

Zadanie I - Opis Przedmiotu Zamówienia

I. Wstęp

Niniejsze zapytanie dotyczy zaprojektowania, dostawy oraz zaimplementowania infrastruktury informatycznej na potrzeby Szczecińskiego Parku Naukowo Technologicznego sp. z o. o. (SPNT) wraz ze wszystkimi niezbędnymi urządzeniami sieciowymi oraz z odpowiednim poziomem gwarancji (w tym wsparcia) zdalnego lub w siedzibie Zamawiającego, w sposób opisany w Umowie z Wykonawcą, SIWZ i Opisie Przedmiotu Zamówienia. Wykonawca zapewni dostawę, montaż i uruchomienie zaoferowanego sprzętu i oprogramowania w lokalizacji SPNT tj. Szczecin, ul. Niemierzyńska 17A pomieszczenie serwerowni. Czynności związane z uruchomieniem muszą być przeprowadzone przez personel posiadający wymagane przez producenta zaoferowanego rozwiązania uprawnienia we współpracy z Zamawiającym i zgodnie z jego wymaganiami.

Poniższy opis stanowi przykładowy projekt zawierający wszystkie niezbędne założenia oraz elementy aktywne całego systemu jak również wymagania minimalnych parametrów funkcjonalno-technicznych jakie muszą spełniać zaproponowane w ofercie urządzenia i systemy. Oferent może zaproponować swoją koncepcję równoważną, jednakże musi ona zawierać urządzenia spełniające wszystkie założenia funkcjonalno-techniczne opisane w niniejszym dokumencie, a także wszystkie założenia funkcjonalne dotyczące działania sieci SPNT. Ogólne założenia funkcjonalne jakimi muszą się charakteryzować oferowane rozwiązania:

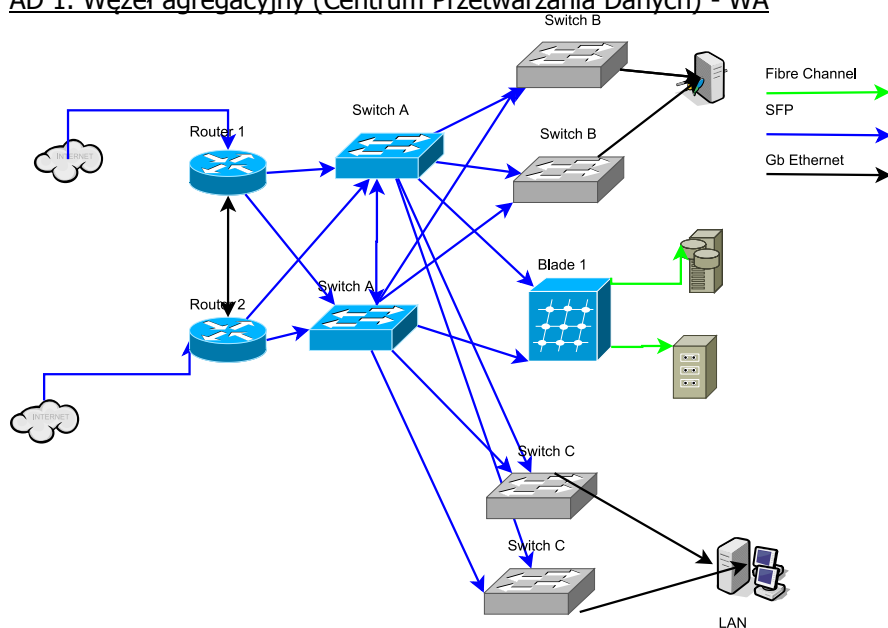
1. wysoka niezawodność oraz dostępność do zasobów sieciowych
2. wysoka wydajność
3. łatwe zarządzanie
4. łatwość rozbudowy
5. modularność i elastyczność w implementacji najnowszych technologii

II. Opis Koncepcji

Infrastruktura SPNT zostanie podzielona na 3 główne bloki funkcjonalne:

1. Węzeł agregacyjny (Centrum Przetwarzania Danych) - WA
2. Węzeł sieciowy - WS
3. Węzeł dostęp do Internetu - WI

AD 1. Węzeł agregacyjny (Centrum Przetwarzania Danych) - WA



Koncepcja budowy infrastruktury serwerowej (CPD) zakłada stworzenie:

- środowiska, które umożliwi łatwe i szybkie tworzenie, uruchamianie oraz zarządzanie środowiskami serwerowymi oraz wirtualnymi,
- tworzenia kopii bezpieczeństwa danych przetwarzanych i przechowywanych w systemie CPD.

System CPD powinien zostać zbudowany w taki sposób by pozwolił w przyszłości na łatwą rozbudowę, zarówno pod kątem wydajności, pojemności jak i funkcjonalności jaką ma zapewnić.

Elementy serwerowe i pamięci masowych CPD

Do budowy rozwiązania wybrano rozwiązanie oparte o serwery kasetowe. Pozwala to zapewnić odpowiednią moc obliczeniową oraz możliwość łatwej rozbudowy w przyszłości. Dane przechowywane przez system powinny być składowane na współdzielonej macierzy dyskowej. Połączenia pomiędzy serwerami a macierzą powinny być w pełni redundantne, tak by system nie posiadał pojedynczych punktów awarii. Dodatkowo w ramach projektu powinien zostać dostarczony dedykowany serwer zarządzający serwer backupu oraz biblioteka taśmowa. Sprzęt ten ma zapewnić możliwość tworzenia kopii zapasowych w całym środowisku.

Oprogramowanie do wirtualizacji zasobów

Oprogramowanie, które zostanie dostarczone w ramach projektu, ma umożliwić uruchomienie na opisanym wcześniej sprzęcie wielu różnych środowisk.

Oprogramowanie wirtualizacyjne powinno być instalowane bezpośrednio na serwerach fizycznych typu blade bez konieczności instalacji innego systemu operacyjnego. Dostarczone licencje powinny pozwolić na uruchomienie oprogramowania wirtualizacyjnego na 7 serwerach typu blade dostarczonych w ramach tego projektu.

Wraz z systemem wirtualizacyjnym należy dostarczyć oprogramowanie zapewniające centralną konsolę zarządzającą.

Oprogramowanie do tworzenia kopii bezpieczeństwa

Dostarczone oprogramowanie ma zapewnić możliwość tworzenia kopii bezpieczeństwa na maszynach fizycznych przewidzianych do administrowania. Tworzenie kopii powinno być w pełni automatyczne i bazować na kalendarzu. Dane powinny być kopiowane na dostarczoną w ramach projektu bibliotekę taśmową i macierz.

AD 2. Węzeł sieciowy - WS

WS odpowiedzialny będzie za prawidłowy i bezawaryjny transport danych dla wszystkich aplikacji zainstalowanych w CPD. Dwa przełączniki skonfigurowane w wirtualnym stosie odpowiadać będą za połączenie świata IP ze środowiskiem „Storage`owym”. Oba przełączniki wyposażone będą w min. 24 porty typu SFP+ (10GB), które wykorzystane zostaną do podłączenia

- wirtualnego stosu (DC) z przełącznikami LAN,
- węzłem IP dostępu do Internetu
- farmą serwerów (Blade).
- obecną infrastrukturą serwerową SPNT

Komunikację z przełącznikami dla siecią LAN zapewnią redundantne linki pracujące z prędkością 10GE zestawione pomiędzy dwoma przełącznikami centralnymi.

Centralnym punktem w sieci SPNT będzie:

- 2 przełączniki centralne typu A
- 2 przełączniki dostępowe typu B
- 5 przełączników dostępowych typu C

Przełączniki dostępowe typu C odpowiadają za bezpośrednie podłączenie urządzeń końcowych (PC, notebook, drukarka, itp.) do infrastruktury sieciowej. Węzeł ten będzie sprawował funkcję węzła dostępowo – agregacyjnego. Centralny węzeł wyposażony będzie w mechanizmy zapobiegające pojedynczym punktom awarii. Połączenie pomiędzy urządzeniami realizowane będzie z wykorzystaniem standardowych połączeń Ethernet 10Gbps. Wszystkie przełączniki typu A i C będą zlokalizowane w jednym miejscu tzn. nie będą one rozdystrybuowane w różnych miejscach/kondygnacjach budynku.

AD. 3 Wezeł dostęp do Internetu - WI

Dostęp do sieci Internet zrealizowany będzie w oparciu dwa urządzenia dostępowe. Oba urządzenia muszą zapewnić funkcjonalność

- routera,
- firewall.

Podstawowym założeniem dla tego bloku funkcjonalnego jest bezpieczny dostęp do Internetu jak i do zasobów wewnątrz sieci DC z Internetu. Dwa, równolegle pracujące, zapewniające failover za pomocą protokołu VRRP, urządzenia dostępowe będą odpowiedzialne za wyznaczenie strefy bezpieczeństwa oraz zapewnienie bezpiecznej komunikacji poprzez dynamiczny protokół BGP. W tym celu zestawione zostaną dwa niezależne łącza od dwóch różnych dostawców ISP zakończone interfejsami:

- 1000Base BX10-D - 1 szt.
- SFP LCSM 1310nm (na20km) - 1 szt.

Firewall będzie chronił strefę DMZ. Dla zachowania niezawodności blok funkcjonalny WI jest w pełni zdublowany oraz połączony redundantnymi ścieżkami o przepustowości 10Gbps (SFP+) z blokiem WS.

III. Opis usług związanych z realizacją przedmiotu zamówienia:

1. Instalacja oprogramowania do wirtualizacji na serwerach fizycznych (7 szt.) z pełnym profilowaniem, aktualizacją systemów operacyjnych, instalacją dodatkowych, niezbędnych sterowników do dostarczonego sprzętu. Przeprowadzenie dla min. czterech osób, wyznaczonych przez Zamawiającego, instruktażu obejmującego proces instalacji, aktualizacji i konfiguracji wdrożonego środowiska systemowego.
2. Zainstalowane środowisko wirtualne musi zapewniać nieprzerwaną pracę, umożliwiać przenoszenie serwerów wirtualnych pomiędzy poszczególnymi serwerami fizycznymi z zachowaniem stanu aplikacji i usług. Zaimplementowane przez Wykonawcę rozwiązanie musi gwarantować równomierne rozłożenie obciążenia hostów, rozumianych przez Zamawiającego jako aktywne serwery fizyczne, pod kątem optymalizacji obciążenia CPU oraz pamięci RAM. Przygotowanie wyspecyfikowanych przez Zamawiającego bezpośrednich ścieżek dostępu do zasobów blokowych. Wdrożenie komunikacji pomiędzy hostami w poszczególnych lokalizacjach i między nimi. Opisane funkcjonalności muszą być realizowane w oparciu o oprogramowanie do wirtualizacji opisane w niniejszym dokumencie.
3. Instalacja i konfiguracja wymaganego przez Zamawiającego oprogramowania do zarządzania infrastrukturą sprzętową, opisanego w części XI niniejszego dokumentu.
4. Instalacja i konfiguracja wymaganego przez Zamawiającego oprogramowania do wykonywania kopii zapasowych i archiwizacji, opisanego w części XI niniejszego dokumentu, w szczególności: obsługi biblioteki taśmowej centralnej konsoli zarządzającej środowiskiem archiwizacji, informującej o zdarzeniach i stanie urządzeń archiwizujących
5. uruchomienie usługi BGP w środowisku WI
6. uruchomienie VLAN
7. przeniesienie struktury logicznej sieci funkcjonującej obecnie w środowisku Zamawiającego do nowej infrastruktury opisanej w części XI niniejszego dokumentu. Obecnie z sieci Zamawiającego korzysta 100 użytkowników pogrupowanych w 20 sieciach wirtualnych (VLAN).

IV. Testowanie zaimplementowanego rozwiązania

Przeprowadzenie testów zaimplementowanego rozwiązania:

- a) efektywności optymalizacji obciążenia CPU oraz pamięci RAM serwerów opisanych w części XI niniejszego dokumentu,
- b) testowania poprawności tworzenia się kopii zapasowych,
- c) testowanie poszczególnych bloków funkcjonalnych WA, WS, WI.

V. Opracowanie dokumentacji powykonawczej

Dokumentacja musi zawierać:

1. Opis infrastruktury sprzętowej z podziałem na lokalizacje, z wyszczególnieniem konfiguracji sprzętowej, numerów seryjnych, adresów MAC i adresów IP.
2. Opis logicznej i fizycznej struktury zależności i połączeń:
 - a. okablowania (LAN, SAN /NAS),
 - b. zależności działania hostów i elementów pośredniczących (kolejność uruchamiania poszczególnych elementów infrastruktury).

VI. Wymagania formalne

1. Zamawiający może zażądać od dostawcy potwierdzenia od producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent spełnia wymagania producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych oraz oświadczenia potwierdzonego przez polskie przedstawicielstwo producenta potwierdzającego pochodzenie produktu z oficjalnego kanału dystrybucyjnego, pod rygorem wykluczenia z postępowania.
2. Zamawiający wymaga aby wszystkie licencje dostarczone były wraz z rocznym wsparciem technicznym, świadczonym na wszystkich trzech poziomach. Zamawiającym musi mieć możliwość zgłaszania problemów w trybie 7dni / 24h.
3. Do oferty należy załączyć Informacje o oferowanym produkcie (załącznik nr 7 do SIWZ) oferowanego sprzętu z wymaganiami SIWZ. Dla każdej pozycji Zamawiający wymaga potwierdzenie w formie spełnia/nie spełnia oraz dodatkowo podania faktycznych parametrów oferowanego sprzętu i oprogramowania w taki sposób, aby oceniający byli w stanie stwierdzić czy zaoferowany sprzęt spełnia wymagania specyfikacji SIWZ.
4. Wszystkie oferowane urządzenia i oprogramowanie należy jednoznacznie wskazać w ofercie poprzez wpisanie ich do Informacje o oferowanym produkcie (załącznik nr 7 do SIWZ) w postaci ich nazwy, producenta oraz jednoznacznych identyfikatorów, kodów producenta, typu oferowanych produktów.
5. Dodatkowo w celu potwierdzenia, że oferowana dostawa (przedmiot zamówienia wskazany przez wykonawcę w Informacje o oferowanym produkcie (załącznik nr 7 do SIWZ) odpowiada wymaganiom określonym przez zamawiającego, wykonawca zobowiązany jest dołączyć do oferty opis urządzeń wchodzących w skład przedmiotu zamówienia, a w szczególności dokumentacji technicznej, specyfikacji technicznej, itp., dla każdego zaoferowanego urządzenia czy oprogramowania, potwierdzającego spełnianie wymagań zamawiającego. Załączone dokumenty muszą wskazywać rzeczywiste parametry zaoferowanych urządzeń.
6. Zamawiający wyraża zgodę, aby załączone do oferty dokumenty, o których mowa w pkt 2, zostały złożone w języku angielskim.
7. Zamawiający wymaga, aby załączone do oferty dokumenty sporządzone w języku obcym, innym niż określony w pkt. 6, złożone zostały wraz z tłumaczeniem na język polski.
8. Zamawiający, przed podjęciem ostatecznej decyzji i podpisaniem umowy, zastrzega sobie prawo wezwania oferenta, którego oferta jest na pierwszym miejscu według przyjętych kryteriów przetargowych, do zestawienia przez oferenta środowiska testowego i zaprezentowanie oferowanego rozwiązania w celu potwierdzenia spełnienia wszystkich wymaganych w SIWZ parametrów minimalnych. W przypadku niespełnienia w testach choć jednego z deklarowanych w ofercie parametrów Oferta taka zostanie odrzucona, jako niespełniająca postanowień SIWZ.
9. Podane poniżej parametry w ujęciu tabelarycznym są minimalnymi parametrami jakie muszą posiadać oferowane produkty. Aby oferta była zgodna w wymaganiami wszystkie te parametry muszą być spełnione poprzez oferowane rozwiązania.

VII. Wymagania ogólne dotyczące wszystkich elementów systemu

1. Wszystkie urządzenia muszą być fabrycznie nowe i wyprodukowane po 01/01/2012.
2. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001:2000 lub inną normą równoważną.
3. W momencie oferowana wszystkie elementy oferowanej architektury muszą być dostępne do dostarczania przez producenta.
4. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.

5. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych, objęte gwarancją, której wymagania zostały szczegółowo opisane do każdego urządzenia w tabelach opisujących wymagania.
6. Do każdego dostarczonego wraz z serwerem systemu operacyjnego muszą być załączone oryginalne dokumenty licencyjne uprawniające do używania systemu operacyjnego określonego dla każdego z serwerów
7. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.
8. Do każdego urządzenia musi być dostarczony komplet nośników umożliwiających odtworzenie oprogramowania zainstalowanego w urządzeniu.
9. Wszystkie serwery muszą posiadać Certyfikat „B” (dla obudowy) lub oznakowanie CE produktu albo spełniać normy równoważne.
10. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.

VIII. Wymagania dotyczące rozszerzonej gwarancji i wsparcie zdalne lub w siedzibie Zamawiającego na sprzęt i systemy informatyczne (w tym oprogramowanie)

VIII.1. Wymagania dotyczące rozszerzonej gwarancji i wsparcie zdalne lub w siedzibie Zamawiającego na sprzęt

1. 12 miesięcy od daty podpisania końcowego protokołu odbioru.
2. W ramach rozszerzonej gwarancji i wsparcie w siedzibie Zamawiającego świadczone będzie:
 - 2.1 Wsparcie
 - a. Konfigurację zdalną urządzeń,
 - b. Udostępnienie i utrzymanie zdalnego serwisu oraz zarządzania urządzeniami za pomocą VPN.
 - 2.2 Identyfikacja
 - a. Zdalna diagnoza i kwalifikacja problemu.
 - b. Przeprowadzenie testów lub symulacji celem ustalenia źródła problemu.
 - 2.3 Usuwanie awarii
 - a. Usunięcie uszkodzenia przez zdalną korektę oprogramowania sprzętowego lub wgranie uaktualnienia (Update).
 - 2.4 Okresowe przeglądy techniczne na miejscu instalacji sprzętu w wymiarze co najmniej raz na kwartał
 - a. Przegląd i analizę logów oraz konfiguracji wszystkich urządzeń,
 - b. Sprawdzenie stanu wszystkich połączeń,
 - c. Wgranie i konfiguracja nowych wersji oprogramowania dla sprzętu w przypadku ich publikacji dla poszczególnych urządzeń,
 - d. Raport pisemny z przeglądu,
3. Wykonawca zapewni dostęp do serwisu w trybie 7/24/365 dla awarii:
 - 3.1 kategorii A krytycznej.
 - a. czas reakcji na zgłoszenie i przystąpienie do usunięcia awarii w siedzibie zamawiającego nie więcej niż 45 minut,
 - b. czas usunięcia awarii do 12 godzin,
 - c. w uzasadnionych przypadkach czas określony w pkt 3.b może ulec zmianie za zgodą Zamawiającego.
 - 3.2 kategorii B nie krytycznej.
 - a. czas reakcji na zgłoszenie i przystąpienie do usunięcia awarii nie więcej niż 4 godziny.

- b. czas usunięcia awarii kategorii do 2 dni roboczych.

3.3 Zamawiający każdorazowo określa i definiuje jakiej kategorii jest zgłoszenie awarii.

- 4. Zamawiający zapewni dostęp fizyczny do siedziby w trybie 7/24/365 dla osób wskazanych przez Wykonawcę.
- 5. Usługi serwisu mają być świadczone przez wykwalifikowany, doświadczony personel posiadający stosowne umiejętności i wiedzę potwierdzone ukończonymi i aktualnymi certyfikowanymi szkoleniami producentów sprzętu.

VIII.2. Wymagania dotyczące rozszerzonej gwarancji i wsparcie zdalne lub w siedzibie Zamawiającego na oprogramowanie informatyczne dostarczone w ramach zamówienie.

- 1. Ilość Godzin – 1200 godzin, lub 12 miesięcy od daty podpisania końcowego protokołu odbioru.
- 2. W ramach rozszerzonej gwarancji i wsparcie w siedzibie Zamawiającego świadczone będzie:
 - 2.1 Wsparcie
 - a. Konfigurację zdalną urządzeń i usług (nie związana z realizacją gwarancji na sprzęt zwykłej lub rozszerzonej na sprzęt, polegającej np. na wymianie lub naprawie sprzętu).
 - b. Udostępnienie i utrzymanie zdalnego serwisu oraz zarządzania usługami za pomocą VPN.
 - c. Doradztwo w zakresie sprzętu i usług.
 - 2.2 Identyfikacja
 - a. Zdalna diagnoza i kwalifikacja problemu.
 - b. Przeprowadzenie testów lub symulacji celem ustalenia źródła problemu.
 - 2.3 Usuwanie awarii
 - a. Usunięcie uszkodzenia przez zdalną korektę oprogramowania lub wgranie uaktualnienia (Update).
- 3. Wykonawca zapewni dostęp do serwisu w trybie 7/24/365 dla awarii:
 - 3.4 kategorii A krytycznej.
 - a. czas reakcji na zgłoszenie i przystąpienie do usunięcia awarii w siedzibie zamawiającego nie więcej niż 45 minut.
 - b. czas usunięcia awarii do 12 godzin.
 - c. w uzasadnionych przypadkach czas określony w pkt 3.b może ulec zmianie za Zgodą Zamawiającego.
 - 3.5 kategorii B nie krytycznej.
 - a. czas reakcji na zgłoszenie i przystąpienie do usunięcia awarii nie więcej niż 4 godziny.
 - b. czas usunięcia awarii kategorii do 2 dni roboczych.
 - 3.6 Zamawiający każdorazowo określa i definiuje jakiej kategorii jest zgłoszenie awarii.
- 4. Zamawiający zapewni dostęp fizyczny do siedziby w trybie 7/24/365 dla osób wskazanych przez Wykonawcę.
- 5. Usługi serwisu mają być świadczone przez wykwalifikowany, doświadczony personel posiadający stosowne umiejętności i wiedzę potwierdzone ukończonymi i aktualnymi certyfikowanymi szkoleniami.

Kategorie zgłoszeń gwarancyjnych:

Kategoria A – krytyczna, obejmująca wszystkie defekty i uszkodzenia, które spowodowały lub prawdopodobnie spowodują całkowitą niesprawność urządzenia (systemu).

Kategoria B – każde poważne pogorszenie funkcjonalności lub wydajności urządzenia (systemu) mające wpływ na jakość usług, noszące cechy uszkodzenia, awarii lub defektu, a nie zawarte w kategorii A.

IX. Instruktaż

Wymagane jest także zapewnienie dedykowanego min. dwudniowego instruktażu z zakresu konfiguracji i zarządzania urządzeń. Instruktaż musi być przeprowadzony dla 4 osób w języku polskim na miejscu instalacji sprzętu u Klienta. Instruktaż musi obejmować proces instalacji, aktualizacji i konfiguracji wdrożonego środowiska. Instruktaż musi być przeprowadzony przez osobę posiadającą certyfikat świadczący o autoryzacji do przeprowadzenia szkoleń danego producenta. Zamawiający może wymagać potwierdzenia tego certyfikatu przed podpisaniem umowy.

Zakres instruktażu:

- a) konfiguracja serwera blade, dodawanie i usuwanie fizycznych serwerów, zmiana zasobów fizycznych, diagnostyka i monitoring, rozwiązywanie problemów,
- b) konfiguracja i odtwarzanie macierzy, tworzenie dysków logicznych, diagnostyka i monitoring, rozwiązywanie problemów, zarządzanie przestrzenią dyskową,
- c) konfiguracja biblioteki taśmowej, diagnostyka i monitoring, rozwiązywanie problemów, migracja nośników.

X. Opis zespołu projektowego

Zespół projektowy powinien składać się z minimum 4 specjalistów z doświadczeniem zawodowym udokumentowanym wg. poniższego opisu. Zamawiający wymaga podania na etapie składania oferty składu całego zespołu projektowego.

1. Minimum jedna osoba spełniająca poniższe wymagania minimalne :
 - a. Certyfikat VMWare Datacenter Design (VCAP5-DCD) lub równoważny
 - b. Certyfikat specjalisty technicznego na poziomie Intermediate producenta zaproponowanego systemu Blade
 - c. MASE Master Accredited System Engineer – HP Proliant High Availability and Clustering Solutions lub równoważny
 - d. ASE Accredited System Engineer ProCurve Networking and Mobility lub równoważny
 - e. Certificate of Completion: CA ARCServe Backup for Windows: Implementation 200 Exam lub równoważny
2. Minimum jedna osoba spełniająca łącznie wszystkie poniższe wymagania minimalne :
 - a. Posiada tytuł Cisco Certified Network Professional w specjalizacji security lub równoważny
 - b. Posiada tytuł Cisco Certified Network Professional w specjalizacji routing and switching lub równoważny

XI. Opis parametrów technicznych i funkcjonalnych

Szafa teleinformatyczna z konsolą administratora - sztuk 1	
Wymagania funkcjonalno-techniczne	
Obudowa	Szafa serwerowa z miejscem 42U, wyposażona w drzwi ażurowe wraz z zamkiem, przednie i tylne (drzwi tylnie dzielone – dwustronne) oraz ściany boczne (każda ściana boczna dzielona na 3 części), elementy stabilizacyjne zapewniające bezpieczeństwo pracy oraz elementy zasłaniające puste miejsca w szafie (zaślepki wielkości 1U lub 2U, pozwalające na zamaskowanie miejsca o wysokości 20U).
Listwy zasilające	Szafa wyposażona w komponenty umożliwiające fizyczną instalację oraz dystrybucję redundantnego zasilania do wszystkich instalowanych w niej urządzeń (osobne ścieżki do redundantnych zasilaczy). 2 moduły dystrybucji zasilania 32A, każdy zapewniający 4 gniazd połączeniowych IEC 320 C-19 (min. 4 obwody), połączenie do zasilania poprzez złącze IEC-309 32A. Kabel zasilający o długości minimum 1,7 m. Min. 2 moduły dystrybucji zasilania 32A, każdy zapewniający 28 gniazd połączeniowych IEC 320 C-13 (min. 4 obwody), połączenie do zasilania poprzez złącze IEC-309 32A. Kabel zasilający o długości minimum 1,7 m.
KVM	8 portowy przełącznik KVM, wraz z kompletem okablowania umożliwiającym połączenie do obudowy serwerów za pomocą portów VGA/USB. Przełącznik KVM powinien być wyposażony w port IP pozwalający na zdalny dostęp z wykorzystaniem sieci IP, z możliwością przesyłania obrazu rozdzielczości 1280x1024. Przełącznik KVM powinien zapewniać menu ekranowe do wyboru urządzenia lub za pośrednictwem skrótu klawiaturowego.
Konsola	Konsola LCD, o wysokości max 1U wraz z klawiaturą i urządzeniem wskazującym. Ekran LCD powinien mieć przekątną wyświetlacza nie mniejszą niż 17" i rozdzielczości 1280x1024 pikseli.

System monitoringu szaf	<p><u>Interfejsy:</u> TCP/IPv4, TCP/IPv6, SNMPv1, SNMPv3, Telnet, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS-Server, SMTP, XML, Syslog, LDAP. Złącze sieciowe RJ45 Ethernet wg IEEE 802.3 przez 10/100BaseT z obsługą PoE - Power over Ethernet. Złącze USB 1: wymagane do konfiguracji systemu, Złącze USB 2: dla pendriva do zapisu danych lub i aktualizacji oprogramowania min. 32 GB, Złącze szeregowo: RS232 RJ12 wymagane dla podłączenia modułu wyświetlacza, jednostki GSM (wymagana) wysyłającej komunikaty alarmowe SMS, modułu komunikacji alternatywnej dla sieci z urządzeniem przez ISDN.</p> <p><u>Wejścia/ wyjścia:</u> Wejścia cyfrowe (zacisk): min. dwa dla podłączenia do monitorowania zew. Urządzeń Wyjście przełącznikowe (zacisk): zestyk przełączny NO/NC maks. 24 V DC,1 A dla przyporządkowania dowolnych alarmów z monitorowanych czujników, możliwość podłączenia sygnału akustycznego i świetlnego Wyjściowa magistrala CAN-Bus RJ45 umożliwiająca podpięcie do systemu min. 32 czujniki oraz umożliwiająca podpięcie łącznej długości przewodów min. 100m, Generator sygnałów piezo: jeden</p> <p><u>Obsługa/sygnały:</u> Możliwość resetowania urządzenia do ustawień fabrycznych, Lokalne zatwierdzanie zdarzeń systemu, Lokalny zintegrowany w urządzeniu generator sygnałów alarmowych z możliwością zdalnego włączania i wyłączania. Lokalny zintegrowany w urządzeniu wskaźnik optyczny sygnalizujący status systemu ok./alarm/ostrzeżenie/status sieci</p> <p><u>Funkcje:</u> Zegar czasu rzeczywistego z NTP z buforem energii (24h) bez baterii/akumulatora. Zintegrowany w urządzeniu serwer WEB - graficzny interfejs administracji systemu włącznie z oprogramowaniem umożliwiającym zdalne bezpłatne administrowanie systemem, wymagane LDAP. Zintegrowany w urządzeniu serwer OPC umożliwiający podłączenie stanowiska dyspozytorskiego. Zintegrowane w urządzeniu czujniki temperatury oraz czujnik otwarcia drzwi IR</p> <p><u>Wymagane czujniki:</u> Zewnętrzny czujnik temp. i wilgotności względnej powietrza IP30 (5 sztuk). Zewnętrzne czujniki ze stykiem kontaktronowym dostępu np. drzwi, okien (10 sztuk) umożliwiające łączenie szeregowo pod jednym portem do min. 5 szt.</p> <p><u>Zasilanie redundantne systemu:</u> Zasilanie redundantne: dwa wejścia 24 VDC gniazdo z sieci i zacisk. Obsługa zasilania PoE - Power over Ethernet</p> <p><u>Dopuszczalne warunki pracy dla urządzeń monitoringu:</u> Wilgotność względna powietrza w zakresie od 5 do 95% bez kondensacji, oraz temp. od 0 do 55 stop. C</p>
-------------------------	--

Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Certyfikaty	Szafa musi być wyprodukowana zgodnie z normą ISO 9001.
Wymagania dodatkowe – obowiązkowe	
	Zamawiający wymaga fizycznej instalacji szafy w uzgodnionej lokalizacji i podłączenia oraz testów zasilania.
Wymagania dotyczące gwarancji	
	Minimum pięć lat gwarancji od momentu dostawy z czasem reakcji do końca następnego dnia roboczego od zgłoszenia awarii. Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.

Szafa teleinformatyczna - sztuk 3	
Wymagania funkcjonalno-techniczne	
Obudowa	Szafa serwerowa z miejscem 42U, wyposażona w drzwi ażurowe wraz z zamkiem, przednie i tylne (drzwi tylne dzielone – dwustronne) oraz ściany boczne (każda ściana boczna dzielona na 3 części), elementy stabilizacyjne zapewniające bezpieczeństwo pracy oraz elementy zasłaniające puste miejsce w szafie (zaśleпки wielkości 1U lub 2U, pozwalające na zamaskowanie miejsca o wysokości 20U).
Listwy zasilające	Szafa wyposażona w komponenty umożliwiające fizyczną instalację oraz dystrybucję redundantnego zasilania do wszystkich instalowanych w niej urządzeń (osobne ścieżki do redundantnych zasilaczy). 2 moduły dystrybucji zasilania 32A, każdy zapewniający 4 gniazd podłączeniowych IEC 320 C-19 (min. 4 obwody), podłączenie do zasilania poprzez złącze IEC-309 32A. Kabel zasilając o długości minimum 1,7 m. Min. 2 moduły dystrybucji zasilania 32A, każdy zapewniający 28 gniazd podłączeniowych IEC 320 C-13 (min. 4 obwody), podłączenie do zasilania poprzez złącze IEC-309 32A. Kabel zasilając o długości minimum 1,7 m.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Certyfikaty	Szafa musi być wyprodukowana zgodnie z normą ISO 9001.
Wymagania dodatkowe – obowiązkowe	
	Zamawiający wymaga fizycznej instalacji szafy w uzgodnionej lokalizacji i podłączenia oraz testów zasilania.
Wymagania dotyczące gwarancji	
	Minimum pięć lat gwarancji od momentu dostawy z czasem reakcji do końca następnego dnia roboczego od zgłoszenia awarii. Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.

Obudowa dla serwerów blade - sztuk 1 (A)	
Wymagania funkcjonalno-techniczne	
Obudowa	O wysokości maksymalnie 10U do instalacji w szafie teleinformatycznej 19".
Ilość obsługiwanych serwerów	Umożliwiająca instalację minimum 14 dwuprocessorowych serwerów blade bez potrzeby rozbudowy o dodatkowe elementy (przełączniki LAN/FC, zasilacze, wentylatory etc.).
Rodzaj obsługiwanych serwerów	Możliwość umieszczania dostarczanych serwerów blade.

<p>Sposób agregacji/ wyprowadzeń sygnałów LAN</p>	<p>Dwa przełączniki Ethernet w standardzie 10Gb wyprowadzające sygnały z minimum 2 portów sieciowych 10Gb na serwerach blade. Urządzenia te muszą umożliwiać agregację i wyprowadzenie sygnałów Ethernet z obudowy z zachowaniem redundancji połączeń. Na każdy przełącznik minimum 6 porty zewnętrzne obsadzone modułami SFP+. Możliwość rozbudowy każdego przełącznika do min. 56 portów 10Gb Ethernet bez konieczności wymiany urządzenia. Urządzenia muszą umożliwić wyprowadzenie sygnału ze wszystkich portów Ethernet w każdym serwerze. Jeśli w serwerach blade znajdują się dodatkowe karty LAN (oprócz wymaganych portów 10Gb), należy uwzględnić odpowiednie przełączniki LAN w celu wyprowadzenia dodatkowych portów na zewnątrz obudowy.</p>
<p>Sposób agregacji/ wyprowadzeń sygnałów FC</p>	<p>Dwa przełączniki FC w standardzie 8Gb w układzie redundantnym wyprowadzające sygnały z minimum 2 portów FC na serwerach blade. Urządzenia te muszą umożliwiać agregację i wyprowadzenie sygnałów FC z obudowy z zachowaniem redundancji połączeń. Każdy przełącznik musi posiadać minimum 6 zewnętrznych portów w tym 4 porty wyposażone w moduły SFP.</p>
<p>Inne standardy komunikacyjne</p>	<p>Możliwość instalacji w obudowie przełączników w innych standardach komunikacyjnych w tym przełączników InfiniBand, przełączników FC 16 Gb i przełączników Ethernet z portami zewnętrznymi 40 Gb.</p>

<p>Zarządzanie połączeniami LAN i FC z serwerami blade</p>	<p>Możliwość przydzielania adresów MAC i WWN predefiniowanych przez producenta rozwiązania serwerów blade dla poszczególnych wnek na serwery. Przydzielenie adresów musi powodować zastąpienie fizycznych adresów kart Ethernet i FC na serwerze blade. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnekami w obudowie. Funkcjonalność ta może być realizowana zarówno poprzez moduły LAN i FC w obudowie jak i poprzez dodatkowe oprogramowanie producenta serwerów blade. Jeżeli funkcjonalność ta wymaga licencji lub oprogramowania, należy je dostarczyć razem z rozwiązaniem.</p> <p>Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak, aby między wydzielonymi sieciami nie było komunikacji. Przełączniki LAN muszą obsługiwać karty z możliwością wirtualizacji interfejsów sieciowych na poziomie sprzętowym (umożliwiający pracę wirtualnych interfejsów w trybach: 1Gb Ethernet, 10Gb Ethernet i FCoE i iSCSI). Przełącznik powinien umożliwiać ustawienie ilości wirtualnych portów „virtual NIC” na porcie fizycznym.</p> <p>Wymagana jest możliwość boot’owania systemów operacyjnych zainstalowanych na poszczególnych serwerach blade bezpośrednio z macierzy FC.</p>
<p>Zarządzanie</p>	<p>Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera. Zdalne udostępnianie napędu CD-ROM, FDD, obrazu ISO na potrzeby serwera z możliwością bootowania z w/w napędów. Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego. Dostęp zdalny z poziomu przeglądarki internetowej bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu. Co najmniej 2 moduły zarządzania Hot-Plug w ramach obudowy w celu zapewnienia redundancji. W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów w ramach obudowy. Graficzna wizualizacja statusów komponentów.</p>

Zasilanie i chłodzenie	Zasilacze o konstrukcji modularnej z możliwością dokładania i wymiany modułów na gorąco. System zasilania zainstalowany wewnątrz obudowy, zdolny do dostarczenia mocy, jaką może potrzebować obudowa w pełni obsadzona serwerami i wszystkimi możliwymi opcjami (serwery w pełni obsadzone opcjami). Zasilanie typu hot-swap oraz redundancja typu N+N. Wymiana zasilacza nie może powodować konieczności odłączenia zewnętrznej infrastruktury zasilania (kable zasilającego) dla pozostałych zasilaczy, jak również nie może powodować konieczności wyjęcia lub odłączenia wentylatorów (pojedynczego wentylatora lub modułu wentylatorów). Zestaw redundantnych wiatraków (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie blade. Wentylatory niezależne od zasilaczy, wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia zasilacza/zasilaczy.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w wersji elektronicznej i drukowanej w języku polskim lub angielskim
Wymagania dodatkowe – obowiązkowe	
	Zamawiający wymaga fizycznej instalacji obudowy blade w oferowanej szafie i wykonania testów uruchomieniowych. Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.
Wymagania dotyczące gwarancji	
Warunki gwarancji dla obudowy	minimum pięć lat gwarancji z czasem reakcji w ciągu 4 godzin od zdiagnozowania problemu, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera.

Serwer typu blade - sztuk 14 (dla obudowy typ A)	
Wymagania funkcjonalno-techniczne	
Obudowa	Typu blade do instalacji w oferowanej obudowie serwerów blade.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon).
Procesor	Osiągający w oferowanym serwerze wynik 415 pkt. w konfiguracji dwuprocesorowej w teście SPECint_rate_base2006. Wymagana jest obecność protokołu potwierdzającego osiągnięty wynik na stronie: www.spec.org (wydruk ze strony należy dołączyć do oferty).

Liczba procesorów	2
Pamięć RAM	64GB RAM ECC DDR3 z możliwością rozbudowy do 768 GB.
Interfejsy sieciowe	<ul style="list-style-type: none"> • Minimum 2 interfejsy (fizyczne) 10Gb Ethernet z opcją wirtualizacji portów (podziału każdego fizycznego portu na 4 niezależne wirtualne porty w tym iSCSI lub FCoE). Porty wirtualne posiadające własne adresy MAC oraz widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe. Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej. • Minimum 2 interfejsy (fizyczne) FC 8Gbps
Porty USB	1 port USB wewnętrzny. 1 port USB na przedzie obudowy.
Wspierane systemy operacyjne	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise, VMware
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Wymagania dodatkowe – obowiązkowe	
	Zamawiający wymaga fizycznej instalacji oferowanych serwerów w dedykowanej obudowie blade oraz wykonania testów uruchomieniowych. Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.
Wymagania dotyczące gwarancji	
Warunki gwarancji	Przynajmniej pięć lat gwarancji z czasem reakcji w ciągu 4 godzin od zdiagnozowania problemu przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera.

Alternatywnie dopuszcza się poniższe rozwiązanie:

Obudowy dla serwerów Blade umożliwiające zainstalowanie min. 14 serwerów Blade (B)	
Wymagania funkcjonalno-techniczne	
Obudowa	O wysokości maksymalnie 10U do instalacji w szafie teleinformatycznej 19".
Ilość obsługiwanych serwerów	Umożliwiająca instalację minimum 8 dwuprocesorowych serwerów blade bez potrzeby rozbudowy o dodatkowe elementy (przełączniki LAN/FC, zasilacze, wentylatory etc.). Wymagana jest dostawa takiej liczby obudów, by podłączyć 14 serwerów Blade.
Rodzaj obsługiwanych serwerów	Możliwość umieszczania dostarczanych serwerów blade

<p>Sposób agregacji/ wyprowadzeń sygnałów LAN</p>	<p>Dopuszcza się rozwiązanie, którego architektura zakłada wykorzystanie modułów Pass-through w obudowie i centralnych modułów przełączających dla wielu obudów poza obudową. Należy dostarczyć 2 moduły przełączające, oraz po 2 moduły pass-through na każdą obudowę. Każdy moduł pass-through musi być dołączony do modułu przełączającego za pomocą pasma 40GE. Dopuszcza się zastosowanie modułów przełączających i pass-through wspólnie dla technologii 10GE oraz FC. Moduły przełączające należy dołączyć do sieci LAN oraz SAN za pomocą interfejsów 4x8G FC oraz 2x10GE każdy.</p>
<p>Sposób agregacji/ wyprowadzeń sygnałów FC</p>	<p>Wymagania na porty FC mogą być zrealizowane za pomocą portów 10GE/FCoE i wspólnych modułów przełączających. Zaproponowane rozwiązanie musi pozwalać na podłączenie serwera Backup, macierzy oraz biblioteki taśmowej za pomocą protokołu FC</p>
<p>Zarządzanie połączeniami LAN i FC z serwerami blade</p>	<p>Możliwość przydzielania adresów MAC i WWN predefiniowanych przez producenta rozwiązania serwerów blade dla poszczególnych wnek na serwery. Przydzielenie adresów musi powodować zastąpienie fizycznych adresów kart Ethernet i FC na serwerze blade. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnekami w obudowie. Funkcjonalność ta może być realizowana zarówno poprzez moduły LAN i FC w obudowie jak i poprzez dodatkowe oprogramowanie producenta serwerów blade. Jeżeli funkcjonalność ta wymaga licencji lub oprogramowania, należy je dostarczyć razem z rozwiązaniem.</p> <p>Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak, aby między wydzielonymi sieciami nie było komunikacji. Przełączniki LAN muszą obsługiwać karty z możliwością wirtualizacji interfejsów sieciowych na poziomie sprzętowym (umożliwiający pracę wirtualnych interfejsów w trybach: 1Gb Ethernet, 10Gb Ethernet i FCoE i iSCSI). Przełącznik powinien umożliwiać ustawienie ilości wirtualnych portów „virtual NIC” na porcie fizycznym.</p> <p>Wymagana jest możliwość boot'owania systemów operacyjnych zainstalowanych na poszczególnych serwerach blade bezpośrednio z macierzy FC.</p>

Zarządzanie	Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera. Zdalne udostępnianie napędu CD-ROM, FDD, obrazu ISO na potrzeby serwera z możliwością bootowania z w/w napędów. Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego. Dostęp zdalny z poziomu przeglądarki internetowej bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu. Co najmniej 2 moduły zarządzania Hot-Plug w celu zapewnienia redundancji. W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów w ramach obudowy. Graficzna wizualizacja statusów komponentów.
Zasilanie i chłodzenie	Zasilacze o konstrukcji modularnej z możliwością dokładania i wymiany modułów na gorąco. System zasilania zainstalowany wewnątrz obudowy, zdolny do dostarczenia mocy, jaką może potrzebować obudowa w pełni obsadzona serwerami i wszystkimi możliwymi opcjami (serwery w pełni obsadzone opcjami). Zasilanie typu hot-swap oraz redundancja typu N+N. Wymiana zasilacza nie może powodować konieczności odłączenia zewnętrznej infrastruktury zasilania (kable zasilającego) dla pozostałych zasilaczy, jak również nie może powodować konieczności wyjęcia lub odłączenia wentylatorów (pojedynczego wentylatora lub modułu wentylatorów). Zestaw redundantnych wiatraków (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie blade. Wentylatory niezależne od zasilaczy, wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia zasilacza/zasilaczy.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w wersji elektronicznej i drukowanej w języku polskim lub angielskim
Wymagania dodatkowe – obowiązkowe	
	Zamawiający wymaga fizycznej instalacji obudowy blade w oferowanej szafie i wykonania testów uruchomieniowych. Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.
Wymagania dotyczące gwarancji	
Warunki gwarancji dla obudowy	minimum pięć lat gwarancji z czasem reakcji w ciągu 4 godzin od zdiagnozowania problemu, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera.

Serwer typu blade - sztuk 14 (dla obudowy typ B)	
Wymagania funkcjonalno-techniczne	
Obudowa	Typu blade do instalacji w oferowanej obudowie serwerów blade.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon).
Procesor	Osiągający w oferowanym serwerze wynik 415 pkt. w konfiguracji dwuprocesorowej w teście SPECint_rate_base2006. Wymagana jest obecność protokołu potwierdzającego osiągnięty wynik na stronie: www.spec.org (wydruk ze strony należy dołączyć do oferty).
Liczba procesorów	2
Pamięć RAM	64GB RAM ECC DDR3 z możliwością rozbudowy do 768 GB.
Interfejsy sieciowe	<ul style="list-style-type: none"> • Minimum 2 interfejsy (fizyczne) 10Gb Ethernet z opcją wirtualizacji portów (podziału każdego fizycznego portu na 4 niezależne wirtualne porty w tym iSCSI lub FCoE). Porty wirtualne posiadające własne adresy MAC oraz widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe. Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej. • Minimum 2 interfejsy FCoE realizowane za pomocą interfejsów 10GbE. Zaproponowane rozwiązanie musi umożliwiać podłączenie macierzy, serwera Backup i biblioteki taśmowej za pomocą protokołu FC 8 Gb zgodnie ze schematem z rozdziału II.
Porty USB	1 port USB wewnętrzny. 1 port USB na przedzie obudowy.
Wspierane systemy operacyjne	Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise, VMware
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Wymagania dodatkowe – obowiązkowe	
	Zamawiający wymaga fizycznej instalacji oferowanych serwerów w dedykowanej obudowie blade oraz wykonania testów uruchomieniowych. Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.
Wymagania dotyczące gwarancji	
Warunki gwarancji	Przynajmniej pięć lat gwarancji z czasem reakcji w ciągu 4 godzin od zdiagnozowania problemu przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera.

Macierz dyskowa - sztuk 1	
Wymagania funkcjonalno-techniczne	
Obudowa	Modułowa do instalacji w standardowej szafie Rack 19".
Kontrolery	Dwa redundantne kontrolery udostępniające w sumie nie mniej niż 8 połączeń FC 8Gb i 4 połączenia iSCSI minimum 1Gb. RAID 0,1,5,6,10. Wymagane jest, aby architektura wewnętrzna macierzy wykorzystywała standard SAS 2.0.
„Cache”	Co najmniej 16GB pamięci „cache”. Pamięć „cache” przeznaczona dla procesu zapisu musi być zabezpieczona przed skutkami awarii jednego z kontrolerów.
Dyski	Macierz musi obsługiwać dyski SSD (o pojemnościach 200GB i 400GB), SAS (o pojemnościach 146GB, 300GB, 600GB, 900GB) i NL-SAS lub SATA (o pojemnościach 500GB, 1TB, 2TB, 3TB) pozwalając na rozbudowę do co najmniej 120 dysków. Macierz musi obsługiwać dyski 2,5" i 3,5". Macierz musi umożliwiać mieszanie dysków SAS, NL-SAS i SSD w ramach jednej półki dyskowej. Dostawa ma obejmować 24 dyski SAS o pojemności 900GB i 12 dysków NL SAS o pojemności 2 TB.
Migracja danych	Macierz musi mieć możliwość wykonywania migracji woluminów w ramach zasobów dyskowych bez zatrzymywania aplikacji z nich korzystających. Macierz musi posiadać możliwość migracji danych z zewnętrznych zasobów dyskowych.
Funkcje kopiujące	Macierz musi obsługiwać min 60 kopii migawkowych na macierz. Licencja na tą funkcjonalność musi być zawarta w cenie. Kopie danych typu „snapshot”, muszą być wykonywane przez macierz jako pojedyncza operacja w co najmniej trzech możliwych trybach: <ul style="list-style-type: none"> • kopia pełna, • kopia wskaźnikowa, • przyrostowa kopia pełna. Macierz musi mieć możliwość odtworzenia zawartości woluminu logicznego z kopii typu „snapshot” bez konieczności kopiowania danych za pośrednictwem serwera.
„Mirroring” woluminów	Funkcjonalność konfigurowania woluminu dyskowego posiadającego dwie kopie fizyczne na różnych grupach dyskowych i różnego typu (np.: jedna kopia z nadalokacją druga bez). W przypadku zapisu macierz zapisuje do obu kopii synchronicznie. W przypadku odczytu czyta tylko z jednej kopii. Kiedy jedna kopia jest niedostępna macierz automatycznie korzysta tylko z dostępnej kopii a po naprawie brakującej kopii automatycznie synchronizuje dane. Wolumin mirrorowany może być przekształcony w zwykły wolumin albo poprzez usunięcie jednej kopii albo poprzez wyodrębnienie jednej kopii w osobny wolumin.

Nadalokacja	Funkcjonalność dynamicznej alokacji przestrzeni dyskowej większej niż jest dostępna fizycznie oraz możliwość wyłączenia tej funkcjonalności dla wybranych woluminów.
Bezpieczeństwo	Wszystkie krytyczne komponenty takie jak: kontrolery dyskowe, pamięć „cache”, zasilacze i wentylatory muszą być zdublowane w taki sposób, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Brak pojedynczego punktu awarii. Wszelkie połączenia pomiędzy elementami składowymi macierzy (wszystkie ścieżki) muszą być redundantne. Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu „hot-swap”. Wentylatory typu „hot-swap”.
Zarządzanie	Interfejs zarządzający GUI, CLI nie wymagający instalacji dodatkowego oprogramowania na stacji zarządzającej. Możliwość zmiany mikrokodu bez przerywania dostępu do danych. Monitorowanie stanu pracy za pośrednictwem protokołu SNMP. Automatyzacja procesu informacji o stanie urządzenia, w tym informacji o awariach za pomocą wiadomości przesyłanych drogą elektroniczną.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim
Certyfikaty	Macierz musi być wyprodukowana zgodnie z normą ISO 9001.
Wymagania dodatkowe – obowiązkowe	
	W cenie macierzy zawarta powinna być instalacja i konfiguracja sprzętu i oprogramowania oraz wsparcie i prawo do poprawek i nowych wersji dla oprogramowania na okres 5 lat.
	Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.
Wymagania dotyczące gwarancji	
Warunki serwisu i gwarancji dla macierzy	Minimum pięć lat gwarancji z czasem reakcji na zgłoszenie awarii maksymalnie w ciągu 4 godzin od zgłoszenia. Bezpośredni dostęp do certyfikowanych inżynierów producenta macierzy. Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji firmware i sterowników (na płytach CD lub stronach internetowych). Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta.

Serwer kopii zapasowych - 1 sztuka	
Wymagania funkcjonalno-techniczne	
Obudowa	O wysokości maksymalnie 2U, dedykowana do zamontowania w szafie rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon)
Procesor	Osiągający w oferowanym serwerze wynik 430 pkt. w konfiguracji dwuprocesorowej w teście SPECint_rate_base2006. Wymagana jest obecność protokołu potwierdzającego osiągnięty wynik na stronie: www.spec.org (wydruk ze strony należy dołączyć do oferty).
Liczba procesorów	1
RAM	Minimum 48 GB DDR3, z technologią ECC, możliwość rozszerzenia pamięci do minimum 384 GB.
Gniazda PCI	Minimum 6 slotów PCIe 3.0 (możliwość opcjonalnego zastosowania jednej karty PCI-X).
Interfejsy sieciowe	4 porty typu 1Gb Ethernet. Karty sieciowe muszą wspierać load balancing, failover i TCP/IP Offload Engine. 2 porty 10Gb Ethernet.
Interfejsy FC	Dwa porty FC 8Gb umożliwiające połączenie z oferowaną biblioteką taśmową za pośrednictwem przełączników w obudowa blade.
Kontroler	Kontroler macierzowy SAS/SATA z 512MB pamięci cache, umożliwiający konfigurację dysków w RAID 0/1/10/5/50.
Napęd optyczny	Wewnętrzny napęd DVD-ROM
Dyski twarde	8 x 900 GB SAS Możliwość rozbudowy do 16 dysków SAS/SATA
Inne porty	1 port RJ-45 dedykowany dla interfejsu zdalnego zarządzania. 8 portów USB 1 port szeregowy
Video	Zintegrowana karta graficzna. 2 porty VGA (z przodu i z tyłu).
Zasilanie	Redundantne. Hot-Swap.
Zarządzanie	Zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzania serwerem poprzez połączenie w sieci TCP/IP przy użyciu przeglądarki internetowej, pozwalający m.in. na dostęp do konsoli serwera, włączanie/wyłączanie serwera, reinstalację systemu operacyjnego, zdalne podłączenie napędów.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Wymagania dodatkowe – obowiązkowe	
	Zamawiający wymaga fizycznej instalacji serwera w oferowanej szafie rack oraz wykonania testów uruchomieniowych

	Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.
Wymagania dotyczące gwarancji	
Warunki gwarancji	Przynajmniej pięć lat gwarancji z czasem reakcji w ciągu 4 godzin od zdiagnozowania problemu, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta serwera.
System operacyjny	
	64 bitowy system Windows 2012 Server lub równoważny, kompatybilny z oprogramowaniem do backupu

Biblioteka taśmowa - 1 sztuka	
Wymagania funkcjonalno-techniczne	
Napędy	2 x LTO5 z możliwością rozbudowy do 4. Napędy z mechanizmem automatycznie dostosowującym prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie przynajmniej 40-120 MB/s.
Typ obudowy	Do instalacji w standardowej szafie Rack 19".
Interfejs	Natywny FC.
Liczba slotów	Minimum 44 slotów na taśmy, minimum 3 sloty WE/WY. Możliwość automatycznego przemieszczania nośników z wykorzystaniem jednego robota, który musi mieć dostęp do wszystkich napędów i wszystkich slotów.
Liczba taśm	Minimum 48 taśm LTO-5 oraz 1 tasiemka czyszcząca. Zamawiający wymaga dostarczenia kodów kreskowych pozwalających na oznaczenie minimum 60 taśm.
Wymagania dodatkowe – obowiązkowe	
Warunki dodatkowe	Zamawiający oczekuje instalacji i konfiguracji biblioteki taśmowej w oferowanej infrastrukturze (połączenia z serwerem kopii zapasowych poprzez połączenie bezpośrednie FC). Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.
Wymagania dotyczące gwarancji	
Warunki gwarancji	minimum pięć lat gwarancji z czasem reakcji w następnym dniu roboczym, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu.
Wymagania dotyczące instruktazu stanowiskowego dla serwerów, biblioteki oraz macierzy	
	Wymagane jest także zapewnienie dedykowanego minimum dwudniowego instruktazu w zakresie konfiguracji i zarządzania urządzeniami. Instruktaż musi być przeprowadzony dla 4 osób w języku polskim na miejscu instalacji sprzętu u Klienta.

Zakres instruktażu	<ul style="list-style-type: none"> • konfiguracja serwera blade, dodawanie i usuwanie fizycznych serwerów, zmiana zasobów fizycznych, diagnostyka i monitoring, rozwiązywanie problemów • konfiguracja i odtwarzanie macierzy, tworzenie dysków logicznych, diagnostyka i monitoring, rozwiązywanie problemów, zarządzanie przestrzenią dyskową • konfiguracja biblioteki taśmowej, diagnostyka i monitoring, rozwiązywanie problemów, migracja nośników
--------------------	---

Serwer zarządzania - 3 sztuki	
Wymagania funkcjonalno-techniczne	
Obudowa	O wysokości maksymalnie 1U, dedykowana do zamontowania w szafie Rack 19" z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon)
Procesor	Osiągający w oferowanym serwerze wynik 250 pkt. w konfiguracji dwuprocesorowej w teście SPECint_rate_base2006. Wymagana jest obecność protokołu potwierdzającego osiągnięty wynik na stronie: www.spec.org (wydruk ze strony należy dołączyć do oferty).
Liczba procesorów	1
RAM	Minimum 48 GB DDR3, z technologią ECC, możliwość rozszerzenia pamięci do minimum 768 GB.
Gniazda PCI	Minimum 2 sloty PCIe 3.0. (możliwość opcjonalnego zastosowania jednej karty PCI-X)
Interfejsy sieciowe	2 porty typu 1Gb Ethernet. Karty sieciowe muszą wspierać load balancing, failover i TCP/IP Offload Engine.
Kontroler	Kontroler macierzowy SAS/SATA konfigurację dysków w RAID 0/1/10.
Napęd optyczny	Wewnętrzny napęd DVD-ROM
Dyski twarde	2 x 146 GB 15.000 obrotów na minutę hot-swap. Możliwość rozbudowy do 8 dysków SAS/SATA.
Inne porty	1 port RJ-45 dedykowany dla interfejsu zdalnego zarządzania. Min. 7 portów USB 1 port szeregowy
Video	Zintegrowana karta graficzna. 2 porty (z przodu i z tyłu).
Zasilanie	Redundantne. Hot-Swap.

Zarządzanie	Zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie serwerem poprzez połączenie w sieci TCP/IP przy użyciu przeglądarki internetowej, pozwalający m.in. na dostęp do konsoli serwera, włączanie/wyłączanie serwera, reinstalację systemu operacyjnego, zdalne podłączenie napędów.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
Wymagania dodatkowe – obowiązkowe	
	Zamawiający wymaga fizycznej instalacji serwera w oferowanej szafie Rack oraz wykonania testów uruchomieniowych. Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.
wymagania dotyczące gwarancji	
Warunki gwarancji	minimum pięć lat gwarancji z czasem reakcji w ciągu 4 godzin od zdiagnozowania problemu, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu.
System operacyjny	
	64 bitowy system Windows 2012 Server lub równoważny, kompatybilny z oprogramowaniem do backupu

Przełącznik centralny typ A - ilość 2 sztuki	
Wymagania funkcjonalno-techniczne	
obudowa	wolnostojąca, montaż w 19-calowym stelażu telekomunikacyjnym (standard EIA) lub w specjalnej szafce na sprzęt (akcesoria montażowe w komplecie). Montaż wyłącznie w pozycji poziomej, wysokość 1U.
Porty	Min. 24 porty 10 Gigabitowe w standardzie SFP+: <ul style="list-style-type: none"> • 2 dla podłączenia routera(ów) 1000BASE-T SFP RJ45, • 4 dla podłączenia przełączników w obudowie typu blade 10 Gb/s SR (SFP+), • 8 dla podłączenia przełączników typu A standardzie 10 Gb/s (SFP+), • 2 dla podłączenia przełączników typu B standardzie 10 Gb/s (SFP+), • 2 dla połączenia przełączników centralnych typu D między sobą wyposażone w przetworniki (GBIC) lub kable umożliwiające podłączenie powyższych przełączników za pomocą pojedynczych ścieżek
Przepustowość	min. 367 Mpps
wydajność	min. 488Gb/s
Wielkość bufora	min. 3,6 GB

Przełączanie w warstwie	2 i 3 modelu OSI
Zasilacze	Dwa wbudowane (wewnętrzne) zasilacze dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia, możliwość instalacji zasilaczy 36-72V DC
wentylatory	Wymienne (moduł) wentylatory, wymieniane podczas pracy urządzenia, możliwość wyboru kierunku przepływu powietrza Front to Back lub Back to Front poprzez instalacje odpowiedniego modułu wentylatorów. Wentylatory muszą zapewniać nadmiarowość.
Port USB	min. 1
opóźnienie	nie może być wyższe niż 1.7 us dla pakietów 64 bajty w trybach Cut Through oraz Store and Forward
Tablica adresów MAC	o wielkości min. 128000 pozycji
Wielkość tablicy routingu	min. 12.000 wpisów
Budowa	Możliwość łączenia urządzeń w stos działający jako jeden wirtualny przełącznik. Urządzenia muszą mieć możliwość łączenia w ramach stosu z wykorzystaniem standardowych połączeń Ethernet 10Gbps.
Obsługa	Obsługa ramek Jumbo
	Obsługa Loop Detection
	Routing IPv4 – statyczny i dynamiczny (min. RIP v1 i v2, OSFP, BGP)
	Routing IPv6 – statyczny i dynamiczny (min. RIPng, OSPFv3, BGP+, IS-ISv6)
	Możliwość wyboru sposobu obsługi kolejek – Strict Priority; Weighted Round Robin, Weighted Fair Queuing WFQ, WRR + SP
	Możliwość przypisania pakietów do Voice VLAN'u z wykorzystaniem mapowania zakresów MAC
	Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
	Obsługa sieci IEEE 802.1Q VLAN – 4094 sieci VLAN oraz IEEE 802.1ad QinQ
	Możliwość automatycznej separacji ruchu VoIP w wydzielonym VLANie (Voice VLAN)
	Obsługa IGMP v1/v2/v3 oraz IGMP Snooping
	Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
	Obsługa Policy Based Routing
	Obsługa PIM-SSM, PIM-DM i PIM-SM (dla IPv4 i IPv6)
	Obsługa Multicast VLAN
	Obsługa Multicast Source Discovery Protocol (MSDP)
	Obsługa ECMP (Equal Cost Multi Path)
	Obsługa Virtual Router Redundancy Protocol (VRRP)

	Obsługa Bidirectional Forwarding Detection (BFD)
	DHCP Snooping
	Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.
	Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
	Obsługa standardu 802.1p. Wsparcie dla Remarking 802.1p
	Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p
	RADIUS Accounting
	Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
	Zarządzanie poprzez port konsoli, SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
	Syslog
	sFlow i IPFIX
	RMON
	Obsługa uRPF
	Obsługa OAM (802.3ah) i CFD (802.1ag)
	IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED
	Network Time Protocol (NTP) v3
wymagania dotyczące oprogramowania	
oprogramowanie	Możliwość przechowywania wielu wersji oprogramowania na przełączniku
	Możliwość przechowywania wielu plików konfiguracyjnych na przełączniku, możliwość uploadu i downloadu pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
	Pełna zgodność z oprogramowaniem zarządzającym zaoferowanym w ramach zamówienia w zakresie monitorowania i konfiguracji.
	Bezpłatne aktualizacje przez cały okres posiadania sprzętu - dostępne na stronie producenta
wymagania dotyczące gwarancji	
Gwarancja	min. 36 miesięcy. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.
Wymagania dodatkowe – obowiązkowe	
dokumentacja użytkownika	Zamawiający wymaga dokumentacji w wersji elektronicznej i drukowanej w języku polskim lub angielskim
Instalacja	Zamawiający wymaga fizycznej instalacji w oferowanej szafie i wykonania testów uruchomieniowych. Wsparcie i prawo do poprawek i nowych wersji dla oprogramowania na okres min. 36 miesięcy.
	Wymagane jest także zapewnienie dedykowanego min. dwudniowego instruktażu z zakresu konfiguracji i zarządzania urządzeń. Instruktaż

	musi być przeprowadzony dla 4 osób w języku polskim na miejscu instalacji sprzętu u Klienta.
	Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.

Przełącznik brzegowy typ B - ilość 2 szt

Wymagania funkcjonalno-techniczne

Obudowa	wolnostojąca, montaż w 19-calowym szelazhu telekomunikacyjnym (standard EIA) lub w specjalnej szafce na sprzęt (akcesoria montażowe w komplecie). Montaż wyłącznie w pozycji poziomej, wysokość 1U.
Porty	Min. 44 porty 10BASE-T/100BASE-TX/1000BASE-T oraz min. 4 porty combo - 10BASE-T/100BASE-TX/1000BASE-T i SFP Gigabit. Min. dwa sloty rozszerzeń umożliwiające zainstalowanie dodatkowo min. 4 portów 10 Gb/s. Zainstalowany moduł lub moduły posiadające min. 2 porty 10 Gb/s (SFP+) wyposażone w przetworniki (GBIC) lub kable umożliwiające podłączenie do przełączników centralnych typu D za pomocą dwóch niezależnych ścieżek
Przepustowość	Przepustowość: min. 142,9 Mpps
Budowa	Możliwość łączenia urządzeń w klastry (min. 8 urządzeń w ramach klastra) i zarządzania całością takiej grupy poprzez jeden adres IP Możliwość łączenia urządzeń w stos działający jako jeden wirtualny przełącznik. Urządzenia muszą być łączone w ramach stosu z wykorzystaniem standardowych połączeń Ethernet 10Gbps.
Wydajność	min. 192 Gbps
Przepustowość	min. 142,9 Mpps
Obsługa	Tablica adresów MAC o wielkości min. 16.000 pozycji
	Obsługa ramek Jumbo
	Obsługa routingu statycznego, min. 32 wpisy
	Obsługa ruchu Multicast: IGMP Snooping v1/v2/v3, MLD Snooping v1/v2 Obsługa min. 1000 grup multicast
	Wsparcie dla IPv6: zarządzenie przełącznikiem: pingv6, tracertv6, Telnetv6, TFTPv6, DNSv6, syslogv6, FTPv6, SNMPv6, DHCPv6, RADIUS dla IPv6
	IEEE 802.1w Rapid Spanning Tree Protocol, IEEE 802.1s Multiple Spanning Tree Protocol, Smart Link lub równoważny, Rapid Ring Protection Protocol (RRPP) lub równoważny
	Obsługa IEEE 802.1ad QinQ i Selective QinQ, sieci IEEE 802.1Q VLAN – min. 4094 sieci VLAN
	Elastyczność w konfiguracji sieci VLAN – każdy port powinien posiadać możliwość przypisania do wielu sieci VLAN taggowanych, jak i do wielu sieci VLAN

	nie-taggowanych
	Możliwość automatycznej separacji ruchu VoIP w wydzielonym VLAN'ie (Voice VLAN)
	Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
	BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BPDU w celu przeciwdziałania pętlom
	Wsparcie dla DHCP Relay, DHCP client oraz DHCP Protection
	Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
	Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
	Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
	Obsługa standardu 802.1p – min. 8 kolejek na porcie
	Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
	Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
	sFlow
	Funkcja mirroringu portów: 1 to 1 Port mirroring, Many to 1 port mirroring
	Inteligentny port mirroring - kopowanie ruchu wybranego przy pomocy listy ACL z wybranego portu lub VLANu na lokalny lub zdalny port
	Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x: <ul style="list-style-type: none"> • Obsługa następujących trybów uwierzytelniania – EAP-MD5, PAP, CHAP, PEAP, EAP-TLS • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x • Możliwość uwierzytelniania wielu użytkowników na jednym porcie • Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników
	LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED.
	Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
	TACACS+ i RADIUS Network Login
	RADIUS Accounting
	sMożliwość centralnego uwierzytelniania administratorów na serwerze RADIUS

	Zarządzanie poprzez port konsoli (port szeregowy RS-232), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
	Syslog
	NTPv3
wymagania dotyczące oprogramowania	
oprogramowanie	Możliwość przechowywania wielu wersji oprogramowania na przełączniku
	Możliwość przechowywania wielu plików konfiguracyjnych na przełączniku, możliwość uploadu i downloadu pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
	Management VLAN
	Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
	DLDP - Device Link Detection Protocol
	Kontrola ruchu broadcast
	Pełna zgodność z oprogramowaniem zarządzającym zaoferowanym w ramach zamówienia w zakresie monitorowania i konfiguracji.
	Bezpłatne aktualizacje przez cały okres posiadania sprzętu - dostępne na stronie producenta
wymagania dotyczące gwarancji	
min. 36 miesięcy. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzenia. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.	
Wymagania dodatkowe – obowiązkowe	
dokumentacja użytkownika	Zamawiający wymaga dokumentacji w wersji elektronicznej i drukowanej w języku polskim lub angielskim
Instalacja	Zamawiający wymaga fizycznej instalacji w oferowanej szafie i wykonania testów uruchomieniowych.
	Wymagane jest także zapewnienie dedykowanego min. dwudniowego instruktażu z zakresu konfiguracji i zarządzania urządzeń. Instruktaż musi być przeprowadzony dla 4 osób w języku polskim na miejscu instalacji sprzętu u Klienta. instruktażu obejmującego proces instalacji, aktualizacji i konfiguracji wdrożonego środowiska systemowego. Instruktaż musi być przeprowadzony przez osobę posiadającą certyfikat świadczący o autoryzacji do przeprowadzenia szkoleń danego producenta. Zamawiający może wymagać potwierdzenia tego certyfikatu przed podpisaniem umowy.
	Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.

Przełącznik brzegowy typ C - ilość 5 szt.	
Wymagania funkcjonalno-techniczne	
Obudowa	wolnostojąca, montaż w 19-calowym stelażu telekomunikacyjnym (standard EIA) lub w specjalnej szafce na sprzęt (akcesoria montażowe w komplecie). Montaż wyłącznie w pozycji poziomej, wysokość 1U.
Porty	Min. 44 porty 10BASE-T/100BASE-TX/1000BASE-T oraz min. 4 porty combo - 10/100/1000 Mbit oraz mini-GBIC.
	Min. dwa sloty rozszerzeń umożliwiające zainstalowanie dodatkowo min. 4 portów 10 Gb/s. Zainstalowany moduł lub moduły posiadające min. 2 porty 10 Gb/s (SFP+) wyposażone w przetworniki (GBIC) lub kable umożliwiające podłączenie do przełączników centralnych typu D za pomocą dwóch niezależnych ścieżek
Przepustowość	min. 142,9 Mpps
Wydajność	min. 192 Gbps
budowa	Możliwość łączenia urządzeń w klastry (min. 8 urządzeń w ramach klastra) i zarządzania całością takiej grupy poprzez jeden adres IP Możliwość łączenia urządzeń w stos działający jako jeden wirtualny przełącznik. Urządzenia muszą być łączone w ramach stosu z wykorzystaniem standardowych połączeń Ethernet 10Gbps.
Obsługa	Tablica adresów MAC o wielkości min. 16.000 pozycji
	Obsługa ramek Jumbo
	Obsługa routingu statycznego, min. 32 wpisy
	Obsługa ruchu Multicast: IGMP Snooping v1/v2/v3, MLD Snooping v1/v2
	Obsługa min. 1000 grup multicast
	Wsparcie dla IPv6: zarządzanie przełącznikiem: pingv6, tracertv6, Telnetv6, TFTPv6, DNSv6, syslogv6, FTPv6, SNMPv6, DHCPv6, RADIUS dla IPv6
	IEEE 802.1w Rapid Spanning Tree Protocol, IEEE 802.1s Multiple Spanning Tree Protocol, Smart Link lub równoważny, Rapid Ring Protection Protocol (RRPP) lub równoważny
	Obsługa IEEE 802.1ad QinQ i Selective QinQ, sieci IEEE 802.1Q VLAN – min. 4094 sieci VLAN
	Elastyczność w konfiguracji sieci VLAN – każdy port powinien posiadać możliwość przypisania do wielu sieci VLAN taggowanych, jak i do wielu sieci VLAN nie-taggowanych
	Możliwość automatycznej separacji ruchu VoIP w wydzielonym VLAN'ie (Voice VLAN)
	Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętłom	

	Wsparcie dla DHCP Relay, DHCP client oraz DHCP Protection
	Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
	Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
	Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
	Obsługa standardu 802.1p – min. 8 kolejek na porcie
	Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
	Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
	sFlow
	Funkcja mirroringu portów: 1 to 1 Port mirroring, Many to 1 port mirroring
	Inteligentny port mirroring - kopiowanie ruchu wybranego przy pomocy listy ACL z wybranego portu lub VLANu na lokalny lub zdalny port
	Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x: <ul style="list-style-type: none"> • Obsługa następujących trybów uwierzytelniania – EAP-MD5, PAP, CHAP, PEAP, EAP-TLS • Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x • Możliwość uwierzytelniania wielu użytkowników na jednym porcie • Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS • Przypisanie profilu QoS dla użytkownika lub grupy użytkowników
	LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED.
	Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
	TACACS+ i RADIUS Network Login
	RADIUS Accounting
	Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
	Zarządzanie poprzez port konsoli (port szeregowy RS-232), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
	Syslog
	NTPv3
wymagania dotyczące oprogramowania	
Oprogramowanie	Możliwość przechowywania wielu wersji oprogramowania na przełączniku

	<p>Możliwość przechowywania wielu plików konfiguracyjnych na przełączniku, możliwość uploadu i downloadu pliku konfiguracyjnego w postaci tekstowej do stacji roboczej</p> <p>Management VLAN</p> <p>Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego</p> <p>DLDP - Device Link Detection Protocol</p> <p>Kontrola ruchu broadcast</p> <p>Pełna zgodność z oprogramowaniem zarządzającym zaoferowanym w ramach zamówienia w zakresie monitorowania i konfiguracji</p> <p>Bezpłatne aktualizacje przez cały okres posiadania sprzętu - dostępne na stronie producenta. Wsparcie i prawo do poprawek i nowych wersji dla oprogramowania na okres min. 36 miesięcy.</p>
wymagania dotyczące gwarancji	
min. 36 miesięcy. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzenia. Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.	
Wymagania dodatkowe – obowiązkowe	
dokumentacja użytkownika	Zamawiający wymaga dokumentacji w wersji elektronicznej i drukowanej w języku polskim lub angielskim
Instalacja	<p>Zamawiający wymaga fizycznej instalacji w oferowanej szafie i wykonania testów uruchomieniowych.</p> <p>Wymagane jest także zapewnienie dedykowanego min. dwudniowego instruktażu z zakresu konfiguracji i zarządzania urządzeń. Instruktaż musi być przeprowadzony dla 4 osób w języku polskim na miejscu instalacji sprzętu u Klienta. instruktażu obejmującego proces instalacji, aktualizacji i konfiguracji wdrożonego środowiska systemowego. Instruktaż musi być przeprowadzony przez osobę posiadającą certyfikat świadczący o autoryzacji do przeprowadzenia szkoleń danego producenta. Zamawiający może wymagać potwierdzenia tego certyfikatu przed podpisaniem umowy.</p>
	Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.

Router dostępowy- ilość 2 sztuki

Wymagania funkcjonalno-techniczne

obudowa	wolnostojąca, montaż w 19-calowym stelażu telekomunikacyjnym (standard EIA) lub w specjalnej szafce na sprzęt (akcesoria montażowe w komplecie). Montaż wyłącznie w pozycji poziomej, wysokość 1U.
---------	--

Processor	Min. 32 rdzenie, min. 1.2 GHz
Porty	1. Min. 12 portów Ethernet 10/100/1000Mbit 2. Min. 4 porty SFP+ umożliwiające podłączenie przełączników w standardzie 10 Gb/s (SFP+), wyposażone w przetworniki (GBIC) lub kable umożliwiające podłączenie powyższych przełączników za pomocą pojedynczych ścieżek, oraz łącz operatorów: 1000Base BX10-D , SFP LCSM 1310nm
Przepustowość	min. 1300 kpps przy ramce 1518 B i 25 regułach filtrowania, min 23 Mpps dla samego routingu (pomiar wg RFC 2544)
wydajność	min. 15 Gbit/s przy ramce 1518b i 25 regułach filtrowania (pomiar wg RFC 2544)
Pamięć operacyjna	Min. 4 GB, możliwość rozbudowy do min. 16GB
Pamięć nieulotna	Min. 1 GB
Port USB	min. 1, umożliwiający podłączenie modemu GSM
Konsola szeregową	Dostępna przez port RS323C
Wsparcie dla VPN	Poufność danych -IPSec oraz SSL VPN, sprzętowe wspomaganie szyfrowania
Routing	Wsparcie dla protokołów dynamicznego routingu - BGP, OSPF
VLAN	Możliwość tworzenia interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
Firewall	zapora ogniowa klasy Stateful Inspection wykrywanie ruchu P2P Klasyfikacja ruchu wg <ul style="list-style-type: none"> • źródłowego adresu MAC • źródłowego / docelowego adresu IP • źródłowego / docelowego portu i zakresu portów • protokołu IP • zawartości pakietu • rozmiaru pakietu
Profilowanie ruchu	Kontrola pasma - ograniczenia prędkości i ustawienie priorytetów dla poszczególnych klasyfikacji ruchu
wymagania dotyczące oprogramowania	
	Konfiguracja routeraz z poziomu przeglądarki internetowej oraz konsol tekstowej (SSH)
oprogramowanie	Możliwość wykonywania automatycznej kopii konfiguracji i przechowania jej na routerze oraz przesłania przez FTP
	Logowanie komunikatów na zewnętrzny serwer Syslog
	Możliwość przechowywania wielu plików konfiguracyjnych na przełączniku, możliwość uploadu i downloadu pliku konfiguracyjnego w postaci tekstowej do stacji roboczej

	Bezpłatne aktualizacje przez cały okres posiadania sprzętu - dostępne na stronie producenta
	Bezpłatne aktualizacje przez cały okres posiadania sprzętu - dostępne na stronie producenta
wymagania dotyczące gwarancji	
Gwarancja	min. 12 miesięcy.
Wymagania dodatkowe – obowiązkowe	
Instalacja	Wymagane jest także zapewnienie dedykowanego min. dwudniowego instruktażu z zakresu konfiguracji i zarządzania urządzeń. Instruktaż musi być przeprowadzony dla 4 osób w języku polskim na miejscu instalacji sprzętu u Klienta.
	Urządzenie musi być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisowa producenta na terenie Polski.

Platforma do zarządzania siecią

System musi być zbudowany w architekturze klient – serwer.

Licencja na system powinna umożliwiać zarządzanie 65-ma urządzeniami sieciowymi różnych producentów.

System musi minimalnie wspierać instalację części serwerowej na platformach Windows Server 2003 SP2 oraz Red Hat Enterprise Linux 5.

System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność.

System zarządzania musi spełniać podstawowe funkcje:

- Automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet
- Monitorowanie stanu urządzeń po protokole SNMP
- Konfiguracja urządzeń po protokole SNMP
- Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach
- Konfiguracja VLANów na zarządzanych urządzeniach
- Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania
- Zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń
- Możliwość wysyłania alarmów np. mailem lub SMS'em
- Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta
- Obrazowanie sieci w postaci mapki wraz z wyróżnianiem kolorami występujących alarmów
- Lokalizowanie użytkowników po adresie IP lub MAC
- Możliwość zdefiniowania polityki zmieniającej ustawienia sieci w przypadku wykrycia ataku sieciowego
- Możliwość utworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym
- Funkcja Telnet / SSH proxy umożliwiająca zarządzanie CLI przez przeglądarkę Internetową.
- Funkcja zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem android.
- Dla wszystkich obsługiwanych standardowo urządzeń musi być dostępne nie tylko monitorowanie ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń.
- Dostęp do systemu zarządzania musi być realizowany przez przeglądarkę internetową.
- Niezbędne jest aby system zarządzania był w stanie podłączyć się i importować dane z LDAP / Active Directory
- System powinien mieć możliwość autentykacji użytkowników w oparciu o LDAP i Radius

- System powinien mieć możliwość zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, Email.
- Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń
- System powinien mieć możliwość zarządzania siecią wirtualną poprzez integracje SOAP z VMWare VirtualCenter Server oraz Microsoft Hyper-V vManager.
- System powinien mieć możliwość zarządzania siecią wirtualną dla serwerów Microsoft Hyper-V poprzez profil Power shell oraz WMI.
- System powinien wspierać zarządzanie conajmniej dla 6000 modeli urządzeń.
- System powinien mieć możliwość automatycznej aktualizacji przez Internet.
- System powinien mieć możliwość implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów.
- System powinien posiadać kontekstową funkcję pomocy zmieniającą zawartość w zależności od wyświetlanego kontekstu.

Muszą być dostępne moduły umożliwiające rozbudowę i integrację systemu o następujące funkcjonalności:

- Zarządzanie dostępem użytkowników z wykorzystaniem 802.1x
- Zarządzanie klientami na stacjach roboczych w ramach implementacji technologii Network Access Control
- Zarządzenie infrastrukturą Wi-Fi z wykorzystaniem kontrolerów bezprzewodowych
- Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA
- Obsługa informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników
- Zarządzenie systemem telefonii IP
- Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS
- Zarządzanie dostępem zdalnym Ipsec/VPN
- Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych SFLOW, NetStream v5 oraz analizy kontentu pakietów SMTP, FTP, HTTP
- Zarządzanie Firewallami

Oprogramowanie do wirtualizacji

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone dowolną liczbę rdzeni oraz do 2TB pamięci fizycznej RAM.
4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-8 procesorowych.
5. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM.
6. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 4 porty szeregowo i 3 porty równoległe i 20 urządzeń USB .
8. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
9. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
10. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.

11. Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista, Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows 7, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware, FreeBSD, Mac OS X.
12. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
13. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
14. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance.
15. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku.
16. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
17. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
18. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
19. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn.
20. Rozwiązanie musi zapewniać taki mechanizm bezpiecznego uaktualniania aplikacji i systemów operacyjnych wirtualnych maszyn, poprzez który można wprowadzać poprawki na pojedyncze wirtualne maszyny jak i na całe grupy wirtualnych maszyn. Dla bezpieczeństwa wspomniany mechanizm musi pozwalać na automatyczne wykonywanie kopii migawkowych przed aktualizacją.
21. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.
22. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
23. Rozwiązanie musi mieć możliwość automatycznego równoważenia obciążenia serwerów fizycznych poprzez przenoszenie pracujących wirtualnych maszyn pomiędzy nimi. Mechanizm ten musi być wyposażony w możliwość definiowania reguł przenoszenia np. przeniesienie maszyny wirtualnej wymusza przeniesienie innej lub równoważenie następuje w obrębie zdefiniowanych grup wirtualnych maszyn pomiędzy wybranymi serwerami fizycznymi.
24. Rozwiązanie musi mieć możliwość oszczędzania energii elektrycznej poprzez automatyczne wyłączenie wskazanych serwerów fizycznych w przypadku braku obciążenia generowanego przez wirtualne maszyny i automatycznego ich włączenia w sytuacji wzrostu obciążenia.
25. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi.
26. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
27. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny które na nim pracowały były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym.
28. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.

29. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
30. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN)
31. Zamawiający wymaga dostarczenia licencji oprogramowania objętej 12-to miesięcznym wsparciem producenta spełniające powyższe wymagania dla 7 serwerów typu blade opisanych w niniejszym dokumencie. Zamawiający wymaga dostarczenie jednego systemu do zarządzania serwerami wirtualnymi.

Oprogramowanie do back-up

Oprogramowanie do backupu powinno charakteryzować się następującymi cechami:

1. Oprogramowanie powinno być przeznaczone dla średnich i dużych firm, które mają rozbudowane środowisko informatyczne celem sprostania rozwojowi tego środowiska.
2. Program powinien umożliwiać wykonywanie backupów w środowisku heterogenicznym
3. Oprogramowanie powinno oferować backup serwerów pracujących pod systemami operacyjnymi takimi jak: Windows 2000, Windows 2003, Windows 2008, Redhat Linux, Suse Linux, Solaris SPARC, Solaris x86, IBM AIX, HP-UX
4. Powinien umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej i oferować backup zasobów po sieci LAN lub SAN.
5. Powinien być łatwy w instalacji, konfigurowaniu i zarządzaniu poprzez interface graficzny (GUI), jak również poprzez interfejs tekstowy CLI. Powinien umożliwiać pełne dostosowanie do środowiska klienta.
6. Dla serwerów backupowanych, musi istnieć możliwość multipleksowania zapisów – jednoczesnego zapisu na jeden napęd z kilku klientów/serwerów. Funkcjonalność ta musi być dostępna bez pośrednictwa dysków, to znaczy serwer backupowy zapisuje multipleksowane dane bezpośrednio na napędy taśmowe.
7. Musi posiadać funkcję umożliwiającą wykonywanie backupu wieloma równoległymi strumieniami – multistreaming. Funkcjonalność ta musi być dostępna bez pośrednictwa dysków, to znaczy serwer backupowy zapisuje dane bezpośrednio na napędy taśmowe
8. Automatyczny backup bazujący na kalendarzu. Możliwość backupu typu: full, incremental, differential.
9. Musi umożliwiać wykonywanie skryptów przed i po backupie (np. uruchamianych przed backupem bazy oraz po wykonaniu backupu off-line bazy, kasowanie redo logów)
10. Do przechowywania danych wykorzystywane powinny być bezobsługowe biblioteki taśmowe bądź lokalne dyski.
11. Powinien posiadać możliwość równoczesnego zapisu/ odczytu na wielu napędach taśmowych w tym samym czasie.
12. Oprogramowanie musi zapewniać deduplikację danych podlegających backupowi na nośniki dyskowe w czasie rzeczywistym.
13. Oprogramowanie musi zapewniać realizację backupu w scenariuszu D2D2T.
14. Oprogramowanie musi wykorzystywać relacyjną bazę danych do przechowywania informacji o środowisku jak i zadaniach backupowych. Jeśli zachodzi taka potrzeba zamawiający wymaga dostarczenia licencji na taką bazę danych.
15. Oprogramowanie musi zapewnić możliwość automatycznej weryfikacji stanu nośników backupowych niezależnie od zadań backupowych.
16. Oprogramowanie powinno umożliwić definicję różnych klas użytkowników korzystających z rozwiązania posiadających różne uprawnienia np.: operator backupu, administrator backupu, operator odtwarzania etc.
17. Musi mieć możliwość zintegrowania się z technologią VCB (Vmware Consolidate Backup) lub vStorage API (vSphere) celem wydajnego backupu danych z możliwością odtwarzania pojedynczych plików (zawartych w VMDK) dla systemów Windows
18. Musi wspierać najnowsze wersje systemów do wirtualizacji środowisk: vSphere 5.0, Hyper-V 2.0
19. Musi oferować integrację dla backupu środowisk wirtualnych opartych o Microsoft Hyper-V, z technologią przywracania pojedynczych plików z maszyn wirtualnych Windows z backupu całej maszyny wirtualnej.

20. Dla środowisk Vmware odtwarzanie danych z backupu pełnego, różnicowego czy blokowego musi być dostępne niezależnie gdzie znajdują się dane (dyski, taśmy, VTL, deduplikacja)
21. Powinien potrafić backupować online bazy danych, np. Oracle, Exchange, SQL Server, Sybase.
22. Powinien posiadać możliwość backupu online danych z systemu SharePoint Portal Server z możliwością przywracania pojedynczych elementów
23. Backup i odtwarzanie serwera Exchange powinno umożliwiać odtworzenie na poziomie pojedynczej wiadomości w skrzynkach użytkowników,
24. Odtwarzanie Microsoft Active Directory na poziomie pojedynczych elementów (np. OU czy pojedynczy atrybutów)
25. Powinien posiadać również wbudowany mechanizm do backupowania otwartych plików
26. Powinien potrafić wykorzystywać do backupu mechanizm kopii migawkowych systemu Microsoft Windows (VSS)
27. Posiadać funkcje disaster-recovery umożliwiające proste i szybkie automatyczne odtworzenie serwera po awarii.
28. Możliwość szyfrowania danych przesyłanych przez sieć LAN. Opcja powinna być ściśle zintegrowana z produktem do backupu i wykorzystywać algorytm AES 256bit.
29. Możliwość kompresji na kliencie backupowym przed wysłaniem danych przez sieć.
30. System powinien mieć możliwość monitorowania i alterowania poprzez email
31. Powinien posiadać zaawansowane funkcje monitoringu oraz generowania raportów.
32. Umożliwiać graficzną reprezentację zadań, statusu poszczególnych backupów oraz środowisk backupu dla środowisk lokalnych jak i zdalnych
33. Zamawiający wymaga dostarczenia licencji oprogramowania objętej 3 letnim wsparciem producenta spełniającej powyższe wymagania dla następujących systemów:
 - 3 hostów Vmware vSphere pozwalające na backup dowolnej ilości maszyn wirtualnych
 - 1 serwera backupu, dla którego jest możliwość backupu systemu
 - 1 biblioteka taśmowa (2 x LTO5)