Szczegółowy Opis Przedmiotu Zamówienia

Dostawa infrastruktury wraz ze wsparciem technicznym w ramach projektów CAPAP, ZSIN – Faza II, K-GESUT.

Spis treści

Spis tabel

Spis rysunków

1 Wstęp

Niniejszy dokument opisuje przedmiot zamówienia na *Dostawa infrastruktury wraz ze wsparciem technicznym w ramach projektów CAPAP, ZSIN – Faza II, K-GESUT*.

Celem zamówienia jest zapewnienie wydajnego i niezawodnego środowiska infrastrukturalnego udostępniającego usługi dostarczone w ramach projektów współfinansowanych ze środków Unijnych tj. *CAPAP, ZSIN – Faza II, K-GESUT*.

Zamówienie współfinansowane jest ze środków Programu Operacyjnego Polska Cyfrowa - Oś 2 Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych”.

2 Słownik pojęć

Terminy i skróty ogólne	
BDOO	Baza Danych Obiektów Ogólnogeograficznych o szczegółowości odpowiadającej mapie ogólnogeograficznej w skali 1: 250 000 – Magazyn danych KSZBDOT.
BDOT10k	Baza danych obiektów topograficznych o szczegółowości odpowiadającej mapie topograficznej w skali 1: 10 000 - Magazyn danych KSZBDOT.
BGP	ang. Border Gateway Protocol.
CAPAP	Centrum Analiz Przestrzennych Administracji Publicznej.
Cloud Computing	Model przetwarzania w chmurze obliczeniowej.
Czas obsługi	Maksymalny czas, liczony od momentu poprawnego zgłoszenia do momentu przekazania, przez Wykonawcę, rozwiązania i potwierdzenia przez Zamawiającego możliwości zamknięcia zgłoszenia.
Czas reakcji	Czas liczony od momentu pozyskania informacji o zdarzeniu (Incydent, zgłoszenie) do powiadomienia zgłaszającego o sposobie i terminie realizacji zdarzenia lub do momentu eskalacji tego zdarzenia.
Dyrektywa INSPIRE	Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE).
Dzień roboczy	8 godzin roboczych w ramach Godzin pracy GUGiK.
EMUiA	Ewidencja Miejscowości, Ulic i Adresów.
enviDMS	Projekt model bazy danych przestrzennych dotyczących środowiska przyrodniczego wraz z systemem zarządzania w aspekcie kartograficznych opracowań tematycznych.
e-PUAP	Elektroniczna Platforma Usług Administracji Publicznej – portal internetowy udostępniający informacje na temat usług publicznych realizowanych drogą elektroniczną.
GBDOT	Projekt „Georeferencyjna Baza Danych Obiektów Topograficznych (GBDOT) wraz z krajowym systemem zarządzania" realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet VII Społeczeństwo informacyjne – Budowa elektronicznej administracji.

Terminy i skróty ogólne	
Geoportal	Portal internetowy zgodny z dyrektywą INSPIRE, pełniący rolę brokera, udostępniającego użytkownikom dane i usługi geoprzestrzenne poprzez wyszukanie żądanych informacji, którego dysponentem jest Główny Geodeta Kraju. Rozwijany w ramach projektu Geoportal2. System GEOPORTAL wraz z Systemami dziedzinowymi.
GEOPORTAL 2	Projekt rozwoju infrastruktury informacji przestrzennej w Polsce, realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet VII Społeczeństwo informacyjne – Budowa elektronicznej administracji. Projekt stanowi kontynuację projektu Geoportal.gov.pl.
Godzina robocza	Okres trwający godzinę zegarową w ramach Godzin pracy Zamawiającego.
Godziny pracy Zamawiającego	Od 8.15 do 16.15, od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy i dni wolnych u Zamawiającego, o których Zamawiający poinformował Wykonawcę.
GUGiK	Główny Urząd Geodezji i Kartografii.
HSM	z ang. hardware security module, urządzenie stanowiące element infrastruktury PKI posiadające sprzętowe zabezpieczenia oraz certyfikat świadczący o klasie bezpieczeństwa.
IIP	Infrastruktura Informacji Przestrzennej.
Incydent	Nieplanowana przerwa lub obniżenie jakości usługi biznesowej.
Incydent standardowy	Każdy inny nie będący Incydentem pilnym ani Incydentem krytycznym.
Incydent krytyczny	Incydent uniemożliwiający korzystanie z usług biznesowych w co najmniej jednej lokalizacji.
Incydent pilny	Incydent uniemożliwiający korzystanie z usług biznesowych na co najmniej jednym stanowisku w lokalizacji.
IPE	Integrująca Platforma Elektroniczna
ISOK	Projekt ISOK (Informatyczny System Osłony Kraju przed nadzwyczajnymi zagrożeniami) realizowany przez konsorcjum Krajowy Zarząd Gospodarki Wodnej, Instytut Meteorologii i Gospodarki Wodnej, Główny Urząd Geodezji i Kartografii, Rządowe Centrum Bezpieczeństwa i Instytut Łączności.
ITIL	Kodeks postępowania dla działów informatyki, zawierający zbiór zaleceń jak efektywnie i skutecznie oferować usługi informatyczne.
KSZBDOT	Krajowy System Zarządzania Bazą Danych Obiektów Topograficznych.
NMPT	Numeryczny Model Pokrycia Terenu.

Terminy i skróty ogólne	
NMT	Numeryczny Model Terenu.
Oprogramowanie standardowe	Gotowe oprogramowanie publicznie dostępne w sprzedaży, stanowiące dla organizacji alternatywny sposób pozyskania poza samodzielnym ich wytworzeniem. Oprogramowanie Standardowe jest produktem typu COTS (Commercial Off-The-Shelf).
OPZ	Opis przedmiotu zamówienia.
POPC	Program Operacyjny Polska Cyfrowa.
PRINCE 2	Metodyka zarządzania projektami. Właścicielem metodyki jest Office Government Commerce.
PRNG	Państwowy Rejestr Nazw Geograficznych.
Problem	Przyczyna jednego lub wielu Incydentów.
Pryncypia Architektury Korporacyjnej	Materiał opracowany w ramach Zespołu do spraw rozwoju strategii informatyzacji administracji publicznej w Ministerstwie Administracji i Cyfryzacji https://mac.gov.pl/projekty/architektura-korporacyjna-panstwa.
PZGiK	Państwowy Zasób Geodezyjny i Kartograficzny.
RCiWN	Rejestr Cen i Wartości Nieruchomości.
RPO	(ang. recovery point objective) – akceptowalny poziom utraty danych wyrażony w czasie
RTO	(ang. recovery time objective) – czas w jakim należy przywrócić proces po wystąpieniu awarii
SCMIS	(ang. supplier and contract management information system) System Zarządzania Dostawcami i Umowami
SIG	Systemy Informatyczne GUGiK - Zestaw metod, narzędzi i wytycznych dotyczących realizacji projektów w Głównym Urzędzie Geodezji i Kartografii. W szczególności są to systemy informatyczne działające w infrastrukturze sprzętowo programowej Zamawiającego oraz w odniesieniu do przyszłości także systemy i narzędzia planowane do budowy i wdrożenia.
SIWZ	Specyfikacja Istotnych Warunków Zamówienia.
SSO	ang. Single Sign On. Szczególna forma uwierzytelnienia pozwalająca użytkownikowi uwierzytelnić się tylko raz i uzyskać dostęp do zasobów wielu systemów, do których nadano użytkownikowi uprawnienia.

Terminy i skróty ogólne	
Strony	Zamawiający i Wykonawca.
SZBI	System Zarządzania Bezpieczeństwem Informacji.
SZNMT	System Zarządzania Numerycznym Modelem Terenu.
TERYT 2	Projekt TERYT 2 - Państwowy rejestr granic i powierzchni jednostek podziałów terytorialnych kraju realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet VII Społeczeństwo informacyjne – Budowa elektronicznej administracji.
TERYT 3	Projekt TERYT 3 - Rozbudowa systemów do prowadzenia rejestrów adresowych – Etap I, realizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, lata 2007-2013, Priorytet VII Społeczeństwo informacyjne – Budowa elektronicznej administracji.
UE	Unia Europejska.
UMM	Uniwersalny Moduł Mapowy.
Umowa	Umowa, która zostanie podpisana na realizację Zamówienia.
Usługi Asysty	Wsparcie Zamawiającego przez Wykonawcę. Szczegółowy zakres wsparcia będzie określony w chwili wystąpienia takiej potrzeby i może dotyczyć rozwoju systemu, np. dodawania nowych funkcjonalności lub modyfikacji aktualnego systemu.
Ustawa IIP/Ustawa o IIP	Ustawa o Infrastrukturze Informacji Przestrzennej (Dz .U. nr 76, poz. 489) z 4 marca 2010r.
Ustawa PGiK, PGiK	Ustawa z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne (Dz.U. 2010, nr 193 poz. 1287).
WMS	Web Map Service (WMS) to międzynarodowy standard udostępniania danych przestrzennych w Internecie w postaci rastrowej. Standardy techniczne dostępne są na stronie Open Geospatial Consortium (OGC).
WMTS	Web Map Tile Service (WMTS) to międzynarodowy standard udostępniania danych przestrzennych w Internecie w postaci rastrowych, predefiniowanych fragmentów mapy tzw. kafli. Proces generowania kafli jest uruchamiany po aktualizacji danego produktu natomiast pliki zapisywane są na serwerach w odpowiedniej strukturze. Zastosowanie takiego rozwiązania przyspiesza odpowiedź usługi na zapytanie użytkownika o fragment mapy ponieważ zwracana jest już wcześniej przygotowana grafika w przeciwieństwie do usługi WMS, która generuje plik graficzny każdorazowo po otrzymaniu takiego zlecenia.
WODGiK	Wojewódzki Ośrodek Dokumentacji Geodezyjnej i Kartograficznej.
Wykonawca	Podmiot, który zawrze z Zamawiającym umowę sprawie wykonania Zamówienia.

Terminy i skróty ogólne	
Wykonawca rozwoju i budowy usług	Podmiot, który będzie realizował zadania związane z rozwojem systemów SIG w ramach działania budowy i udostępniania usług w ramach Projektów CAPAP, ZSIN Faza II i K-GESUT, współfinansowanych ze środków Programu Operacyjnego Polska Cyfrowa Oś 2 Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych”.
Wykonawca systemów	Podmiot, który będzie realizował zadania związane z rozwojem systemów SIG w ramach działania budowy i udostępniania usług w ramach Projektów CAPAP, ZSIN Faza II i K-GESUT, współfinansowanych ze środków Programu Operacyjnego Polska Cyfrowa Oś 2 Działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych”.
Zamawiający	Główny Urząd Geodezji i Kartografii.
Zamówienie	Zamówienie publiczne, którego przedmiot w sposób szczegółowy został opisany w SOPZ.
Zgłoszenie standardowe	Dowolna prośba użytkownika o informację, konsultację, poradę, standardową zmianę lub nadanie dostępu do usługi / aplikacji.
Zintegrowany moduł mapowy PZGiK	Produkty powstające w ramach narzędzi do udostępniania danych, dedykowane dla poszczególnych branż i grup odbiorców. Zintegrowane moduły mapowe będą udostępniać dane, usługi i analizy najbardziej istotne i najbardziej adekwatne dla potrzeb przedstawicieli danej branży.
ZSIN	Zintegrowany System Informacji o Nieruchomościach.

Tabela 1 Słownik pojęć

3 Opis organizacji zamówienia

Główny Urząd Geodezji i Kartografii (GUGiK) jest urzędem obsługującym Głównego Geodetę Kraju, który wykonuje zadania określone w szczególności w Ustawie Prawo Geodezyjne i Kartograficzne, Ustawie o Infrastrukturze Informacji Przestrzennej. GUGiK realizuje szereg projektów, w ramach których powstają systemy informatyczne.

Przedmiotem działalności GUGiK jest m.in. wykonywanie czynności materialno-technicznych służących realizacji zadań publicznych przypisanych Głównemu Geodecie Kraju, m.in. w zakresie:

- baz danych i systemów zarządzania centralnego zasobu geodezyjnego i kartograficznego;
- utrzymania serwerów katalogowych i serwerów metadanych;
- tworzenia i obsługi usług sieciowych dotyczących zbiorów i usług danych przestrzennych,
- interoperacyjności zbiorów i usług danych przestrzennych;
- wdrażania i utrzymywania rozwiązań technicznych zapewniających określoną przepisami wydajność i dostępność serwisów geoportalu infrastruktury informacji przestrzennej;
- dostępności i ciągłości działania systemów teleinformatycznych;
- bezpieczeństwa systemów i sieci teleinformatycznych.

Projekt, rozumiany jako realizacja przedmiotowej Umowy, musi być realizowany zgodnie z metodyką zarządzania projektami PRINCE2.

W odniesieniu do metodyki PRINCE2, niniejsze zamówienie będzie realizowane, jako Grupa Zadań wykonywana w ramach projektu.

Zakres odpowiedzialności i uprawnień dla poszczególnych ról projektowych należy rozumieć zgodnie z zaleceniami metodyki PRINCE2. W odniesieniu do tej metodyki kierownik projektu niniejszego postępowania po stronie Wykonawcy rozumiany będzie, jako kierownik grupy zadań, podlegający bezpośrednio kierownikowi Projektu ze strony Zamawiającego.

Wykonawca zobowiązany będzie realizować swoje prace głównie w siedzibie Centralnego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej, ul. Jana Olbrachta 94 B w Warszawie oraz dodatkowo w Głównym Urzędzie Geodezji i Kartografii, Centrum Zarządzania ASG-EUPOS w Katowicach, ul. Graniczna 29, 40-017 Katowice. Zamawiający przewiduje zdalny dostęp do infrastruktury przez VPN dla Wykonawcy.

Raport z wykonania usług Wykonawcy, będący podstawą rozliczeń prac Wykonawcy, weryfikowany będzie przez Zamawiającego (Główny Urząd Geodezji i Kartografii), w porozumieniu z Centralnym Ośrodkiem Dokumentacji Geodezyjnej i Kartograficznej.

3.1 Struktura organizacyjna

Projekty CAPAP, ZSIN - Faza II i K-GESUT są realizowane zgodnie z metodyką zarządzania projektami PRINCE2. Metodyka PRINCE 2 została wdrożona i była wykorzystywana przez Główny Urząd Geodezji i Kartografii przy realizacji wszystkich projektów w ramach Programu Operacyjnego Innowacyjna Gospodarka, w tym:

1) GEOPORTAL.GOV.PL
   Cel projektu:
   - uruchomienie portalu internetowego udostępniającego dane i usługi geoprzestrzenne oraz przetworzenie wybranych opracowań geodezyjnych i kartograficznych do postaci numerycznej.

   Termin zakończenia realizacji: październik 2008 r.
2) TERYT 2 - Państwowy rejestr granic i powierzchni jednostek podziałów terytorialnych kraju
   Cel projektu:
   - udostępnienie on-line Państwowego Rejestru Granic i Powierzchni Jednostek Podziałów Terytorialnych Kraju oraz realizacja i wdrożenie rozwiązań związanych z prowadzeniem rejestrów adresowych.

   Termin zakończenia projektu: grudzień 2012 r.
3) GEOPORTAL 2 - Rozbudowa infrastruktury informacji przestrzennej w zakresie rejestrów georeferencyjnych oraz związanych z nimi usług.
   Cel projektu:
   - umożliwienie powszechnego dostępu i stosowania informacji przestrzennej w Polsce poprzez rozbudowę infrastruktury informacji przestrzennej w zakresie rejestrów georeferencyjnych oraz związanych z nimi usług.

   Termin zakończenia projektu: grudzień 2015 r.
4) GBDOT - Georeferencyjna Baza Danych Obiektów Topograficznych (GBDOT) wraz z krajowym systemem zarządzania.
   Cel projektu:
   - Budowa zharmonizowanej bazy danych zawierającej informacje o lokalizacji obiektów przestrzennych i zjawisk na obszarze całego kraju, w szczególności w zakresie bazy danych obiektów topograficznych (BDOT10k) i bazy danych obiektów ogólnogeograficznych (BDOO), zawierających informacje o obiektach topograficznych z kategorii tj.:
     - Sieć wodna;
     - Sieć komunikacyjna (drogi i koleje);
     - Sieć uzbrojenia terenu;
     - Kompleksy pokrycia terenu;

- Budynki, budowle i urządzenia; ;
- Kompleksy użytkowania terenu;
- Inne obiekty przestrzenne.

- Budowa Krajowego Systemu Zarządzania Bazą Danych Obiektów Topograficznych wraz z centrum zapasowym.

Termin zakończenia projektu: listopad 2015 r.

5) ISOK - Informatyczny System Osłony Kraju przed nadzwyczajnymi zagrożeniami.
   Projekt był realizowany w ramach konsorcjum w skład którego wchodzą:
   - Krajowy Zarząd Gospodarki Wodnej (lider konsorcjum).
   - Instytut Meteorologii i Gospodarki Wodnej;
   - Główny Urząd Geodezji i Kartografii;
   - Instytut Łączności;

   Cel projektu:
   - stworzenie systemu osłony społeczeństwa, gospodarki i środowiska przed nadzwyczajnymi zagrożeniami poprzez stworzenie elektronicznej platformy informatycznej wraz z niezbędnymi rejestrami referencyjnymi, która stanowić będzie narzędzie do zarządzania kryzysowego.

   Główny cel projektu w zakresie realizowanym przez Główny Urząd Geodezji i Kartografii:
   - budowa referencyjnych, zharmonizowanych i interoperacyjnych baz danych przestrzennych do których docelowo dostęp będzie możliwy dzięki usługom uruchamianym w ramach realizacji projektu GEOPORTAL 2.

   Termin zakończenia projektu: grudzień 2015 r.
6) TERYT 3 – Rozbudowa systemów do prowadzenia rejestrów adresowych – Etap I.
   Cel projektu:
   - zapewnienie obywatelom, przedsiębiorcom i organom administracji publicznej dostępu przy pomocy środków komunikacji elektronicznej do kompletnych, wiarygodnych i aktualnych danych z rejestrów adresowych (w tym również obejmujących lokalizację przestrzenną).

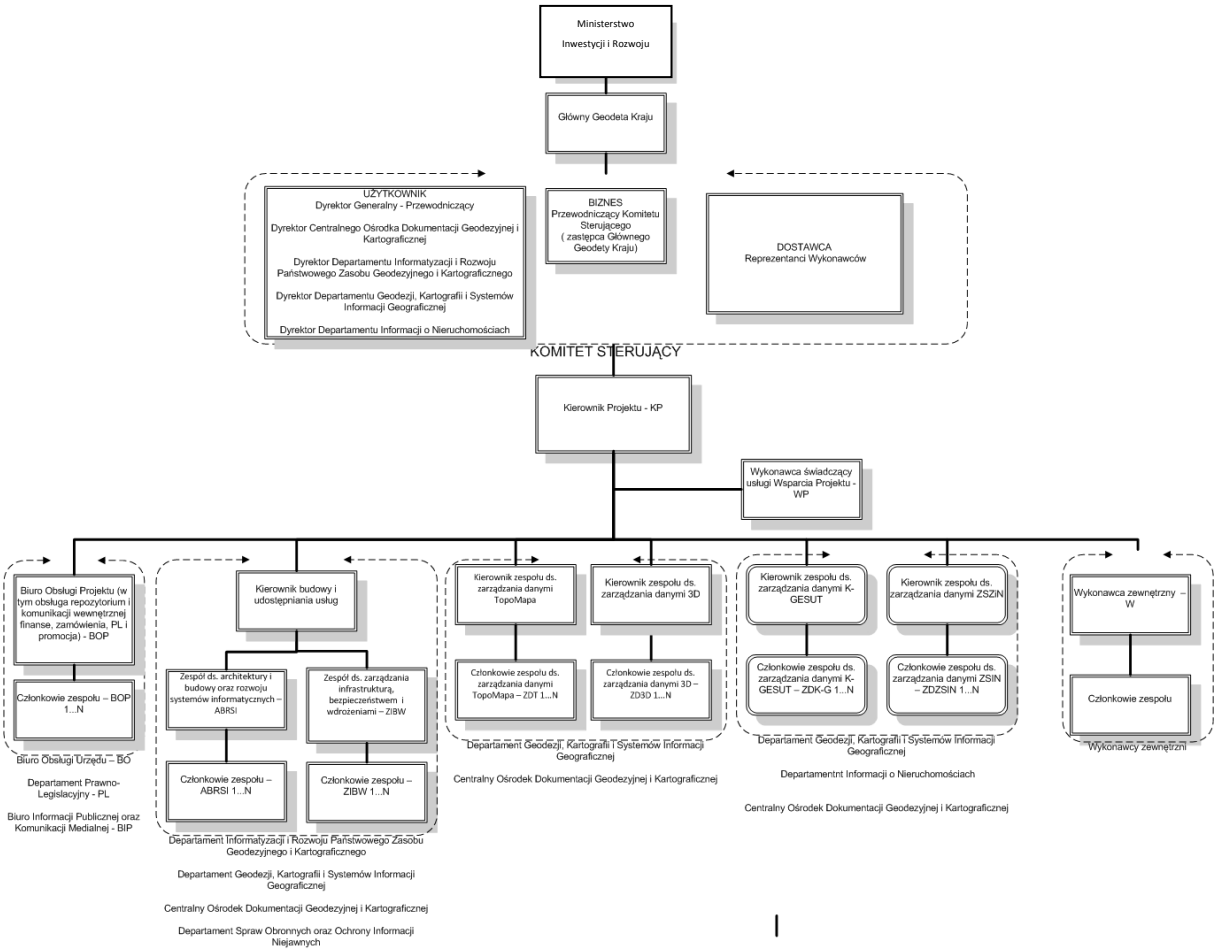
   Termin zakończenia projektu: grudzień 2015 r.
7) ZSIN – Budowa Zintegrowanego Systemu Informacji o Nieruchomościach – Faza I.
   Cel projektu:
   - usprawnienie procesu obsługi spraw prowadzonych przez administrację publiczną
   - w zakresie rejestracji nieruchomości oraz zapewnienia obywatelom i przedsiębiorcom dostępu do wiarygodnych i aktualnych informacji o nieruchomościach gromadzonych w rejestrach publicznych.

   Termin zakończenia projektu: grudzień 2015 r.

Z uwagi na wieloletnie doświadczenia Zamawiającego związane ze stosowaniem metodyki PRINCE2, metodyka zastosowana w ramach realizacji POPC będzie opierała się również o dotychczasowe doświadczenia z jej stosowania.

Na poniższym rysunku przedstawiona została struktura organizacyjna zarządzania projektem.

Rysunek 1 Struktura organizacyjna



Zakres odpowiedzialności i uprawnień dla poszczególnych ról projektowych należy rozumieć zgodnie z zaleceniami metodyki PRINCE2. W odniesieniu do tej metodyki kierownik projektu niniejszego postępowania po stronie Wykonawcy rozumiany będzie, jako kierownik grupy zadań, podlegający bezpośrednio kierownikom projektów CAPAP, ZSIN-Faza II i K-GESUT (po stronie Zamawiającego).

Wykonawca zobowiązany będzie do realizacji działań zarządczych (m.in. zarządzanie ryzykiem, zarządzanie zagadnieniami, zarządzanie komunikacją) zgodnie z wytycznymi, które zostaną przekazane przez Zamawiającego po podpisaniu Umowy. Wytyczne będą zawierać w szczególności procedury postępowania (np. procedura zgłaszania ryzyka) oraz zasady dla obszaru zarządczego (np. klasyfikacja ryzyk projektowych, wzory Rejestrów), które zostały ustanowione dla projektu.

3.2 SIG

W ramach Głównego Urzędu Geodezji i Kartografii powstała inicjatywa SIG - inicjatywa mająca na celu wypracowanie i wdrożenie spójnego systemu zasad działania dla wszystkich inicjatyw/projektów

realizowanych przez Główny Urząd Geodezji i Kartografii. Inicjatywa powstała w wyniku dostrzeżenia potrzeby zarządzania wszystkimi przedsięwzięciami realizowanymi przez Główny Urząd Geodezji i Kartografii, których rezultatami jest dostarczenie rozwiązań informatycznych wspierających realizację zadań Głównego Urzędu Geodezji i Kartografii. Inicjatywa SIG swoim zakresem wpływa na sposób realizacji projektów CAPAP, ZSIN - Faza II i K-GESUT, gdyż dostarcza wewnętrznych standardów i wytycznych, a także dobrych praktyk wypracowanych w oparciu o doświadczenia ze zrealizowanych projektów.

Inicjatywa ta została podzielona na 3 główne obszary:

- obszar architektury, którego celem jest zapewnienie spójności budowanych rozwiązań na poziomie systemów informatycznych;
- obszar realizacji, którego celem jest zapewnienie spójnej realizacji projektów/przedsięwzięć;
- obszar utrzymania, którego celem jest zapewnienie jednolitego sposobu utrzymania wyników projektów/przedsięwzięć.

W ramach zapewniania **spójnej architektury rozwiązania** SIG realizowane są następujące działania z obszarów:

- integracji warstwy biznesowej, w ramach której powstały:
    - jednolity katalog usług biznesowych planowanych/udostępnianych w ramach projektów/przedsięwzięć;
    - mapa usług biznesowych przedstawiająca powiązania pomiędzy usługami biznesowymi;
    - mapa produktów dostarczanych w ramach projektów/przedsięwzięć wraz z powiązaniami pomiędzy nimi;
    - standardy jednolitej dokumentacji;
    - pryncypia architektoniczne;
    - Rada Architektury i Biuro Architektury rozwiązująca zagadnienia dot. integracji systemów informatycznych;
- integracji warstwy IT, w ramach której powstały:
    - wytyczne i standardy dotyczące integracji pomiędzy systemami i dotyczące reużywalności poszczególnych komponentów;
    - model statyczny SIG przedstawiający architekturę rozwiązań;
    - scenariusze integracji dla systemów informatycznych;
    - ujednolicone modele wymagań;

  - diagram przepływu danych;
  - metoda wymiarowania usług na potrzeby szacowania zapotrzebowania na infrastrukturę;
- infrastruktury, uwzględniającej optymalne wykorzystanie istniejącej infrastruktury.

Architektura rozwiązania została opracowana w taki sposób, aby zapewnić możliwość dostosowania wdrażanych rozwiązań do nowych wytycznych cyfryzacji, w sposób optymalny pod względem kosztów i czasu.

Jednolity sposób realizacji inicjatyw w ramach SIG obejmuje:

- realizację w oparciu o wytyczne metodyki PRINCE2;
- stosowania zbioru wytycznych w obszarach zarządzania jakością, konfiguracją, ryzykiem i komunikacją;
- wsparcie narzędziowe w obszarze organizacji, architektury i utrzymania.

Jednolity sposób utrzymania SIG osiągnięty został poprzez:

- stworzenie spójnego modelu utrzymania bazującego na dobrych praktykach ITIL;
- świadczenie usług biznesowych na ustalonych parametrach;
- zapewnienie mechanizmów organizacyjnych i technicznych ciągłego monitorowania.

Inicjatywa SIG objęła swoim zasięgiem znaczącą większość systemów informatycznych, które były wytwarzane i dostarczane dla GUGiK. Systemy informatyczne istotne z perspektywy Projektów CAPAP, ZSIN - Faza II i K-GESUT opisane zostały w poniższych podrozdziałach.

Architekturę logiczną SIG przedstawia Rysunek 2 Architektura logiczna SIG.

Rysunek 2 Architektura logiczna SIG

Podstawowym elementem architektury SIG jest szyna usług, która zapewnia komunikację pomiędzy Systemem Geoportal, poszczególnymi systemami dziedzinowymi, pozostałymi systemami i aplikacjami (m.in. Systemem PZGiK, Modułem SDI, Uniwersalnym Modułem Mapowym, a także narzędziami do zarządzania metadanymi – Edytorem i Walidatorem metadanych oraz narzędziami do harmonizacji). System Geoportal dodatkowo korzysta z Magazynów danych Geoportal stanowiących replikę publikacyjną danych dziedzinowych, które produkowane są za pomocą systemów dziedzinowych (magazyny produkcyjne systemów dziedzinowych oraz magazyny pomocnicze Modułu SDI, UMM i narzędzi do zarządzania metadanymi).

Opis poszczególnych komponentów architektury SIG znajduje się w poniższych podrozdziałach.

Zamawiający posiada dokumentację poszczególnych komponentów. Dokumentacja zostanie udostępniona Wykonawcy po zawarciu umowy.

W rozdziale 5 Opis techniczny posiadanej infrastruktury przedstawione zostały informacje dotyczące technologii zastosowanej w systemach informatycznych GUGiK.

4 Przedmiot zamówienia

Przedmiotem Zamówienia jest doposażenie infrastruktury sprzętowej oraz oprogramowania dla środowiska SIG, wraz z udzieleniem nieograniczonej w czasie licencji.

W ramach dostawy oprogramowania wyróżnia się:

1. Rozwiązanie NAS typ A – 1 szt.
2. Rozwiązanie NAS typ B - 1 szt.
3. Macierz blokowa – 1 szt.
4. Serwery blade – 4 szt.
5. Serwery bazodanowe – 2 szt.
6. Serwery RACK – 5 szt.
7. Firewall do sieci Internet – 2 szt.
8. Router BGP – 2 szt.
9. Przełącznik SAN – 2 szt.
10. Oprogramowanie do wykonywania kopii zapasowej środowiska wirtualizacji – 1 komplet (73 szt.)
11. Komplet pamięci RAM – 4 komplety.

5 Opis techniczny posiadanej infrastruktury

Niniejsza część przedstawia zestawienie posiadanej przez Zamawiającego infrastruktury.

Dla elementów infrastruktury, dla których wsparcie wygasło, Zamawiający planuje uruchomić takie Postępowania.

5.1 Infrastruktura sprzętowa

Poniżej przedstawione komponenty znajdują się w lokalizacji Warszawa.

ID	Nazwa	Ilość	Wsparcie do	Opis
Serwery				
1	IBM BladeCenter HX5	8	31.12.2017	VMware vSphere 6.x
2	IBM BladeCenter HS22V	2	31.12.2017	przeznaczone na szynę usług – OracleVM + Oracle ESB
3	IBM System x3650 M4	1	31.12.2017	backup
4	HP BL660c Gen8	4	10.12.2016	VMware vSphere 6.x
5	HP BL660c Gen8	1	30.12.2019	VMware vSphere 6.x
6	HP BL660c Gen8	2	14.12.2017	VMware vSphere 6.x
7	HP BL660c Gen8	2	09.12.2017	VMware vSphere 6.x
8	HP BL660c Gen8	2	30.09.2018	VMware vSphere 6.x
9	HP BL660c Gen9	2	30.11.2018	VMware vSphere 6.x
10	HP ProLiant	7	brak	monitoring
11	DELL PowerEdge R630	1	11.12.2022	System ARAKIS
Klatki Blade				
1	IBM BladeCenter H Chassis	2	31.12.2017	
2	HP BLc7000	1	10.12.2016	
3	HP BLc7000	1	30.12.2019	
Jednolita infrastruktura bazodanowa				
1	Oracle Exadata X2-2 HalfRack z rozbudowaną pamięcią RAM do 1152 GB	1	08.06.2018	1) Rozbudowa pojemności - Exadata Expansion Half Rack HC; 2) Rozbudowa pojemności – 2 serwery Storage X5-2 HC;

Warstwa składowania				
1	IBM SoNAS 2851-RXA	1	31.12.2017	
2	IBM Storwize V7000	1	31.12.2017	
3	IBM Storwize V7000 Gen. 2	1	16.06.2018	
4	SuperMicro MBD-X11SAE-F/846BE16-R920B	1	15.12.2022	
5	IBM TS3310 Tape Library	1	31.12.2017	
6	EMC DataDomain DD2500	1	15.12.2019	stanowi środowisko składowania kopii zapasowych dla maszyn wirtualnych oraz baz danych
Warstwa sieciowa				
1	Juniper SRX3400	2	31.12.2017	Firewall Klaster
2	NLB F5 BIG-BT-5250V	2	25.06.2018	klaster active-passive
3	VPN Cisco ASA 5510 K9	1	31.12.2017	
4	Juniper EX2200-24T	4	31.12.2017	
5	Juniper EX4200-48T	4	31.12.2017	
6	Juniper J6350	2	31.05.2015	
7	IBM RackSwitch G8124E	1	31.12.2017	
8	Thales nShield Connect 1500	2	31.12.2017	
9	IBM System Storage SAN B-Type Switch	2	31.12.2017	

Tabela 2 Infrastruktura sprzętowa

Poniżej przedstawione komponenty znajdują się w lokalizacji Katowice.

ID	Nazwa	Ilość	Wsparcie do	Opis
Serwery				
1	IBM System x3650 M4	3	31.12.2017	backup
Warstwa składowania				
1	IBM Storwize V7000	1	31.12.2017	
2	EMC DataDomain DD2500	1	15.12.2019	stanowi replikę danych z EMC DataDomain DD2500 z Warszawy
3	Biblioteka taśmowa IBM	1	31.12.2017	

	TS3310			

Tabela 3 Komponenty Katowice

5.2 Główna infrastruktura programowa

ID	Nazwa	Wersja	Wsparcie do
1.	Oracle Directory Services Plus - Processor Perpetual	12.1.3	31.12.2016
2.	Oracle Directory Services Plus - Named User Plus Perpetual	12.1.3	31.12.2016
3.	Oracle SOA Suite for Oracle Middleware - Processor Perpetual	12.1.3	31.12.2016
4.	Oracle SOA Suite for Oracle Middleware - Named User Plus Perpetual	12.1.3	31.12.2016
5.	Oracle WebLogic Suite - Processor Perpetual	12.1.3	31.12.2016
6.	Oracle WebLogic Suite - Named User Plus Perpetual	12.1.3	31.12.2016
7.	Oracle WebLogic Server Standard Edition - Processor Perpetual	10.3.3.0	31.12.2016
8.	Oracle WebLogic Server Standard Edition - Named User Plus Perpetual	10.3.3.0	31.12.2016
9.	Oracle VM	3.3.1	brak
10.	Oracle Database Enterprise Edition - Processor Perpetual	11.2.0.3.27	31.12.2016
11.	Oracle Database Enterprise Edition - Named User Plus Perpetual	11.2.0.3.27	31.12.2016
12.	Oracle Real Application Clusters - Processor Perpetual	11.2.0.3.27	31.12.2016
13.	Oracle Diagnostics Pack - Processor Perpetual	11.2.0.3.27	31.12.2016
14.	Oracle Tuning Pack - Processor Perpetual	11.2.0.3.27	31.12.2016
15.	Oracle Spatial and Graph - Processor Perpetual	11.2.0.3.27	31.12.2016
16.	Oracle Spatial and Graph - Named User Plus Perpetual	11.2.0.3.27	31.12.2016
17.	vSphere Enterprise Plus	6.0	31.12.2018

18.	vCenter Standard	6.0	31.12.2018
19.	SYMC NETBACKUP SERVER AND 5 STD CLIENT STARTER PACK 7.6 WIN/LNX/SOLX64 TIER 2 MULTI PROD BNDL	7.6	brak
20.	SYMC NETBACKUP ENTERPRISE SERVER 7.6 WIN/LNX/SOLX64 1 SERVER TIER 2	7.6	brak
21.	SYMC NETBACKUP CLIENT APPLICATION AND DATABASE PACK 7.6 WIN/LNX/SOLX64 1 SERVER TIER 4	7.6	brak
22.	SYMC NETBACKUP CLIENT APPLICATION AND DATABASE PACK 7.6 WIN/LNX/SOLX64 1 SERVER TIER 1	7.6	brak
23.	SYMC NETBACKUP DATA PROTECTION OPTIMIZATION OPTION 7.6 XPLAT 1 FRONT END TB	7.6	brak
24.	SYMC NETBACKUP ENTERPRISE CLIENT 7.6 WIN/LNX/SOLX64 1 SERVER TIER 3	7.6	brak
25.	SYMC NETBACKUP ENTERPRISE SERVER 7.6 WIN/LNX/SOLX64 1 SERVER TIER 2	7.6	brak
26.	SYMC NETBACKUP OPTION SHARED STORAGE OPTION 7.6 XPLAT 1 DRIVE	7.6	brak
27.	SYMC NETBACKUP OPTION LIBRARY BASED TAPE DRIVE 7.6 XPLAT PER DRIVE	7.6	brak
28.	SYMC NETBACKUP OPTION NDMP 7.6 XPLAT PER SERVER TIER 4	7.6	brak
29.	SYMC NETBACKUP STANDARD CLIENT 7.6 XPLAT 1 SERVER	7.6	brak
30.	Trend Micro Deep Security - Anti-malware - per CPU (Socket)	9.6	26.12.2018
31.	MS Windows DataCenter	od 2008 do 2012 R2	brak
32.	HP Service Manager	9.33	brak
33.	HP Real User Monitor Engine	9.23	brak

34.	HP SiteScope	11.23	brak
35.	HP Performance Manager	9.03	brak
36.	HP Network Node Manager	9.23	brak
37.	HP BSM	9.23	brak

Tabela 4 Infrastruktura programowa

5.3 Środowiska przetwarzania

1. Środowisko backup-owe.
2. Środowiska testowe (w szczególności aplikacji, bazy danych, szyny usług).
3. Środowiska produkcyjne (w szczególności aplikacji, bazy danych, szyny usług).
4. Środowisko utrzymania i monitorowania.

5.4 Usługi technologiczne

1. Szyna usług.
2. Usługa warstwy aplikacji.
3. Usługa dostępu do bazy danych.
4. Usługa kopii zapasowych.
5. Usługa utrzymania i monitorowania.
6. Usługa dostępu blokowego SAN.
7. Usługa NAS.

5.5 Zestawienia lokalizacji

1. GUGiK, Warszawa, ul. Jana Olbrachta 94B.

2. GUGiK, Centrum Zarządzania ASG-EUPOS w Katowicach, ul. Graniczna 29, 40-017 Katowice.

5.6 Serwerownia

5.6.1 Lokalizacja Warszawa

Obecnie serwerownia zlokalizowana w GUGiK przy ul. Olbrachta 94B w Warszawie składa się z jednego pomieszczenia.

Zamawiający zapewnia redundantne przyłącza internetowe w lokalizacji Warszawa oraz łącze punk-punkt Warszawa-Katowice.

5.6.2 Lokalizacja Katowice

Obecnie serwerownia zlokalizowana w Katowicach udostępnia miejsce dodatkowo na 1 szafę (42U) (poza zainstalowanymi obecnie urządzeniami). Przeznaczeniem lokalizacji jest zdalne przechowywanie kopii zapasowej. Zasilanie nie posiada gwarancji podtrzymania.

5.7 Warstwa aplikacyjna

Obecna infrastruktura warstwy aplikacyjnej składa się z 25 serwerów Blade (posiadających łącznie 13TB pamięci operacyjnej RAM, 350 rdzeni Intel, serwery bezdyskowe), umiejscowionych w czterech klatkach Blade. Urządzenia pod względem parametrów pamięci i procesora nieznacznie się różnią, jednak wszystkie są oparte na architekturze x86. Powyżej wymienione urządzenia są wykorzystywane jako elementy chmury obliczeniowej opartej o platformę wirtualizacyjną VMware vSphere Enterprise Plus.

Do ochrony antywirusowej środowiska wirtualizacyjnego wykorzystywane jest oprogramowanie Trend Micro Deep Security.

Obecnie w środowisku wirtualizacyjnym (VMware) funkcjonuje ok. 870 maszyn wirtualnych (sumarycznie środowiska produkcyjne i testowe), opartych o systemy operacyjne: Windows Server (Active Directory), Linux – Centos.

5.8 Warstwa szyny usług

Warstwa składa się z czterech serwerów typu blade, na których jest uruchomione rozwiązanie wirtualizacyjne Oracle VM, a w ramach niego oprogramowanie szyny usług SOA Oracle Service Bus 12c (Usługi infrastrukturalne np.: SAML WebSSO, usługa uwierzytelniania grubego klienta, usługa monitorowania) oraz szyna usług OGC - iMapESB (usługi przestrzenne OGC np.: WMS, WFS, CSW) uruchomiona w klastrze VMware. Dostawcą tożsamości dla obu szyn jest LDAP.

5.9 Warstwa bazy danych

Infrastruktura warstwy bazy danych oparta jest o skonsolidowane rozwiązanie sprzętowo – programowe – Exadata Half Rack X2. Rozwiązanie składa się z serwerów (4 węzły bazodanowe (łącznie 1134 GB RAM i 48 Rdzeni CPU x86)) i sprzętu typu storage (360 TB pojemności użytecznej), który jest zarządzany w jednolity sposób za pomocą dedykowanego oprogramowania zintegrowanego z oprogramowaniem bazodanowym. Oprogramowanie zapewnia funkcjonalności typowej relacyjnej bazy danych i jest wzbogacone o funkcjonalności umożliwiające elastyczne

zarządzanie dedykowaną infrastrukturą sprzętową. Wykorzystywane są następujące opcje Oracle Database Enterprise Edition: RAC, Spatial, Partitioning, Diagnostic Pack, Tuning Pack.

Obecnie w środowisku bazy danych istnieje ok. 60 instancji baz danych.

5.10 Warstwa storage i magazyny danych

Warstwa storage składa się z macierzy dyskowej - dostęp blokowy oraz NAS. Wśród urządzeń wyróżniamy główne elementy takie jak:

- IBM SoNAS 2851-RXA – Usługę dostępu sieciowego NAS (głównie CIFS, NFS, FTP), pojemność użyteczna - 560 TB;
- SuperMicro MBD-X11SAE-F/846BE16-R920B z oprogramowaniem open-e - Usługę dostępu sieciowego NAS (głównie CIFS, NFS, FTP), pojemność użyteczna - 200 TB;
- IBM Storwize V7000 wraz z półkami rozszerzającymi, usługę dostępu blokowego (dla maszyn wirtualnych oraz bezdyskowych serwerów Blade), pojemność użyteczna – 141 TB.

5.11 Warstwa sieci

Warstwa sieci składa się z urządzeń sieciowych umożliwiających działanie sieci LAN i sieci SAN.

Obecna infrastruktura to:

1. Juniper SRX3400 Firewall Klaster – 2 szt;
2. NLB F5 BIG-BT-5250V – 2 szt;
3. Terminator VPN Cisco 5510 K9 – 1 szt;
4. Switche LAN (Juniper EX 4200-48T – 4 szt., EX2200-24T – 4 szt.)
5. Switche SAN (IBM System Storage SAN48B-5) - 2szt;
6. Switch LAN (IBM System Networking RackSwitch G8124E) - 1szt;
7. HSM (Thales nShield Connect 1500) 2szt;
8. Klaster Router (Juniper J6350) 2szt.

5.12 Warstwa dostępowa

Łącza:

- Dwa niezależne łącza dostępowe do Internetu (500 Mbps, 300 Mbps);
- Wydzielone połączenie do sieci OST 112;
- Łącze point-to-point (Katowice – Warszawa) o przepustowości 512 Mbps.

Metody dostępu:

- Dostęp za pomocą VPN CISCO Client z lokalną usługą po http;
- Dostęp przez przeglądarkę www z szyfrowaniem (https);
- Tunel IPSec (VPN Poin To Point);
- SSL VPN F5 z lokalną usługą po http.

5.13 Środowisko backupowe

Środowisko backupowe złożone jest z urządzenia do deduplikacji EMC DataDomain DD2500, biblioteki taśmowej TS3310 wraz z taśmami magnetycznymi LTO oraz serwera zarządzania backupem.

Rozwiązanie sprzętowe zarządzane jest przez oprogramowanie do backupu danych Veritas NetBackup. Oprogramowanie jest zainstalowane na serwerze do zarządzania backupem oraz w ramach środowiska aplikacyjnego.

Środowisko backupowe ma za zadanie wykonywanie kopii zapasowych z baz danych, warstwy aplikacyjnej , NAS, maszyn wirtualnych oraz szyny usług.

Elementem składowym środowiska backupowego jest Centrum Zapasowe w Katowicach, spełniające rolę miejsca przechowywania danych (maszyn wirtualnych i baz danych) w dodatkowej lokalizacji, innej niż Centrum Podstawowe w Warszawie. Środowisko Centrum Zapasowego w Katowicach składa się z analogicznych rozwiązań jak w Centrum Podstawowym (serwer zarządzania backup z oprogramowaniem Symantec NetBackup, biblioteka taśmowa i deDuplikacja EMC DataDomain DD2500).

5.14 Środowisko monitoringu

W ramach warstwy wykorzystywane jest oprogramowanie do monitorowania – Nagios, Centreon zbierające dane z infrastruktury oraz Nagvis wizualizujący zebrane dane.

W ramach warstwy wykorzystywane są także inne metody zbierania informacji o parametrach działania systemu, m.in. mechanizmy wbudowane w oprogramowanie do wirtualizacji VMware ESX, mechanizmy wbudowane w urządzenia sieciowe.

System monitoringu HP w oparciu o wybrane elementy (HP Real User Monitor Engine, HP SiteScope 11.23, HP Performance Manager, HP Network Node Manager, HP BSM)

Do zbierania informacji o parametrach działania poszczególnych elementów infrastruktury wykorzystywane są również mechanizmy wbudowane w posiadane oprogramowanie, m.in. oprogramowanie do wirtualizacji VMware ESX, mechanizmy wbudowane w urządzenia sieciowe.

6 Ogólna koncepcja docelowego rozwiązania

W ramach postępowania zakładane jest doposażenie posiadanego środowiska infrastrukturalnego, które umożliwi wydajne funkcjonowanie infrastruktury SIG z uwzględnieniem prywatnej chmury obliczeniowej administracji publicznej.

Podstawową cechą docelowej infrastruktury ma być zwiększenie mocy obliczeniowej i pojemności.

Centrum danych w Katowicach ma pełnić funkcję zdalnego centrum przechowywania kopii zapasowych danych. Replikacja odbywać się będzie przy pomocy dedykowanego łącza punkt-punkt.

7 Dostawa infrastruktury i oprogramowania

Dostarczone w ramach postępowania poszczególne elementy infrastruktury muszą spełniać poniższe wymagania:

1. Wszystkie oferowane urządzenia muszą być fabrycznie nowe (na dzień dostawy urządzenia nie mogą być starsze niż 6 miesięcy od daty produkcji oraz nie mogą być używane).
2. Oferowany sprzęt musi pochodzić z produkcji seryjnej i nie może być prototypem.
3. Dla dostarczanych rozwiązań musi istnieć możliwość wykupienia wsparcia technicznego u producenta danego rozwiązania.
4. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2000 lub normą równoważną. Zgodne z prawem obowiązującym w Unii Europejskiej dostarczone elementy infrastruktury muszą spełniać wytyczne dyrektywy CE (Conformité Européenne) i muszą być oznaczone znakiem CE.
5. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
6. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
7. Oferowane urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, a gwarancja (wsparcie techniczne) musi pochodzić od producenta i być świadczona przez sieć serwisową producenta na terenie Polski.
8. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: wkładek optycznych, kabli zasilających, kabli FC, kabli Ethernet, kabli optycznych Ethernet 10-40 Gbps oraz innych akcesoriów, niezbędnych do przeprowadzenia prawidłowej instalacji urządzeń.
9. Na dzień złożenia oferty oferowane urządzenia nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.

Dla wyspecyfikowanej infrastruktury oraz oprogramowania, Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji (na oprogramowanie) Zamawiającemu lub przeniesie na Zamawiającego niewyłączne uprawnienia licencyjne na czas nieoznaczony, tj. nieograniczony w czasie na korzystanie z dostarczonego oprogramowania.

Procedura przekazania oraz odbioru przedmiotu dostawy (infrastruktura sprzętowa wraz z oprogramowaniem) odbywać się będzie na poniższych zasadach:

1. Wykonawca zobowiązany jest przeprowadzić dostawę zgodnie z terminem określonym w ofercie.
2. Wykonawca zobowiązany jest przed przeprowadzeniem dostawy powiadomić (pisemnie lub poprzez wiadomość e-mail) Zamawiającego o planowanej dostawie (lub jej części), na co najmniej 3 dni robocze przed jej przeprowadzeniem.
3. Wykonawca zobowiązany jest przeprowadzić dostawę przedmiotu dostawy w godzinach uzgodnionych z Zamawiającym.
4. Po dostarczeniu przez Wykonawcę infrastruktury sprzętowej oraz oprogramowania podpisywany jest przez Strony, Protokół Odbioru Ilościowego stanowiący Załącznik nr 1, stwierdzający faktyczną ilość sztuk dostarczonej infrastruktury sprzętowej oraz oprogramowania.
5. Po zainstalowaniu i podstawowym skonfigurowaniu wszystkich dostarczonych elementów infrastruktury, zgodnie z zakresem przedstawionym w wymaganiach szczegółowych dla poszczególnych jednostek sprzętowych, Zamawiający zweryfikuje w terminie nie przekraczającym 14 dni, czy dostarczony przedmiot dostawy jest zgodny z OPZ. Po weryfikacji podpisywany jest Protokół Odbioru Dostawy.

Szczegółowe warunki wsparcia technicznego dla wszystkich wyspecyfikowanych w rozdziale 7 elementów infrastruktury:

1. Wykonawca udzieli Zamawiającemu nieodpłatną usługę wsparcia technicznego na dostarczoną infrastrukturę sprzętową.
2. Okres usługi wsparcia technicznego zarówno dla sprzętu i oprogramowania będzie obowiązywał dla poszczególnych elementów infrastruktury - od dnia zainstalowania poszczególnych elementów infrastruktury, do dnia podpisania przez Zamawiającego Protokołu Odbioru Dostawy oraz od dnia podpisania przez Zamawiającego Protokołu Odbioru Dostawy przez okres zgodny z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego”.
3. Usługa wsparcia technicznego obejmuje zobowiązanie Wykonawcy do terminowego usuwania wad i usterek sprzętu komputerowego oraz innych elementów stanowiących przedmiot dostawy.
4. Prawo do pobierania i instalowania aktualizacji firmware oraz oprogramowania systemowego, udostępnianego przez producenta sprzętu, w czasie trwania usługi wsparcia technicznego.
5. Prawo do pobierania i instalowania aktualizacji sygnatur bezpieczeństwa, udostępnianych przez producenta sprzętu, w czasie trwania usługi wsparcia technicznego.

6. Wykonawca zobowiązuje się do przyjmowania zgłoszeń w okresie trwania wsparcia technicznego (zgodnego z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego") w trybie 24/7
7. Wykonawca zobowiązuje się, iż w okresie usługi wsparcia technicznego na warunkach obowiązujących od momentu podpisania przez Zamawiającego Protokołu Odbioru dostawy, czas reakcji na zgłoszoną wadę lub usterkę, nastąpi nie później niż do końca kolejnego dnia od momentu zgłoszenia wady lub usterki.
8. Wykonawca zobowiązuje się, że w okresie usługi wsparcia technicznego na warunkach obowiązujących od momentu podpisania Protokołu Odbioru Dostawy, do dokonania bezpłatnej naprawy dostarczonego sprzętu, nie później niż do końca kolejnego dnia licząc od dnia, w którym dokonano zgłoszenia wady lub usterki, danego urządzenia.
9. Naprawa, zostanie dokonana w miejscu, w którym sprzęt został zainstalowany.
10. W przypadku braku możliwości wykonania przez Wykonawcę, naprawy w miejscu i w terminie, o którym mowa powyżej, Wykonawca zobowiązuje się dostarczyć i odpowiednio skonfigurować oraz zainstalować takie samo urządzenie wolne od wad i zapewni jego prawidłowe działanie. Po uruchomieniu urządzenia zastępczego zostanie spisany protokół wymiany urządzenia.
11. W przypadku uszkodzenia nośnika danych w stopniu takim, że nie będzie możliwa jego dalsza eksploatacja, Wykonawca zobowiązany jest do wymiany uszkodzonego nośnika danych na nowy. Uszkodzony nośnik danych pozostaje u Zamawiającego.
12. Wykonawca pokrywa wszelkie koszty związane z naprawami gwarancyjnymi.
13. Zamawiający ma prawo do dokonywania rozbudowy infrastruktury sprzętowej, zgodnie z dokumentacją techniczną i zaleceniami producenta, przez wykwalifikowanych pracowników, bez utraty wsparcia technicznego. Wykonawca nie ponosi odpowiedzialności za uszkodzenia przedmiotu Umowy powstałe z winy Zamawiającego.
14. Wsparcie techniczne (m.in. reakcja i czas naprawy) może być realizowane bezpośrednio przez Wykonawcę, przy czym Wykonawca zapewnia wykupienie gwarancji producenta na okres wskazany w ofercie.
15. Wykonawca zobowiązany jest do dostarczenia potwierdzenia wykupienia wsparcia technicznego u producentów sprzętu.

Wykonawca zobowiązany jest dostarczyć następujące elementy infrastruktury:

W wypadku wystąpienia w niniejszym Opisie Przedmiotu Zamówienia zastrzeżonych nazw własnych producentów lub produktów, zgodnie z art. 29 ust. 3 ustawy – Prawo Zamówień Publicznych,

dopuszcza się oferowanie produktów w pełni równoważnych do wymaganych przy pełnym zagwarantowaniu przez Wykonawcę zachowania całkowitej projektowanej funkcjonalności.

7.1 Rozwiązanie NAS typ A

Wymagania dotyczące dodatkowej przestrzeni dyskowej (tier II) dla istniejącej Jednolitej Infrastruktury Bazodanowej oraz centralnego urządzenia NAS, świadczącego usługę systemu pamięci masowej typu NAS i pamięci obiektowej.

1. Wymogi ogólne
   1.1. Oferowane rozwiązanie ma spełniać dwie role: dodatkowej przestrzeni dyskowej (tier II) dla istniejącej Jednolitej Infrastruktury Bazodanowej oraz centralnego urządzenia NAS świadczącego usługę systemu pamięci masowej typu NAS i pamięci obiektowej.
   1.2. Podsystem pamięci masowej spełniający wymagania NAS Typ A musi:
   - być podłączony do istniejącej Jednolitej Infrastruktury Bazodanowej za pomocą interfejsów o przepustowości całkowitej wynoszącej minimum 80 Gb/s realizowanych w technologii InfiniBand 40Gb/s lub 10 Gb Ethernet (łącze optyczne), połączenia muszą być redundantne;
   - zapewniać przepustowość dla ładowania danych bazodanowych do istniejącej Jednolitej Infrastruktury Bazodanowej nie niższą niż 2GB/s;
   - umożliwiać obsługę protokołów plikowych: NFS v3/v4, CIFS/SMB v2/v3, HTTP, WebDAV, FTP/SFTP/FTPS, Obiekty (REST). Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej.

   1.3. Usługa systemu pamięci masowej oferowanego urządzenia musi być wspierana przez producenta istniejącej Jednolitej Infrastruktury Bazodanowej.
   1.4. System pamięci masowej ma być dostarczony w zestawie z szafą/szafami RACK 19” o wysokości maksymalnej 42U i głębokości maksymalnej 1200mm.
2. Kontrolery systemu
   2.1. Kontrolery podsystemu pamięci masowej muszą obsługiwać zarządzaną przestrzeń dyskową, jej konfigurację, obsługę RAID i wszystkie wymienione niżej serwisy danych oraz zaawansowane funkcje monitoringu. Wymagane jest aby kontrolery pracowały w układzie Activ-Activ Concurent. Wymagane jest aby kontrolery oferowanego urządzenia były rozwiązaniem jednolitym technologicznie - wszystkie wymagane zapytaniem funkcjonalności myszą być możliwe do uruchomienia bez konieczności instalacji dodatkowych "głowic" czy urządzeń czy modułów zewnętrznych tego samego producenta lub firm trzecich. Ten sam

wymóg dotyczy wymaganych zapytaniem interfejsów - instalacja łączy Ethernet, Fibre Channel i InfiniBand. Zamawiający nie dopuszcza spełnienia wymogu poprzez użycie wszelkiego typu wirtualizatorów i urządzeń warstw pośrednich.

2.2. W celu zapewnienia odpowiedniej wydajności, pojedynczy kontroler podsystemu pamięci masowej musi posiadać sumarycznie nie mniej niż 4 jednostki CPU, a sumaryczna liczba rdzeni obliczeniowych nie może być mniejsza niż 72 na kontroler.

2.3. Kontrolery modułu pamięci podsystemu pamięci masowej muszą być wyposażone w szybką pamięć cache w oparciu o pamięć DRAM, a sumaryczna ilość pamięci cache dla całej macierzy musi być nie mniejsza niż 3000 GB.

2.4. Podsystem pamięci masowej musi umożliwiać rozbudowę pamięci DRAM o pamięć Cache L2 typu flash SSD. Rozbudowa do co najmniej 486 TB pamięci Cache L2.

3. Interfejsy

3.1. Podsystem pamięci masowej musi być wyposażony w:

- minimum 8 interfejsów 10Gb Base-T Ethernet;
- minimum 4 interfejsy, po dwa na każdy kontroler w technologii InfiniBand 40Gb/s i 4 interfejsy 10Gb Ethernet SFP+ lub 12 interfejsów 10Gb Ethernet SFP+;
- minimum 4 interfejsy 16Gb FC i obsługiwać protokół NDMP.

4. Serwisy danych

4.1. Podsystem pamięci masowej musi:

- posiadać funkcjonalność oraz licencje umożliwiające wykonanie kompresji danych oraz kopii chwilowych (snapshot) dla całej oferowanej przestrzeni dyskowej;
- mieć funkcjonalność zdalnej replikacji asynchronicznej. Jeżeli funkcjonalność ta wymaga licencji - powinna być ona zawarta w ofercie dla pełnej pojemności macierzy wyznaczonej jej zakresem skalowalności. System replikacji ma być w pełni kompatybilny z systemem pamięci masowej NAS typ B, oferowanym dla lokalizacji zapasowej (wymagania pkt.7.2). Połącznie w zespół replikacji zdalnej dwóch macierzy ma być rozwiązaniem jednolitym technologicznie i nie może wymagać instalacji urządzeń firm trzecich;
- wspierać możliwość transparentnej migracji danych z innych urządzeń świadczących sieciowe usługi plikowe. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej;
- mieć możliwość wykonywania cienkich (ang. thin clone / thin copy) kopii danych w trybie odczytu i zapisu. Jeżeli funkcjonalność ta wymaga licencji - powinna być ona

zawarta

w ofercie dla pełnej pojemności macierzy wyznaczonej jej zakresem skalowalności;

- mieć funkcjonalność szyfrowania danych mechanizmem AES 256-bit dla całej oferowanej przestrzeni dyskowej.

5. Możliwość podłączenia oferowanego podsystemu pamięci masowej typu NAS (wg. wymagania NAS typ A) do wewnętrznej magistrali InfiniBand istniejącej Jednolitej Infrasrtuktury Bazodanowej Zamawiającego.
6. Szczegółowe wymagania techniczne
   6.1. Podsystem pamięci masowej musi:
   - umożliwiać równoczesną obsługę wielu poziomów RAID tj. co najmniej RAID 0, 1, 5, 6 i 10 lub równoważnych;
   - być wyposażony w minimum 1600 GB pamięci flash SSD dla danych, pełniącej funkcję akceleratora dla klasycznych dysków obrotowych;
   - być wyposażony w minimum 2460 TB netto w RAID 6 na dyskach nie mniejszych niż 10 TB (poj. dysku brutto);
   - umożliwiać rozbudowę przestrzeni dyskowej poprzez dołożenie dodatkowych dysków twardych / dodatkowych półek dyskowych, do wielkości 7,2 PB przestrzeni surowej przy wykorzystaniu dysków nie większych niż 10 TB oraz bez konieczności zmiany architektury/generacji macierzy.

   6.2. Pojedyncza półka dyskowa do oferowanego podsystemu pamięci masowej musi mieć możliwość obsługi min. 24 napędów dyskowych.

   6.3. Dyski przeznaczone na dane muszą znajdować się w półkach dyskowych. W kontrolerach macierzowych mogą znajdować się jedynie pamięć cache oraz dyski przeznaczone na system operacyjny modułu pamięci masowej.
7. Zarządzanie
   7.1. Podsystem pamięci masowej musi:
   - umożliwiać zarządzanie zarówno z poziomu linii komend (CLI), jak również poprzez interfejs graficzny (GUI). Dostęp do urządzenia bezpośrednio z poziomu standardowych przeglądarek internetowych oraz klientów SSH. Wymagane jest wsparcie dla następujących metod zarządzania macierzą: HTTPS, SSH, SNMP v1/v2c, IPMI, RESTful API, OpenStack Cinder;
   - posiadać narzędzie umożliwiające obserwację danych wydajnościowych oraz ich graficzną prezentację w postaci wykresów. Monitorowanie wydajności macierzy musi być możliwe na podstawie parametrów takich jak: przepustowość sieci, przepustowość

dysków, liczba operacji I/O dla dysków oraz kontrolerów, opóźnienia zapisów/odczytów. Statystyki pracy elementów urządzenia muszą być widoczne w czasie rzeczywistym. Jeżeli uruchomienie takiej funkcjonalność wymaga licencji lub oprogramowania, taka licencja/oprogramowanie musi zostać dostarczona;

- mieć możliwość gromadzenia oraz prezentowania graficznego bieżących oraz historycznych danych wydajnościowych w postaci wykresów w GUI urządzenia.

8. Usług instalacji i wstępnej konfiguracji

Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:

- instalację fizyczną,
- podłączenie do sieci LAN/SAN,
- podłączenie do istniejącej Jednolitej Infrastruktury Bazodanowej
- aktualizację oprogramowania systemowego urządzenia,
- instalację jednej puli dyskowej i jej prezentacja do min. 2 serwerów

7.2 Rozwiązanie NAS typ B

Wymagania dotyczące podsystemu pamięci masowej typu NAS w lokalizacji zapasowej:

1. Wymogi ogólne
   1.1. Kontrolery podsystemu pamięci NAS muszą obsługiwać zarządzaną przestrzeń dyskową, jej konfigurację, obsługę RAID i wszystkie wymienione niżej serwisy danych oraz zaawansowane funkcje monitoringu. Wymagane jest aby kontrolery pracowały w układzie Activ-Activ Concurent. Wymagane jest aby kontrolery oferowanego urządzenia były rozwiązaniem jednolitym technologicznie - wszystkie wymagane zapytaniem funkcjonalności myszą być możliwe do uruchomienia bez konieczności instalacji dodatkowych "głowic" czy urządzeń czy modułów zewnętrznych tego samego producenta lub firm trzecich. Ten sam wymóg dotyczy wymaganych zapytaniem interfejsów - instalacja łączy Ethernet, Fibre Channel i InfiniBand. Zamawiający nie dopuszcza spełnienia wymogu poprzez użycie wszelkiego typu wirtualizatorów i urządzeń warstw pośrednich.
   1.2. W celu zapewnienia odpowiedniej wydajności, pojedynczy kontroler macierzy dyskowej typu NAS musi posiadać sumarycznie nie mniej niż 2 jednostki CPU, a sumaryczna liczba rdzeni obliczeniowych nie może być mniejsza niż 36 na kontroler.

1.3. Kontrolery modułu pamięci masowej muszą być wyposażone w szybką pamięć cache w oparciu o pamięć DRAM, a sumaryczna ilość pamięci cache dla całej macierzy musi być nie mniejsza niż 1500 GB.

1.4. Podsystem pamięci masowej musi umożliwiać rozbudowę pamięci DRAM o pamięć Cache L2 typu flash SSD. Rozbudowa do co najmniej 204TB pamięci Cache L2.

1.5. System pamięci masowej ma być dostarczony w zestawie z szafą/szafami RACK 19" o wysokości maksymalnej 42U i głębokości maksymalnej 1200mm.

2. Interfejsy

2.1. Podsystem pamięci masowej musi być wyposażony w:

- minimum 8 interfejsy 10Gb Base-T Ethernet,
- minimum 4 interfejsy 10Gb Ethernet SFP+,
- minimum 4 interfejsy 16Gb FC i obsługiwać protokół NDMP.

3. Serwisy Danych

3.1. Podsystem pamięci masowej musi:

- umożliwiać obsługę protokołów plikowych: NFS v3/v4, CIFS/SMB v2/v3, HTTP, WebDAV, FTP/SFTP/FTPS, Obiekty (REST). Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej;
- mieć funkcjonalność zdalnej replikacji asynchronicznej. Jeżeli funkcjonalność ta wymaga licencji - powinna być ona zawarta w ofercie dla pełnej pojemności NAS wyznaczonej jej zakresem skalowalności. System replikacji ma być w pełni kompatybilny z usługą podsystemu pamięci masowej pełniącym funkcję dodatkowej przestrzeni dyskowej (tear II) dla istniejącej Jednolitej Infrastruktury Bazodanowej oraz urządzenia NAS lokalizacji centralnej (NAS typ A wymagania pkt. 7.1). Połącznie w zespół replikacji zdalnej dwóch macierzy typu NAS ma być rozwiązaniem jednolitym technologicznie i nie może wymagać instalacji urządzeń firm trzecich;
- wspierać możliwość transparentnej migracji danych z innych urządzeń świadczących sieciowe usługi plikowe. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej;
- posiadać funkcjonalność oraz licencje umożliwiające wykonanie kompresji danych oraz kopii chwilowych (snapshot) dla całej oferowanej przestrzeni dyskowej;
- mieć możliwość wykonywania cienkich (ang. thin clone / thin copy) kopii danych w trybie odczytu i zapisu.

- mieć funkcjonalność szyfrowania danych mechanizmem AES 256-bit dla całej oferowanej przestrzeni dyskowej.

4. Szczegółowe wymagania techniczne

4.1. Podsystem pamięci masowej musi:

- umożliwiać równoczesną obsługę wielu poziomów RAID tj. co najmniej RAID 0, 1, 5, 6 i 10 lub równoważnych;
- być wyposażony w minimum 2280 TB netto w RAID 6 na dyskach nie mniejszych niż 10TB (poj. dysku brutto).
- być wyposażony w minimum 800 GB pamięci flash SSD dla danych, pełniącej funkcję akceleratora dla klasycznych dysków obrotowych.
- umożliwiać rozbudowę przestrzeni dyskowej poprzez dołożenie dodatkowych dysków twardych / dodatkowych półek dyskowych, do wielkości 3,0 PB przestrzeni surowej przy wykorzystaniu dysków nie większych niż 10 TB oraz bez konieczności zmiany architektury/generacji macierzy.

4.2. Pojedyncza półka dyskowa do oferowanego modułu pamięci masowej musi mieć możliwość obsługi minimum 24 napędów dyskowych.

4.3. Dyski przeznaczone na dane muszą znajdować się w półkach dyskowych. W kontrolerach macierzowych mogą znajdować się jedynie pamięć cache oraz dyski przeznaczone na system operacyjny modułu pamięci masowej.

5. Zarządzanie

5.1. Podsystem pamięci masowej musi:

- umożliwiać zarządzanie zarówno z poziomu linii komend (CLI), jak również poprzez interfejs graficzny (GUI). Dostęp do urządzenia bezpośrednio z poziomu standardowych przeglądarek internetowych oraz klientów SSH.Wymagane jest wsparcie dla następujących metod zarządzania macierzą: HTTPS, SSH, SNMP v1/v2c, IPMI, RESTful API, OpenStack Cinder;
- posiadać narzędzie umożliwiające obserwację danych wydajnościowych oraz ich graficzną prezentację w postaci wykresów. Monitorowanie wydajności macierzy musi być możliwe na podstawie parametrów takich jak: przepustowość sieci, przepustowość dysków, liczba operacji I/O dla dysków oraz kontrolerów, opóźnienia zapisów/odczytów. Statystyki pracy elementów urządzenia muszą być widoczne w czasie rzeczywistym. Jeżeli uruchomienie takiej funkcjonalność wymaga licencji lub oprogramowania, taka licencja/oprogramowanie musi zostać dostarczona;

- mieć możliwość gromadzenia oraz prezentowania graficznego bieżących oraz historycznych danych wydajnościowych w postaci wykresów w GUI urządzenia.

6. Usług instalacji i wstępnej konfiguracji

Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:

- instalację fizyczną,
- podłączenie do sieci LAN/SAN,
- aktualizację oprogramowania systemowego urządzenia,
- instalację jednej puli dyskowej i jej prezentacja do min. 2 serwerów.

7.3 Macierz blokowa

Macierz dyskowa rozumiana jako zestaw dysków twardych kontrolowanych przez nadmiarowe, dedykowane kontrolery macierzowe bez jakichkolwiek dodatkowych urządzeń pośrednich czy serwerów wirtualizujących.

1. Typ obudowy:
   1.1. Macierz musi być przystosowana do montażu w szafie rack 19”
2. Kontrolery:
   2.1. Oferowane urządzenie musi posiadać minimum 2 kontrolery pracujące w trybie Active-Active z funkcją Mirrored cache.
   2.2. Komunikacja pomiędzy wszystkimi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem protokołów FC/Ethernet/Infiniband.
   2.3. Dla zapewnienia najwyższej wydajności, maksymalna konfiguracja macierzy musi wspierać tworzenie wolumenów rozłożonych na wszystkich dyskach macierzy (tzw. wide-striping) i ich jednoczesne, aktywne udostępnianie ze wszystkich kontrolerów macierzy.
   2.4. Macierz musi:
      - posiadać min. 128 GiB wbudowanej pamięci cache (bez posiłkowania się dyskami SSD),posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych.
3. Interfejsy:
   3.1. Macierz musi posiadać min. 8 interfejsów FC 16Gb i 4 interfejsy 1Gb

4. Przestrzeń dyskowa:
   4.1. Macierz musi:
   - obsługiwać dyski SSD, SAS i Nearline SAS. Musi umożliwiać mieszanie napędów dyskowych SSD, SAS i Nearline SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. być wyposażona w dyski posiadające podwójne interfejsy.obsługiwać mechanizmy RAID zgodne z RAID0, RAID1 lub RAID10, RAID5 lub RAID50 oraz RAID6 lub RAID60 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping).

   4.2. Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: kontroler,półka dyskowa, dysk, zasilacz.

   4.3. Możliwość definiowania różnych poziomów RAID na tych samych dyskach fizycznych. Jeżeli nie jest możliwe uzyskanie takiej funkcjonalności, dla uzyskania podobnej wydajności wymagane jest zrealizowanie żądanej pojemności większą o 50% liczbą dysków fizycznych.

   4.4. Macierz musi umożliwiać definiowanie globalnych dysków spare lub odpowiedniej zapasowej przestrzeni dyskowej. Oferowana konfiguracja dyskowa musi zawierać rekomendowaną przez producenta ilość dysków spare lub odpowiednią zapasową przestrzeń dyskową.

   4.5. Wymagana minimalna wielkość użytkowej przestrzeni dyskowej:
   - SSD: min. 50TiB w RAID 6, przy zastosowaniu min. 24 dysków
   - SAS 10k: min. 460TiB w RAID 6, przy zastosowaniu min. 360 dysków

   4.6. Macierz musi, w dostarczonej konfiguracji, przy obciążeniu losowym (ang. random) o charakterystyce R/W = 50%/50% dla bloku 8 kB, być w stanie osiągnąć dla poszczególnych typów dysków, minimalną wydajność na poziomie:
   - SSD: 200 tys. IOps
   - SAS 10k: 40 tys.Iops

   Wykonawca jest zobowiązany do przedstawienia, dla zaproponowanej konfiguracji, szacunków wydajności na podstawie danych katalogowych lub raportu z dedykowanego narzędzia producenta.

   4.7. Możliwość rozbudowy do min. 576 dysków twardych bez konieczności dodawania lub wymiany kontrolerów macierzy.

5. Funkcjonalności:
   5.1. Zarządzanie grupami dyskowymi oraz dyskami logicznymi:

- Macierz musi umożliwiać dynamiczne zwiększania pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych.
- Macierz musi umożliwiać zmianę technologii dyskowej oraz poziomu zabezpieczenia RAID dla wolumenu dyskowego w sposób transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów.

Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy."

5.2. Thin Provisioning:

- Macierz musi umożliwiać tworzenie zasobów dyskowych typu Thick oraz Thin.
- Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny, bez konieczności ręcznego uruchamiania dodatkowych procesów na kontrolerach macierzy (wymagana obsługa standardu T10 SCSI UNMAP).

Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy.

5.3. Wewnętrzne kopie migawkowe

Macierz musi umożliwiać wykonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach danej macierzy, za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa ma być wykonywana bez alokowania dodatkowej przestrzeni dyskowej na jej potrzeby. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.

Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy."

5.4. Wewnętrzne kopie pełne

Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach danej macierzy, za pomocą wewnętrznych kontrolerów macierzowych. Wykonana kopia danych musi mieć możliwość zabezpieczenia innym poziomem RAID oraz innej grupie/puli dyskowej niż dane źródłowe.

Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy."

5.5. Migracja danych w obrębie macierzy:

Macierz dyskowa musi umożliwiać migrację danych, bez przerywania do nich dostępu, pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów

logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy.

Funkcjonalność musi umożliwiać istnienie zasobu LUN, który fizycznie będzie znajdował się na różnych typach dysków (SSD, SAS, NL) obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów.

Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy.

5.6. Zdalna replikacja danych

Macierz musi umożliwiać replikację zdalną w następujących trybach: jeden do jednego, jeden do wielu, wiele do jednego oraz replikację jednego wolumenu logicznego (tych samych danych) do dwóch innych niezależnych ośrodków za pomocą replikacji synchronicznej i asynchronicznej. Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zamiany ról oryginału i kopii (dla określonej pary dysków logicznych LUN macierzy) z poziomu interfejsu administratora.

Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.

Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem różnych portów macierzy FC/IP.

5.7. Zarządzanie wydajnością

Macierz musi umożliwiać konfigurację gwarancji wydajności typ QoS (możliwość definiowania progów minimalnych i maksymalnych) dla wybranych wolumenów logicznych w zakresie takich parametrów jak: wydajność w IOPS, wydajność w MB/s, opóźnienie w ms.

Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy.

5.8. Redukcja objętości danych

Macierz musi umożliwiać deduplikację i kompresję danych na poziomie blokowym (co najmniej w odniesieniu do danych na dyskach SSD). Musi istnieć możliwość uruchomienia deduplikacji i kompresji (niezależnie i łącznie) na poziomie pojedynczych wolumenów logicznych. Deduplikacja i kompresja danych musi odbywać się w locie, przed zapisaniem danych na dyskach macierzy. Musi istnieć możliwość wykonania operacji odwrotnej – wyłączenia deduplikacji i kompresji na określonych wolumenach logicznych. Deduplikacja i

kompresja nie mogą być realizowane za pomocą zewnętrznego urządzenia lub oprogramowania.

Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy.

5.9. Partycjonowanie macierzy

Macierz musi umożliwiać podział macierzy na minimum 8 odseparowanych macierzy logicznych zarządzanych przez dedykowanych administratorów.

Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy.

6. Nadmiarowość:

6.1. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.

6.2. Macierz musi:

- umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory,mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy,umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania dostępu do danych,umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii.

6.3. Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego.

6.4. Macierz musi umożliwiać tworzenie skryptów użytkownika do automatyzacji różnych zadań.

6.5. Oprogramowanie do zarządzania macierzą musi zapewniać stałe monitorowanie jej stanu oraz umożliwiać konfigurowanie jej zasobów dyskowych.

Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów.

Wymagane jest monitorowanie bieżących parametrów pracy macierzy, w tym minimum:

- prezentowanie stanu macierzy, adresu zarządzającego IP macierzą, nazwy macierzy (model), numeru seryjnego i poziomu oprogramowania układowego macierzy;
- prezentowanie dostępnej przestrzeni na macierzy z zaznaczeniem przestrzeni wolnej do zapisu i już zapisanej (zaalokowanej);
- prezentacji w formie graficznej grup dyskowych, dysków, szablonów dysków. Konieczne jest prezentowanie tych danych w formie mapy określającej powiązania logiczne

pomiędzy tymi komponentami – np. które dyski (wolumeny) należą do danej grupy dyskowej;

- tworzeniu szablonów dysków, składających się z nazwy, przyporządkowania do grupy dyskowej, pojemności dysku, typu (Thin, Full), sposobu udostępniania (prywatny dysk dedykowany serwerowi lub dysk współdzielony pomiędzy kilkoma serwerami). Z danego szablonu musi istnieć możliwość tworzenia dysku (wolumenu) o wskazanych w szablonie parametrach;

Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy.

6.6. Wymaga się aby oprogramowanie do zarządzania macierzą pochodziło od producenta macierzy.

7. Współpraca ze środowiskiem serwerowym

7.1. Macierz musi:

- umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności - co najmniej dwoma ścieżkami. Macierz dyskowa musi wspierać obsługę minimum 128 hostów podłączonych poprzez sieć SAN. wspierać między innymi następujące systemy operacyjne na podłaczonych hostach: Windows, Linux, VMware, IBM AIX, Oracle Solaris, HP-UX. Macierz musi posiadać wsparcie dla różnych systemów klastrowych, co najmniej VMware Metrocluster, HPE Serviceguard Metrocuster, Microsoft Cluster. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów.

7.2. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów.

Preferowane jest rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. W przypadku stosowania rozwiązań firmowych/własnych – konieczna jest ich certyfikacja dla platform: Windows 2012+, Linux RedHat 7.x+, Suse12+, VMware 5,5+

Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby hostów wspieranych przez oferowaną macierz.

8. Wymagania dodatkowe:

8.1. Instalacja lub uruchamianie dodatkowej funkcjonalności macierzy dyskowej nie może powodować zmniejszenia dostępnego obszaru pamięci cache danych kontrolerów macierzowych.

9. Usługi instalacji i konfiguracji wstępnej:

- Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:instalacja fizyczna,
- podłączenie SAN oraz LAN,
- inicjalizacja macierzy,
- aktualizacja oprogramownia systemowego utworzenie i prezentacja testowego zasobu dyskowego maks. do dwóch hostów fizycznych (z pojedynczym OS).

Wymiana dysków SSD w ramach wsparcia technicznego producenta, w związku ze zużyciem bloków pamięci > 95%, w oferowanej macierzy blokowej, musi być zgodna z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego".

7.4 Serwery blade

1	Wymagania ogólne:
1.1	Zainstalowane 2 procesory, minimum 12 rdzeni każdy, x86 - 64 Bit osiągające w testach SPECint_rate2006 wynik Base nie gorszy niż 1100 punktów w konfiguracji dwuprocesorowej.
1.2	Zainstalowane 1TB RAM DDR4 LoadReduces DIMM w modułach min. 64GB. Minimum 16 slotów na pamięć.
1.3	Minimum jeden wewnętrzny port USB umożliwiający instalację pamięci Flash.
1.4	Minimum 2 sloty PCI-Express x8 (szybkość slotu).
1.5	Dwa Interfejsy SAN FC 16Gb.
1.6	Minimum 2 Interfejsy sieciowe 20GbE lub minimum 4 interfejsy sieciowe 10GbE
1.7	Wspierane systemy operacyjne: MS Windows 2012 R2, MS Windows 2016, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware 6.0, VMware 6.5, VMware 6.7.
2	Usługi instalacji i wstępnej konfiguracji.

Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:

- instalację w infrastrukturze blade
- aktualizację FW

7.5 Serwery bazodanowe

Wymagania ogólne:

1) Zainstalowane 4 procesory, minimum 24 rdzeni każdy, x86 - 64 bit z taktowaniem min. 2,1GHz i mocą nie przekraczającą 145W.
2) Zainstalowane 2048 GB RAM DDR4 LoadReduces DIMM w modułach min. 64GB.
3) 2 dyski SSD typu Hot Swap każdy o pojemności minimum 240GB.
4) Kontroler dysków obsługujący poziomy RAID 0/1 z 2GB Cache podtrzymywanym bateryjnie.
5) 4 redundantne zasilacze typu Hot-plug.
6) Zestaw redundantnych wentylatorów.
7) Minimum 2 sloty PCI-Express x16 (szybkość slotu).
8) Dwa interfejsy SAN FC 16Gb.
9) Minimum 2 interfejsy sieciowe 1GbE i 4 interfejsy sieciowe 10GbE z wkładkami SFP+ SR.
10) Wspierane systemy operacyjne: MS Windows 2012 R2, MS Windows 2016, Red Hat Enterprise Linux, CentOS.
11) Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.
    Wraz z serwerem należy dostarczyć oprogramowanie do zarządzania serwerem, pozwalające na:
    a) Inwentaryzację sprzętu serwerowego, monitoring zdrowia - „health status”,
    b) zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci),
    c) zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego,
    d) zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu,
    e) monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć i zasilania.
12) Usługi instalacyjne:
    Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:
    - instalację w szafie RACK
    - aktualizację FW
    - konfigurację karty zdalnego monitoringu i zarządzania

7.1 Serwery RACK

Wymagania ogólne:

1. Zainstalowany 1 procesor, maksimum 6 rdzeni, x86 - 64 Bit osiągający w testach SPECint_rate2006 wynik Base nie gorszy niż 812 punktów w konfiguracji dwuprocesorowej.
2. Zainstalowane 512GB RAM DDR4 LoadReduces DIMM w modułach min. 64GB.
3. 2 dyski SSD typu Hot Swap, każdy o pojemności minimum 960GB.
4. Kontroler dysków obsługujący poziomy RAID 0/1 z 2GB Cache podtrzymywanym bateryjnie.
5. 2 redundantne zasilacze typu Hot-plug o mocy min. 500W
6. Zestaw redundantnych wentylatorów.
7. Minimum 2 sloty PCI-Express x16 (szybkość slotu).
8. Dwa Interfejsy SAN FC 16Gb.
9. Minimum 4 Interfejsy sieciowe 1GbE i 2 Interfejsy sieciowe 10GbE (wkładki SFP+ SR)
10. Wspierane systemy operacyjne: MS Windows 2012 R2, MS Windows 2016, Red Hat Enterprise Linux, CentOS.
11. Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.

    Wraz z serwerem należy dostarczyć oprogramowanie do zarządzania serwerem, pozwalające na:

    a. Inwentaryzację sprzętu serwerowego, monitoring zdrowia - „health status”,
    b. zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci),
    c. zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego,
    d. zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu,
    e. monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć i zasilania.

12. Usługi instalacyjne:

Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:

1. instalację w szafie RACK
2. aktualizację FW
3. konfigurację karty zdalnego monitoringu i zarządzania

7.2 Firewall do sieci Internet

Wymagania podstawowe dla Firewall do sieci Internet:

1	Wymagania podstawowe:
1.1	System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
1.2	System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 18 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 9 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń.
1.3	System zabezpieczeń firewall musi być wyposażony w co najmniej 4 porty Ethernet 100/1G/10G, 16 portów 1G/10G SFP/SFP+, 4 porty 40G QSFP+.
1.4	Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.
1.5	System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.
1.6	System zabezpieczeń firewall musi obsługiwać nie mniej niż 20 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy

routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.

1.7 System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).

1.8 System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.

1.9 Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 18 Gbit/s.

1.10 System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.

1.11 System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

1.12 System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.

1.13 System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

1.14 System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji,

wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.

1.15 System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

1.16 Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.

2 Wymagania podstawowe - identyfikacja użytkowników

2.1 System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

3 Wymagania ochrony: IPS, AV, anty-spyware, URL, zero-day:

3.1 System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

3.2 System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

3.3 System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

3.4 System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

3.5 System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

3.6 System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

3.7 System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

3.8 System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

3.9 System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.

3.10 System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.

3.11 System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.

4 Wymagania w zakresie: NAT, DoS, IPSEC VPN, SSL VPN, QoS:

4.1 System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.

4.2 System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

4.3 System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.

4.4 System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.

4.5 System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.

4.6 System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.

4.7 System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.

5 Wymagania w zakresie zarządzania i raportowania:

5.1 Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.

5.2 System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.

5.3 System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.

6 Dostęp do urządzenia i zarządzanie z sieci

6.1 Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.

6.2 System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.

6.3 System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).

6.4 System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.

6.5 System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.

6.6 System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.

6.7 System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.

7 Wymagania w zakresie środowiska wirtualnego Vmware

7.1 System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.

8 Wymagania rozszerzone w zakresie wymagań podstawowych

8.1 Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).

8.2 Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).

8.3 System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.

8.4 Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).

8.5 Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.

8.6 Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.

8.7 System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

8.8 System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.

8.9 System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.

8.10 System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.

8.11 System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.

8.12 System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

9 Wymagania rozszerzone w zakresie identyfikacji użytkowników

9.1 System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu

łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.

9.2 System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.

9.3 Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

10 Wymagania rozszerzone w zakresie identyfikacji użytkowników

10.1 System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.

10.2 System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.

10.3 Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

11 Wymagania rozszerzone w zakresie ochrony IPS, AV, anty-spyware, URL, zero-day

11.1 System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.

11.2 System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

11.3 System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

11.4 System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).

12 Wymagania rozszerzone w zakresie NAT, DoS, IPSEC VPN, SSL VPN, QoS

12.1 System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.

12.2 System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

13 Wymagania rozszerzone w zakresie zarządzania i raportowania

13.1 System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.

13.2 System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

13.3 System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.

13.4 System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.

13.5 System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.

13.6 System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.

13.7 System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

14 Usługi instalacyjne i konfiguracyjne:

Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:

- instalację w szafie RACK,
- nadanie adresu IP dla sieci zarządzającej,

- aktualizację FW.

7.3 Router BGP

1. Wymagania
   1.1. Urządzenie musi być wyposażone w minimum: dwa porty 4 porty typu Combo 1GEthernet (1GBase-T/SFP), 2 porty 10GbEthernet SFP+, 16 portów SFP. Porty SFP mają być obsadzone wkładkami SFP: 4x1000Base-LX, 4x1000Base-SX, 8x1000Base-T. Wkładki SFP/SFP+ muszą pochodzić od producenta urządzenia.
   1.2. Urządzenie musi posiadać minimum jeden wolny slot na rozbudowę o dodatkowe porty.
   1.3. Musi istnieć możliwość rozbudowy urządzenia do 36 portów 1GbEthernet lub 6 portów 10GbEthernet. Rozbudowa może być wykonana poprzez wymianę istniejących portów.
   1.4. Urządzenie musi posiadać dodatkowo:
      - port konsoli szeregowy RJ-45,
      - port USB,
      - port Ethernet do zarządzania out-of-band.
   1.5. Wysokość urządzenia nie może przekraczać 2U.
   1.6. Urządzenie musi być wyposażone w dwa redundantne zasilacze 230V. Musi jednak istnieć możliwość jego wyposażenia w dwa redundantne zasilacze na prąd stały.
   1.7. Urządzenie musi posiadać możliwość wymiany wentylatorów.
   1.8. Urzadzenie musi posiadać modularny system operacyjny.
   1.9. Wymagana jest minimalna przepustowość urządzenia: 20Gbps i 15Mpps.
   1.10. Wymagana jest wydajność dla IPSec na poziomie minimum: 4.8Gbps.
   1.11. Wymagana jest tablica routingu RIB była wielkości 4mln.
   1.12. Urządzenie musi być zbudowane w technologii pozwalającej na połączenie dwóch urządzeń tego typu w klaster działający jako jedno logiczne urządzenie.
   1.13. Wymagana jest ochrona procesora przed atakami DoS
   1.14. Wymagane jest wsparcie dla:
      - protokołów routingu: RIP/RIPng, OSPF/OSPFv3, IS-IS/IS-ISv6, BGP/BGP4+, PIM/PIM6, MSDP, MBGP, policy based routing,
      - protokołów MPLS: LDP, MPLS TE, L3 VPN, L2 VPN, VPLS, Multicast VPN, 6PE, 6vPE
      - rozwiązań związanych z bezpieczeństwem: filtrowanie pakietów, pełnostanowy firewall, wykrywanie ataków, ochrona control plane przez ograniczanie ruchu, uRPF, L2TP, GRE, IPSec VPN, Auto-discovery VPN (ADVPN) i Group Domain VPN (GDVPN)

- funkcji QoS: kolejkowanie, zapobieganie przeciążeniom, priorytetyzacja, hierarchiczny QoS

1.15. Wymagane jest wsparcie dla następujących standardów BGP:

- RFC 1657 Definitions of Managed Objects for BGPv4
- RFC 1772 Application of the BGP
- RFC 1773 Experience with the BGP-4 Protocol
- RFC 1774 BGP-4 Protocol Analysis
- RFC 1965 BGP4 confederations
- RFC 1966 BGP Route Reflection An alternative to full mesh IBGP
- RFC 1997 BGP Communities Attribute
- RFC 1998 PPP Gandalf FZA Compression Protocol
- RFC 2385 BGP Session Protection via TCP MD5
- RFC 2439 BGP Route Flap Damping
- RFC 2842 Capability Advertisement with BGP-4
- RFC 2858 BGP-4 Multi-Protocol Extensions
- RFC 2918 Route Refresh Capability
- RFC 4271 A Border Gateway Protocol 4 (BGP-4)
- RFC 4272 BGP Security Vulnerabilities Analysis
- RFC 4274 BGP-4 Protocol Analysis
- RFC 4275 BGP-4 MIB Implementation Survey
- RFC 4276 BGP-4 Implementation Report
- RFC 4277 Experience with the BGP-4 Protocol
- RFC 4360 BGP Extended Communities Attribute
- RFC 4451 BGP MULTI_EXIT_DISC (MED) Considerations
- RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
- RFC 4486 Subcodes for BGP Cease Notification Message
- RFC 4724 Graceful Restart Mechanism for BGP
- RFC 4760 Multiprotocol Extensions for BGP-4
- RFC 4893 BGP Support for Four-octet AS Number Space
- RFC 5065 Autonomous System Confederations for BGP RFC 5291 Outbound Route Filtering Capability for BGP-4
- RFC 5292 Address-Prefix-Based Outbound Route Filter for BGP-4
- RFC 5398 Autonomous System (AS) Number Reservation for Documentation Use
- RFC 5883 BFD for Multihop Paths

1.16. Wsparcie dla następujących standardów i protokołów związanych z zarządzaniem urządzeniem:

- RFC 1155 Structure and Mgmt Information (SMIv1)
- RFC 1157 SNMPv1/v2c
- RFC 1305 NTPv3
- RFC 1901 (Community based SNMPv2)
- RFC 1901-1907 SNMPv2c, SMIv2 and Revised MIB-II
- RFC 1902 (SNMPv2)
- RFC 1908 (SNMP v1/2 Coexistence)
- RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0
- RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1
- RFC 2271 FrameWork
- RFC 2452 MIB for TCP6
- RFC 2454 MIB for UDP6
- RFC 2573 (SNMPv3 Applications)
- RFC 2576 (Coexistence between SNMP V1, V2, V3)
- RFC 2578-2580 SMIv2
- RFC 2579 (SMIv2 Text Conventions)
- RFC 2580 (SMIv2 Conformance)
- RFC 2819 (RMON groups Alarm, Event, History and Statistics only)
- RFC 2819 RMON
- RFC 3410 (Management Framework)
- RFC 3416 (SNMP Protocol Operations v2)
- RFC 3417 (SNMP Transport Mappings)
- SNMP v3 and RMON RFC support
- SSHv1/SSHv2 Secure Shell
- TACACS/TACACS+

1.17. Wsparcie dla następujących protokołów związanych z QoS:

- IEEE 802.1P (CoS)
- RFC 2309 Recommendations on queue management and congestion avoidance in the Internet
- RFC 2474 DiffServ Precedence, including 8 queues/port
- RFC 2474 DiffServ precedence, with 4 queues per port
- RFC 2474 DS Field in the IPv4 and IPv6 Headers

- RFC 2474 DSCP DiffServ
- RFC 2474, with 4 queues per port
- RFC 2475 DiffServ Architecture
- RFC 2597 DiffServ Assured Forwarding (AF)
- RFC 2597 DiffServ Assured Forwarding (AF)- partial support
- RFC 2598 DiffServ Expedited Forwarding (EF)
- RFC 2697 A Single Rate Three Color Marker
- RFC 2698 A Two Rate Three Color Marker
- RFC 2751 Signaled Preemption Priority Policy Element
- RFC 3247 Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)
- RFC 3260 New Terminology and Clarifications for DiffServ
- RFC 3662 A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services
- RFC 4594 Configuration Guidelines for DiffServ Service Classes

1.18. Wsparcie dla następujących standardów sieciowych RFC i IETF:

- IEEE 802.1ad Q-in-Q
- IEEE 802.1ag Service Layer OAM
- IEEE 802.1AX-2008 Link Aggregation
- IEEE 802.1D MAC Bridges
- IEEE 802.1p Priority
- IEEE 802.1Q (GVRP)
- IEEE 802.1Q VLANs
- IEEE 802.1s Multiple Spanning Trees
- IEEE 802.1v VLAN classification by Protocol and Port
- IEEE 802.1w Rapid Reconfiguration of Spanning Tree
- IEEE 802.1X PAE
- IEEE 802.3 Type 10BASE-T
- IEEE 802.3ab 1000BASE-T
- IEEE 802.3ac (VLAN Tagging Extension)
- IEEE 802.3ad Link Aggregation (LAG)
- IEEE 802.3ae 10-Gigabit Ethernet
- IEEE 802.3ag Ethernet OAM
- IEEE 802.3z 1000BASE-X
- RFC 1305 NTPv3

- RFC 3623 Graceful OSPF Restart
- RFC 3704 Unicast Reverse Path Forwarding (URPF)
- RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
- RFC 3768 Virtual Router Redundancy Protocol (VRRP)
- RFC 3784 ISIS TE support
- RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)
- RFC 5880 Bidirectional Forwarding Detection

2. Usługi instalacyjne i konfiguracyjne:

Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:

- instalację w szafie RACK,
- nadanie adresu IP dla sieci zarządzającej,
- aktualizację oprogramowania.

7.4 Przełącznik SAN

1. Wymagania

1.1. Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.

1.2. W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8, 4 lub 2 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.

1.3. Przełącznik FC musi być wyposażony, w co najmniej 36 aktywnych portów FC obsadzonych wkładkami SFP 16Gb/s.

1.4. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC.

1.5. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 1536 Gb/s end-to-end full duplex.

1.6. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 1,2µs.

1.7. Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.

1.8. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19".

1.9. Przełącznik FC posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie „na gorąco" bez przerywania pracy przełącznika.

1.10. Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.

1.11. Przełącznik FC musi wspierać mechanizm balansowania ruchu, pomiędzy co najmniej 6 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.

1.12. Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Jednoczesne wykorzystanie obu mechanizmów powinno zapewnić dla dowolnej pary komunikujących się urządzeń końcowych uzyskanie kanału komunikacyjnego o zagregowanej przepustowości 768Gb/s half duplex.

1.13. Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.

1.14. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. Dopuszczalne jest wykonanie restartu przełącznika przy operacji wymiany kodu, przy jednoczesnym zapewnieniu redundancji połączeń FC pomiędzy przełącznikami FC, a urządzeniami, zapewniając bezprzerwowy dostęp do zasobów.

1.15. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:

a. mechanizm szyfrowania i kompresji wybranych połączeń ISL wspierany, na co najmniej 2 portach przełącznika FC. Symetryczny klucz szyfrujący nie może być krótszy niż 256-bitów.
b. mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric
c. uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP
d. uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP
e. szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.
f. definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)
g. definiowane kont administratorów w środowisku RADIUS i LDAP
h. szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
i. obsługa SNMP v1 oraz v3
j. IP Filter dla portu administracyjnego przełącznika
k. wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
l. wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP

1.16. Przełącznik FC musi mieć możliwość konfiguracji przez:

a. polecenia tekstowe w interfejsie znakowym konsoli terminala,
b. przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.

1.17. Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:

a. logowanie zdarzeń poprzez mechanizm „syslog”,
b. port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla wkładek SFP 16Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric.
c. FC ping
d. FC traceroute
e. kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika.

1.18. Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 8Gb/s.

1.19. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC.

1.20. Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S.

1.21. W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne

usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisanie dedykowanego administratora.

1.22. Musi istnieć możliwość połączenia wybranych logicznych przełączników wydzielonych w różnych fizycznych przełącznikach FC za pomocą dedykowanych połączeń ISL. Połączone w ten sposób przełączniki muszą tworzyć pojedynczą sieć fabric.

1.23. Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.

1.24. Przełącznik FC musi obsługiwać protokół FCP na dowolnych portach przełącznika.

1.25. Usługi instalacyjne i konfiguracyjne:

Wymaga się wykonania usług instalacji i konfiguracji wstępnej, zawierających minimum:

- instalację w szafie RACK,
- nadanie adresu IP dla sieci zarządzającej,
- aktualizację FW.

7.5 Oprogramowanie do wykonywania kopii zapasowej środowiska wirtualizacji

Dostarczenie 1 kompletu licencji na oprogramowanie do wykonywania kopii bezpieczeństwa posiadanego przez Zamawiającego środowiska wirtualizacji VMware vSphere Enterprise plus na:

1) 4 szt. dostarczanych serwerów blade,
2) 2 szt. Dostarczanych serwerów bazodanowych,
3) 5 szt. Dostarczanych serwerów RACK,
4) 13 szt. posiadanych przez Zamawiającego serwerów (sumarycznie 52 CPU i 528 rdzeni):
   a) 7 szt. serwerów, każdy po 4 CPU 12 core/CPU,
   b) 6 szt. serwerów, każdy po 4 CPU 8 core/CPU.

Wszystkie licencje mają być dostarczone wraz ze wsparciem technicznym z czasem trwania wsparcia technicznego, zgodnym z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego”, świadczonym

przez producenta będącego licencjodawcą oprogramowania, które powinno umożliwiać zgłaszanie problemów 5 dni w tygodniu przez 12h na dobę oraz pobieranie i instalowanie nowych poprawek, wersji oprogramowania.

Wymaganie:

1 Oferowane licencje muszą zapewnić backup / odtwarzanie środowiska VMware składającego się z 20 serwerów ESX posiadających łącznie 40 fizycznych procesorów

2 System centralnego backupu musi umożliwiać dla powyżej definiowanego środowiska VMware backup/odtwarzanie nielimitowanej liczby maszyn wirtualnych: Zarówno backup obrazów maszyn wirtualnych jak również backup ze środka maszyn wirtualnych wszystkimi dostępnymi agentami oprogramowania backupowego

3 Wymaga się by w ramach oferowanych licencji system umożliwiał backup maszyn wirtualnych w każdym trybie:
   a) Jako obrazy maszyn wirtualnych VMware(pliki vmdk)
   b) Ze środka, agentem plikowym / bazodanowym / aplikacyjnym dla systemów plików Oracle, SQL, Sybase, DB2, Exchange, Lotus, Sharepoint

4 Musi być możliwość backupu jak powyżej dla dowolnej liczby maszyn wirtualnych w ramach zaintonowanych serwerów ESX.

5 Serwer backupu musi być dostarczony do zainstalowania na 2 fizycznych serwerach zarządzających backupem i odtwarzaniem całości zabezpieczanego środowiska.

6 Oferowany system musi tworzyć centralny system backupu wykonujący kopie zapasowe oraz zapewniać przechowywanie wszystkich zdeduplikowanych kopii zapasowych na dyskach posiadanego prze Zamawiającego de-duplikatora.

7 Całość backupów musi być składowana na posiadanym przez Zamawiającego de-duplikatorze EMC DataDomain..

8 Oprogramowanie backupowe musi być wspierane (kompatybilne) z posiadanym przez Zamawiającego de-duplikatorem EMC DataDomain.

9 Każdy z serwerów backupu musi umożliwiać:
   a) zarządzanie backupem lokalnego środowiska i związanych z nim zdalnych lokalizacji
   b) przechowywanie backupów na dyskach posiadanego przez Zamawiającego de-duplikatora
   c) zarządzanie replikacją między przez Zamawiającego de-duplikatorami

d) odtworzenie zreplikowanych backupów ze zdalnego urządzenia backupowego również w przypadku całkowitego zniszczenia zdalnego ośrodka czyli zniszczenia całości zdalnego środowiska backupu

e) stanowić kompletny system centralnego backupu z agentami do backupu plików, baz danych, środowisk wirtualnych.

10 Dostarczony system musi przechowywać kopie zapasowe na dyskach posiadanego przez Zamawiającego de-duplikatora EMC DataDomain.

11 Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Debian, CentOS, Ubnutu, Novell OES), FreeBSD.

12 Backup zasobów plików z powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami w mniejszej specyfikacji.

13 Oprogramowanie backupowe musi umożliwiać backup całych obrazów maszyn wirtualnych systemu VMware.

14 Oprogramowanie backupowe musi w trakcie backupu przesyłać do posiadanego przez Zamawiającego de-duplikatora tylko unikalne bloki, czyli bloki nie znajdujące się na oferowanym de-duplikatorze skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN.

15 Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego.

16 Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być nigdy więcej odczytany, chyba, że zmieni się jego zawartość.

17 W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte.

18 Oferowanie oprogramowanie backupowe musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk typu Dziadek – ojciec –syn, to znaczy utworzenia polityki w której zdefiniowano:

a) Czas przechowywania backupów dziennych,

b) Czas przechowywania backupów tygodniowych,

c) Czas przechowywania backupów miesięcznych,

d) Czas przechowywania backupów rocznych.

19 Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:

a) wybranych typów plików,

b) dla całych katalogów,

c) dla pojedynczych plików

20 Oferowane rozwiązanie musi mieć możliwość zdefiniowania by ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatnie ważny backup tego zasobu jest trzymany bezterminowo. Jedynie administrator może zdecydować o jego usunięciu.

21 Serwery backupu muszą zarządzać replikacją backupów znajdujących się na de-duplikatorze. Całość konfiguracji replikacji backupów musi odbywać się z konsoli serwera backupu. Konfiguracja zadań replikacji nie może wymagać jakichkolwiek działań na de-duplikatorze.

22 Wymaga się by replikacja między backupów znajdujących się na de-duplikatorach odbywała się w obu kierunkach jednocześnie:

a) Backupy z de-duplikatora z ośrodka podstawowego do de-duplikatora z ośrodka zapasowego

b) Backupy z de-duplikatora z ośrodka zapasowego do de-duplikatora z ośrodka podstawowego

23 Całość replikacji zarządzana tylko i wyłącznie z poziomu oprogramowania backupowego (serwerów backupu)

24 Musi istnieć możliwość zdefiniowania kalendarza replikacji między serwerami oraz zdefiniowania które zadania backupowe podlegają replikacji.

25 Serwer backupu musi udostępniać (pokazywać w konsoli GUI) backupy które zostały do niego zreplikowane ze zdalnej lokalizacji. Musi być możliwość odtworzenia backupów zreplikowanych do lokalnego serwera backupu / de-duplikatora ze zdalnej lokalizacji. Odtworzenie musi dobywać się poprzez interfejs GUI. Odtworzenie musi być możliwe w przypadku całkowitej niedostępności zdalnego systemu backupu (nieodstępność zdalnego serwera backupu oraz zdalnego de-duplikatora).

26 Każdy serwer backupu w każdej lokalizacji musi udostępniać (pokazywać w konsoli GUI) zarówno lokalne backupy jak wszystkie również backupy zreplikowane do ośrodka zdalnego.

27 W przypadku odtwarzania danych w ośrodku A w trakcie definiowania zadania odtwarzania musi być możliwość zdefiniowania czy odtwarzamy backupy z lokalnej kopii (znajdujące się na

lokalnym oferowanym de-duplikatorze) czy też odtwarzamy ze zdalnej kopii z ośrodka B (znajdujące się na zdalnym oferowanym de-duplikatorze w lokalizacji B).

28 Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min, administrator, monitoring, tylko wykonywanie odtworzenia) w systemie backupowym.

29 Konsola musi udostępniać raporty dotyczące zajętości przestrzeni przeznaczonej na deduplikaty.

30 Oprogramowanie backupowe musi mieć możliwość limitowania wielkości zadania backupowego. Jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowych

31 Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak by odpowiednia moc procesora zostawić dla innych zadań.

32 Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.0.

33 Oprogramowanie backupowe musi umożliwiać dla środowisk VMware następujące typy backupu:

a. Backup całych maszyn wirtualnych
b. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk
c. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware)
d. Wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane przy pomocy technologii CBT systemu VMware to znaczy do medium backupowego z systemu VMware muszą być transferowane tylko zmienione bloki.

34 Jednocześnie z punktu widzenia systemu backupowego musza to być backupy pełne (full backupy). To znaczy z punktu widzenia systemu backupu muszą to być backupy identyczne z wykonywanym od zera pełnym backupem.

a. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane.
b. Wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk)

35 Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla de-duplikacji powyżej.

36 Powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.

37 Oferowany system musi pozwalać na szybkie odtworzenie

a. całych obrazów maszyn wirtualnych
b. pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej

38 Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych VMware dostarczając następujące funkcjonalności:

a. Odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu.
b. Odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu.
c. Odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux.
d. Możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows). Powyższa metoda nie może fizycznie odtwarzać backupów a jedynie pozwalać na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie.

39 Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.

40 Rozwiązanie backupowe musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z medium backupowego bez konieczności odtwarzania (Instant Access).

41 Oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej celem ich przeszukiwania (wymagane przeszukiwanie po nazwach plikó jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej.

42 Oprogramowanie backupowe musi mieć możliwość backupu / odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter.

43 Skalowalność rozwiązania dla środowisk VMware musi być na poziomie:

a. Minimum 3000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu.
b. Minimum 100 maszyn wirtualnych backupowanych w ciągu godziny w ramach pojedynczej instancji systemu backupu.

44 Rozwiązanie backupowe musi umożliwiać backup i odtwarzanie w tym samym czasie minimum 50 maszyn wirtualnych VMware.

45 Oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware. Musi istnieć możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware.

46 Weryfikacja maszyn wirtualnych musi zapewniać minimum:

a. Odtworzenie maszyny wirtualnej na zdefiniowanym Data Center / Data Store,
b. Weryfikacja podstawowych procesów,
c. Możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej.

47 Informacja w konsoli systemu backupu o poprawnej / niepoprawnej weryfikacji maszyny wirtualnej.

48 Administrator (właściciel) danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej.

49 Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware/HyperV dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym.

50 Rozwiązanie backupowe musi pozwalać automatyczne polityki backupowe dla:

a. Folderu,
b. Resource Pool systemu VMware.

51 Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware.

52 Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych.

53 Oferowany system musi automatycznie naprawiać problemy związane ze snapshotami VMware. W przypadku gdy system VMware nie usunie snapshotu, oprogramowanie backupowe musi automatycznie ponawiać usunięcie snapshotu a w przypadku konieczności automatycznie konsolidować maszyny wirtualne VMware.

54 Backup oraz odtworzenie maszyn wirtualnych VMware musi być możliwy z poziomu graficznego interfejsu, linii komend oraz przez REST API.

55 Musi istnieć możliwość odtworzenia danych:

a. z zabezpieczanego serwera / komputera,
b. z konsoli systemu backupowego.

56 System backupu musi mieć funkcjonalność wyrzutu na taśmę.

57 Opcja wyrzutu na taśmę musi być elementem niniejszej oferty.

58 System backupu musi mieć możliwość bezpośredniego raportowania o błędach do serwisu producenta.

59 System backupu musi mieć możliwość instalacji agentów jako plików msi. Musi istnieć możliwość automatyzacji agentów poprzez uruchomienie skryptu instalującego agenta na zabezpieczanej maszynie i przyporządkowującego maszynę automatycznie do określonej polityki backupowej.

60 System backupu musi mieć możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji od producenta.

61 System backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu.

62 W ramach licencji musi być zapewniona możliwość monitorowania, raportowania.

7.6 Komplet pamięci RAM

32 sztuki pamięci RAM 32GB dla Serwera BL660c Gen8, zgodnie z poniższym:

1. DIMM Capacity - 32GB
2. DIMM Native Speed (MHz) - 1333
3. Voltage – LV

8 Dostawa i konfiguracja nowej infrastruktury

Etap rozpoczyna się po podpisaniu Umowy.

W zakresie usług świadczonych przez Wykonawcę będzie m.in. instalacja i wstępna konfiguracja dostarczanej infrastruktury zgodnie z poniższym:

1. Przygotowania „Planu instalacji i konfiguracji" i uzyskania jego akceptacji przez Zamawiającego – dokument musi zawierać szczegółowe informacje nt. sposobu implementacji wraz z harmonogramem realizacji poszczególnych czynności. Wykonawca przygotuje i przedstawi do akceptacji Zamawiającego „Plan instalacji i konfiguracji" najpóźniej w terminie 14 dni od dnia podpisania Umowy. Wykonawca zobowiązany będzie do utrzymania aktualności opracowanego dokumentu w toku bieżącej realizacji przedmiotu umowy. Wykonawca dopełni wszystkich starań aby zapewnić realizację usługi instalacji i konfiguracji w jak najkrótszym czasie. Każda planowana niedostępność elementów infrastruktury i usług musi być przedstawiona w planie instalacji i konfiguracji, i musi uzyskać akceptację Zamawiającego.
2. Instalacji i wstępnej konfiguracji zgodnie z zaakceptowanym przez Zamawiającego „Planem instalacji i konfiguracji". Sprzęt musi zostać zainstalowany we wskazanym przez Zamawiającego miejscu w serwerowni – wskazanym w „Planie instalacji i konfiguracji", w uzgodnionej lokalizacji, tak aby zapewnić maksymalną możliwą ciągłość działania poszczególnych warstw infrastruktury.
3. Sporządzenia kompletu dokumentacji powykonawczych dla poszczególnych elementów infrastruktury i oprogramowania zgodnie z rozdziałem 9. Dokumentacja.
4. Przeprowadzenia testów akceptacyjnych. Testy będą prowadzone przez Zamawiającego, przy wsparciu Wykonawcy.

Etap ten przewidziany jest również na usuwanie przez Wykonawcę wszelkich nieprawidłowości wykrytych podczas testów oraz niezgodności funkcjonalnych wobec „Planu instalacji i konfiguracji". Przeprowadzenie testów z wynikiem pozytywnym jest jednym z warunków odbioru wybranej pozycji z „Planu instalacji i konfiguracji".

Jeżeli w którejkolwiek z warstw obecnie posiadanego przez Zamawiającego rozwiązania wymagany będzie demontaż sprzętu, czynność ta leży w obowiązku Wykonawcy. Czynność deinstalacji należy przeprowadzić w taki sposób aby Zamawiający nie stracił posiadanej gwarancji na posiadany sprzęt.

Realizacja prac ma być realizowana zgodnie z przyjętymi procedurami utrzymaniowymi.

W trakcie instalacji i konfiguracji Wykonawca zobowiązany jest zapewnić jak najkrótszy okres niedostępności systemu.

9 Dokumentacja

Wykonawca przekaże w ramach realizacji przedmiotu zamówienia niżej wymienioną dokumentację:

- instrukcję instalacji, konfiguracji i administracji dostarczonego oprogramowania,
- opis obsługi codziennej systemu zabezpieczeń,
- opis konfiguracji zastosowanego sprzętu,
- dokumentację zastosowanej instalacji,
- procedury instalacji,
- dokumentację konfiguracji i parametryzacji,
- procedury konfiguracji.

W ramach poniższego rozdziału przedstawiono opis dokumentacji, która powinna zostać przekazana przez Wykonawcę w ramach realizacji przedmiotu zamówienia. Terminy przekazywania poszczególnych dokumentacji zostaną ustalone z Wykonawcą w ramach „Planu instalacji i konfiguracji".

10 Dodatkowe zobowiązania Wykonawcy

Dodatkowe zobowiązania Wykonawcy niewskazane gdzie indziej:

1. Wymagania ogólne:
    a. dostawa niezbędnego okablowania zasilającego dla dostarczanych urządzeń oraz okablowania LAN/SAN
    b. rozprowadzenie okablowania LAN/SAN
    c. wykonanie oznakowania urządzeń oraz kabli LAN/SAN
    d. utylizacja opakowań po dostarczonym sprzęcie
2. Wszelkie działania Wykonawcy w ramach realizacji przedmiotu zamówienia będą oparte o uznane standardy i metodyki wykorzystywane w danym obszarze m.in. ITIL 2011 Edition. Wykonawca będzie realizował przedmiot zamówienia z najwyższą starannością, efektywnością oraz zgodnie z najlepszą praktyką i wiedzą zawodową.
3. Wykonawca zobowiązany jest wykonać w całości przedmiot zamówienia w terminach określonych w niniejszym dokumencie.
4. Wykonawca zobowiązany jest dokonać z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na przedmiot zamówienia.
5. Wykonawca będzie zobowiązany, w trakcie realizacji umowy, stosować się do wytycznych bezpieczeństwa systemów IT oraz do wytycznych bezpieczeństwa stosowanych u Zamawiającego. Wytyczne zostaną przekazane po podpisaniu umowy.
6. Wykonawca będzie współpracował z Zamawiającym na każdym etapie wykonywania przedmiotu zamówienia w ramach realizacji zamówienia.
7. Wykonawca będzie udzielał Zamawiającemu każdorazowo na wniosek Zamawiającego, pełnej informacji na temat stanu realizacji przedmiotu zamówienia zgodnie z obowiązującą Strony procedurą.
8. Wykonawca będzie współdziałał z osobami wskazanymi przez Zamawiającego. Zamawiający do realizacji powierzonych mu zadań ma prawo desygnować swoich przedstawicieli lub przekazać te zadania do realizacji stronie trzeciej.
9. Wszelkie dane i informacje wytwarzane przez Wykonawcę i utrzymywane w ramach realizacji przedmiotu zamówienia są własnością Zamawiającego. Wykonawca zobowiązany jest do przekazania Zamawiającemu wszystkich danych i informacji oraz dokumentów wytwarzanych i gromadzonych w ramach realizacji przedmiotu zamówienia po zakończeniu umowy. Wykonawca jest zobowiązany do zachowania poufności wszystkich danych i informacji, w których posiadanie wejdzie podczas realizacji przedmiotu Umowy.

11 Dodatkowe zobowiązania Zamawiającego

Dodatkowe zobowiązania Zamawiającego niewskazane gdzie indziej:

1. Udostępnienie dokumentów, materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, niezbędnych do realizacji przedmiotu zamówienia.
2. Udzielanie Wykonawcy na bieżąco niezbędnych do realizacji przedmiotu zamówienia wyjaśnień oraz przekazywania niezbędnych informacji.
3. Informowanie Wykonawcy o wszelkich czynnościach podejmowanych w związku z realizacją projektu, jeśli będą one miały związek z realizacją przedmiotu zamówienia przez Wykonawcę.
4. Umożliwienie Wykonawcy dostępu do posiadanych przez Zamawiającego obiektów, sprzętu, oprogramowania oraz dokumentacji, niezbędnych do realizacji przedmiotu zamówienia, zgodnie z wewnętrznymi regulacjami Zamawiającego w zakresie bezpieczeństwa.
5. Prowadzenie biura projektu, w tym prowadzenie repozytorium dokumentacji.

12 Załączniki

Załącznik numer 1 - Protokół Odbioru Ilościowego