Załącznik nr 1

Specyfikacja techniczna – Zadanie nr 1

Wymagania ogólne dla urządzeń i oprogramowania

- całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski;
- całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana we wcześniejszych projektach;
- całość sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres 60 miesięcy (chyba, ze zapisy szczegółowe SIWZ stanowią inaczej);

Warunki gwarancji i wsparcia technicznego dla sprzętu i oprogramowania sieciowego:

Sprzęt

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. 5-letnia gwarancja (chyba, ze zapisy szczegółowe SIWZ stanowią inaczej); serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
- Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań
- W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Wnioskodawca dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 30 dni roboczych od momentu zgłoszenia usterki;
- Wnioskodawca otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;

Oprogramowanie

- oprogramowanie powinno posiadać min. 1-roczne wsparcie (chyba, ze zapisy szczegółowe stanowią inaczej) – dostarczanie aktualizacji, zdalne (telefon lub e-mail, www) wsparcie techniczne w zakresie rozwiązywania problemów z konfiguracją i użytkowaniem oprogramowania

Miejsce Instalacji

- Dostawa, montaż i instalacja w ramach niniejszego postępowania przetargowego odbędzie się w czasie i miejscu wskazanym przez Zamawiającego.

Montaż i uruchomienie

- Zamawiający wymaga aby wraz z dostawą sprzętu przeprowadzić jego instalację, konfigurację oraz uruchomienie. Wszelkiego typu elementy połączeniowe np.: kable, zakończenia itp. powinny zostać ujęte w wycenie.
- Przekazanie elementów systemu nastąpi w drodze protokołu przekazania do użytkowania, który będzie potwierdzał jego prawidłową instalację i działanie.

Jeżeli zapisy szczegółowe nie specyfikują inaczej Zamawiający oczekuje prac w zakresie:

- Wniesienia, ustawienia i fizycznego montażu wszystkich dostarczonych urządzeń w dostarczonej szafie rack w pomieszczeniu (miejscach) wskazanych przez zamawiającego z uwzględnieniem wszystkich lokalizacji.
- Urządzenia, które nie są montowane w szafach teleinformatycznych powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego.
- Usunięcia opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
- Podłączenia całości rozwiązania do infrastruktury Zamawiającego.
- Wykonania procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
- Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
- Wykonania połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
- Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające, kable elektryczne).

Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia, **w ramach jednego weekendu (Piątek godz. 16:00 - Sobota godz. 22:00)** po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym.

UWAGA. Powyższe zapisy gwarancyjne, oraz czas wykonania obowiązują jedynie w przypadku braku szczegółowych zapisów w poniższym opisie przedmiotu zamówienia.

W celu potwierdzenia ważności oferty i spełniania wymaganych warunków, Wykonawca załączy na etapie składania oferty następujące dokumenty i oświadczenia według poniższych zasad:

- Oświadczenie gwarancyjne producenta na oferowany sprzęt:
    - Serwer Wirtualizacyjny

Oznaczenia i definicje

1.1. Oznaczenia i skróty literowe

SRV-I - Serwer Wirtualizacjny
MD - Macierz dyskowa
ETH - połączenie ETHERNET o przepustowości co najmniej 1Gb/s
SAS - połączenie SAS o przepustowości co najmniej 6Gb/s

Standaryzacja PRZEPUSTOWOŚCI

W celu uniknięcia nieporozumień związanych z pojęciem przepustowości, które użyte jest w późniejszym tekście wymagań Zamawiający podaje wartości, które należy przyjąć przy obliczaniu przepustowości na potrzeby niniejszej specyfikacji.

Standard	Przepustowość [Gb/s]
DDR3-1066 ; -1333 ; -1600 DDR4 RDIMM – 800 ; - 2133	8,5 ; 10,6 ; 12,8 [GB/s] 16000 ; 32000 [Mb/s]
10 Gb Ethernet ; 1 Gb Ethernet	10 ; 1
16 Gb ; 8 Gb ; 4 Gb FC	16 ; 8 ; 4
QDR ; DDR ; SDR InfiniBand	10 ; 5 ; 2,5
EDR ; FDR Infiniband	26 ; 14
12G ; 6G ; 3G SAS	12 ; 6 ; 3
6G ; 3G ; 1,5 SATA	6 ; 3 ; 1,5

Tabela 1 Standaryzacja przepustowości

Jeśli port używa zwielokrotnionych linii jego przepustowość na potrzeby niniejszej specyfikacji należy przyjąć jako iloczyn liczby linii i wyżej podanej przepustowości (przykład: przepustowość 4X QDR INFINIBAND na potrzeby niniejszej specyfikacji wynosi 40 Gb/s).

Jeśli transmisja na linii zachodzi równocześnie w dwu kierunkach to dla potrzeb niniejszej specyfikacji należy przyjąć nie wartość dwukrotnie wyższą, ale dokładnie taką jaka znajduje się podanej tabeli.

W zapisach niniejszej specyfikacji wymagana przez Zamawiającego przepustowość, a opisana w niniejszym akapicie jest oznaczana dużą literą (PRZEPUSTOWOŚĆ) w odróżnieniu od innych przepustowości.

Równoważność kanałów komunikacyjnych

W miejscach gdzie Zamawiający wyspecyfikował rodzaj kanału komunikacyjnego jako równoważny kanał komunikacyjny Zamawiający dopuszcza kanał komunikacyjny o IDENTYCZNYM protokole, ale o większej prędkości. Zamawiający nie dopuszcza innego niż wyspecyfikowany protokołu pomimo, że zamienny protokół będzie posiadał większą PRZEPUSTOWOŚĆ.

Przykład:

a. Dla wymagania ETHERNET 10Gb jako równoważne NIE JEST akceptowane połączenie o większej PRZEPUSTOWOŚCI, ale jedynie o większej prędkości. W tym wypadku ETHERNET 100Gb.
b. Analogicznie dla wymagania FC 8Gb jako równoważne AKCEPTOWANE jest jedynie połączenie FC, ale o większej prędkości. W tym wypadku FC 16Gb lub więcej.

1.2. Definicja MOC OBLICZENIOWA

Wzór 1. Maksymalna (szczytowa) teoretyczna moc obliczeniowa procesora

Rproc = C * I * F,

gdzie:

- Rproc - moc obliczeniowa w GFlops
- C - liczba rdzeni procesora
- I - liczba instrukcji zmiennoprzecinkowych typu dodawanie i mnożenie w podwójnej precyzji wykonywanych przez pojedynczy rdzeń procesora w czasie jednego cyklu zegarowego (np. dla procesora Intel Xeon (seria 5600) I wynosi 4, dla procesorów AMD Opteron I wynosi 4),
- F - częstotliwość zegara procesora w GHz.

Dla potrzeb niniejszej specyfikacji Zamawiający jako częstotliwość zegara przyjmuje nominalną częstotliwość zegara procesora podawaną przez producenta procesora przy handlowym opisie procesora. Pomimo, że procesor może pracować z częstotliwością niższą lub wyższą niż wyżej wspomniana częstotliwość jako częstotliwość do obliczenia mocy obliczeniowej procesora w niniejszej specyfikacji należy przyjąć właśnie częstotliwość podawaną przy opisach handlowych przez producentów procesorów.

W zapisach niniejszej specyfikacji wymagana przez Zamawiającego moc obliczeniowa zdefiniowana we wzorze 1 i opisana w niniejszym akapicie jest oznaczana dużą literą (MOC OBLICZENIOWA) w odróżnieniu od innych mocy obliczeniowych.

1.3. Definicja Macierz Dyskowa

Dla potrzeb niniejszej specyfikacji jako Macierz Dyskowa Zamawiający dopuszcza każde urządzenie które dodatkowo równocześnie spełnia następujące właściwości:

a) dyski znajdują się wewnątrz urządzenia
b) dyski połączone są znajdującą się wewnątrz urządzenia magistralą połączeń do wspólnych portów wejścia / wyjścia urządzenia
c) wymagana magistrala połączeń nie jest w postaci kabli dostępnych z zewnątrz
d) na zewnątrz urządzenia dostępne jedynie są porty wejścia / wyjścia, do których dołącza się kable sygnałowe do transmisji pomiędzy dyskami, a pozostałą częścią infrastruktury,

W zapisach niniejszej specyfikacji tak określone urządzenie jest „Macierz Dyskowa” i oznaczana jest dużą literą w odróżnieniu od innych urządzeń.

1.4. Konwencja zapisów

a) Zapis „SAS / FC” lub „USB / SD” użyty w dalszej części specyfikacji oznacza jedną z dwóch technologii: albo SAS albo FC, albo USB albo SD.

b) Nazwy pisane z dużej litery są stosowanymi na potrzeby niniejszej specyfikacji nazwami własnymi np. Serwer BLADE, Lokalne Dyski.

c) Słowa „LUB” lub „ALBO” napisane z dużej litery oznaczają kwalifikator logiczny i nie są używane w potocznym znaczeniu.
Przykład:
   i. Jeśli Zamawiający wymaga odporności Systemu na awarię elementu A ALBO elementu B oznacza to, że System nie musi być odporny na RÓWNOCZESNĄ awarię elementu A i elementu B.
   ii. Jeśli Zamawiający wymaga odporności systemu na awarię elementu A LUB elementu B oznacza to, że system nie tylko ma być odporny na awarię jednego z dwu elementów A albo B, ale też musi być odporny na równoczesną awarię obu elementów i A i B.

2. Wymagania ogólne

2.1. Jakość sprzętu

a) Cały dostarczony sprzęt musi być fabrycznie nowy, tzn. nieużywany przed dniem dostarczenia, z wyłączeniem używania niezbędnego dla przeprowadzenia testów jego poprawnej pracy.
b) Dostarczone elementy oraz dostarczone wraz z nimi oprogramowanie muszą pochodzić z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych.

3. Wymagania szczegółowe

3.1. Serwer pod wirtualizację – 1 szt.

Zamawiający wymaga jednego serwera wirtualizacyjnego o wysokości maksymalnie 1U, spełniającego ŁĄCZNIE poniższe warunki:

Komponent	Minimalne wymagania
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" HotPlug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Posiadająca dodatkowy przedni panel zamykany na klucz, chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów cztero, sześcio, ośmio, dziesięcio dwunasto lub czternastordzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona

	jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Dwa procesory dwunastordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku a) Procesory dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku minimum 950 punktów w teście SPECint_rate_base2006 dostępnym na stronie internetowej www.spec.org dla konfiguracji dwuprocesorowej; do oferty należy załączyć wydruk z wynikiem testu dla oferowanego modelu serwera b) MOC OBLICZENIOWA serwera co najmniej 840,0 GFlops, gdzie MOC OBLICZENIOWA definiowana jest wzorem: Rproc = C * I * F, gdzie: • Rproc - moc obliczeniowa w GFlops • C - liczba rdzeni procesora • I - liczba instrukcji zmiennoprzecinkowych typu dodawanie i mnożenie w podwójnej precyzji wykonywanych przez pojedynczy rdzeń procesora w czasie jednego cyklu zegarowego (np. dla procesora Intel Xeon (seria 5600) wynosi 4, dla procesorów AMD Opteron wynosi 4), • F - częstotliwość zegara procesora w GHz. Dla potrzeb niniejszej specyfikacji Zamawiający jako częstotliwość zegara przyjmuje nominalną częstotliwość zegara procesora podawaną przez producenta procesora przy handlowym opisie procesora. Pomimo, że procesor może pracować z częstotliwością niższą lub wyższą niż wyżej wspomniana częstotliwość jako częstotliwość do obliczenia mocy obliczeniowej procesora w niniejszej specyfikacji należy przyjąć właśnie częstotliwość podawaną przy opisach handlowych przez producentów procesorów. Do oferty należy załączyć wynik testu dla oferowanego modelu serwera wraz z oferowanym modelem procesora lub samego procesora.

Pamięć RAM	128 lub 256 GB pamięci RAM typu RDIMM o częstotliwości pracy 2400MHz. Płyta powinna obsługiwać do min. 384GB pamięci RAM, na płycie głównej powinno znajdować się minimum 12 slotów przeznaczonych dla pamięci Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, Lockstep
Sloty PCI Express	Min. dwa sloty x16 generacji 3 min. 1 slot x8 generacji 3, Min. 1 x1 generacji 2, Min. 1 x8 generacji 2
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	min. 3 porty USB 2.0 oraz 2 porty USB 3.0 , 4 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232.
Interfejsy sieciowe/FC	Wbudowana czteroportowa karta Gigabit Ethernet. Dwuportowy kontroler do sieci SAN
Kontroler dysków	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID : 0, 1, 5, 6, 10, 50, Pamięć cache min. 1GB
Wewnętrzna pamięć masowa	Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS i SSD. Zainstalowane 6 dysków twardych 4TB 7,2 RPM Zainstalowane 2 dyski SAS – 600 GB Zainstalowany wewnętrzny modułu dedykowany dla hypervisora wirtualizacyjnego, wyposażony w 2 jednakowe nośniki typu flash z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Napęd optyczny	Wbudowany napęd DVD-RW
System diagnostyczny	Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
System Operacyjny	Z zainstalowanym systemem operacyjnym. Licencje na serwerowy system operacyjny muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów

	wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

	13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18. Mechanizmy logowania w oparciu o: a. Login i hasło, b. Karty z certyfikatami (smartcard), c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.. 20. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b. Usługi katalogowe oparte o LDAP i pozwalające

	na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych. c. Zdalna dystrybucja oprogramowania na stacje robocze. d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f. Szyfrowanie plików i folderów. g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i. Serwis udostępniania stron WWW. j. Wsparcie dla protokołu IP w wersji 6 (IPv6), k. Wsparcie dla algorytmów Suite B (RFC 4869), l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m. Wbudowane mechanizmy wirtualizacji

	(Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii. Obsługi 4-KB sektorów dysków iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) 26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. 31. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
Zasilacze	Dwa redundantne zasilacze o mocy maks. 750W każdy o sprawności Titanium.
Wentylatory	Minimum 5 redundantne wentylatory.

Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM 2.0. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Karta zarządzająca	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,) - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów - wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla IPv6 - wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer - integracja z Active Directory - możliwość obsługi przez dwóch administratorów jednocześnie - wsparcie dla dynamic DNS - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej - możliwość podłączenia lokalnego poprzez złącze RS-232 - możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta - Wsparcie dla protokołów– WMI, SNMP, IPMI, WSMan, Linux SSH - Możliwość oskryptowywania procesu wykrywania urządzeń - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram - Szczegółowy opis wykrytych systemów oraz ich komponentów - Możliwość eksportu raportu do CSV, HTML, XLS - Grupowanie urządzeń w oparciu o kryteria użytkownika - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - Automatyczne skrypty CLI umożliwiające dodawanie i

	edycję grup urządzeń - Szybki podgląd stanu środowiska - Podsumowanie stanu dla każdego urządzenia - Szczegółowy status urządzenia/elementu/komponentu - Generowanie alertów przy zmianie stanu urządzenia - Filtry raportów umożliwiające podgląd najważniejszych zdarzeń - Integracja z service desk producenta dostarczonej platformy sprzętowej - Możliwość przejęcia zdalnego pulpitu - Możliwość podmontowania wirtualnego napędu - Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu - Kreator umożliwiający dostosowanie akcji dla wybranych alertów - Możliwość importu plików MIB - Przesyłanie alertów „as-is" do innych konsol firm trzecich - Możliwość definiowania ról administratorów - Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) - Możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów - Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych - możliwość automatycznego przywracania ustawień serwera,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) zapisanych na dedykowanej pamięci flash wbudowanej na karcie zarządzającej
Gwarancja	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia ,możliwość zgłaszania awarii w trybie 24x7x365. W przypadku awarii dyski twarde pozostają własnością zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę

	producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
	Firma serwisująca musi posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty. Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem – dokumenty potwierdzające załączyć do oferty.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE.

3.2. Oprogramowanie Wirtualizacyjne – 1 szt.

Wymagania minimalne
Licencje muszą umożliwiać uruchamianie wirtualizacji na serwerach fizycznych o łącznej liczbie 6 fizycznych procesorów oraz jednej konsoli do zarządzania całym środowiskiem.
Wszystkie licencje powinny być dostarczone wraz z 1 rocznym wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów przez 12h na dobę / 5 dni w tygodniu.

3.2.1. Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym i nie może być częścią innego systemu operacyjnego.
3.2.2. Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego.
3.2.3. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest możliwość przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna.
3.2.4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do 1TB pamięci operacyjnej.
3.2.5. Oprogramowanie do wirtualizacji musi zapewnić możliwość przydzielenia maszynom wirtualnym do 64 procesorów wirtualnych.
3.2.6. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
3.2.7. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
3.2.8. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, SLES 11, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 4, RHEL3, RHEL 2.1, Solaris wersja 10 dla platformy x86, NetWare 6.5, NetWare 6.0, NetWare

6.1, Debian, CentOS, FreeBSD, Asianux, Ubuntu 7.04, SCO OpenServer, SCO Unixware, Mac OS X.

3.2.9. Rozwiązanie musi zapewniać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania trybu XP mode w Windows 7 a także instalacji wszystkich funkcjonalności w tym Hyper-V pakietu Windows Server 2012 na maszynie wirtualnej.

3.2.10. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek, minimum IE i Firefox.

3.2.11. Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root.

3.2.12. Rozwiązanie musi umożliwiać składowanie logów ze wszystkich serwerów fizycznych i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania.

3.2.13. Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.

3.2.14. Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.

3.2.15. Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.

3.2.16. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.

3.2.17. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP.

3.2.18. Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.

3.2.19. Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 64TB.

3.2.20. Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej.

3.2.21. Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.

3.2.22. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.

3.2.23. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.

3.2.24. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.

3.2.25. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej.

3.2.26. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.

3.3. Macierz Dyskowa – 1 szt.

Parametry podstawowe – wymagania minimalne	
Interfejs napędów pamięci masowej	Serial ATA,Serial ATA II,Serial ATA III
Rozmiary napędów pamięci masowej	2.5/3.5 "
usługa RAID	Tak
Poziomy raid	0,1,5,6,10,JBOD
Zatoka hot-swap	Tak
Obsługiwane systemy plików	ext3,ext4,FAT32,HFS+,NTFS
Zainstalowane urządzenie pamięci masowej	TAK – 6 x 6 TB (dedykowane do pracy w oferowanej macierzy)
Obsługiwane rodzaje dysków	HDD,SSD
Ilość obsługiwanych rozmiarów dysków pamięci	Min. 8
Obudowa	Do instalacji w standardowej szafie RACK 19”. Wysokość maksymalnie 2U wraz z kompletem szyn do montażu w szafie Rack z możliwością instalacji minimum 8 dysków
Procesor	
Taktowanie procesora	3.2 GHz
Liczba rdzeni procesora	Min. 2
L3 cache	Min 3 MB
Pamięć	
Maksymalna pamięć operacyjna RAM	32 GB
Gniazda pamięci	4
Wewnętrzna pamięć RAM	4 GB
Wielkość pamięci	512 MB

flash	
Sieć komputerowa	
Przewodowa sieć lan	Tak
Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
Wi-Fi	Nie
Klient DHCP	Tak
Serwer DHCP	Tak
Zgodny z Jumbo Frames	Tak
obsługa iSCSI	Tak
Gotowy Wake-On-LAN	Tak
Obsługiwane protokoły sieciowe	CIFS/SMB, SMB2.1, SMB3.0, AFP (v3.3), NFS(v3), FTP, FTPS, SFTP, TFTP, HTTP(S), Telnet, SSH, iSCSI, SNMP, SMTP, SMSC
Łączność/porty	
Liczba portów USB 2.0	4
Ilość portów USB 3.0 (3.1 Gen 1) Typu-A	4
Ilość portów HDMI	1
Ilość portów Ethernet LAN (RJ-45)	4
Rama montażowa	
• sumaryczna wysokość urządzeń: 42U • wymiary: 1888x600x600 mm • stabilna konstrukcja • zestaw jezdny w komplecie	

3.4. OPROGRAMOWANIE DO BACKUPU ŚRODOWISKA WIRTUALIZACYJNEGO - 1 Szt.

WYMAGANIA MINIMALNE

Zamawiający wymaga dostarczenia wymaganej liczby licencji oprogramowania w celu zapewnienia poprawnej pracy w dostarczonym środowisku wirtualizacyjnym.

3.4.1. Oprogramowanie do archiwizacji powinno współpracować z infrastrukturą wirtualizacji opartą na VMware ESX oraz ESXi w wersjach 3.5, 4.0, 4.1, 5, 5.5

oraz 6, jak również Hyper-V 2008 R2 i Hyper-V 2012 (w tym obsługa formatu dysków wirtualnych *.vhdx)

3.4.2. Rozwiązanie powinno współpracować z hostami ESX i ESXi zarządzanymi przez VMware

3.4.3. Rozwiązanie powinno współpracować z hostami Hyper-V zarządzanymi przez System Center Virtual Machine Manager, zgrupowanymi w klastry jak i nie zarządzanymi (standalone)

3.4.4. Rozwiązanie nie może instalować żadnych swoich komponentów (agent) w archiwizowanych maszynach wirtualnych.

3.4.5. Rozwiązanie musi wspierać backup wszystkich systemów operacyjnych w wirtualnych maszynach, które są wspierane przez VMware i Hyper-V

3.4.6. Rozwiązanie powinno mieć możliwość instalacji na następujących systemach operacyjnych zarówno w wersji 32 jak i 64 bitowej:

3.4.6.1. Microsoft Windows XP SP3

3.4.6.2. Microsoft Windows Server 2003 SP2

3.4.6.3. Microsoft Windows Vista SP2

3.4.6.4. Microsoft Windows Server 2008 SP2

3.4.6.5. Microsoft Windows Server 2008 R2

3.4.6.6. Microsoft Windows 7 SP1

3.4.6.7. Windows Server 2012

3.4.6.8. Windows 8

3.4.7. Rozwiązanie powinno dawać możliwość odzyskiwania całych obrazów maszyn wirtualnych z obrazów, pojedynczych plików z systemu plików znajdujących się wewnątrz wirtualnej maszyny. Rozwiązanie musi umożliwiać odzyskiwanie plików z następujących systemów plików:

3.4.7.1. Linux

3.4.7.1.1. ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS

3.4.7.2. Unix

3.4.7.2.1. JFS, XFS, UFS

3.4.7.3. BSD

3.4.7.3.1. UFS, UFS2

3.4.7.4. Solaris

3.4.7.4.1. UFS, ZFS

3.4.7.5. Mac

3.4.7.5.1. HFS, HFS+

3.4.7.6. Windows

3.4.7.6.1. NTFS, FAT, FAT32

3.4.8. Rozwiązanie powinno umożliwiać natychmiastowe odzyskanie wirtualnej maszyny i jej uruchomienie bez kopiowania na storage podłączony do hostów ESX (wbudowana funkcjonalność NFS Server) i Hyper-V

3.4.9. Rozwiązanie musi zapewniać szybkie odzyskiwanie danych ze skrzynek pocztowych Microsoft Exchange 2010/2013 bez potrzeby uruchamiania maszyny wirtualnej (odzyskiwanie bezpośrednio z bazy danych *.EDB)

3.4.10. Rozwiązanie powinno umożliwiać indeksowanie plików zawartych w archiwach maszyn wirtualnych z systemem operacyjnym Windows w celu szybkiego ich przeszukiwania

3.4.11. Rozwiązanie powinno w pełni korzystać z mechanizmów zawartych w VMware vStorage API for Data Protection a w szczególności być zgodnym z mechanizmem Changed Block Tracking

3.4.12. Rozwiązanie powinno mieć wbudowane mechanizmy podobne do technologii CBT również dla platformy Hyper-V w celu przyśpieszenia procesu backupu.
3.4.13. Rozwiązanie powinno korzystać z mechanizmów VSS (Windows Volume Shadowcopy) wbudowanych w najnowsze systemy operacyjne z rodziny Windows.
3.4.14. Rozwiązanie powinno mieć wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji zajmowanej przez archiwa przestrzeni dyskowej
3.4.15. Rozwiązanie powinno mieć możliwość instalacji centralnej konsoli do zarządzania większą ilością serwerów archiwizujących oraz jednoczesnego zarządzania backupami środowiska VMware i Hyper-V
3.4.16. Dostęp do tej konsoli powinien być realizowany przez przeglądarkę WWW
3.4.17. Rozwiązanie powinno mieć wbudowany mechanizm informowania o pomyślnym lub niepomyślnym zakończeniu procesu archiwizacji poprzez email, zapis do Event Log'u Windows lub wysłanie komunikatu SNMP.
3.4.18. Rozwiązanie powinno mieć możliwość rozbudowy procesu archiwizacji o dowolne skrypty tworzone przez administratora i dołączane do zadań archiwizacyjnych
3.4.19. Rozwiązanie powinno mieć wbudowaną możliwość replikacji wirtualnych maszyn pomiędzy hostami ESX i ESXi oraz w tym możliwość replikacji ciągłej
3.4.20. Rozwiązanie powinno mieć wbudowaną możliwość replikacji maszyn wirtualnych pomiędzy hostami Hyper-V
3.4.21. Rozwiązanie powinno być zgodne z konfiguracją rozproszonego przełącznika VMware (Distributed Virtual Switch)
3.4.22. Rozwiązanie powinno mieć możliwość automatycznej zmiany numeracji IP maszyn przywracanych w środowiskach centrum zapasowego w przypadku awarii centrum podstawowego
3.4.23. Rozwiązanie powinno mieć możliwość integracji z macierzami HP Lefthand i oprogramowanie HP StoreVirtual. Rozwiązanie musi umożliwiać odzyskiwanie wirtualnych maszyn, plików z tych maszyn i uruchamianie maszyn bezpośrednio z migawki wykonanej przez rozwiązanie HP (tzw. SAN Snapshot)
3.4.24. Rozwiązanie musi umożliwiać zapisanie konfiguracji całej instalacji w celu przywrócenia jej po reinstalacji całego systemu.

3.5. Firewall/UTM – szt. 1

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Dla elementów systemu bezpieczeństwa obsługujących Zamawiającego, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych

systemów zabezpieczeń oraz łączy sieciowych.

3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. System realizujący funkcję Firewall powinien dysponować minimum 16 portami Ethernet 10/100/1000 Base-TX
6. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
7. W zakresie Firewall'a obsługa nie mniej niż 2,5 mln jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę
8. Przepustowość Firewall'a: nie mniej niż 2,5 Gbps
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 400 Mbps
10. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 30 GB. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.
12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN
    - Ochrona przed atakami - Intrusion Prevention System
    - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
    - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
    - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
    - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
    - Możliwość analizy ruchu szyfrowanego protokołem SSL
    - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
    - Możliwość dwu-składnikowego uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side

jak i server side w ramach modułu IPS) - minimum 900 Mbps

14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 200 Mbps
15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    - Praca w topologii Hub and Spoke oraz Mesh
    - Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
19. Translacja adresów NAT adresu źródłowego i docelowego.
20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
22. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
23. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
25. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW.
26. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
27. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:
    - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu

- haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
- haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
- Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    - ICSA lub EAL4 dla funkcji Firewall
    - ICSA lub NSS Labs dla funkcji IPS
    - ICSA dla funkcji: SSL VPN, IPSec VPN
29. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
30. Serwisy i licencje
    - W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń.
31. Gwarancja oraz wsparcie

1) Gwarancja: System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej.

2) Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego.
Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 / 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5 /24x7.

Oferent winien przedłożyć dokumenty:
- oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej
- oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)

3) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4) Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

3.6. Przełącznik typ I 48 port – szt. 5

Zarządzania	
Zarządzanie przez stronę www	Tak
Łączność	
Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48
Ilość portów SFP	4
Ilość slotów Modułu SFP	4
Sieć komputerowa	
Standardy komunikacyjne	IEEE 802.1D,IEEE 802.1p,IEEE 802.1Q,IEEE 802.1s,IEEE 802.1w,IEEE 802.3,IEEE 802.3ab,IEEE 802.3af,IEEE 802.3at,IEEE 802.3az,IEEE 802.3u,IEEE 802.3x
Pełny dupleks	Tak
Podpora kontroli przepływu	Tak
Agregator połączenia	Tak
Automatyczne MDI/MDI-X	Tak
Protokół drzewa rozpinającego	Tak
Przekazanie (audycja) Danych	

Szybkość transmisji danych	10/100/1000 Mbps
Przepustowość rutowania/przełączania	100 Gbit/s
Przepustowość	77 000 000 Mpps
Maksymalna szybkość przesyłania danych	1 Gbit/s
światłowód	
Złącze światłowodowe	SFP
Protokoły	
Protokoły zarządzające	LLDP, SNMP, LLDP-MED, SNMPv1/v2c/v3
Design	
Możliwości montowania w stelażu	Tak, wraz z przełącznikiem należy dostarczyć szyny do montażu w szafie rack.
Rozmiar układu	19” , wielkość 1 U
Diody LED	Tak
Zasilanie przez Ethernet	
Obsługa PoE	TAK (jeden z oferowanych przełączników powinien zapewniać funkcjonalność PoE) - 802.3af,IEEE 802.3at

3.7. Przełącznik typ II 24 port – szt. 2

Cechy zarządzania	
Typ przełącznika	Managed
Zarządzanie przez stronę www	Tak
Łączność	
Podstawowe przełączanie RJ-45 Liczba portów Ethernet	24
Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)
Ilość portów SFP	4
Ilość slotów Modułu SFP	4
Sieć komputerowa	
Standardy komunikacyjne	IEEE 802.1D,IEEE 802.1p,IEEE 802.1Q,IEEE 802.1s,IEEE 802.1w,IEEE 802.3,IEEE 802.3ab,IEEE 802.3af,IEEE 802.3at,IEEE 802.3az,IEEE 802.3u,IEEE 802.3x
Pełny dupleks	Tak
Podpora kontroli przepływu	Tak
Agregator połączenia	Tak
Automatyczne MDI/MDI-X	Tak
Protokół drzewa rozpinającego	Tak
Przekazanie (audycja) Danych	
Szybkość transmisji danych	10/100/1000 Mbps
Przepustowość rutowania/przełączania	56 Gbit/s
Przepustowość	41 600 000 Mpps

Maksymalna szybkość przesyłania danych	1 Gbit/s
światłowód	
Złącze światłowodowe	SFP
Protokoły	
Protokoły zarządzające	LLDP, SNMP, LLDP-MED, SNMPv1/v2c/v3
Design	
Możliwości montowania w stelażu	Tak, wraz z przełącznikiem należy dostarczyć szyny do montażu w szafie rack.
Rozmiar układu	19" , wielkość 1 U

3.8. Zasilacz awaryjny 6 kV - modularny – szt. 1

Lp.	Opis wymagań techniczno-funkcjonalnych	Konfiguracja minimalna Zamawiającego
1	Technologia	VFI (true on-line, podwójne przetwarzanie energii)
2	Moc znamionowa	6 kVA / 5,4 kW
3	Wyjściowy współczynnik mocy (PF)	0,9
4	Napięcie wejściowe	230 Vac
5	Sposób zasilania	Rozdzielone zasilanie prostownika i Bypassu wewnętrznego – zasilanie dwutorowe. Podłączane na listwie zaciskowej.
6	Tolerancja napięcia wejściowego przy obciążeniu 70-100%; bez przechodzenia na baterie	160 – 276 Vac
7	Tolerancja napięcia wejściowego przy obciążeniu mniejszym od 70%; bez przechodzenia na baterie	120 – 276 Vac
8	Częstotliwość wejściowa	Wymagana 40-70 Hz
9	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 95%
10	Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode	nie mniejsza niż 99%
11	Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.
12	Napięcie wyjściowe	230 Vac
13	Częstotliwość wyjściowa	50/60Hz (programowalna)
14	Zintegrowane bezprzerwowe przełączniki obejściowe (by-pass)	Statyczny przełącznik (SCR) oraz ręczny odłącznik serwisowy na UPSie
15	Zewnętrzny bezprzerwowy bypass serwisowy pozwalający odłączyć UPS na wypadek awarii	Wymagany – montaż na UPSie
16	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu	Wymagane

	naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem	
17	Czas podtrzymania	Minimum 15 min przy obciążeniu 5400 W
18	Baterie	Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 5-6 lat, umieszczone w zewnętrznych modułach bateryjnych.
19	Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%
20	Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%
21	Stabilność częstotliwości wyjściowej:	bez synchronizacji: ± 0,05%
22	Współczynnik szczytu	3:1
23	Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD w języku polskim oraz sygnalizacją akustyczną	Wymagane
24	Złącze interfejsów	RS232, USB, REPO
25	Wyjściowa listwa do wpięcia UPS do instalacji stałej	Wymagana możliwość podłączenia przewodów o przekroju min 6mm2
26	Gniazda wyjściowe IEC320 na zasilaczu UPS	Wymagane minimum gniazd 4 szt x IEC 320-C13 2 szt x IEC 320-C19
27	Karta sieciowa SNMP	Wymagane
28	Interfejs EPO (do wyłącznika ppoż.)	Wymagane
29	Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS
30	Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
31	Poziom hałasu w odległości 1m,	< 50 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
32	Rejestr zdarzeń	Dziennik zdarzeń w UPS-ie
33	Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
34	Zabezpieczenie przed zwrotnym podaniem napięcia niebezpiecznego do obwodu zasilającego UPS	Wymagane

35	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa, kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane
36	Wymiary zasilacza UPS w szafie rack	Maks 3U
37	Wymiary dodatkowego modułu bateryjnego w szafie rack	Maks 3U
38	Waga zasilacza kg	<50 kg
39	Instrukcja w języku polskim	Wymagane
40	Gwarancja	24 miesiące

3.9. Punkt dostępowy sieci WLAN – szt. 15

Praca	
Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
Maksymalny transfer danych przez bezprzewodowy LAN	1300 Mbit/s
Maksymalna szybkość przesyłania danych	1300 Mbit/s
2,4 GHz	Tak
5 GHz	Tak
Maksymalny zakres wewnętrzny (pomieszczenie)	120 m
Przycisk reset	Tak
Łączność	
Ilość portów Ethernet LAN (RJ-45)	2
Liczba portów USB 2.0	1
Ochrona	
Szyfrowanie / bezpieczeństwo	AES,TKIP,WEP,WPA,WPA2
Antena	
Poziom wzmocnienia anteny (max)	3 dBi
Ilość anten	3
Inne	
Zestaw do montażu	TAK
Obsługa PoE	TAK, z oferowanego przełącznika
Wraz z punktami dostępowymi Zmawiający wymaga dostarczenia sprzętowego kontrolera do zarzadzania powstała siecią WLAN, dedykowanego dla oferowanych AP.	

3.10. Wymagania wstępne

Celem prac jest :

- przygotowanie nowego środowiska wirtualnego zbudowanego w oparciu o dostarczony serwer, macierz, oprogramowanie do wirtualizacji oraz system backupu i archiwizacji,
- stworzenie wydajnej sieci komputerowej w oparciu o dostarczone przełączniki sieciowe, oraz punkty dostępowe sieci bezprzewodowej WLAN
- Zabezpieczenie pracy urządzeń aktywnych poprzez instalacje urządzenia UPS.

Na tak przygotowane środowisko wirtualne Zamawiający wymaga zmigrowania wykorzystywanych systemów IT na fizycznych serwerach.

Środowisko wirtualne powinno zostać zabezpieczone poprzez dostarczony, zainstalowany i skonfigurowany system backup i archiwizacji danych.

Zamawiający wymaga odseparowania składowania danych backupu od danych produkcyjnych.

Zamawiający wymaga wykorzystania istniejącej infrastruktury sieciowej tj. podłączenia jej do nowych urządzeń sprzętowych oraz oprogramowania.

Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa.

Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.

W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową. Zamawiający w tym celu wyznaczy ze swojej strony Kierownika Projektu z odpowiednimi kompetencjami.

Zamawiający wymaga następującego zakresu usług w ramach prowadzonego projektu realizowanego w porozumieniu z Zamawiającym:

a) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia.
b) Sporządzenia Dokumentacji Wykonawczej, według której nastąpi realizacja. Dokumentacja Wykonawcza musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności:
    - testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności
    - sposób odbioru uzgodniony z Zamawiającym
    - listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu
    - opis przypadków, w których projekt dopuszcza niedziałanie systemu
c) Realizacja wdrożenia nastąpi według Planu Wdrożenia, po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą.
d) Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Dokumentacją Powykonawczą.

Wykonawca powinien zapewnić możliwość wykonania kopii zapasowej maszyn oraz innych migrowanych danych obecnych na posiadanych przez Zamawiającego serwerach na zewnętrzny zasób dyskowy o parametrach nie gorszych niż wykorzystywane obecnie przez Zamawiającego. Dopiero po wykonaniu takowej kopii zapasowej – nie wcześniej - Wykonawca może rozpocząć przeprowadzanie wszystkich opisywanych prac instalacyjnych i konfiguracyjnych.

Konieczność wykonania kopii zapasowej dotyczy również wszystkich urządzeń sieciowych Zamawiającego, których parametry konfiguracji będą w czasie wdrożenia modyfikowane.

3.11. Montaż i fizyczne uruchomienie systemu

a) Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez zamawiającego z uwzględnieniem wszystkich lokalizacji.
b) Urządzenia, które nie są montowane w szafach teleinformatycznych powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego.
c) Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
d) Podłączenie całości rozwiązania do infrastruktury Zamawiającego (zapewniając redundancje połączeń).
e) Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
f) Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
g) Wykonanie modernizacji sieci elektrycznej celem podłączenia dostarczonego UPS'a.
h) Podłączenie UPS'a do sieci elektrycznej.
i) Przepięcie, podłączenie wszystkich urządzeń w szafie teleinformatycznej na zasilanie z UPS'a.
j) Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
k) Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
l) Demontaż „starych" urządzeń IT z szafy teleinformatycznej, które nie będą już wykosztowane.
m) Wykonania projektu rozmieszczenia i połączenia lokalnych urządzeń (np.: VLAN MANAGEMENT).
n) Wykonania projektu struktury adresacji urządzeń sieciowych lokalnych.
o) Wykonania projektu architektury sieci VLAN – sieci wirtualne.
p) Wykonania projektu podłączenia i wykorzystania systemu macierzowego oraz backupowego do systemu serwerowego.
q) Określenie wymagań związanych z polityką bezpieczeństwa.
r) Opracowanie dokumentacji wykonawczej i powykonawczej.

3.12. Uruchomienie dostarczonego środowiska wirtualizacyjnego

Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie:

a) Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta (na dostarczone konto Urzędu).
b) Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego - aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
c) Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach.
d) Instalacja sieciowego systemu operacyjnego – na istniejącym serwerze (po migracji zasobów).
e) Instalacja oprogramowania do zarzadzania środowiskiem wirtualizacyjnym na dedykowanym istniejącym fizycznym serwerze S1.
f) Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.
g) Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
h) Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Zamawiającego. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN Zamawiającego, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
i) Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.
j) Przygotowanie koncepcji wirtualizacji fizycznych maszyn.
k) Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.
l) Migracja istniejącej infrastruktury do nowo stworzonego środowiska wirtualnego w tym usługa katalogowa Active Directory (dwa kontrolery domeny).
m) Konfiguracja uprawnień w środowisku wirtualizacyjnym - integracja z usługą katalogową
n) Konfiguracja powiadomień o krytycznych zdarzeniach (email).

3.13. URUCHOMIENIE OPROGRAMOWANIA DO WYKONYWANIA KOPII ZAPASOWYCH ŚRODOWISKA WIRTUALNEGO

- Instalacja oraz uruchomienie dostarczonego środowiska wykonywania kopii zapasowych (Serwerem backupu powinien zostać fizyczny S1 z wykorzystaniem dostarczonej macierzy).
- Przygotowanie i wykreowanie odpowiedniej przestrzeni dyskowej na potrzeby backupu z uwzględnieniem odpowiedniego poziomu bezpieczeństwa.
- Prezentacji przestrzeni dyskowej do serwera S1 (konfiguracja wolumenów logicznych).
- Aktywacja wymaganych licencji.
- Wykorzystanie i wdrożenie koncepcji backupu w oparciu o schemat DISK-to-DISK (serwer wirtualizacyjny z dyskami -macierz dyskowa).

Konfiguracja zadań wykonywania kopii zapasowych wirtualnych maszyn według poniższych wymagań:

- kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
- kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
- kopie maszyn wirtualnych muszą być replikowane na wskazany przez Zamawiającego zasób dyskowy
- kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
- kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;
- musi istnieć możliwość odtworzenia:
    - całej wirtualnej maszyny;
    - dysku wirtualnej maszyny;
    - pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa);
- konfiguracja powiadomień o wykonaniu kopii zapasowej (e-mail).

3.14. URUCHOMIENIE LOKALNEGO SERWERA SMTP

Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux.
Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z:

- Urządzeń sieciowych
- Serwerów
- Macierzy dyskowej
- Systemu zarządzania kopiami zapasowymi
- Systemu wirtualizacji serwerów

Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email.

3.15. REKONFIGURACJA SIECI LAN

Obecnie serwery oraz stacje robocze oraz serwery znajdują się w jednej sieci VLAN.
Zamawiający wymaga zaplanowania oraz przeprowadzenia rekonfiguracji sieci LAN w sposób umożliwiający separację oraz filtrowanie ruchu pomiędzy serwerami a stacjami roboczymi. Rekonfiguracja powinna objąć dostarczone przełączniki sieciowe (VLAN) oraz urządzenie bezpieczeństwa Firewall/UTM (polityki bezpieczeństwa).
Zamawiający wymaga zaplanowania oraz przeprowadzenia konfiguracji urządzenia bezpieczeństwa firewall w celu zapewnienia możliwości wykorzystania polityk bazujących na poświadczeniach użytkownika w oparciu o wykorzystywaną usługę katalogową Active Directory.

Zamawiający wymaga uruchomienia dostarczonych przełączników LAN co najmniej w zakresie:

- Podłączenie przełączników do infrastruktury Zamawiającego
- Konfiguracja protokołu drzewa rozpinającego
- Konfiguracja mechanizmów automatycznej dystrybucji sieci VLAN pomiędzy wszystkimi przełącznikami
- Konfiguracja elementów bezpieczeństwa oferowanych przez dostarczone przełączniki, a w szczególności:
    - Mechanizm monitorowania przydziału adresów IP przez serwery DHCP, ochrona przed nieautoryzowanymi serwerami DCHP;
    - Mechanizm monitorowania prawidłowego użycia protokołu ARP przez stacje końcowe w celu zapobieżenia nadużyciom oraz atakom typu „man in the middle"
    - Mechanizm filtrujący ruch na portach dostępowych, do których przyłączone zostaną stacje końcowe, zezwalając na ruch jedynie z adresu IP przydzielonego przez serwer DHCP;
    - Implementacja mechanizmów 802.1x na wybranych portach z wykorzystaniem dostarczanego serwera uwierzytelniającego wbudowanego w system domenowy, tak aby w przypadku braku autoryzacji dozwolony był ruch np. tylko do Internetu, a w przypadku poprawnej autoryzacji możliwy był dostęp do zasobów sieciowych urzędu. Uwierzytelnienie powinno zostać oparte o certyfikat komputera jak i użytkownika (dynamiczna zmiana sieci VLAN w oparciu o przynależność do grupy użytkowników w systemie domenowym).
    - Implementacja mechanizmów zabezpieczających się przed spoofingiem adresów źródłowych – ip source guard
    - Konfiguracja dostępu do urządzeń z wykorzystaniem mechanizmów AAA w oparciu o serwer uwierzytelniający wbudowany w system domenowy. Administrator ma podlegać autentykacji, autoryzacji wykonywanych operacji administracyjnych lub konfiguracyjnych na urządzeniu oraz wszelkie wykonywane operacje mają być logowane na serwerze uwierzytelniającym.
    - Zapewnienie bezpiecznego środowiska zarządzającego dla urządzeń – dostęp jedynie z dedykowanej stacji zarządzającej, jeżeli to możliwe zbudowanie odseparowanego segmentu zarządzającego wykorzystującego interfejsy kart zarządzających out-of-band management (jeżeli zaproponowane urządzenia będą posiadać interfejsy tego typu).
- Implementacja dostępnych mechanizmów Quality of Service:
    - Konfiguracja kolejkowania traktującego ruch pochodzący od telefonów IP oraz ruch zarządzający jako priorytetowy;
    - Implementacja mechanizmów zapobiegających wysycaniu pasma na łączach pomiędzy przełącznikami, routerami oraz firewall'em poprzez niepożądany ruch sieciowy np. ruch generowany przez stacje zainfekowane wirusem (Scaveger QoS);

3.16. Zamawiający wymaga uruchomienia dostarczonego Firewall/UTM co najmniej w zakresie

- Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
- Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.
- Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email)
- Przygotowanie projektu włączenia urządzenia do sieci LAN Zamawiającego
- Konfiguracja uwierzytelniania w oparciu o wykorzystywaną przez Zamawiającego usługę katalogową – Active Directory
- Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla:
  - Serwerów
  - Sieci MANAGEMENT
  - Stacji Roboczych (Użytkownicy)
  - Stacji roboczych (Administratorzy)
  - Sieci bezprzewodowej
- W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (Active Directory), nie zaś o adresy IP, czy MAC
- Dla urządzeń typu INFOKIOSK, System Wizualizacji Treści – polityki powinny być budowane w oparciu o adresy MAC
- W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności:
  - kontrola dostępu - zapora ogniowa klasy Stateful Inspection
  - ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar
  - ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
  - kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
  - kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
  - kontrola pasma oraz ruchu [QoS, Traffic shaping]
  - Kontrola aplikacji oraz rozpoznawanie ruchu P2P
  - Ochrona przed wyciekiem poufnej informacji (DLP)
  - Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)
  - Inspekcja ruchu SSL
  - Ochrony przez atakami na stacje klienckie
  - Kontrola pasma

- Konfiguracja logowania i raportowania do alternatywnego serwera SYSLOG – min. 200G (instalacja i konfiguracja serwera SYSLOG spoczywa na Wykonawcy). Zamawiający na potrzeby instalacji serwera SYSLOG udostępnia infrastrukturę wirtualizacyjną. **Jeśli dla zapewnienia tej funkcjonalności wymagane są jakiekolwiek licencje – ich dostarczenie spoczywa na Wykonawcy. Zamawiający dopuszcza wykupienie usługi logowania zdarzeń u producenta urządzenia.**

3.17. TERMIN WYKONANIA PRAC INSTALACYJNO-WDROŻENIOWYCH. ODDANIE SYSTEMU DO EKSPLOATACJI.

Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia, w ramach jednego weekendu (piątek godz. 16:00 - sobota godz. 22:00) po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Zamawiającym. Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszych dwóch dni roboczych następujących po pracach wdrożeniowo – instalacyjnych w godzinach od 7.30 do 16.00.

W tym czasie przedstawiciele Wykonawcy zobowiązani są do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji. W tym czasie przedstawiciele Wykonawcy dokonają także przeszkolenia dwóch pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań.

3.18. OPRACOWANIE DOKUMENTACJI POWYKONAWCZEJ

Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Zamawiający jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.

3.19. OPIEKA SERWISOWA

Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy, od momentu podpisania protokołu odbioru, z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny, z zakresu realizowanego wdrożenia oraz powstałego sytemu teleinformatycznego. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych.

Zamawiający nie dopuszcza możliwości pracy zdalnej.

Wykonawca zapewni przyjmowanie zgłoszeń w Godzinach Roboczych, przez które rozumie się godziny od 7.00 do 17.00 w Dni Robocze.

Prace serwisowe mogą być realizowane po godzinach pracy Urzędu w tym również w dni wolne. Termin realizacji prac wyznacza Zamawiający, a Wykonawca jej przyjmuje.

W ramach opieki serwisowej Zamawiający wymaga dwóch wizyt serwisowych w siedzibie Urzędu. Czas pojedynczej wizyty serwisowej 8 godz. – jeden dzień roboczy.

W przypadku jeżeli producent Standardowego Oprogramowania Systemowego, Standardowego Oprogramowania Aplikacyjnego lub sprzętu komputerowego udostępni jakiekolwiek aktualizacje, nowe wersje, patche, zmiany itp. (dalej łącznie zwane aktualizacjami), Wykonawca w ramach Usług Serwisu zapewni Zamawiającemu takie aktualizacje niezwłocznie po ich udostępnieniu.

W przypadku stwierdzenia, że przyczyna Wady leży w Standardowym Oprogramowaniu Systemowym, Standardowym Oprogramowaniu Aplikacyjnym lub oprogramowaniu dostarczanym przez Wykonawcę w ramach Infrastruktury Technicznej, Wykonawca w Czasie Naprawy jest zobowiązany do wykonania Obejścia, a do usunięcia Wady jest zobowiązany niezwłocznie po zapewnieniu odpowiedniej poprawki przez producenta Standardowego Oprogramowania Systemowego lub Standardowego Oprogramowania Aplikacyjnego. W celu uniknięcia wątpliwości w takim przypadku wykonanie Obejścia w Czasie Naprawy stanowi należyte wykonanie Umowy i nie jest podstawą do naliczenia kar umownych z tytułu niedochowania Czasu Naprawy, co nie zwalnia Wykonawcy z obowiązku usunięcia Wady po udostępnieniu odpowiedniej poprawki przez producenta oprogramowania.

Łączny wymiar usług związanych z opieką serwisową nie przekroczy 240 godzin.