Szczegółowy opis wymagań dotyczących przedmiotu zamówienia

Przedmiotem zamówienia jest **budowa redundantnego środowiska HA w oparciu o trzy serwery typu Blade, przełącznik sieciowy, router oraz rozbudowę współdzielonej macierzy dyskowej Fujitsu DX90S2 wraz z wdrożeniem**.

Zakres zamówienia obejmuje:

1. Dostawę trzech serwerów typu Blade wraz z szafą, instalacją oraz opieką techniczną przez okres nie krótszy niż 36 miesięcy;
2. Dostawę przełącznika HP kompatybilnego z posiadanym przez zamawiającego modelem HP 4208vl, celem utworzenia stosu;
3. Rozbudowę posiadanej przez zamawiającego macierzy Fujitsu Eternus DX90 S2;
4. Dostawę urządzenia firewall/VPN/UTM;
5. Wykonanie projektu technicznego zakresu prac oraz wdrożenie.

Całość prac musi być wykonana na podstawie zaakceptowanego projektu technicznego stworzonego na podstawie istniejących elementów infrastruktury oraz konsultacji ze służbami informatycznymi zamawiającego. Projekt techniczny ma być przedstawiony do akceptacji w terminie 3 tygodni od daty podpisania umowy. W ciągu 3 dni roboczych zamawiający przekaże uwagi do projektu technicznego. Po akceptacji projektu wykonawca będzie mógł przystąpić do prac wdrożeniowych. W terminie 2 tygodni od daty podpisania protokołu odbioru jakościowego wykonawca przedstawi dokumentację powykonawczą dotyczącą wykonanych działań do akceptacji. W terminie 3 dni roboczych zamawiający przedstawi uwagi do dokumentacji.
Wszystkie elementy serwerów i innych urządzeń będą pracować w trybie ciągłym (przez 24 godziny na dobę, 365 dni w roku) i muszą zapewniać wydajną, stabilną i nieprzerwaną pracę pod maksymalnym obciążeniem wszystkich podzespołów (procesory, pamięć, interfejsy sieciowe, itd.).

Wymagania:

Oferowany sprzęt /podzespoły /usługi muszą bezwzględnie spełniać minimalne wymagania wyszczególnione w Tabeli 1 – Wymagania podstawowe. W kolumnie "Oferta wykonawcy" Wykonawca musi wypełnić wszystkie pola wpisując nazwę producenta, model, ewentualnie numer katalogowy oraz parametry techniczne oferowanego sprzętu lub potwierdzając, że oferowany sprzęt /podzespół /usługa spełnia wymagania zamawiającego.

Tabela 1 – Wymagania podstawowe

Budowa redundantnegobudowa redundantnego środowiska HA w oparciu o trzy serwery typu Blade, przełącznik sieciowy, router oraz rozbudowę współdzielonej macierzy dyskowej Fujitsu DX90S2 wraz z wdrożeniem.	
1. Serwery typu Blade – 3 szt. **(zainstalowane w szafie Blade)**	Producent sprzętu, ewentualnie model, nr katalogowy *(proszę podać):* ....
Wymagania Zamawiającego	*Oferta Wykonawcy (Tak/Nie, deklaracja)*
Obudowa: 1) typu Blade, zgodna z zaoferowaną szafą Blade, dostarczone przez jednego producenta, 2) możliwość instalacji 2 dysków SSD w obudowie serwera, 3) dioda pozwalająca na wizualną identyfikację serwera w szafie, 4) diodowa sygnalizacja: pracy, usterki, aktywności połączeń LAN;	

Procesory: 1) zainstalowane dwa procesory 8-rdzeniowe, osiągające co najmniej 655 punktów w teście SPECint_rate2006,	
Płyta główna: 1) zaprojektowana i wyprodukowana przez producenta serwera, 2) obsługa minimum dwóch procesorów dwunastordzeniowych, 3) obsługa minimum 1024 GB pamięci operacyjnej typu DDR3 (minimum 24 złącza pamięci) z technologiami Advanced ECC, Chipkill (SDDC), 4) wyposażona w zintegrowany kontroler RAID 0/1, 5) minimum dwa złącza dla kart nakładkowych FC/Ethernet 10Gbit/IB typu mezzanine PCI Express gen. 3.0 x 8, 6) wsparcie dla TPM 1.2 (możliwość integracji), 7) możliwość instalacji modułu flash do obsługi wirtualizatora (wewnętrzne złącze, niedostępne z zewnątrz serwera);	
Pamięć RAM: minimum 128GB DDR3 1600 MHz każdy;	
Zainstalowane dyski SSD: 1) 2 dyski typu SSD o pojemności min. 100GB każdy, 2) kontroler RAID z min. 512 MB cache, obsługa grup RAID 0, 1 dla dysków wewnętrznych oraz RAID 10, 5, 50, 6, 60 dla dysków zewnętrznych;	
Interfejsy I/O, złącza: 1) minimum 4 interfejsy LAN typu 10 Gbit/s, w tym co najmniej dwa z możliwością podziału na 4 funkcje logiczne na każdy port (przydział 4 adresów MAC), wsparcie iSCSI, FcoE, 2) porty muszą być podłączone poprzez backplane do switchy zainstalowanych w obudowie blade (po 2 porty na każdy z zamontowanych przełączników w obudowie), 3) dedykowany interfejs serwisowy typu LAN 1Gbit/s do obsługi sprzętowej karty zarządzającej;	
Zarządzanie: 1) zintegrowany z płytą główną kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0 umożliwiający zdalny restart serwera i pełne zarządzanie, włącznie z przejęciem zdalnym konsoli graficznej oraz zdalnego podłączenia napędów na poziomie sprzętowym, 2) dedykowana karta LAN 1Gbit/s do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną	

kartę sieciową współdzieloną z systemem operacyjnym serwera;	
Inne: 1) elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne, 3) ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji, 4) możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta komputera;	
Serwis: dostępność części zamiennych przez co najmniej 5 lat od momentu zakupu serwera (oświadczenie producenta);	
Szafa Blade – 1 szt.	
Wymagania Zamawiającego	*Oferta Wykonawcy (Tak/Nie, deklaracja)*
Typ szafy: 1) do montażu w szafie 19" rack, 2) wysokość nie więcej niż 6U wraz z wymaganymi modułami chłodzenia, zasilania itp., 3) maksymalna waga szafy w maksymalnej konfiguracji nie więcej niż 120KG, 4) wyposażona w 2 złącza USB 2.0, 1x LAN, 1x serial dostępne od frontu (możliwość konfiguracji i obsługi serwerów oraz zarządzania szafą poprzez złącza dostępne z przodu szafy);	
Możliwości rozbudowy: 1) możliwość instalacji co najmniej 8 niezależnych serwerów kasetowych wyposażonych w 2 procesory 12 rdzeniowe oraz nie mniej niż 1024GB pamięci operacyjnej RAM na każdy serwer, 2) możliwość instalacji kaset typu storage wyposażonych w minimum 4 dyski SAS 2.0 każdy, współdzielenie zasobów każdej kasety dyskowej co najmniej dla 2 serwerów w obrębie tej samej obudowy blade,	

3) możliwość instalacji kaset typu storage wyposażonych w napęd w standardzie LTO-4 lub nowszym, SAS;	
Architektura I/O: 1) pełne wsparcie producenta szafy dla instalacji switchy i kart 10Gbit LAN oraz Infiniband, 2) wymagane minimum 4 wnęki do instalacji modułów komunikacyjnych typu przełącznik LAN 1Gbit/s, LAN 10Gbit/s, FC 8Gbit, FC pass-thru, QDR InfiniBand 40Gbit;	
Sposób wyprowadzeń sygnałów LAN, FC, IB: 2 switche 10Gbit, każdy umożliwiający wyprowadzenie dwóch portów 10GbE z każdego serwera możliwego do zamontowania w szafie;	
Zarządzanie, dostęp: Wymaga się, aby dostarczone rozwiązanie było wyposażone w dwie, redundantne karty zarządzające (tzw. Management blade) umożliwiające/ wyposażone w: 1) pełna administracja szafy za pośrednictwem interfejsu Web, 2) dedykowany port serwisowy LAN RJ-45 dla każdej karty zarządzającej, 3) funkcję cyfrowego KVM realizowaną dla każdego z serwerów, 4) dwa porty zarządzające o predkości 1Gbit/s, 5) wsparcie dla LDAP i ADS, Szafa wraz z kartami zarządzającymi musi umożliwiać: 1) weryfikację zużycia energii całej szafy, konfiguracji polityk ograniczających zużycie energii w czasie oraz na bazie raportów utylizacji i zużycia energii przez pojedyncze serwery Blade jak i całą szafę, podgląd graficzny danych historycznych, 2) bez konieczności rozbudowy o dodatkowe elementy sprzętowe, wirtualizację zasobów I/O dla całej szafy Blade (co najmniej wirtualizacja adresacji WWN dla FC, MAC i IP dla Ethernet dla wszystkich serwerów zainstalowanych w szafie), 3) dostarczona infrastruktura serwerowa powinna pracować bez przerw czy obniżenia wydajności serwerów nawet w przypadku uszkodzenia obydwóch modułów zarządzających, 4) zdalne mapowanie napędów optycznych CD/DVD oraz FDD lub obrazów (ISO/IMG) tychże nośników niezależnie dla każdego z zainstalowanych w szafie serwerów na poziomie sprzętowym (dostęp do urządzenia zdalnego z poziomu BIOS), 5) realizacja funkcji cyfrowego KVM poprzez niezależne przekierowanie konsoli graficznej każdego z zainstalowanych w szafie serwerów na	

poziomie sprzętowym wraz z emulacją myszy i klawiatury (niezależnie od typu zainstalowanego OS), połączenie szyfrowane SSL/SSH, 6) zdalna identyfikacja fizycznego serwera i szafy za pomocą sygnalizatora optycznego, 7) zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera, 8) dostęp do interfejsu zarządzania – zdalny z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu, 9) automatyczne wykrywanie i identyfikacja urządzeń zainstalowanych w ramach infrastruktury (serwery, obudowy Blade, karty zarządzające) i prezentacja infrastruktury w postaci graficznej, 10) monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć, dyski twarde, interfejsy sieciowe; Ponadto szafa musi być wyposażona w wyświetlacz dostępny z przodu szafy, zapewniający podstawową konfigurację szafy, monitorowanie podstawowych funkcji oraz sygnalizowanie i wyświetlanie alarmów; wyświetlacz musi posiadać możliwość schowania/zamknięcia lub innego skutecznego zabezpieczenia przed przypadkowym uszkodzeniem;	
<u>Zasilanie:</u> Redundantne zasilacze wymienne w trakcie pracy, pozwalające na zasilenie w pełni obsadzonej szafy: 1) redundancja co najmniej typu N+N – wymaga się, aby utrata połowy zasilaczy nie powodowała zatrzymania lub zmniejszenia wydajności serwerów zainstalowanych w szafie, 2) szafa powinna umożliwiać optymalizowanie obciążenia zainstalowanych zasilaczy celem osiągnięcia maksymalnej sprawności pracy zasilaczy i minimalizacji zużycia energii, 3) sprawność maksymalna pojedynczego zasilacza nie mniej niż 92% (potwierdzone w dokumentacji technicznej producenta serwera dostępnej publicznie), 4) stan i parametry pracy muszą być monitorowane zdalnie (przez kartę zarządzającą) Każdy z zasilaczy musi realizować funkcję auto-restart, 5) system zasilania musi pracować w sieci o napięciu 230V/50Hz;	
<u>Chłodzenie:</u> 1) szafa wyposażona w redundantne chłodzenie (wentylatory) umożliwiające poprawną pracę w pełni wyposażonej szafy,	

2) szafa musi umożliwiać wymianę modułów wentylatorów w trakcie pracy;	
2. Przełącznik HP kompatybilny z posiadanym przez zamawiającego modelem HP 4208vl celem utworzenia stosu – 1 szt.	Producent sprzętu, ewentualnie model, nr katalogowy *(proszę podać):* ....
Wymagania Zamawiającego	*Oferta Wykonawcy (Tak/Nie, deklaracj*
1) budowa modularna pozwalającej na instalację min. 192 porty gigabitowe,	
2) moduły wymieniane na gorąco,	
3) przełącznik obsadzony portami: – minimum 20 portów 10/100/1000BaseT oraz minimum 4 porty 1000BASE-SX wraz z modułami 850nm MM,	
4) modularny zasilacz, możliwość zainstalowania drugiego redundantnego modularnego zasilacza,	
5) przepustowość: 48 Mb/s,	
6) wydajność przełączania co najmniej 76,8 Gb/s,	
7) minimum 2 wersje oprogramowania,	
8) obsługa routingu statycznego (minimum 16 tras),	
9) obsługa sieci VLAN IEEE 802.1Q i IEEE 802.1v. obsługa 4094 tagów VLAN oraz minimum 256 jednoczesnych sieci VLAN,	
10) wsparcie dla standardów: IEEE 802.1s Multiple Spanning Tree, IEEE 802.3ad Link Aggregation Protocol (LACP), IEEE 802.1AB Link Layer Discovery Protocol (LLDP), LLDP-MED (Media Endpoint Discovery),	
11) ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection),	
12) wsparcie dla RMON, XRMON i sFlow,	
13) możliwość łączenia przełączników we wspólnie zarządzane klastry (minimum 16 przełączników w klastrze),	
14) obsługa Dynamic ARP protection,	
15) ograniczanie dostępu do określonego portu na podstawie adresu MAC,	
16) ograniczenie dostępu do sieci określonym adresom MAC (MAC address lockout),	
17) mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych,	
18) autentykacja użytkowników w oparciu o: 802.1x, stronę www oraz adres MAC – możliwość autentykacji wielu użytkowników na pojedynczym porcie,	

19) możliwość przechowywania wielu plików konfiguracyjnych,	
20) obudowa maksymalnie 5U umożliwiająca instalację w szafie 19";	
3. Rozbudowa posiadanej przez zamawiającego macierzy Fujitsu Eternus DX90 S2	
Wymagania Zamawiającego	*Oferta Wykonawcy (Tak/Nie, deklaracja)*
Zamawiający wymaga dostarczenia dodatkowego (redundantnego) kontrolera dla posiadanej macierzy Fujitsu Eternus DX90 S2: – kontroler musi być wyposażony w 4 interfejsy iSCSI 10 GbE, każdy interfejs wyposażony w moduł SFP+ LC MMF;	
4. Urządzenie firewall/VPN/UTM do średniego oddziału	Producent sprzętu, ewentualnie model, nr katalogowy *(proszę podać):* ....
Wymagania Zamawiającego	*Oferta Wykonawcy (Tak/Nie, deklaracja)*
1) Firewall musi być dostarczony jako dedykowane urządzenie sieciowe o wysokości 1 U;	
2) Urządzenie musi być wyposażone w co najmniej 2 GB pamięci RAM, pamięć Flash 2 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym;	
3) System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. System operacyjny firewalla musi śledzić stan sesji użytkowników (*stateful processing*), tworzyć i zarządzać tablicą stanu sesji;	
4) Urządzenie musi być wyposażone w nie mniej niż 16 wbudowanych interfejsów Ethernet 10/100/1000 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji);	
5) Urządzenie musi być wyposażone w minimum 4 sloty na dodatkowe karty z modułami interfejsów. Urządzenie musi obsługiwać co najmniej następujące rodzaje kart z modułami interfejsów: ADSL 2/2+, Serial, E1, Gigabit	

Ethernet (SFP);	
6) Urządzenie musi posiadać co najmniej dwa porty wyposażone w moduły SFP w standardzie 1000BASE-LX;	
7) Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 64 strefami bezpieczeństwa z wydajnością nie mniejszą niż 600 Mb/s liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż 200 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 128 000 równoległych sesji oraz zestawić nie mniej niż 8000 nowych połączeń/sekundę;	
8 Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 1 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 300 Mb/s. Urządzenie musi udostępniać użytkownikom wbudowanego klienta IPSec VPN za pośrednictwem strony www i umożliwiać podłączenie nim poprzez VPN dla minimum 25 jednoczesnych użytkowników;	
9) Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 4000 reguł polityki bezpieczeństwa;	
10) Firewall musi mieć możliwość identyfikacji aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z aplikacjami typu Peer-to-Peer i Instant Messaging). Identyfikacja aplikacji musi odbywać się co najmniej przez sygnatury i analizę heurystyczną. Firewall musi identyfikować nie mniej niż 900 różnych aplikacji, w szczególności takich, które są tunelowane w protokołach HTTP i HTTPS – nie mniej niż Skype, Gadu-Gadu, Facebook, Youtube. Dostęp użytkowników do poszczególnych aplikacji musi być konfigurowany przy pomocy reguł filtrowania uwzględniających co najmniej adresy IP oraz wyżej wymienione aplikacje. Kontrola dostępu do dynamicznie identyfikowanych aplikacji musi być wykonywana z przepustowością nie mniej niż 750 Mb/s dla ruchu HTTP. Jeśli do wykorzystania lub aktualizacji bazy funkcji identyfikacji aplikacji wymagane jest posiadanie licencji/subskrypcji – wymaga się dostarczenia niniejszej licencji/subskrypcji na okres co najmniej 3 lat,	
11) Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antywirusowej	

sprawdzający komunikację związaną z pocztą elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać instalowania dodatkowego serwera przez użytkownika. Kontrola antywirusowa musi być wspomagana sprzętowo i realizowana z wydajnością nie mniejszą niż 80 Mb/s dla ruchu HTTP. W celu optymalizacji działania baza definicji wirusów i złośliwego oprogramowania nie może być ściągana lokalnie na urządzenie – porównywanie charakterystyki badanego ruchu z wzorcami wirusów musi odbywać się w serwisie udostępnionym po stronie producenta („w chmurze"). Jeśli do wykorzystania lub aktualizacji bazy funkcji kontroli antywirusowej wymagane jest posiadanie licencji/subskrybcji – nie wymaga się dostarczenia niniejszej licencji/subskrybcji na obecnym etapie,	
12) Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera. Jeśli do wykorzystania lub aktualizacji bazy funkcji kontroli antyspamowej wymagane jest posiadanie licencji/subskrybcji – nie wymaga się dostarczenia niniejszej licencji/subskrybcji na obecnym etapie,	
13) Urządzenie zabezpieczeń musi posiadać wbudowany moduł filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie może wymagać dodatkowego serwera. Jeśli do wykorzystania lub aktualizacji bazy funkcji filtrowania stron WWW wymagane jest posiadanie licencji/subskrybcji – nie wymaga się dostarczenia niniejszej licencji/subskrybcji na obecnym etapie.	
14) Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies,	
15) Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 64 wirtualnych ruterów,	
16) Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN,	
17) Urządzenie musi obsługiwać co najmniej 2000 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie drugiej, firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet,	

18) Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach,	
19) Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych,	
20) Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta;	
21) Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji;	
22) Pomoc techniczna świadczona w języku polskim. Szkolenia z produktu dostępne na terenie RP , w języku polskim;	
23) Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przynajmniej przez okres 3 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych;	
Pozostałe wymagania zamawiającego	*Oferta Wykonawcy (Tak/Nie, deklaracja)*
1) serwery, obudowy, szafa, przełącznik oraz pozostałe elementy konfiguracji muszą być fabrycznie nowe i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce – wymagane oświadczenie producenta /autoryzowanego dystrybutora, że oferowany do przetargu sprzęt spełnia ten wymóg;	

2) elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane (wymagane oświadczenie producenta /autoryzowanego dystrybutora dołączone do oferty) oraz muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne;	
3) ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwerów, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;	
4) możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwerów;	
5) w momencie dostawy sprzętu wykonawca dostarczy oryginalne karty gwarancyjne, instrukcje obsługi w języku polskim /angielskim oraz dokumenty wystawione przez producenta lub autoryzowanego dystrybutora poświadczające datę produkcji sprzętu oraz zakup w autoryzowanym kanale;	
<u>Gwarancja i serwis:</u> 1) nie mniej niż 3 lata gwarancji producenta, w miejscu instalacji, naprawa na następny dzień roboczy od zgłoszenia awarii; 2) dostępność części zamiennych przez co najmniej 5 lat od momentu zakupu serwera (oświadczenie producenta);	
5. Projekt techniczny zakresu prac z wdrożeniem	
Wymagania Zamawiającego	*Oferta Wykonawcy (Tak/Nie, deklaracja)*
<u>Projektu techniczny musi obejmować swoim zakresem minimum:</u> 1) Schemat montażu urządzeń w szafach, 2) Schemat połączeń fizycznych sieci Ethernet, 3) Podział przestrzeni na macierzy dyskowej (na podstawie wymagań i konsultacji przeprowadzonych ze służbami informatycznymi zamawiającego), 4) Konfigurację środowiska sieciowego w ramach dostarczonych przełączników farmy serwerów jak i przełącznika rdzeniowego, 5) Zabezpieczenie środowiska na poziomie access-list,	

6) Propozycję testów akceptacyjnych;	
Wdrożenie obejmować będzie minimum: 1) wykonanie montaży dostarczonych urządzeń w szafie rack, 2) wykonanie połączenia infrastruktury obecnej i nowo wdrażanej, 3) konfigurację dostarczonego przełącznika Ethernet HP 4208vl oraz posiadanego przez zamawiającego HP 4208vl – stos, vlany, ACL, 4) konfigurację rozwiązania Blade – przełączniki Ethernet, moduły zarządzające, serwery, 5) konfigurację sieci SAN iSCSI, 6) konfigurację macierzy dyskowej, 7) testy poprawności działania środowiska;	
Dokumentacja powykonawcza dotycząca zrealizowanych przez wykonawcę działań winna obejmować: 1) opis wykonanych prac, 2) schematy połączeń fizycznych i logicznych, 3) konfigurację oprogramowania i urządzeń, Dokumentacja winna być przekazana zamawiającemu w formie elektronicznej.	
Serwis gwarancyjny przedmiotu zamówienia będzie realizowany przez *(proszę wpisać w kolumnie obok)*	*Nazwa firmy, adres, tel./fax oraz adres e-mail)*..... ....

Miejscowość i data: .....

_____
Imiona i nazwiska osób uprawnionych do reprezentowania wykonawcy

_____
Czytelne podpisy osób uprawnionych do reprezentowania wykonawcy

akceptacja