypadku diagnozy awarii i rejestracji zgłoszenia do Wykonawcy do godziny 15:00 w dniu roboczym, do końca drugiego dnia roboczego, następującego po zgłoszeniu - w przypadku diagnozy i rejestracji zgłoszenia do Wykonawcy po godzinie 15:00 dnia roboczego lub poza godzinami pracy Wykonawcy.
  1. W przypadku zgłoszenia przez Zamawiającego problemu z Priorytetem 1 poza godzinami pracy Zamawiającego, Zamawiający ma obowiązek do podjęcia działań diagnostycznych i naprawczych w trybie określonym w tabeli pkt 7 paragrafu 2.11.3
  2. Zamawiający dopuszcza możliwość fizycznej wymiany sprzętu przez swoich pracowników.
  3. Jeżeli charakter naprawy wymaga przetransportowania sprzętu do Wykonawcy, Wykonawca przetransportuje ten sprzęt we własnym zakresie bez dodatkowych kosztów dla Zamawiającego. Dotyczy to również zwrotu sprzętu po naprawie;

## Wymagania w zakresie szkoleń

W ramach dostarczenia urządzeń i uruchomienia sieci DC Wykonawca zobowiązany jest do przeprowadzenia następujących szkoleń i warsztatów, dotyczących usług zaimplementowanych w sieci DC:

1. Dedykowane warsztaty szkoleniowe dla grupy do 5 pracowników Zamawiającego, obejmujące: Podstawy konfiguracji urządzeń sieciowych dostarczanych w ramach postępowania - wymagany czas trwania szkolenia co najmniej 5 dni (5 x 8 godzin).
2. Zarządzanie urządzeniami sieciowymi, dostępem do urządzeń sieciowych oraz monitoringiem dla grupy do 10 pracowników, zrealizowane w siedzibie Zamawiającego - wymagany czas trwania szkolenia co najmniej 2 dni (2 x 8 godzin):
   1. Zarządzanie konfiguracją urządzeń,
   2. Zarządzanie usługami,
   3. Zarządzanie awariami,
   4. Tworzenie raportów,
   5. Zarządzanie systemem monitoringu,
   6. Zarządzanie platformą usług sieciowych oraz systemu zarządzania i automatyzacji środowiska sieciowego.

W czasie przeprowadzonych warsztatów Wykonawca powinien zapewnić dostęp do laboratorium ze sprzętem, na którym będą testowane konfiguracje i mechanizmy sieciowe.

Zamawiający dopuszcza realizację warsztatów na urządzeniach, które będą dostarczone w ramach przedmiotu zamówienia.

Szkolenia i warsztaty muszą być prowadzone w języku polskim – dopuszcza się wykorzystanie materiałów szkoleniowych opracowanych w języku angielskim. Zamawiający wymaga wystawienie certyfikatu potwierdzającego uczestniczenie w dedykowanych szkoleniach i warsztatach szkoleniowych.

# Tabele

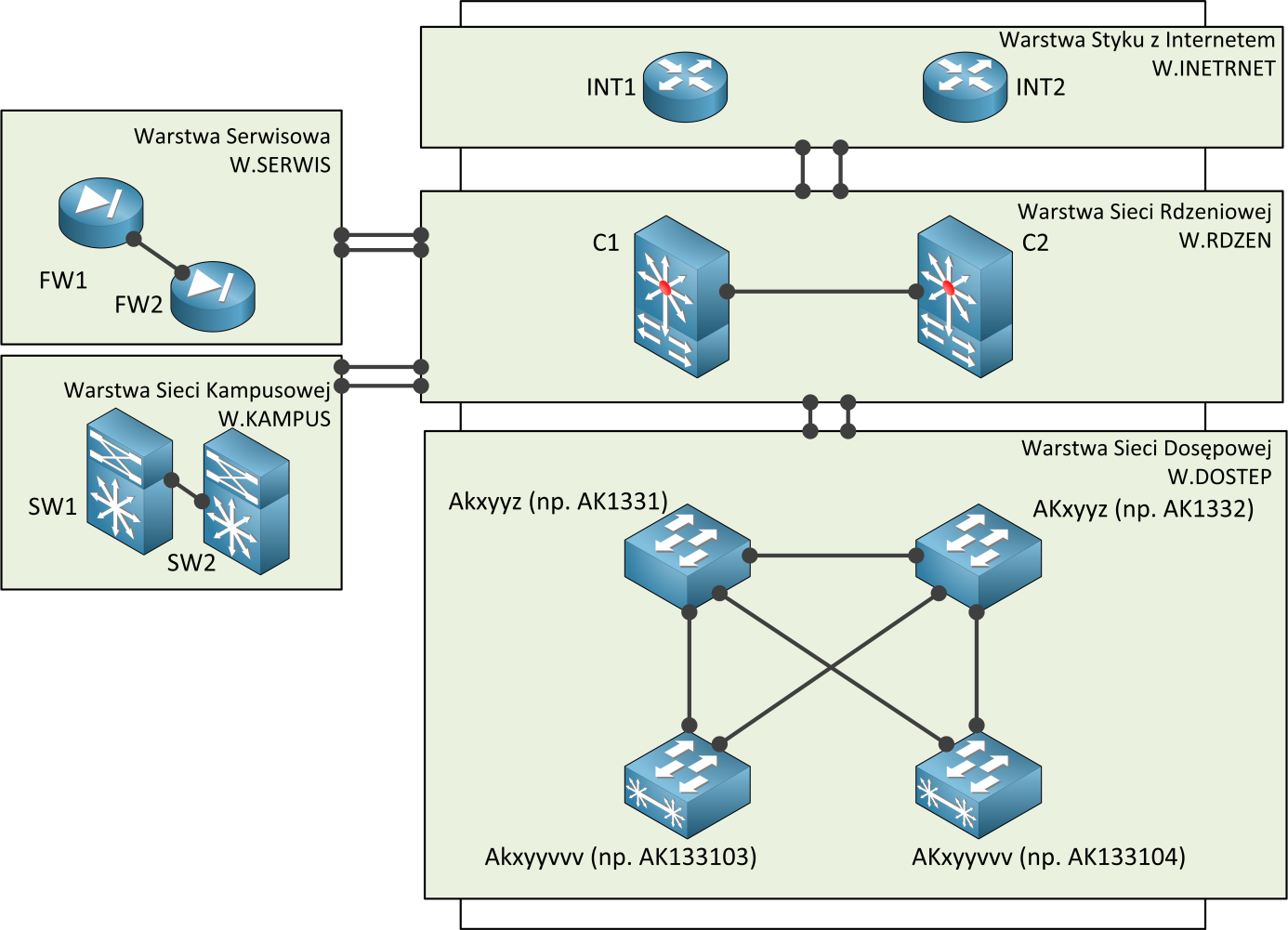
## Zestawienie urządzeń podlegających dostawie

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Nazwa Urządzenia | Liczba | Opis Wymagań |
| 1. | Urządzenie rdzeniowe | 2 | 2.9.1 |
| 2. | Przełącznik dostępowy | 4 | 2.9.2 |
| 3. | Moduł wyniesiony przełącznika dostępowego | 40 | 2.9.2 |
| 4. | Zapora ogniowa | 2 | 2.9.4 |
| 5. | Urządzenie brzegowe sieci | 2 | 2.9.3 |
| 6. | Przełącznik Campus (I) | 1 | 2.9.5 |
| 7. | Przełącznik Campus (II) | 1 | 2.9.6 |
| 8. | Przełącznik agregacji sieci zarządzającej | 1 | 2.9.7 |
| 9. | Przełącznik sieci zarządzającej | 4 | 2.9.8 |
| 10. | Koncentrator VPN sieci zarządzającej | 1 | 2.9.9 |
| 11. | Oprogramowanie do monitoringu parametrów sieciowych | 1 | 2.9.10 |
| 12. | Serwer wspierający zarządzanie siecią | 2 | 2.9.11 |
| 13. | System zarządzania i automatyzacji środowiska sieciowego | 1 | 2.9.12 |
| 14. | Platforma usług sieciowych | 2 | 2.9.13 |
| 15. | Przełącznik KVM 16 portów wraz z kompletem kabli | 2 | 2.9.14 |
| 16. | Serwer przełącznika KVM | 2 | 2.9.15 |
| 17. | Patchpanel światłowodowy realizujący funkcję dystrybucji (PPD) | 20 | 2.9.16 |
| 18. | Patchpanel światłowodowy realizujący funkcję agregacji (PPA) | 10 | 2.9.17 |
| 19. | Patchpanel światłowodowy realizujący funkcje rdzeniowe (PPR) | 2 | 2.9.18 |
| 20. | Kabel połączeniowy do patchpaneli światłowodowych – 35m | 4 | 2.9.19 |
| 21. | Kabel połączeniowy do patchpaneli światłowodowych – 25m | 12 | 2.9.19 |
| 22. | Kabel połączeniowy do patchpaneli światłowodowych – 10m | 10 | 2.9.19 |
| 23. | Kabel połączeniowy do patchpaneli światłowodowych – 5m | 8 | 2.9.19 |
| 24. | Patchcord jednomodowy dupleksowy LC/PC-LC/PC – 0.5m | 10 | 2.9.20 |
| 25. | Patchcord jednomodowy dupleksowy LC/PC-LC/PC – 3m | 6 | 2.9.20 |
| 26. | Patchcord wielomodowy dupleksowy LC/PC-LC/PC – 0,3m | 60 | 2.9.20 |
| 27. | Patchcord wielomodowy dupleksowy LC/PC-LC/PC – 0,5m | 50 | 2.9.20 |
| 28. | Patchcord wielomodowy dupleksowy LC/PC-LC/PC – 1m | 20 | 2.9.20 |
| 29. | Patchcord wielomodowy dupleksowy LC/PC-LC/PC – 3m | 20 | 2.9.20 |
| 30. | Patchcord RJ45 – 1m | 10 | - |
| 31. | Patchcord RJ45 – 3m | 30 | - |

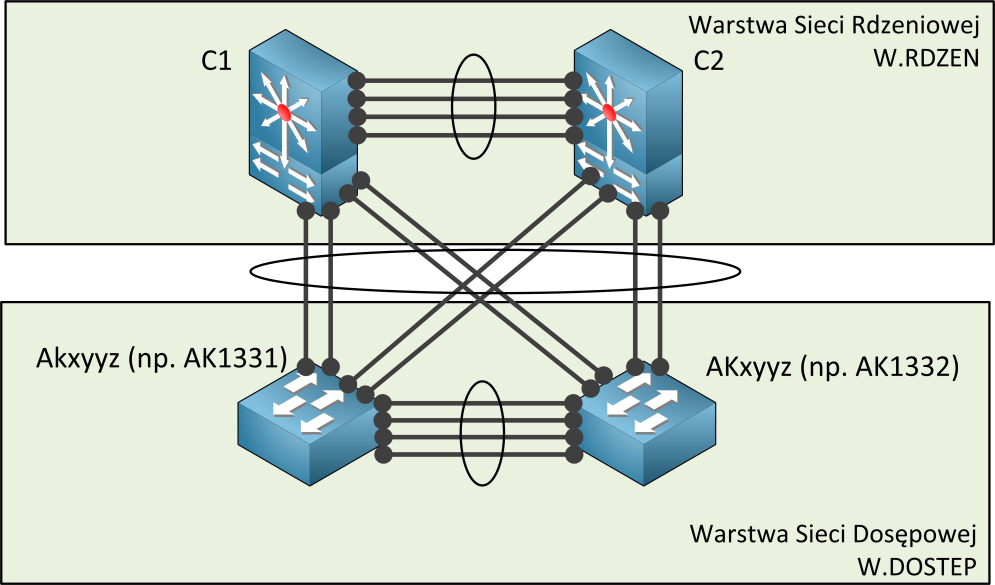
## Zestawienie czynności

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Opis Czynności | Obmiar | Uwagi |
| 1. | Dostawa, zamontowanie, uruchomienie i konfiguracja urządzenia rdzeniowego, wysokość do 21 U | 2 kpl. | Konfiguracja wg. 2.10.2.1 |
| 2. | Dostawa, zamontowanie, uruchomienie i konfiguracja przełącznika dostępowego | 4 kpl. | Konfiguracja wg. 2.10.2.2 |
| 3. | Dostawa, zamontowanie i uruchomienie modułu wyniesionego | 40 kpl. |  |
| 4. | Dostawa, zamontowanie, uruchomienie i konfiguracja zapory ogniowej, wysokość do 2U | 2 kpl. | Konfiguracja wg. 2.10.2.4 |
| 5. | Dostawa, zamontowanie, uruchomienie i konfiguracja urządzenia brzegowego sieci, wysokość do 2U | 2 kpl. | Konfiguracja wg. 2.10.2.3 |
| 6. | Dostawa, zamontowanie, uruchomienie i konfiguracja przełącznika kampusowego | 2 kpl. | Konfiguracja wg. 2.10.2.5 |
| 7. | Dostawa, zamontowanie, uruchomienie i konfiguracja przełącznika agregacji sieci zarządzającej, wysokość 1U | 1 kpl. | Konfiguracja wg. 2.10.2.6 |
| 8. | Dostawa, zamontowanie, uruchomienie i konfiguracja przełącznika sieci zarządzającej, wysokość 1U | 4 kpl. | Konfiguracja wg. 2.10.2.6 |
| 9. | Dostawa, zamontowanie, uruchomienie i konfiguracja koncentratora VPN sieci zarządzającej | 1 kpl. | Konfiguracja wg. 2.10.2.6 |
| 10. | Dostawa, zamontowanie, uruchomienie i konfiguracja serwera wspierającego zarządzanie siecią wraz z niezbędnymi systemami operacyjnymi, wysokość 1U | 2 kpl. | Konfiguracja wg. 2.10.2.6 |
| 11. | Dostawa, zamontowanie, uruchomienie i konfiguracja platformy usług sieciowych, wysokość 1U | 2 kpl. | Konfiguracja wg. 2.10.2.6 |
| 12. | Dostawa, zamontowanie, uruchomienie i konfiguracja systemu zarządzania i automatyzacji środowiska sieciowego, wysokość 1U | 1 kpl. | Konfiguracja wg. 2.10.2.6 |
| 13. | Uruchomienie i konfiguracja oprogramowanie do monitoringu parametrów sieciowych | 1 kpl. | K Konfiguracja wg. 2.10.2.6 |
| 14. | Dostawa, zamontowanie, uruchomienie i konfiguracja przełącznika KVM 16 portów wraz z kompletem kabli | 2 kpl. |  |
| 15. | Dostawa, zamontowanie, uruchomienie i konfiguracja serwera przełącznika KVM | 2 kpl. |  |
| 16. | Dostawa, zamontowanie i podłączenie patchpanela światłowodowego | 32 kpl. |  |
| 17. | Dostawa, położenie kabla połączeniowego oraz podłączenie kabla do odpowiednich patchpaneli światłowodowych | 30 kpl. |  |
| 18. | Wykonanie krosowania pomiędzy dostarczonymi patchpanelami a określonymi urządzeniami sieciowymi | 1 kpl. |  |
| 19. | Opracowanie planu wdrożenia | 1 kpl. | Opis w punkcie 2.10.1 |
| 20. | Wykonanie testów akceptacyjnych | 1 kpl. | Opis w punkcie 2.11.1 |
| 21. | Przeprowadzenie szkoleń | 1 kpl. | Opis w punkcie 2.12 |

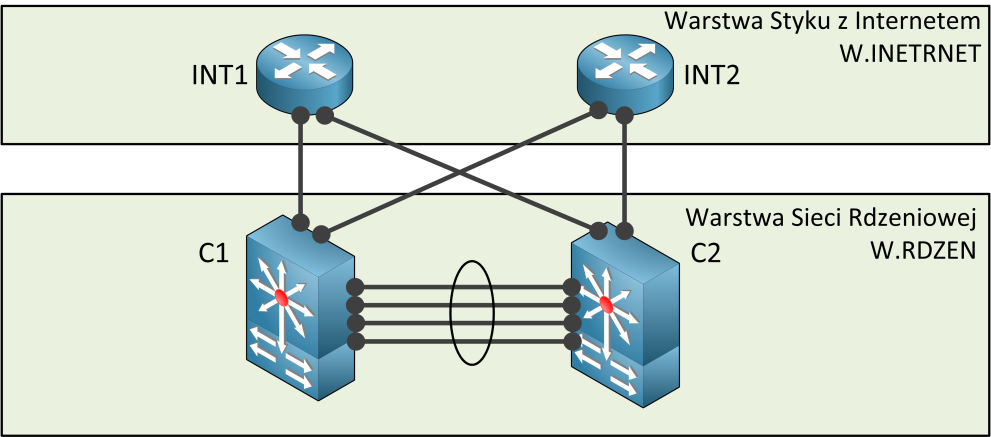
# Rysunki



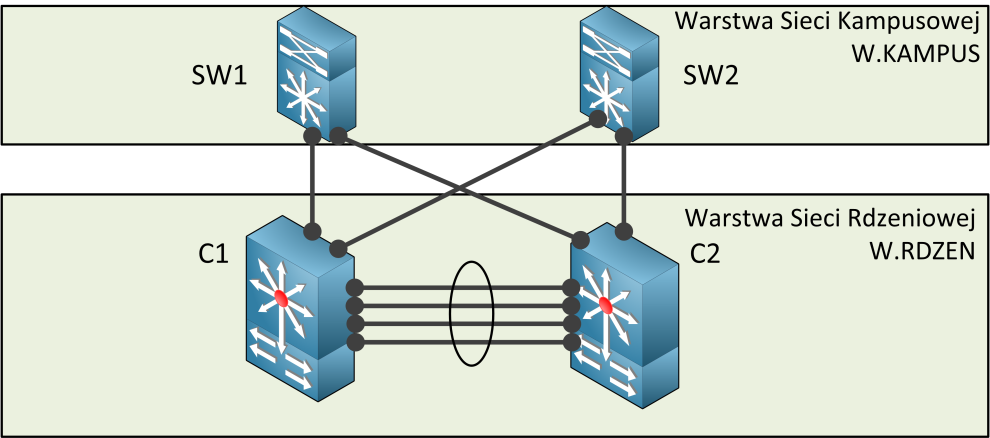
Rysunek 1. Struktura warstwowa sieci DC EXEA



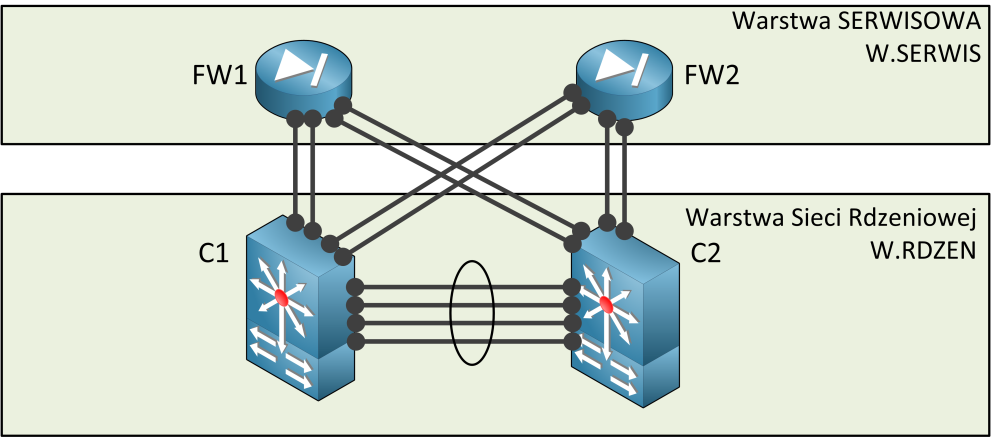
Rysunek 2. Schemat połączeń pomiędzy urządzeniami W.RDZEN a W.DOSTEP



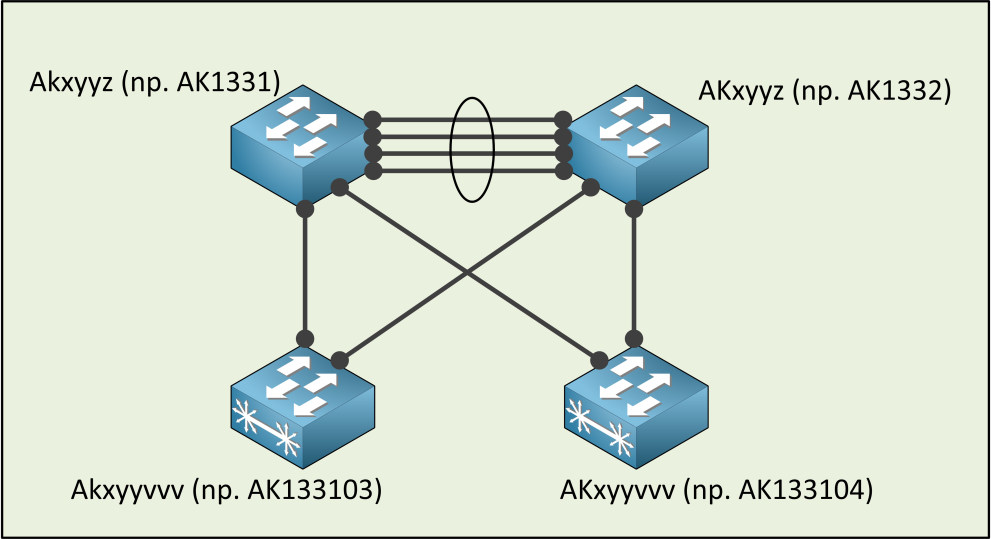
Rysunek 3. Schemat połączeń pomiędzy urządzeniami W.RDZEN a W.INTERNET



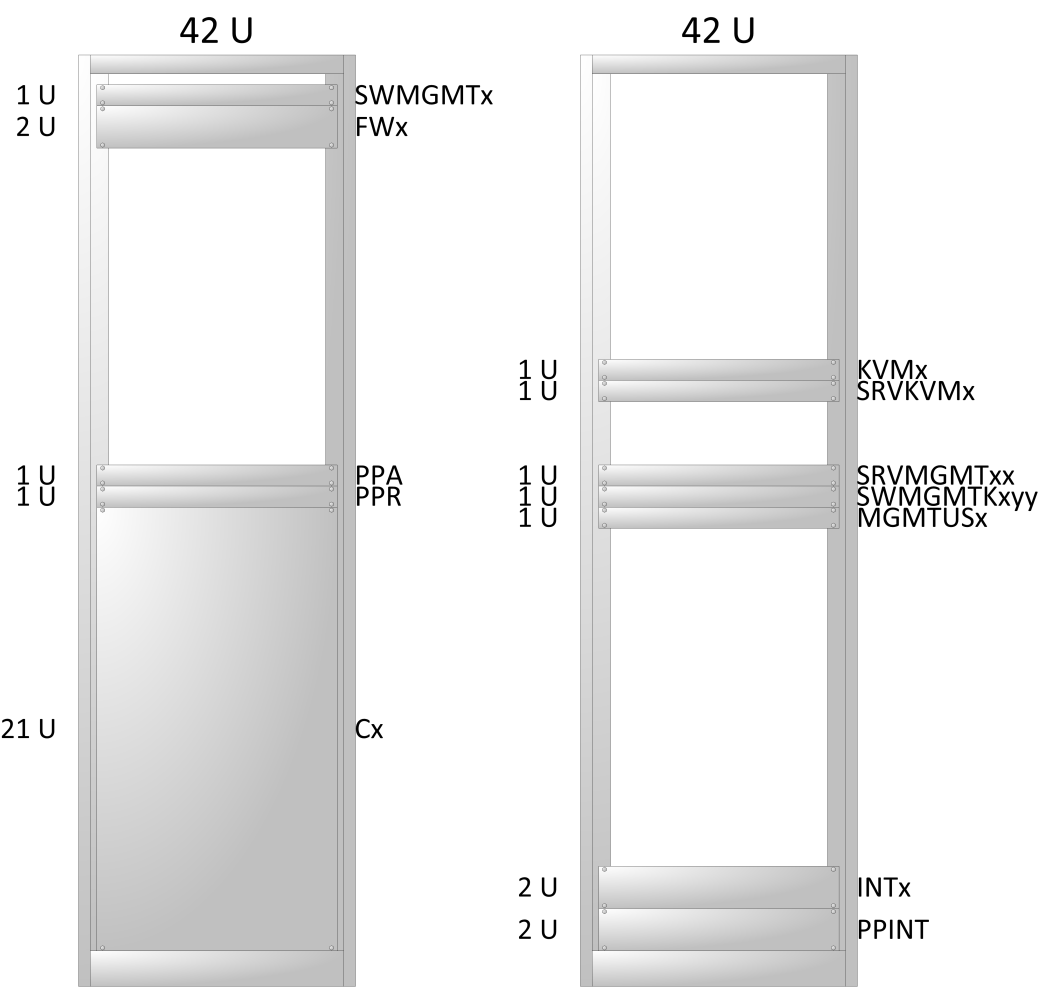
Rysunek 4. Schemat połączeń pomiędzy urządzeniami W.RDZEN a W.KAMPUS



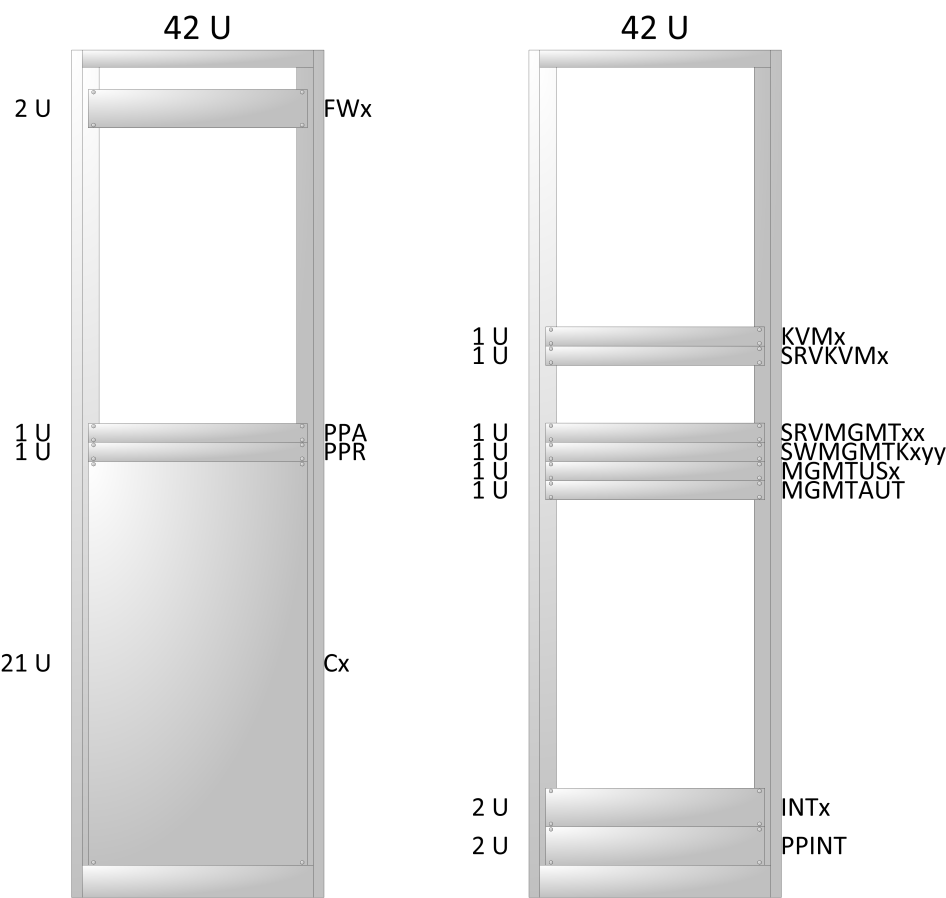
Rysunek 5. Schemat połączeń pomiędzy urządzeniami W.RDZEN a W.SERWIS



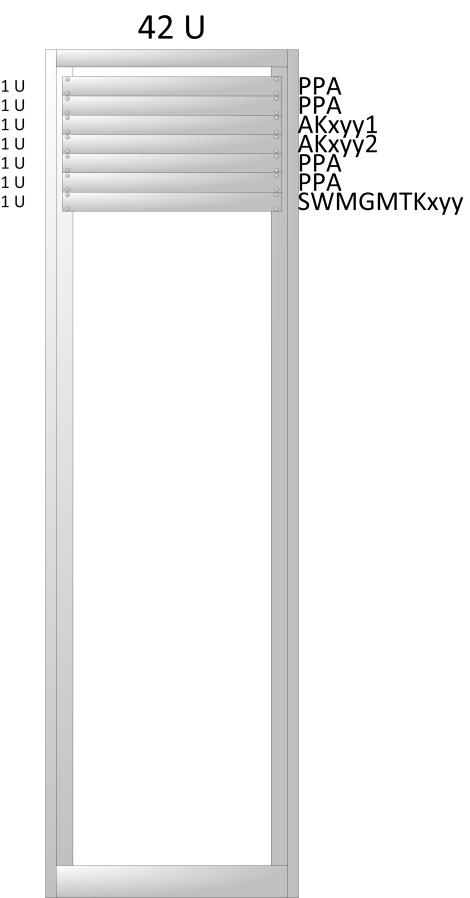
Rysunek 6. Schemat połączeń pomiędzy urządzeniami wewnątrz W.DOSTEP



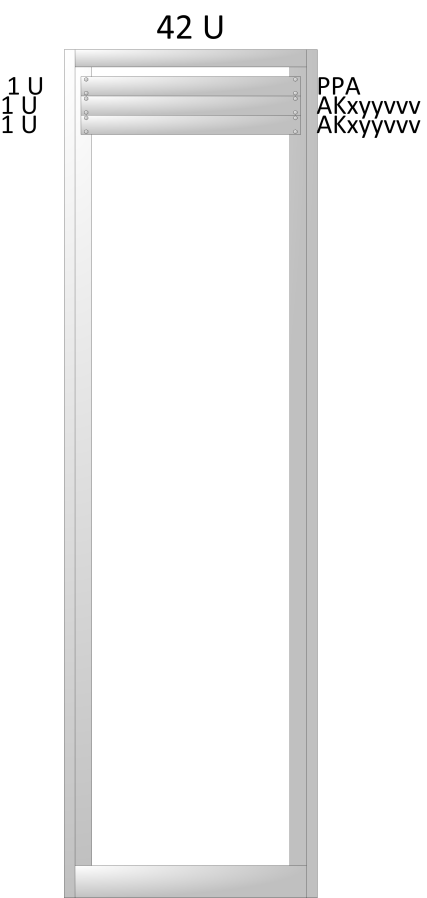
Rysunek 7. Rozmieszczenie urządzeń w blokach GPD1



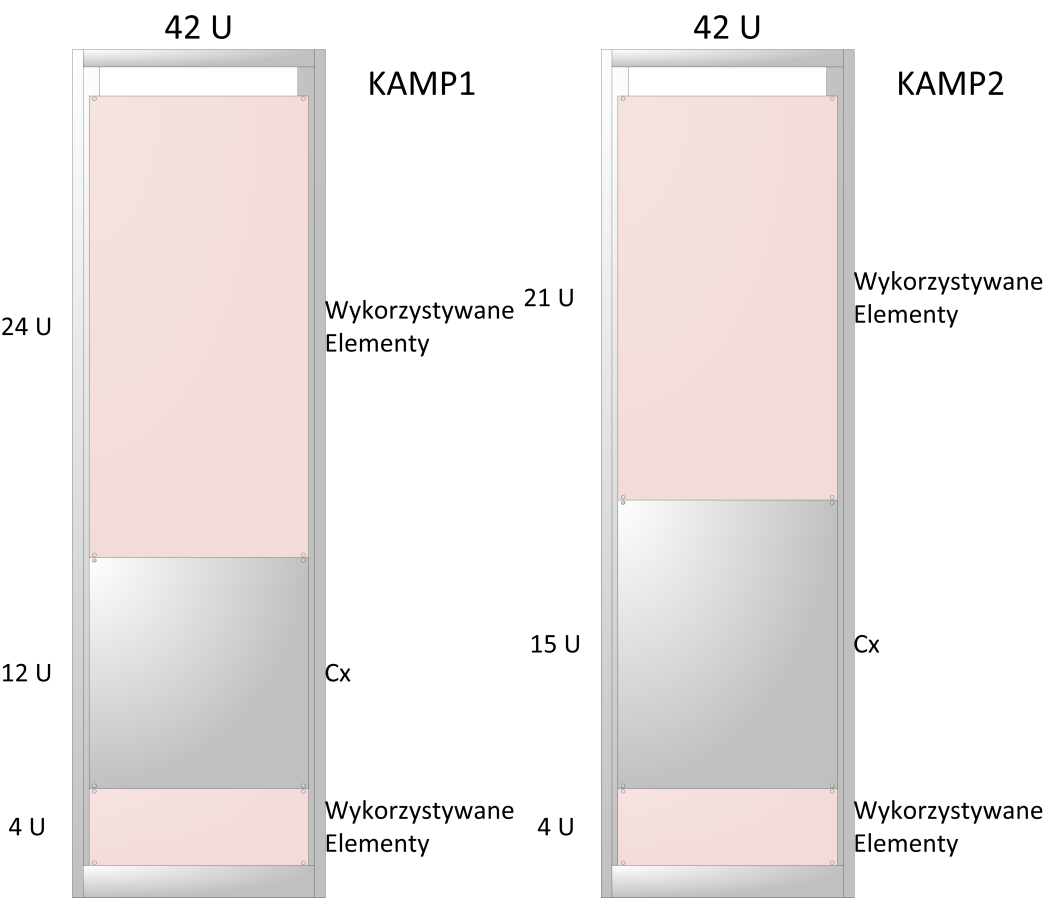
Rysunek 8. Rozmieszczenie urządzeń w blokach GPD2



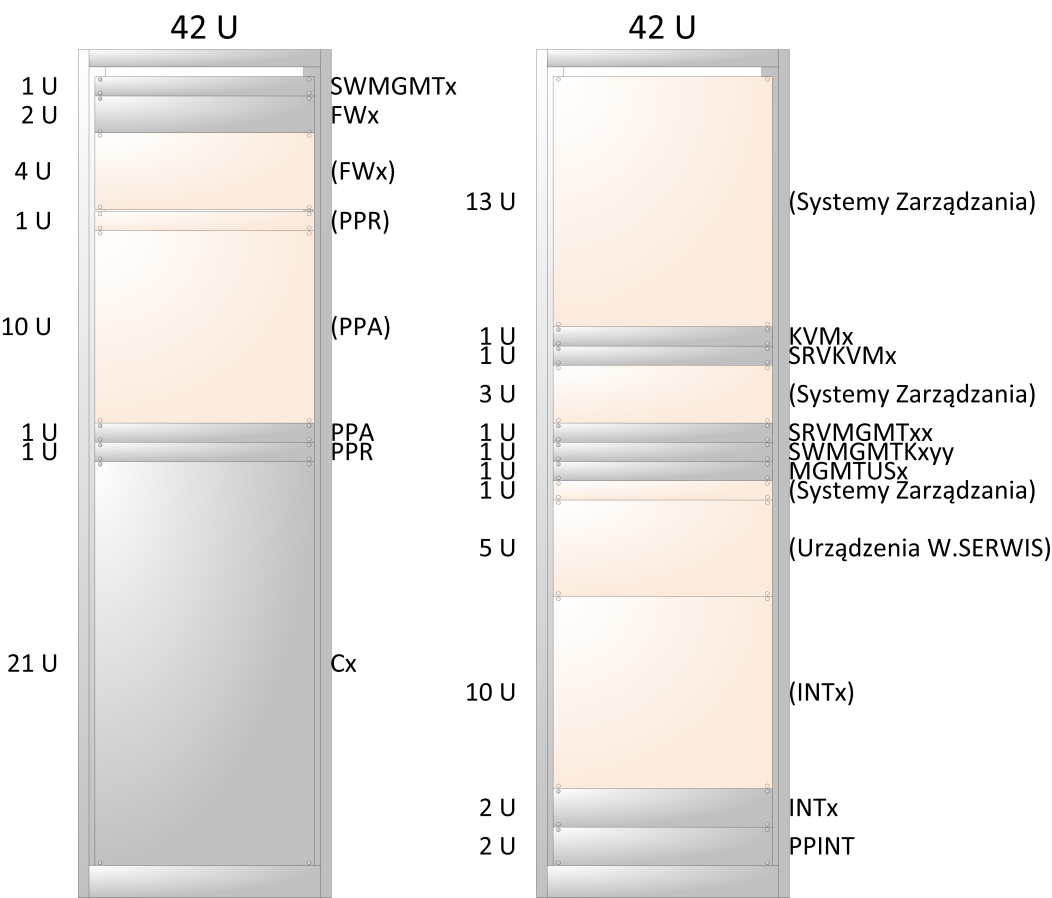
Rysunek 9. Rozmieszczenie urządzeń w blokach EoR



Rysunek 10. Rozmieszczenie urządzeń w blokach ToR



Rysunek 11. Rozmieszczenie urządzeń w blokach KAMPx



Rysunek 12. Plan zabudowy punktu GPDx przy pełnym obłożeniu DC