SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ XVII - POWIAT TRZEBNICKI

Załącznik A17

Postępowanie prowadzone w trybie przetargu nieograniczonego na:

**„Zakup, instalacje i konfiguracje sprzętu komputerowego wraz z oprogramowaniem systemowym i bazodanowym oraz dostawa i wdrożenie wybranych e-usług publicznych wraz z budową POK w 23 JST”**

**w ramach projektu:   
„PLATFORMA ELEKTRONICZNYCH USŁUG GEODEZYJNYCH - PEUG”**

**Działanie 2.1. E-usługi publiczne**

**Regionalny Program Operacyjny Województwa Dolnośląskiego na lata 2014-2020**

Spis treści

[Spis Tabel 2](#_Toc511131097)

[Spis Ilustracji 2](#_Toc511131098)

[1. DIAGNOZA STANU OBECNEGO 3](#_Toc511131099)

[1.1. System PZGiK 3](#_Toc511131100)

[1.2. Zasoby sprzętowo-programowe 3](#_Toc511131101)

[1.3. Zestawienie wdrożonych e-usług w ramach Systemu PZGiK 3](#_Toc511131102)

[2. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIANIA DLA CZĘSCI XVII 4](#_Toc511131103)

[2.1. Infrastruktura sprzętowo-programowa 4](#_Toc511131104)

[2.2. Wymagania – parametry techniczne 5](#_Toc511131105)

[2.2.1. Architektura serwera bazodanowo - aplikacyjnego 5](#_Toc511131106)

[2.2.2. Serwer bazodanowo – aplikacyjny 6](#_Toc511131107)

[2.2.3. Macierz dyskowa – 12 dysków 10](#_Toc511131108)

[2.2.4. Zasilacz awaryjny (UPS) 13](#_Toc511131109)

[2.2.5. Zintegrowane zapory sieciowe 14](#_Toc511131110)

[2.2.6. Przełącznik sieciowy 17](#_Toc511131111)

[2.3. Oprogramowanie 21](#_Toc511131112)

[2.3.1. Środowiska bazodanowe 21](#_Toc511131113)

# Spis Tabel

[Tabela 1 System PZGiK w PODGiK 3](#_Toc511131114)

[Tabela 2 Silnik bazy danych 3](#_Toc511131115)

[Tabela 3 Aktualny stan e-usług udostępnianych w ramach posiadanego Systemu PZGiK 4](#_Toc511131116)

[Tabela 4 Wykaz sprzętu objętego zamówieniem 5](#_Toc511131117)

# Spis Ilustracji

[Rysunek 1 Architektura środowiska bazodanowo – aplikacyjnego active/passive. Opracowanie własne. 5](#_Toc511131118)

# DIAGNOZA STANU OBECNEGO

Poniżej przedstawiono analizę stanu obecnego w zakresie zasobów sprzętowo - programowych, które zostaną wykorzystane przy realizacji zamówienia.

## System PZGiK

Obecnie w powiecie trzebnickim funkcjonuje System PZGiK Ewid2007 (TurboEwid) – Geomatyka Kraków.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Powiat** | **System PZGiK funkcjonujący**  **w Jednostce do prowadzenia bazy GESUT, BDOT500, EGiB** |
| **17** | **trzebnicki** | Ewid 2007 (TurboEwid) - Geomatyka Kraków |

Tabela System PZGiK w PODGiK

EWID2007 firmy Geomatyka Kraków s.c. z desktopowym interfejsem aplikacyjnym TurboEWID oraz sieciowym interfejsem aplikacyjnym WebEWID jest Systemem PZGiK w pełni dostosowanym do najnowszych przepisów wykonawczych Ustawy PGiK. Jest dostosowany do obowiązującego modelu pojęciowego danych oraz do prowadzenia wszystkich zbiorów danych powiatowej części PZGiK (EGiB, RCiWN, BDOT500, GESUT, BDSOG) w postaci jednej zintegrowanej bazy danych. EWID2007 umożliwia eksport i import danych w formatach GML i SWDE oraz własnym natywnym formacie KCD. Umożliwia także aktualizację danych wraz z rejestracją historii zmian na podstawie plików przyrostowych (różnicowych) w formatach: GML i SWDE.

## Zasoby sprzętowo-programowe

W ramach realizacji niniejszego zamówienia planuje się wykorzystanie zasobów sprzętowo-programowych. Poniżej przedstawiony został wykaz posiadanych elementów infrastruktury teleinformatycznej, które zostaną wykorzystane przy realizacji zamówienia.

|  |  |
| --- | --- |
| **Nazwa powiatu** | **Rozwiązania bazodanowe** |
| Powiat trzebnicki | Oracle |

Tabela Silnik bazy danych

## Zestawienie wdrożonych e-usług w ramach Systemu PZGiK

Aktualnie w powiecie trzebnickim w PODGiK zostały wdrożone głównie e-usługi na 3 i 4 poziomie dojrzałości. Szczegółowy wykaz e-usług przedstawiono w poniższej tabeli:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Lp. | Nazwa e-usługi | Poziom 1 | Poziom 2 | Poziom 3 | Poziom 4 | Brak  e-usługi |
| 1 | Przyjęcie wniosku o aktualizację informacji zawartych w ewidencji gruntów i budynków zgodnie z art.24 ust.2b pkt.1, ppkt.h - PGiK |  |  | x |  |  |
| 2 | Przyjęcie wniosku o przeprowadzenie aktualizacji klasyfikacji gruntów |  |  | x |  |  |
| 3 | Przyjęcie wniosku o udostępnienie mapy ewidencji gruntów i budynków |  |  |  | x |  |
| 4 | Przyjęcie wniosku o udostępnienie mapy zasadniczej |  |  |  | x |  |
| 5 | Przyjęcie wniosku o udostępnienie rejestrów, kartotek, skorowidzów, wykazów, zestawień tworzonych z baz danych EGiB |  |  |  | x |  |
| 6 | Przyjęcie wniosku o udostępnienie w postaci elektronicznej zbiorów danych zgodnie z art.40a ust.2 pkt 4 a i b - PGiK |  |  | x |  |  |
| 7 | Przyjęcie wniosku o udostępnienie zbiorów danych bazy BDOT500 |  |  |  | x |  |
| 8 | Przyjęcie wniosku o udostępnienie zbiorów danych bazy BDSOG |  |  |  | x |  |
| 9 | Przyjęcie wniosku o udostępnienie zbiorów danych bazy EGiB |  |  |  | x |  |
| 10 | Przyjęcie wniosku o udostępnienie zbiorów danych bazy GESUT |  |  |  | x |  |
| 11 | Przyjęcie wniosku o udostępnienie zbiorów danych bazy RCiWN |  |  |  | x |  |
| 12 | Przyjęcie wniosku o ujawnienie lub wykreślenie w EGiB umów dzierżawy |  |  | x |  |  |
| 13 | Przyjęcie wniosku o wydanie wypisu lub wypisu i wyrysu lub wyrysu z ewidencji gruntów i budynków |  |  |  | x |  |
| 14 | Przyjęcie wniosku w sprawie koordynacji usytuowania projektowanych sieci uzbrojenia terenu |  |  | x |  |  |
| 15 | Przyjęcie wniosku w sprawie zgłoszenia lub uzupełnienia pracy geodezyjnej/kartograficznej |  |  | x |  |  |
| 16 | Przyjęcie wniosku zgłoszenia zmian danych ewidencji gruntów i budynków zgodnie z art.22 ust.2 - PGiK |  |  | x |  |  |
| 17 | Uwierzytelnienie dokumentów opracowanych przez wykonawcę prac geodezyjnych/kartograficznych |  |  |  | x |  |
| 18 | Zawiadomienie o wykonaniu zgłoszonych prac geodezyjnych/kartograficznych |  |  | x |  |  |
| 19 | Usługa udostępniania materiałów powiatowego zasobu geodezyjnego i kartograficznego |  |  |  | x |  |

Tabela Aktualny stan e-usług udostępnianych w ramach posiadanego Systemu PZGiK

# SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIANIA DLA CZĘSCI XVII

## Infrastruktura sprzętowo-programowa

W ramach realizacji projektu Wykonawca zobowiązany jest dostarczyć następujące elementy infrastruktury sprzętowej wraz z oprogramowaniem systemowym i narzędziowym:

|  |  |  |
| --- | --- | --- |
| Lp. | Nazwa | Ilość |
| - | **-** | **trzebnicki** |
| 1. | Serwery bazodanowo - aplikacyjne | 1 |
| 2. | Macierze dyskowe - 12 dysków | 1 |
| 3. | Zasilacze awaryjne | 1 |
| 4. | Zintegrowane zapory sieciowe | 1 |
| 5. | Przełączniki sieciowe | 1 |
| 6. | Środowiska bazodanowe | 1 |

Tabela Wykaz sprzętu objętego zamówieniem

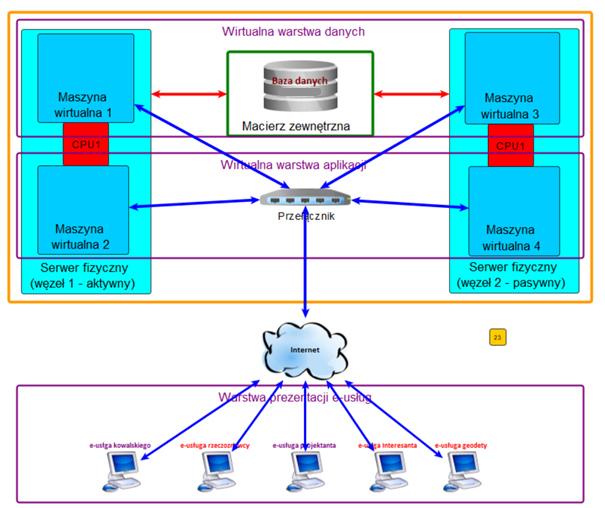
Miejsce dostarczenia wyżej wymienionych elementów infrastruktury sprzętowej wraz z oprogramowaniem systemowym i narzędziowym:

ul. Leśna 1,

55-100 Trzebnica

* 1. Wymagania – parametry techniczne
     1. Architektura serwera bazodanowo - aplikacyjnego

W serwerze należy zastosować mechanizm wirtualizacji, który pozwala na budowę maszyny wirtualnej dla środowiska bazy danych, pracującego w układzie Active / Passive. Poniżej przedstawiono schemat ideowy klastra:



*Rysunek 1 Architektura środowiska bazodanowo – aplikacyjnego active/passive. Opracowanie własne.*

* + 1. Serwer bazodanowo – aplikacyjny

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.001** |
| **Serwer:** Wymaga się, aby serwer byłzłożony z maszyny w której skład wchodzą co najmniej 2 procesory fizyczne. Wymaga się zachowania poprawności licencjonowania środowisk bazodanowych z dostarczeniem odpowiedniej liczby licencji. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.002** |
| **Typ obudowy**: Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.003** |
| Serwer musi być dostosowany do parametrów funkcjonującego Systemu PZGiK, ilości gromadzonych danych, liczby transakcji generowanych przez system, zapasu zakładającego wzrost obciążenia w ramach platformy POK. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.004** |
| **Płyta główna**: Wymaga się, aby płyta główna miała możliwość zainstalowania odpowiedniej liczby procesorów. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.005** |
| **Chipset:** Dedykowany przez producenta procesora do pracy w serwerach o odpowiedniej liczbie procesorów. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.006** |
| **Procesor:** Zainstalowana odpowiednia liczba procesorów szesnasto-rdzeniowych klasy x86 dedykowanych do pracy z zaoferowanym serwerem umożliwiających osiągnięcie wyniku min. 1690 punktów w teście SPECint\_rate\_base2006 dostępnym na stronie www.spec.org dla dwóch procesorów. Należy załączyć wydruk ze strony internetowej potwierdzający osiągniecie wyniku. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.007** |
| Serwer musi posiadać zainstalowaną kartę SAS HBA posiadającą 8 zew. portów (dwa złącza typu Mini-SAS HD). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.008** |
| **Pamięć RAM**: Minimum 128GB DDR4 RDIMM min. 2666MT/s, w kościach min. 64GB. Na płycie głównej musi znajdować się minimum 12 slotów przeznaczonych do instalacji pamięci. Płyta główna musi obsługiwać co najmniej 1.5TB pamięci RAM. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.009** |
| **Zabezpieczenia pamięci RAM**: Memory Rank Sparing, Memory Mirror, SDDC lub mechanizmem ECC. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.010** |
| **Gniazda PCI**: Minimum 4 sloty x8 generacji 3. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.011** |
| **Interfejsy sieciowe:** Wbudowane minimum dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz minimum dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.012** |
| **Dyski twarde:**   * Możliwość instalacji dysków SATA, SAS, SSD. * Zainstalowane co najmniej 2x300GB SAS 12Gb/s 10krpm. * Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia modułu w 2 jednakowe nośniki typu flash o pojemności min. 64GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.013** |
| **Kontroler RAID:** Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.014** |
| **Wbudowane porty:** min. 3 porty USB 2.0, min. 2 porty USB 3.0, min. 4 porty RJ45, min. 1 port VGA, min. 1 port RS232.  Nie dopuszcza się stosowania przejściówek, adapterów oraz rozgałęziaczy i przedłużaczy. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.015** |
| Wymagane jest, aby urządzenie posiadało zintegrowaną **kartę graficzną** umożliwiającą wyświetlanie obrazu w rozdzielczości min. 1920x1200. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.016** |
| Wymaga się, aby były zainstalowane redundantne wentylatory z funkcją pozwalająca na wymianę/podłączenie urządzenia bez konieczności wyłączania/restartowania całego systemu (*Hot swap*).  Wymagany jest nadmiarowy układ chłodzenia (redundancja typu N+1). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.017** |
| Wymaga się, aby były zainstalowane min. 2 kontrolery SAS-HBA do nadmiarowego połączenia z macierzą dyskową. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.018** |
| **Zasilacze:** Minimum dwa zasilacze z możliwością wymiany w trakcie pracy (*Hot swap*).  Wymagany jest nadmiarowy układ chłodzenia (redundancja typu N+1). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.019** |
| Wymaga się, aby urządzenie było wyposażone w kartę zarządzającą wraz z oprogramowaniem zarządzającym, niezależną od zainstalowanego na serwerze systemu operacyjnego posiadającą dedykowany port RJ-45 Gigabit Ethernet umożliwiającą:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika; * możliwość podmontowania zdalnych wirtualnych napędów; * wirtualną konsolę z dostępem do myszy, klawiatury; * wsparcie dla IPv6; * wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; * integracja z Active Directory; * możliwość obsługi przez dwóch administratorów jednocześnie; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; * możliwość podłączenia lokalnego poprzez złącze RS-232.; * możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy; * możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, jak również musi posiadać możliwość konfiguracji wyłączania lub włączania poszczególnych wentylatorów; * możliwość zablokowania konfiguracji oraz odnowienia oprogramowania karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.020** |
| Wymaga się, aby dostarczono dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć i spełniające minimalne wymagania:   * wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; * możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; * wsparcie dla protokołów– WMI, SNMP, IPMI, Linux SSH; * możliwość oskryptowywania procesu wykrywania urządzeń; * możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; * szczegółowy opis wykrytych systemów oraz ich komponentów; * możliwość eksportu raportu do CSV, HTML; * grupowanie urządzeń w oparciu o kryteria użytkownika; * możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach; * automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; * podgląd stanu środowiska; * podsumowanie stanu dla każdego urządzenia; * szczegółowy status urządzenia/elementu/komponentu; * generowanie alertów przy zmianie stanu urządzenia; * filtry raportów umożliwiające podgląd najważniejszych zdarzeń; * integracja z service desk producenta dostarczonej platformy sprzętowej; * możliwość przejęcia zdalnego pulpitu; * możliwość podmontowania wirtualnego napędu; * kreator umożliwiający dostosowanie akcji dla wybranych alertów; * możliwość importu plików MIB; * przesyłanie alertów „as-is” do innych konsol firm trzecich; * możliwość definiowania ról administratorów; * możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów; * aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); * możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; * możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; * moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informacje o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych; * możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.021** |
| **Bezpieczeństwo:**   * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.022** |
| **Warunki gwarancji:**  Gwarancja realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. W przypadku eskalacji zgłoszenia serwisowego producent jest zobowiązany zapewnić dedykowanego opiekuna technicznego, zdalnie koordynującego prace serwisowe. Zamawiający wymaga dostarczenia przez producenta miesięcznych raportów dotyczących częstotliwości występowania usterek, jakości i terminowości wykonywanych napraw, zaleceń dotyczących instalacji nowych sterowników oraz mikrokodu urządzenia.  Wymaga się zapewnienia możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.  W ramach gwarancji musi być dostępna ogólnopolska, telefoniczna infolinia/linia techniczna producenta sprzętu, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.023** |
| **Dokumentacja użytkownika:**   * Zamawiający wymaga dostarczenia dokumentacji w języku polskim; * Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.024** |
| Wymagane jest zapewnienie możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.025** |
| Serwer musi posiadać deklarację CE. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.026** |
| Oferowany serwer musi posiadać status „Certified for Windows” dla systemów: Microsoft Windows 2012 x64, Microsoft Windows 2012R2 x64, Windows Server 2016 x64. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 01.027** |
| Wymagania na serwerowy system operacyjny znajdują się w części wspólnej SOPZ w rozdziale *8.2 Oprogramowanie systemowe*. | |

* + 1. Macierz dyskowa – 12 dysków

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.001** |
| Wymaga się, aby macierz dyskowa posiadała architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez zainstalowane kontrolery i dyski. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.002** |
| **Typ obudowy**: Wymaga się, aby obudowa była dedykowana do zamontowania w szafie rack 19”, maksymalna wysokość 4U RACK, wraz z wszystkimi elementami niezbędnymi do zamontowania w szafie i organizatorem kabli.  Obudowa musi posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii macierzy. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.003** |
| Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia zapewniający ciągłą pracę macierzy bez ograniczeń czasowych i wydajnościowych w przypadku utraty nadmiarowości w danym układzie (zasilania lub chłodzenia). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.004** |
| Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active lub ALUA. Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.005** |
| Wymaga się, aby macierz była wyposażona w minimum 4 porty 12 Gb SAS per kontroler służące do podłączania hostów oraz 4 porty 10GbE lub 16Gb FC. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.006** |
| Wymaga się, aby macierz zawierała łącznie minimum 12 dysków 2,5” SAS o pojemności łącznej minimum 28 TB i prędkości obrotowej minimum 10k RPM. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.007** |
| Wymagana jest możliwość rozbudowy macierzy (bez wymiany kontrolerów macierzy) do co najmniej 144 dysków twardych oraz możliwość rozbudowy macierzy do modelu wyższego (mocniejsze procesory, większa ilość Cache) bez potrzeby zakupu nowych półek dyskowych w tym bez potrzeby migracji danych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.008** |
| Dwa kontrolery macierzy muszą być wyposażone w przynajmniej 8GB pamięci podręcznej Cache każdy.  W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów, muszą być zabezpieczone metodą trwałego zapisu na dysk lub nośnik nie wymagający korzystania z podtrzymania jego zasilania. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.009** |
| Wymagane jest zapewnienie wsparcia dla grup dyskowych RAID: 0, 1, 5, 6, 10.  Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 180 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych NL-SAS.  Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 i RAID6 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.010** |
| Oferowany system dyskowy musi być dostarczony z wstępnie skonfigurowanym RAID 10. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.011** |
| Wymaga się, aby macierz nie posiadała pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w tym: kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.012** |
| Wymaga się, aby macierz dyskowa posiadała dedykowane minimum 4 interfejsy RJ-45 Ethernet obsługujące połączenia z prędkością 100Mb/s i 1Gb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.013** |
| Każdy kontroler macierzy musi pozwalać na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC SAN.  Dla obsługi operacji blokowych I/O w sieci IP/FC SAN kontrolery macierzy muszą wspierać protokoły transmisji: FC, iSCSI, SAS 12G, a ich obsługa odbywa się jednocześnie. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.014** |
| Wymaga się, aby macierz obsługiwała - dla interfejsów iSCSI i interfejsów obsługujących protokoły CIFS i NFS - adresacje IP v.4. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.015** |
| Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.016** |
| Macierz musi zapewniać możliwość szyfrowania danych. Realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.  Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.017** |
| Macierz musi wspierać mieszaną konfigurację dysków SAS, NearLine-SAS i SSD w obrębie każdego pojedynczego modułu obudowy pozwalającego na instalacje dysków hot-plug. Model macierzy pozwala na instalację dysków hot-plug w formacie 2,5” i 3,5”. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.018** |
| Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS).  Zdalne zarządzanie macierzą musi odbywać się bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora.  Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.019** |
| Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego, kontrolerów RAID i dysków bez konieczności wyłączania macierzy i bez konieczności wyłączania ścieżek logicznych FC/iSCSI dla podłączonych serwerów. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.020** |
| Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji: powiększania grup dyskowych, zwiększania rozmiaru woluminu, alokowania woluminu na inną grupę dyskową. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.021** |
| Wymaga się, aby macierz posiadała wsparcie dla co najmniej następujących systemów operacyjnych: Microsoft® Windows Server®, Red Hat Enterprise Linux®, Novell SUSE Linux Enterprise Server, Oracle® Solaris, HP HP-UX, IBM AIX. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.022** |
| Wymaga się, aby macierz posiadała funkcjonalność zdalnej replikacji danych - w trybie synchronicznym i asynchronicznym - po protokołach FC oraz IP bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji.  Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Niniejsza funkcjonalność nie powinna wymagać dostarczenia dodatkowych licencji. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.023** |
| Wymaga się, aby macierz umożliwiała rozproszenie alokacji danych dla pojedynczego woluminu LUN na maksymalnej liczbie obsługiwanych dysków HDD. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.024** |
| Wymaga się, aby macierz obsługiwała mechanizmy Thin Provisioning czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy. Jeżeli taka funkcjonalność wymaga dodatkowych licencji to winno się je dostarczyć wraz z macierzą dla maksymalnej pojemności dyskowej oferowanej macierzy. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.025** |
| Wymaga się, aby model oferowanej macierzy wspierał rozwiązania klasy „wysokiej dostępności”, tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych protokołem FC pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych” należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 02.026** |
| Wymaga się, aby mechanizm AST lub SSD Cache był obsługiwany przy korzystaniu z co najmniej dwóch dostarczonych technologii dyskowych: SSD z SAS lub SSD z NL-SAS. | |

## Zasilacz awaryjny (UPS)

|  |  |
| --- | --- |
| **Identyfikator** | **WF 03.001** |
| Topologia pracy: Line Interactive | |
| Konfiguracja UPS: 1/1 | |

|  |  |  |
| --- | --- | --- |
| **Identyfikator** | **WF 03.002** | |
| **Parametry wejściowe:** | | |
| Nominalne napięcie wejściowe | | 230 V |
| Zmienny zakres napięcia wejściowego w trybie podstawowym | | 140 – 280 V |
| Częstotliwość wejściowa | | 50-60 Hz |
| Kształt prądu wejściowego | | sinusoidalny |
| Typ gniazda wejściowego | | IEC-320 C20,  Schuko CEE 7/ EU1-16P |

|  |  |  |
| --- | --- | --- |
| **Identyfikator** | **WF 03.003** | |
| **Parametry wyjściowe:** | | |
| Znamionowa moc wyjściowa (VA / W) | | 3,0 kVA/2,7 kW |
| Znamionowe napięcie wyjściowe | | 230V |
| Znamionowa częstotliwość wyjściowa | | 50/60 Hz |
| Tolerancja częstotliwości przy pracy z baterii | | +/- 3Hz |
| Kształt napięcia wyjściowego | | sinusoidalny |
| Typowy czas podtrzymania akumulatorowego przy 50% obciążenia (w min) | | 18,0 |
| Typowy czas podtrzymania akumulatorowego przy pełnym obciążeniu (w min) | | 6,0 |
| Awaryjny wyłącznik zasilania | | TAK |
| Gniazda wyjściowe | | 8 x IEC 320 C13 1 x IEC 320 C19 |

|  |  |  |
| --- | --- | --- |
| **Identyfikator** | **WF 03.004** | |
| **Parametry akumulatorów i czas podtrzymania:** | | |
| Przewidywana żywotność baterii | | min. 3 lata |
| Automatyczna regulacja napięcia (AVR) z funkcją korekcji niskich i wysokich napięć | | TAK |
| Powiadomienie o awarii akumulatora | | TAK |
| Bezpiecznik automatyczny | | TAK |
| Bez narzędziowa wymiana baterii „na gorąco” bez konieczności wyłączania zasilacza UPS i odłączania sekcji DC | | TAK |

|  |  |  |
| --- | --- | --- |
| **Identyfikator** | **WF 03.005** | |
| **Kontrola i zarządzanie:** | | |
| Oprogramowanie zapewniające zarządzanie zasilaniem UPS przez sieć | | TAK |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 03.006** |
| **Parametry ogólne:** | |
| **Typ obudowy**: dedykowana do zamontowania w szafie RACK 19” maksymalna wysokość 2U RACK, wraz z wszystkimi elementami niezbędnymi do zamontowania w szafie i organizatorem kabli. Obudowa posiada wyświetlacz LCD z komunikatami sygnalizującymi informacje o stanie poprawnej pracy lub awarii. | |

* + 1. Zintegrowane zapory sieciowe

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.001** |
| Wymaga się, aby urządzenie sieciowe Firewall posiadało wysokość montażową ‘desktop’. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.002** |
| Urządzenie musi być wyposażone w minimum 4 GB pamięci RAM, pamięć Flash 8 GB oraz musi posiadać port konsoli. Urządzenie ma posiada także slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Rozwiązanie musi zapewniać opcje uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.003** |
| System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielone od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.004** |
| System operacyjny firewalla musi śledzić stan sesji użytkowników (ang. stateful processing), tworzyć i zarządzać tablicą stanu sesji. System musi mieć opcję przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.005** |
| Urządzenie musi być wyposażone w minimum 6 wbudowanych interfejsów Ethernet 10/100/1000 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.006** |
| Urządzenie Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy minimum 16 strefami bezpieczeństwa z wydajnością nie mniejszą niż 500 Mb/s liczoną dla ruchu IMIX. Firewall musi przetwarzać nie mniej niż 200 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall ma obsługiwać nie mniej niż 64 000 równoległych sesji oraz musi zestawiać nie mniej niż 5 000 nowych połączeń/sekundę. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.007** |
| Urządzenie Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN jest realizowany sprzętowo. Urządzenie Firewall musi obsługiwać nie mniej niż 256 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 100 Mb/s. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.008** |
| Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Wymaga się, aby urządzenie Firewall umożliwiało zdefiniowanie nie mniej niż 1 000 reguł polityki bezpieczeństwa. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.009** |
| Firewall musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, ang. intrusion prevention) realizowaną sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące DoS/DDoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) odbywa się w regułach polityki bezpieczeństwa. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.010** |
| System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż 200 Mb/s. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków musi być aktualizowana przez producenta min. raz w tygodniu. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.011** |
| Urządzenie firewall musi posiadać wbudowany moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie wymaga użycia dodatkowego serwera. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.012** |
| Urządzenie firewall musi posiadać wbudowany moduł filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie wymaga dodatkowego użycia serwera. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.013** |
| Urządzenie firewall musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.014** |
| Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 32 wirtualnych routerów. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.015** |
| Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.016** |
| Urządzenie musi obsługiwać co najmniej 128 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły:   * Spanning Tree (802.1D), * Rapid STP (802.1W), * oraz Multiple STP (802.1S).   Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.017** |
| Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych ma odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie ma posiadać mechanizm tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie ma posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.018** |
| Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA ma odbywać się przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.019** |
| Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall ma posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.020** |
| Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu wymagana jest możliwość przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.021** |
| Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Wymaga się aby usługi pomocy technicznej oraz szkoleń były świadczone w języku polskim. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 04.022** |
| **Wsparcie techniczne**:  z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres 5 lat oraz aktualnej bazy sygnatur ataków, definicji wirusów, blacklist antyspamowych oraz bazy kategorii stron WWW przez okres 5 lat. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. | |

* + 1. Przełącznik sieciowy

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.001** |
| Wymaga się, aby Wykonawca dostarczył 1 przełącznik sieciowy spełniający poniższe wymagania. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.002** |
| Obudowa przełącznika musi pozwalać na instalację w standardowej szafie RACK 19”. Wielkość maksymalna 1U. Urządzenie musi zostać dostarczone wraz ze wszystkimi elementami niezbędnymi do zamontowania w szafie i organizatorem kabli. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.003** |
| Urządzenie musi być wyposażone w min. 24 porty dostępowe 10/100/1000 RJ-45 oraz min. 2 interfejsy SFP/SFP+ mogące pracować z prędkością 10Gb/s, a także posiadać:   * funkcję łączenia urządzeń w stos, * możliwość obsługi min. 8000 adresów MAC, * matrycę przełączającą min 128 Gb/s, * wydajność przełączania urządzenia na poziomie co najmniej 95 Mpps, * możliwość obsługi co najmniej 1000 sieci VLAN, * możliwość obsługi sprzętowo co najmniej 1500 list kontroli dostępu (ACL), * możliwość obsługi mechanizmów dystrybucji informacji o sieciach VLAN pomiędzy przełącznikami. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.004** |
| Urządzenie musi umożliwiać obsługę protokołów sieciowych zgodnie ze standardami:   * IEEE 802.1x * IEEE 802.1s * IEEE 802.1w * IEEE 802.3x full duplex dla 10BASE-T i 100BASE-TX * IEEE 802.3ad * IEEE 802.1D * IEEE 802.1p * IEEE 802.1Q * IEEE 802.3 10BASE-T * IEEE 802.3u 100BASE-TX * IEEE 802.3z 1000BASE-X * IEEE 802.3ab 100BASE-T | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.005** |
| Urządzenie musi udostępniać wsparcie dla routingu:   * IPv4 i IPv6: routing statyczny, * Routing dynamiczy IPv4 RIP v1/v2, OSPF, * Routing dynamiczny IPv6 RIPng, OSPFv3. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.006** |
| Urządzenie musi udostępniać wsparcie dla mechanizmów multicast:   * IGMP snooping, * Multicast Listener Discovery snooping, * Minimum 1000 grup multicastowych, * IP Multicast VLAN. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.007** |
| Urządzenie musi posiadać mechanizmy związane z zapewnieniem jakości usług w sieci:   * obsługa co najmniej ośmiu kolejek sprzętowych, wyjściowych dla różnego rodzaju ruchu, * mechanizm automatycznej konfiguracji portów do obsługi VoIP, * flow-based QoS z wejściową i wyjściową zmianą parametrów (tzw. remarking), * zarządzanie kolejkowaniem: Stricte Priority (SPQ), Weighted Round Robin (WRR), Deficit Round Robin (DRR), * mechanizm zapobiegania powstawaniu zatorów w sieci E2E-HOL Blocking Protection, * obsługa protokołu CDP. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.008** |
| Urządzenie musi obsługiwać agregowanie połączeń zgodnie z IEEE 802.3AD, nie mniej niż 32 grup LACP do 8 portów każda. Przy wysyłaniu pakietu IP przez interfejs LACP do wyznaczenia fizycznego portu, na który pakiet będzie wysłany musi być brany pod uwagę co najmniej adres IP źródłowy i docelowy tego pakietu, a dla innych protokołów co najmniej adres źródłowy i docelowy, lub źródłowe i docelowe adresy MAC. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.009** |
| Urządzenie musi obsługiwać tablice ARP min. 2000 wpisów i Tablicę Routingu min. 2000 wpisów. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.010** |
| Urządzenie musi umożliwiać obsługę protokołów dynamicznego routingu min. RIP 1 i 2 oraz OSPF. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.011** |
| Urządzenie musi obsługiwać funkcje bezpieczeństwa: sticky MAC, Dynamic Arp Inspection, proxy ARP, DHCP snooping, IP source guard. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.012** |
| Urządzenie musi obsługiwać filtrowanie ruchu wejściowego i wyjściowego co najmniej na poziomie portu i sieci VLAN. Urządzenie musi realizować nie mniej niż 1000 reguł filtrowania ruchu. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05. 013** |
| Przełącznik musi obsługiwać ramki jumbo (9216 bajtów) na wszystkich interfejsach. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.014** |
| Przełącznik musi być przystosowany do pracy ciągłej przy temperaturze otoczenia z zakresu 5 - 40 **°**C. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.015** |
| Przełącznik musi być wyposażony w port konsoli. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.016** |
| Przełącznik musi umożliwiać wgranie systemu operacyjnego z zewnętrznego nośnika danych poprzez łącze szeregowe RJ-45 lub/i RS-232 lub/i USB. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.017** |
| Zarządzanie urządzeniem musi być możliwe za pośrednictwem interfejsu linii komend (CLI) przez port konsoli oraz zdalnie przez telnet lub ssh przez protokół IPv4 oraz IPv6. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.018** |
| Urządzenie musi umożliwiać zapisanie aktualnej konfiguracji. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.019** |
| Przełącznik musi generować logi dotyczące zdarzeń na nim zachodzących. Użytkownik musi mieć dostęp do dokumentacji producenta urządzenia z wyjaśnieniami znaczenia poszczególnych wpisów w logach. Logi te muszą być dostępne lokalnie na urządzeniu oraz przesyłane do innych urządzeń z użyciem protokołu syslog. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.020** |
| Przełącznik musi umożliwiać ustawienie limitów pakietów akceptowanych na wskazanych portach w jednostce czasu (tzw. rate limiting). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.021** |
| Przełącznik musi umożliwiać ustawienie limitów pakietów typu broadcast oraz unicast na każdym interfejsie. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.022** |
| Urządzenie musi wspierać funkcjonalność: Private VLANs (across switches). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.023** |
| Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.024** |
| Urządzenie musi udostępniać informacje o liczbie ramek i bajtów wysłanych i odebranych na poszczególnych portach. Ponadto musi istnieć możliwość obsługi liczników odebranych ramek zawierających błędy na poszczególnych interfejsach oraz liczniki ramek których nie udało się wysłać lub wystąpiły błędy podczas ich wysyłania. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.025** |
| Dostępna musi być funkcja kopiowania (mirroring) ruchu dla pakietów spełniających warunki określone w odpowiednim filtrze. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.026** |
| Urządzenie musi posiadać możliwość diagnostyki kabla, TDR (Time Domain Reflectometer) na wszystkich portach 10/100/1000BASE-T. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.027** |
| Przełącznik musi umożliwiać zdefiniowanie czasu po jakim będzie próbował aktywować porty wyłączone automatycznie ze względu na nieprawidłowości występujące w przyłączonych do nich częściach sieci. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.028** |
| Przełącznik musi posiadać funkcjonalność umożliwiającą monitorowanie ruchu w warstwach 3 do 4 modelu OSI dla pakietów IPv4. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.029** |
| Przełącznik musi obsługiwać protokoły Spanning Tree i Rapid Spannig Tree, zgodnie ze standardem IEEE 802.1D, a także Multiple Spanning Tree zgodnie ze standardem IEEE 802.1Q oraz VLAN Spanning Tree Protocol. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.030** |
| Przełącznik musi posiadać możliwość wyłączenia Spanning Tree oraz filtrowania (ignorowania) ramek BPDU na wskazanych portach. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.031** |
| Przełącznik musi udostępniać informacje dla każdej instancji STP, kiedy przyszedł ostatni pakiet TCN (Topology Change Notification) oraz liczniki pakietów TCN dla każdej instancji STP lub informację z którego interfejsu przyszedł ostatni pakiet TCN. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.032** |
| Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.033** |
| Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie, autoryzowanych każdy indywidualnie. Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.034** |
| Przełącznik musi umożliwiać określanie maksymalnej liczby adresów MAC dopuszczalnych na wskazanym porcie. Po przekroczeniu limitu dopuszczalnych adresów MAC pakiety z adresami źródłowymi MAC nie znajdującymi się w zbudowanej tablicy MAC będą ignorowane. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.035** |
| Przełącznik musi obsługiwać protokół MVR (Multicast VLAN Registration). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.036** |
| Przełącznik musi posiadać funkcjonalność IGMP oraz MLD snooping i wysyła ramki multicastowe tylko do nasłuchujących klientów. Funkcjonalność ta nie może zakłócać poprawnej pracy multicastów IPv6, w tym standardu Neighbor Discovery. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.037** |
| Oprogramowanie urządzenia powinno umożliwiać wersjonowanie kolejnych generowanych plików konfiguracyjnych. Musi być zapewnione przechowywanie na urządzeniu i możliwość odtworzenia co najmniej 2 ostatnich wersji pliku konfiguracyjnego. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.038** |
| Urządzenie musi zapewnić mechanizm automatycznego po każdej zmianie lub cyklicznego o zadanej poprzez kopiowanie pełnej konfiguracji do wskazanego repozytorium plików konfiguracyjnych np. mechanizmem ftp lub scp. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 05.039** |
| **Warunki gwarancji:**  Urządzenie musi być dostarczone wraz z gwarancją producenta obejmującą:   1. Zapewnienie bezpłatnej pomocy technicznej oraz szkolenia z produktu w języku polskim. 2. Zapewnienie wsparcia technicznego świadczonego w języku polskim telefonicznie oraz za pomocą poczty elektronicznej. 3. W okresie trwania gwarancji, w razie konieczności zapewnienie możliwości wymiany uszkodzonego sprzętu, dostępu do wszystkich nowych wersji oprogramowania oferowanych przez producenta (w ramach zakupionej licencji), a także dostępu do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. 4. Wsparcie dla urządzenia umożliwiające zgłaszanie problemów z oprogramowaniem urządzenia do producenta, na poziomie 24/7 przez okres trwania gwarancji. 5. Gwarancję czasu skutecznej naprawy nieprzekraczającej 4 godzin. 6. Dostarczenie urządzenia zamiennego, skonfigurowanego zgodnie z pełną konfiguracją dostarczoną przez Zamawiającego na okres przekraczający czas skutecznej naprawy określony w pkt. e. | |

* 1. Oprogramowanie
     1. Środowiska bazodanowe

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.001** |
| Wymagane jest, aby licencja na środowisko bazodanowe była bezterminowa do pełnego użytku (typu full use) z 3 letnim wsparciem technicznym. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.002** |
| Wymagane jest zapewnienie współpraca z systemem operacyjnym zainstalowanym na serwerze (klastrze) bazodanowo - aplikacyjnym. Wymagana jest niezależność platformy systemowej dla oprogramowania klienckiego/serwera aplikacyjnego od platformy systemowej bazy danych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.003** |
| Wymagane jest, aby oprogramowanie bazodanowe zapewniało możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.004** |
| Wymaga się, aby oprogramowanie bazodanowe przetwarzało dane z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.005** |
| Wymaga się, aby oprogramowanie bazodanowe umożliwiało zagnieżdżanie transakcji – musi istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – ma być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.006** |
| Wymaga się, aby oprogramowanie bazodanowe miało wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.007** |
| Wymaga się, aby była możliwość migracji zestawu znaków bazy danych do Unicode. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.008** |
| Wymaga się, aby oprogramowanie bazodanowe umożliwiało redefiniowanie przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.009** |
| Wymaga się, aby oprogramowanie bazodanowe posiadało funkcję skalowania rozwiązań opartych o architekturę trójwarstwową, tzn.: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.010** |
| Wymaga się, aby oprogramowanie bazodanowe umożliwiało otworzenie wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.011** |
| Wymagane jest wsparcie protokołu XA. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.012** |
| Wymaganie jest wsparcie standardu JDBC 3.0. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.013** |
| Wymagana jest zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.014** |
| Wymaga się, aby motor bazy danych umożliwiał wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Musi istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.015** |
| Wymaga się wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania musi być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.016** |
| Wymaga się, aby procedury i funkcje składowane miały możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje muszą mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe muszą umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.017** |
| Wymaga się, aby była możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.018** |
| Wymaga się, aby oprogramowanie bazodanowe umożliwiało deklarowanie wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy musi umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.019** |
| Wymaga się, aby w przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.020** |
| Wymaga się, aby istniała możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.021** |
| Wymaga się, aby oprogramowanie bazodanowe umożliwiało wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.022** |
| Wymaga się, aby przywileje użytkowników bazy danych były określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu/modyfikacji tabeli, wykonania procedury). Oprogramowanie bazodanowe musi umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.023** |
| Wymaga się, aby oprogramowanie bazodanowe umożliwiało:   * wykonywanie i katalogowanie kopii bezpieczeństwa bezpośrednio przez serwer bazy danych; * zautomatyzowane usuwanie zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów; * integrację z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServe itd); * wykonywanie kopii bezpieczeństwa zarówno w trybie offline oraz w trybie online. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.024** |
| Wymaga się, aby oprogramowanie bazodanowe umożliwiało wykonywanie kopii bezpieczeństwa w trybie online (hot backup). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.025** |
| Wymaga się, aby odtwarzanie umożliwiało odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.026** |
| Wymaga się, aby w przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.027** |
| Wymaga się, aby oprogramowanie bazodanowe posiadało wbudowaną obsługę wyrażeń regularnych była zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.028** |
| Wymaga się, aby była możliwość budowy klastra na węźle obsługiwanym przez maksymalnie 2 procesory. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.029** |
| Wymaga się, aby była możliwość pracy na maszynie wyposażonej maksymalnie w 2 gniazda procesorowe (ang. sockets). | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.030** |
| Wymaga się, aby była możliwość obsługi do 16 wątków. | |

|  |  |
| --- | --- |
| **Identyfikator** | **WF 06.031** |
| Wymaga się, aby producent relacyjnej bazy danych dostarczył usługę pozwalająca na tworzenie kopii zapasowej bazy danych w chmurze należącej do producenta. | |