Załącznik Nr 6 - Szczegółowa specyfikacja przedmiotu zamówienia

Nr referencyjny nadany sprawie przez Zamawiającego: **TARRCI/D_ROZB_IT/POIG_5.3/1/2015**

Przedmiotem zamówienia w ramach prowadzonego postępowania jest dostawa sprzętu IT na potrzeby funkcjonowania Spółki. Zamówienie składa się z poszczególnych zadań, w ramach których planowane są odpowiednie pozycje zakupowe. Każde z zadań wskazanych w niniejszym zestawieniu stanowi odrębną część zamówienia w rozumieniu ustawy Prawo zamówień publicznych.

Poniższa tabela zawiera zestawienie części zamówienia (zadań), zawierających wymagane urządzenia i oprogramowanie.

Tabela 1. Zestawienie zadań oraz sprzętu i oprogramowania

Część zamówienia/ Zadanie	poz.	Nazwa	Ilość
1	1	Osprzęt serwerowy (typ 1)	3
	2	Serwer (typ 1)	4
	3	Serwer (typ 2)	32
	4	Serwer (typ 3)	6
	5	Osprzęt sieciowy (typ 1)	64
	6	Osprzęt sieciowy (typ 2)	1
	7	Osprzęt serwerowy (typ 2)	18
	8	Osprzęt serwerowy (typ 3)	144
2	9	Osprzęt sieciowy (typ 3)	1
	10	Osprzęt sieciowy (typ 4)	1
	11	Osprzęt sieciowy (typ 5)	2
	12	Osprzęt sieciowy (typ 6)	20
	13	Osprzęt sieciowy (typ 7)	14
	14	Osprzęt sieciowy (typ 8)	4
	15	Osprzęt sieciowy (typ 9)	10
	16	Osprzęt sieciowy (typ 10)	16
	17	Osprzęt sieciowy (typ 11)	14
	18	Osprzęt serwerowy (typ 4)	16
	19	Osprzęt inny (typ 1)	3
	20	Oprogramowanie (typ 1)	1
3	21	Storage (typ 1)	1
	22	Osprzęt sieciowy (typ 12)	2
4	23	Storage (typ 2)	2
5	24	Storage (typ 3)	1
6	25	Storage (typ 4)	1
	26	Serwer (typ 4)	2
7	27	Serwer (typ 5)	2
	28	Serwer (typ 6)	8
8	29	Serwer (typ 7)	3
	30	Serwer (typ 8)	1

9	31	Osprzęt sieciowy (typ 13)	1
	32	Osprzęt sieciowy (typ 14)	2
10	33	Osprzęt sieciowy (typ 15)	2
	34	Osprzęt sieciowy (typ 16)	25
	35	Osprzęt inny (typ 2)	3
11	36	Osprzęt sieciowy (typ 17)	2
12	37	Oprogramowanie (typ 2)	1
13	38	Osprzęt sieciowy (typ 18)	2
	39	Osprzęt sieciowy (typ 19)	2
14	40	Oprogramowanie (typ 3)	1

Przedmiot zamówienia zawarty w tabeli nr 1 został następnie uszczegółowiony do parametrów urządzeń i oprogramowania wymaganych do realizacji konkretnych zadań. Przedstawiona w tabelach nr 2.1.1 do 2.14.1 włącznie specyfikacja poszczególnych pozycji zawiera wymagania minimalne, jakie muszą być spełnione przez dostarczone w ramach zamówienia urządzenia i pakiety oprogramowania.

Zadanie 1. Infrastruktura serwerowa

Specyfikacja sprzętu i oprogramowania dla zadania nr 1. Wszystkie elementy będące przedmiotem zamówienia w niniejszym zadaniu nr 1 stanowią rozszerzenie obecnie posiadanej infrastruktury serwerowej Zamawiającego. Z uwagi na to, iż Zamawiający posiada już elementy infrastruktury serwerowej jednego producenta, zamawiając rozszerzające ją elementy posługuje się konkretnymi modelami urządzeń tego producenta z uwagi na kompatybilność i spójność całej infrastruktury jak również z uwagi na brak możliwości podłączenia lub zespolenia elementów pochodzących od różnych producentów.

Tabela 2.1.1. Osprzęt serwerowy (typ 1) – 4 sztuki

l.p.	cecha	wartość
1.	Informacja ogólna	Zamawiający posiada obecnie obudowy do serwerów blade HP C7000 oraz serwery typu blade modele HP BL465c Gen 7 i HP BL465c Gen 8. Celem zamówienia jest doposażenie obecnie posiadanej infrastruktury w kolejne serwery typu blade (pozycje 2.1.2, 2.1.3 i 2.1.4), które będą umieszczone w nowych i obecnie posiadanych obudowach HP C7000. Niektóre z obecnie posiadanych serwerów typu blade zostaną również zamontowane w nowych obudowach dostarczonych w ramach obecnego zamówienia.
2.	Liczba serwerów typu blade	Dostarczona infrastruktura na serwery typu blade musi umożliwiać zainstalowanie serwerów z pozycji 2.1.2, 2.1.3 i 2.1.4 oraz zapewniać miejsce niezbędne do instalacji kolejnych serwerów tego samego typu.
3.	Rodzaj obsługiwanych serwerów	Możliwość umieszczania w ramach jednej infrastruktury wszystkich dostarczanych typów serwerów blade w układzie mieszanym, także serwerów blade w procesorami o architekturze RISC lub EPIC (serwery takie nie są przedmiotem zamówienia, ale muszą być dostępne do rozbudowy). W ramach infrastruktury (pojedynczego zestawu), należy dostarczyć ilość obudów zapewniających powyższe możliwości rozbudowy, każda obudowa wchodząca w skład infrastruktury musi posiadać identyczną konfigurację.
4.	Sposób	Każda obudowa musi posiadać minimum 2 moduły obsługujące 10Gb

	agregacji/wyprowadzeń sygnałów LAN dla pojedynczej obudowy	Ethernet wyprowadzające sygnały z minimum 2 portów sieciowych 10Gb na serwerach. Urządzenia te muszą umożliwiać agregację połączeń LAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów LAN z infrastruktury z zachowaniem redundancji połączeń. Każdy moduł powinien posiadać minimum 8 portów 10Gb przygotowane do obsadzenia modułami SFP+. Wraz z dwoma modułami należy dostarczyć minimum 16 modułów SFP+ 10Gb SR (po 8 sztuk na moduł). Jeśli w serwerze znajdują się dodatkowe karty LAN (oprócz wymaganych 2 portów 10Gb), należy uwzględnić odpowiednie moduły LAN w celu wyprowadzenia dodatkowych portów na zewnątrz obudowy. Wszystkie fizyczne porty każdego modułu sieciowego muszą być aktywne i gotowe do obsługi ruchu sieciowego bez konieczności dokupywania elementów sprzętowych lub dodatkowych licencji.
5.	Sposób agregacji/wyprowadzeń sygnałów FC dla pojedynczej obudowy	Każda obudowa musi posiadać minimum dwa moduły obsługujące 8Gb Fibre-Channel wyprowadzające sygnały z minimum 2 portów FC na serwerach. Urządzenia te muszą obsługiwać agregację połączeń SAN w infrastrukturze blade i muszą obsługiwać wyprowadzenie sygnałów SAN z infrastruktury z zachowaniem redundancji połączeń. Każdy moduł musi posiadać minimum 8 zewnętrznych portów. Wraz z modułami należy dostarczyć minimum 16 modułów FC SFP+ 8Gb SW (po 8 sztuk na moduł). Wszystkie fizyczne porty każdego modułu muszą być aktywne i gotowe do obsługi ruchu sieciowego SAN bez konieczności dokupywania elementów sprzętowych lub dodatkowych licencji. Nie dopuszcza się zastosowania modułów FCoE 10Gb.
6.	Dodatkowa funkcjonalność modułów LAN i SAN	Możliwość przydzielania adresów MAC i WWN predefiniowanych przez producenta rozwiązania blade dla poszczególnych wnęk na serwery w obudowie. Przydzielenie adresów musi powodować zastąpienie fizycznych adresów kart Ethernet i Fibre-Channel na serwerze. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnękami w obudowie. Funkcjonalność ta może być realizowana zarówno poprzez moduły LAN i SAN w infrastrukturze jak i poprzez dodatkowe oprogramowanie producenta serwerów blade. Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak aby między wydzielonymi sieciami nie było komunikacji. Wymagana jest możliwość boot'owania systemów operacyjnych zainstalowanych na poszczególnych serwerach blade bezpośrednio z macierzy w środowisku SAN. Wymagane wszystkie niezbędne licencje na opisaną funkcjonalność dla całej infrastruktury blade. W przypadku sieci LAN, musi istnieć możliwość określenia pasma przepustowości pojedynczego portu LAN na serwerze od 100Mb/s do 10Gb/s. Musi również istnieć możliwość stworzenia wewnętrznej sieci LAN (np. na cele migracji wirtualnych maszyn pomiędzy hostami) w obrębie obudowy pomiędzy serwerami w niej zainstalowanymi. Ruch sieciowy w ramach wewnętrznej sieci nie może być obsługiwany przez inne urządzenia niż moduły komunikacyjne zainstalowane w danej obudowie. Nie dopuszcza się zastosowania zewnętrznych przełączników do obsługi tej wewnętrznej sieci LAN.

7.	Chłodzenie dla pojedynczej obudowy	Każda z obudów na serwery wyposażona w zestaw redundantnych wiatraków (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie blade. Wentylatory niezależne od zasilaczy, wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia zasilacza (zasilaczy).
8.	Zasilanie dla pojedynczej obudowy	Zasilanie trójfazowe, podłączenie dwoma redundantnymi złączami IEC309 5-Pin do zewnętrznego źródła zasilania. Każda z obudów wyposażona w zestaw zasilaczy redundantnych typu Hot Plug. System zasilania zdolny do obsługi awarii połowy z zainstalowanych zasilaczy (dowolne N zasilaczy przy założeniu konfiguracji N + N), wymagane ciągłe dostarczenie mocy niezbędnej do zasilenia maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie. Procesory serwerów winny pracować z nominalną, maksymalną częstotliwością. Wymiana zasilacza nie może powodować konieczności odłączenia zewnętrznej infrastruktury zasilania (kabla zasilającego), jak również nie może powodować konieczności wyjęcia lub odłączenia wentylatorów (pojedynczego wentylatora lub modułu wentylatorów).
9.	Montaż	Infrastruktura musi być przystosowana do montażu w szafie typu rack 19”, umożliwiająca obsadzenie minimum 16 serwerów dwuprocesorowych bez konieczności rozbudowy o kolejne elementy sprzętowe.
10.	Moduły zarządzające	Dwa redundantne, sprzętowe moduły zarządzające , moduły typu Hot Plug. Zintegrowany w modułach zarządzających lub w obudowie, moduł KVM, umożliwiający podłączenie klawiatury, myszy i monitora.
11.	Wymagania dodatkowe	Każda z obudów wchodzących w skład infrastruktury musi posiadać identyczną konfigurację sprzętową w zakresie zasilaczy, wiatraków oraz modułów I/O.
12.	Gwarancja.	Co najmniej 36 miesięcy świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 24 godzin na nowo dostarczone obudowy. Co najmniej 36 miesięcy wsparcia na miejscu instalacji sprzętu z gwarancją usunięcia awarii w ciągu 24 godzin na 4 obudowy HP c7000 obecnie posiadane przez Zamawiającego.

Tabela 2.1.2. Serwer (typ 1) – 4 sztuki

l.p.	cecha	wartość
1.	Procesory (ilość i typ)	Minimum dwa procesory minimum ośmiordzeniowe, x86 - 64 bity, Intel E5-2640v3 lub równoważne procesory minimum ośmiordzeniowe o taktowaniu min. 2.6GHz, osiągające w testach SPECint_rate2006 Result wynik nie gorszy niż 706 punktów. W przypadku zaoferowania procesora równoważnego, wynik testu musi być publikowany na stronie www.spec.org Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów.
2.	Pamięć RAM	96 GB RAM DDR3 Registered DIMMs. Możliwość instalacji w serwerze minimum 512 GB pamięci RAM. Minimum 16 slotów na pamięć.
3.	Wbudowane porty	Min. jeden wewnętrzny port USB 2.0 lub wewnętrzny slot na kartę SD.

		Wraz z serwerem należy dostarczyć moduł typu Flash min. 8GB umożliwiający instalację systemu do wirtualizacji.
4.	Sterownik dysków wewnętrznych	Macierzowy, RAID 0,1.
5.	Sloty rozszerzeń	Minimum 2 sloty PCI-Express x16 (szybkość slotu)
6.	Interfejsy sieciowe (LAN)	Minimum 2 Interfejsy sieciowe 10GbE z możliwością podzielenia każdego interfejsu na 4 karty sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej.
7.	Interfejsy FC (SAN)	Minimum jeden porty FC 16Gb
8.	Interfejsy równoważne FCoE	W przypadku zastosowania modułów FCoE w infrastrukturze blade, wymaga się dostarczenia z serwerem (zamiast powyższych interfejsów LAN i SAN) następujących interfejsów: Minimum 2 porty CNA 10Gb FCoE. Każdy port z możliwością podzielenia na 4 porty LAN (z możliwością określenia przepustowości od 100Mb/s do 10Gb/s, posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe) oraz 1 port FC. Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej.
9.	Wspierane systemy operacyjne	MS Windows Server 2012 , Red Hat Enterprise Linux ,SUSE Linux Enterprise Server, VMware.
10.	Gwarancja	36 miesięcy świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 24 godzin.
11.	Licencje	Jedną licencję CloudSystem Enterprise 8.1. Zamawiający posiada licencję CloudSystem Enterprise. Przedmiot zamówienia ma służyć rozbudowie posiadanego środowiska.

Tabela 2.1.3. Serwer (typ 2) – 32 sztuki

l.p.	cecha	wartość
1.	Procesory (ilość i typ)	Minimum dwa procesory minimum ośmiordzeniowe, x86 - 64 bity, Intel E5-2630v3 lub równoważne procesory minimum ośmiordzeniowe o taktowaniu min. 2.4GHz, osiągające w testach SPECint_rate2006 Result wynik nie gorszy niż 680 punktów. W przypadku zaoferowania procesora równoważnego, wynik testu musi być publikowany na stronie www.spec.org Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów.
2.	Pamięć RAM	128 GB RAM DDR3 Registred DIMMs. Możliwość instalacji w serwerze minimum 512 GB pamięci RAM. Minimum 16 slotów na pamięć.
3.	Wbudowane porty	Min. jeden wewnętrzny port USB 2.0 lub wewnętrzny slot na kartę SD. Wraz z serwerem należy dostarczyć moduł typu Flash min. 8GB umożliwiający instalację systemu do wirtualizacji.
4.	Sterownik dysków wewnętrznych	Macierzowy, RAID 0,1.
5.	Sloty rozszerzeń	Minimum 2 sloty PCI-Express x16 (szybkość slotu)
6.	Interfejsy sieciowe (LAN)	Minimum 2 Interfejsy sieciowe 10GbE z możliwością podzielenia każdego interfejsu na 4 karty sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe). Podział musi być niezależny od zainstalowanego na serwerze systemu

		operacyjnego/platformy wirtualizacyjnej.
7.	Interfejsy FC (SAN)	Minimum jeden porty FC 16Gb
8.	Interfejsy równoważne FCoE	W przypadku zastosowania modułów FCoE w infrastrukturze blade, wymaga się dostarczenia z serwerem (zamiast powyższych interfejsów LAN i SAN) następujących interfejsów: Minimum 2 porty CNA 10Gb FCoE. Każdy port z możliwością podzielenia na 4 porty LAN (z możliwością określenia przepustowości od 100Mb/s do 10Gb/s, posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe) oraz 1 port FC. Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej.
9.	Wspierane systemy operacyjne	MS Windows Server 2012 , Red Hat Enterprise Linux ,SUSE Linux Enterprise Server, VMware.
10.	Gwarancja	36 miesięcy świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 24 godzin.

Tabela 2.1.4. Serwer (typ 3) – 6 sztuk

l.p.	cecha	wartość
1.	Procesory (ilość i typ)	Minimum dwa procesory minimum dwunastordzeniowe, x86 - 64 bity, Intel E5-2680v3 lub równoważne procesory minimum ośmiordzeniowe o taktowaniu min. 2.5GHz, osiągające w testach SPECint_rate2006 Result wynik nie gorszy niż 1040 punktów. W przypadku zaoferowania procesora równoważnego, wynik testu musi być publikowany na stronie www.spec.org Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów.
2.	Pamięć RAM	128 GB RAM DDR3 Registred DIMMs. Możliwość instalacji w serwerze minimum 512 GB pamięci RAM. Minimum 16 slotów na pamięć.
3.	Wbudowane porty	Min. jeden wewnętrzny port USB 2.0 lub wewnętrzny slot na kartę SD. Wraz z serwerem należy dostarczyć moduł typu Flash min. 8GB umożliwiający instalację systemu do wirtualizacji.
4.	Sterownik dysków wewnętrznych	Macierzowy, RAID 0,1.
5.	Sloty rozszerzeń	Minimum 2 sloty PCI-Express x16 (szybkość slotu).
6.	Interfejsy sieciowe (LAN)	Minimum 2 Interfejsy sieciowe 10GbE z możliwością podzielenia każdego interfejsu na 4 karty sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej.
7.	Interfejsy FC (SAN)	Minimum jeden porty FC 16Gb.
8.	Interfejsy równoważne FCoE	W przypadku zastosowania modułów FCoE w infrastrukturze blade, wymaga się dostarczenia z serwerem (zamiast powyższych interfejsów LAN i SAN) następujących interfejsów: Minimum 2 porty CNA 10Gb FCoE. Każdy port z możliwością podzielenia na 4 porty LAN (z możliwością określenia przepustowości od 100Mb/s do 10Gb/s, posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe) oraz 1 port FC. Podział musi być niezależny od zainstalowanego na serwerze systemu

		operacyjnego/platformy wirtualizacyjnej.
9.	Wspierane systemy operacyjne	MS Windows Server 2012 , Red Hat Enterprise Linux ,SUSE Linux Enterprise Server, VMware.
10.	Gwarancja	36 miesięcy świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 24 godzin.

Tabela 2.1.5. Osprzęt sieciowy (typ 1) – 64 sztuk

l.p.	cecha	wartość
1.	Informacja ogólna	Zamawiający w wyniku realizacji postępowania przetargowego z dnia 22.06.2011 otrzymał, wdrożył i wykorzystuje przełączniki SAN HP StorageWorks 8/80 Base. Przedmiotem zamówienia z 22.06.2011 było m.in. dostarczenie przełącznika SAN z 48 aktywnymi portami z możliwością późniejszej, łatwej rozbudowy poprzez dokupienie licencji. Przedmiotem obecnego zamówienia jest rozszerzenie aktywnych portów z 48 do maksymalnych 80 dla każdego z dwóch obecnie posiadanych przez Zamawiającego urządzeniach.
2.	Model przełącznika SAN	HP StorageWorks 8/80 Base (48) Full Fabric Ports Enabled SAN Switch. Zamawiający posiada 2 sztuki.
3.	Specyfikacja	W ramach zamówienia należy dostarczyć licencje i wkładki SFP+ 8Gbit/s na kolejne 32 porty dla każdego z dwóch przełączników SAN (razem 64 licencje i wkładki SFP+ 8Gbit/s) oraz rozszerzenie wsparcia technicznego na całe urządzenia (aktywne, gotowe do wykorzystania 80 portów w każdym urządzeniu) na okres co najmniej 36 miesięcy. Wsparcie powinno zapewniać co najmniej czas reakcji na następny dzień roboczy, realizację napraw w miejscu instalacji urządzenia oraz gwarancję usunięcia awarii w ciągu nie dłuższym niż 14 dni kalendarzowych.

Tabela 2.1.6. Osprzęt sieciowy (typ 2) – 1 sztuka

l.p.	cecha	wartość
1.	Informacje ogólne	System wykrywania i prewencji włamań IPS
2.	Wymagania	W ramach systemu wykrywania i prewencji włamań IPS Zamawiający dysponuje obecnie systemem złożonym z: 1. Sondy IPS TippingPoint 660N o numerze seryjnym 660N-50R1-502B, 2. serwera zarządzającego HP SMS V2 Appliance w/25-IPS System Lic o numerze seryjnym US16DW907Z.
3.	Sonda IPS	W odniesieniu do posiadanej przez Zamawiającego sondy IPS przedmiotem zamówienia jest zakup kompletu licencji obejmujących swoim zakresem: dostęp, obsługę, automatyczną aktualizację z centralnego systemu producenta: a) bazy filtrów, podatności oraz sygnatur, b) bazy reputacji adresów IPv4, IPv6, DNS;, c) bazy filtrów chroniących przed oprogramowaniem „malware”, atakami typu „phishing”, exploitami typu „zero-day”, d) systemu operacyjnego sondy, na okres 3 lat (dopuszczalny 1 rok pod warunkiem braku możliwości świadczenia przez producenta opcji 3 letniej).
4.	Serwer zarządzający	W odniesieniu do serwera zarządzającego, zakup nowego serwera w formie platformy wirtualnej wraz z licencją na obsługę co najmniej dwóch urządzeń (sond IPS w tym posiadanej sondy TippingPoint 660N), oraz licencjami niezbędnymi do uruchomienia usług zarządzania i administracji sondą na okres 3 lat (dopuszczalny 1 rok pod warunkiem braku możliwości świadczenia przez producenta opcji 3 letniej).

5.	Gwarancja	Co najmniej na okres 36 miesięcy gwarancji co najmniej czas reakcji na zgłoszenie na następny dzień roboczy. Zgłoszenia za pomocą połączenia telefonicznego lub email.

Tabela 2.1.7. Osprzęt serwerowy (typ 2) – 18 sztuk

l.p.	cecha	wartość
1.	Informacja ogólna	Rozszerzenie pamięci do posiadanych przez Zamawiającego dwóch serwerów HP ProLiant DL 160 G6 oraz wsparcia serwisowego.
2.	Pełne oznaczenia serwera	HP ProLiant DL 160 G6 (Product NO. 641457-425).
3.	Pamięć (rozszerzenie)	Moduł o pojemności 4GB, DDR3, DIMM 240-pin, 1600 MHz (PC3-12800), ECC, registered.
4.	Gwarancja	Co najmniej 36 miesięcy gwarancji na dostarczone moduły pamięci. Co najmniej 36 miesięcy gwarancji na posiadane przez Zamawiającego dwa serwery HP ProLiant DL 160 G6 (Product NO. 641457-425).

Tabela 2.1.8. Osprzęt serwerowy (typ 3) – 144 sztuk

l.p.	cecha	wartość
1.	Informacja ogólna	Rozszerzenie pamięci do posiadanych przez Zamawiającego 18 serwerów HP BL465c G7 oraz 18 serwerów HP BL465c G8 oraz wsparcia serwisowego.
2.	Pełne oznaczenia serwera	18 serwerów blade HP ProLiant BL465c G7. 18 serwerów blade HP ProLiant BL465c G8.
3.	Pamięć (rozszerzenie)	W każdym obecnie posiadany przez Zamawiającego serwerze HP BL465c G7 jest zainstalowanych 12 modułów pamięci o oznaczeniu HMT31GR7BFR4A-H9. Do każdego z 18 serwerów G7 należy dostarczyć 4 moduły 8GB. Razem 72 moduły dla serwerów HP G7. W każdym obecnie posiadany przez Zamawiającego serwerze HP BL465c G8 jest zainstalowanych 12 modułów pamięci o oznaczeniu NT8GC72C4NG0NL-CG. Do każdego z 18 serwerów G8 należy dostarczyć 4 moduły 8GB. Razem 72 moduły dla serwerów HP G8.
4.	Gwarancja	Co najmniej 36 miesięcy gwarancji na dostarczone moduły pamięci. Co najmniej 36 miesięcy wsparcia serwisowego na posiadane przez Zamawiającego 18 serwerów HP BL465c G7 oraz 18 serwerów HP BL465c G8.

Zadanie 2. Infrastruktura sieciowa

Specyfikacja sprzętu i oprogramowania dla zadania nr 2. Wszystkie elementy będące przedmiotem zamówienia w niniejszym zadaniu nr 2 stanowią rozszerzenie obecnie posiadanej infrastruktury sieciowej Zamawiającego. Z uwagi na to, iż Zamawiający posiada już elementy infrastruktury sieciowej jednego producenta, zamawiając rozszerzające ją elementy posługuje się konkretnymi modelami urządzeń tego producenta z uwagi na kompatybilność i spójność całej infrastruktury jak również z uwagi na brak możliwości podłączenia lub zespolenia elementów pochodzących od różnych producentów.

Tabela 2.2.1. Osprzęt sieciowy (typ 3) – 1 sztuka

l.p.	cecha	wartość
1.	Informacje ogólne	Przełącznik na potrzeby segmentu sieci odpowiedzialnego za agregację sieci zarządzającej. Zamawiający wdrożył już do tej roli przełącznik Cisco Catalyst 3750X (WS-C3750X-12S-E). W celu zwiększenia niezawodności tego elementu Zamawiający zamawia kolejny przełącznik, który musi stanowić redundancję i bezpośredni zamiennik do obecnie posiadanego. Ponadto przedmiotem zamówienia w niniejszym zadaniu jest rozszerzenie wsparcia serwisowego na komponenty sieciowe posiadane obecnie przez Zamawiającego, opisanego w punkcie dotyczącym gwarancji.

2.	Wydajność	Urządzenie musi posiadać tzw. switching engine o wydajności co najmniej 35 Mbps oraz matrycę 160Gbps.
3.	Interfejsy	1. Minimum 12 portów 1 Gbps SFP, 2. Minimum 4 dodatkowe porty uplink 1 Gbps SFP, z możliwością wymiany na 2 uplinki 10 Gbps SFP+, poprzez wymianę/dodanie modułu sprzętowego, 3. Porty SFP muszą umożliwiać ich obsadzanie wkładkami Gigabit Ethernet – minimum 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U oraz modułami CWDM zależnie od potrzeb Zamawiającego. 4. 8 wkładek umożliwiających pracę na dystansie minimum 100 metrów po światłowodzie wielomodowym (standard 1000BASE-SX), 5. Wkładka umożliwiająca podłączenie w standardzie 1000BASE-T – 1 sztuka, 6. Wkładki muszą pochodzić od tego samego dostawcy, co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.
4.	Stosy	1. Urządzenie musi posiadać możliwość tworzenia stosu o przepustowości co najmniej 64Gbps. 2. Urządzenie musi umożliwiać tworzenie stosów z możliwością definiowania QoS globalnie dla stosu.
5.	VLAN	Urządzenie musi posiadać możliwość zdefiniowania co najmniej 1000 aktywnych sieci VLAN oraz co najmniej 128 instancji STP.
6.	przełączanie L3	Urządzenie musi umożliwiać przełączanie w warstwie trzeciej oraz definiowanie routingu w oparciu o protokoły RIP, OSPF, BGPv4, IS-ISv4.
7.	IGMP	Urządzenie musi wspierać IGMP v1 i v2 oraz umożliwiać definiowanie routingu multicasów w oparciu o protokoły PIM i DVMRP.
8.	PBR	Urządzenie musi: a) umożliwiać konfigurację tzw. Policy Based Routing, b) umożliwiać konfigurację portów RSPAN.
9.	Ciągłość pracy sieci	1. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: a. 802.1w b. 802.1s (co najmniej 100 instancji) c. możliwość grupowania portów (channel, trunk, hunt group) zgodnie z 802.3ad (LACP). 2. Urządzenie musi umożliwiać obsługę protokołu FHRP jako dodatkowy mechanizm związany z zapewnieniem ciągłości pracy sieci.
10.	Jakość usług w sieci	Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: a. obsługa co najmniej ośmiu kolejek sprzętowych dla różnego rodzaju ruchu, b. obsługa mechanizmów Shaped Round Robin (nie jest akceptowalne wsparcie tylko mechanizmów WRR), c. obsługa co najmniej jednej kolejki ze statusem strict priority, d. możliwość "re-kolorowania" pakietów przez urządzenie – pakiet przychodzący do urządzenia przez przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS, e. pełne wsparcie dla 64 wartości pola DSCP, f. możliwość ograniczania pasma dostępnego na port (rate limiting) z granulacją do kwantu 8Kbps lub mniejszego.
11.	Bezpieczeństwo	Urządzenie powinno wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a. autoryzację użytkowników/portów przez 802.1x, b. możliwość ograniczenia dostępu użytkowników per port w oparciu o MAC adresy urządzeń, c. możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSH,

		d. możliwość definiowania list dostępowych dla portów urządzenia, dla sieci VLAN – wewnętrznych i zewnętrznych (przy routingu pomiędzy sieciami VLAN), e. możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1x) do serwerów RADIUS lub TACACS+. Możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. isolated ports) z pozostawieniem możliwości komunikacji z portem nadrzędnym (promiscuous port) lub funkcjonalność Private VLAN.
12.	Konfiguracja urządzenia	Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian. Urządzenie musi być oparte o urządzenie o zamkniętej konfiguracji.
13.	Montaż	Urządzenie musi zapewniać możliwość montażu w szafie 19”. Wraz z urządzeniem należy dostarczyć komplet elementów montażowych pozwalających na montaż w szafie 19”.
14.	Zasilanie	Urządzenie musi zawierać redundantne zasilacze o mocy co najmniej 350W każdy pozwalający na zasilanie zmiennoprądowe.
15.	Gwarancja	Co najmniej 36 miesięcy gwarancji, usługa serwisowa świadczona na miejscu instalacji urządzenia, przyjmowanie zgłoszenia musi być możliwe przez 24h na dobę, siedem dni w tygodniu, czas reakcji następny dzień roboczy w przypadku wystąpienia awarii. Maksymalny czas rozwiązania w przypadku awarii pięć dni. Należy dostarczyć gwarancję obejmującą zakresem nowo dostarczany element oraz wszystkie pozostałe elementy infrastruktury sieciowej, które posiada już Zamawiający: 1. Zapora sieciowa Cisco ASA5585 – 2 sztuki (SN:JMX18238074, JMX18238073) wraz z dostarczonymi wkładkami i modułami, 2. Urządzenie rdzeniowe Cisco Nexus 7010 – 2 sztuki (SN: FXS1809Q2KN, FXS1807Q6A3) wraz z dostarczonymi wkładkami i modułami, 3. Urządzenie brzegowe sieci Cisco ASR1002-X – 2 sztuki (SN: FOX1749GPR3, FOX1749G1DX) wraz z dostarczonymi wkładkami i modułami, 4. Przełącznik dostępowy Cisco Nexus 6001 – 4 sztuki (SN: FOC1820R1E4, FOC1820R1GF, FOC1820R1ES, FOC1822R05B) wraz z dostarczonymi wkładkami oraz modułami, 5. Przełącznik Cisco Catalyst serii 4500 – 3 sztuki (SN: FXS1811Q3EF, FXS1814Q285, FXS1810Q2ES) wraz z dostarczonymi wkładkami i modułami, 6. Koncentrator VPN Cisco ASA 5505 – 1 sztuka (SN: JMX1824Z00K), 7. Przełącznik Cisco Catalyst 3750X – 1 sztuka (SN: FDO1821R0LA) wraz z dostarczonymi wkładkami oraz modułami, 8. Przełącznik Cisco Catalyst 2960X – 4 sztuki (SN: FOC1816S49J, FOC1816S48N, FOC1816S48X, FOC1816S48R) wraz z dostarczonymi wkładkami oraz modułami, 9. Przełączniki Cisco Nexus 2248TP-E – 40 sztuk (SN: SSI174106TL, FOX1813GWK1, SSI1741049Z, SSI174106HX, FOX1810G7RK, FOX1810G7RH, FOX1810G7RJ, SSI174106TM, FOX1813GUFE, FOX1817GXFS, FOX1815G3D2, FOX1817GX9L, FOX1810GMQV, FOX1813GRNH, FOX1813GRNJ, FOX1815GQ9D, FOX1810G643, FOX1815GQEE, FOX1815GQEB, FOX1815G1BM, FOX1815GQED, FOX1817GKJK, FOX1815GQ87, FOX1818G5EF, FOX1818G5EH,

		FOX1818G5CE, FOX1815GQ85, FOX1818G5E5, FOX1818G5EM, FOX1818G5EN, FOX1809GD91, FOX1809GD8P, FOX1817GXEJ, FOX1815G3F6, FOX1817GXGS, FOX1817GXGQ, FOX1817GXGR, FOX1817GX9J, FOX1813GUEN, FOX1817GX5Y), 10. Infoblox Grid Master DDI – 2 szt. (SN: 0937000010, 0937000039), 11. Infoblox NetMRI – 1 szt. (SN: 1450201401100024), 12. PRTG Unlimited.

Tabela 2.2.2. Osprzęt sieciowy (typ 4) – 1 sztuka

l.p.	cecha	wartość
1.	Informacje ogólne	Dodatkowy moduł zarządzający do posiadanego przez Zamawiającego przełącznika Catalyst 4507E. Obecnie przełącznik wyposażony jest w jeden moduł zarządzający. Przedmiotem zamówienia jest zakup dodatkowego modułu, który będzie redundantny do obecnie posiadanego o symbolu Cisco WS-X45-SUP7L-E.
2.	Wydajność i przepustowość	Łączna wydajność 520Gbps z zapewnieniem 48Gbps na slot urządzenia. Przepustowość 225Mpps dla routingu IPV4 i 125Mpps dla routingu IPv6.
3.	Interfejsy	1. Dwa interfejsy10 Gigabit Ethernet (SFP+) lub 4 interfejsy 1 Gigabit Ethernet (SFP) działające z pełna szybkością. 2. Wsparcie dla co najmniej 240 portów 10/100/1000Base-T w 7-mio slotowym chassis. 3. Wsparcie dla co najmniej 124 portów 1GE optycznych lub 62 portów 10GE optycznych w 7-mio slotowym chassis. 4. 2 wkładki umożliwiające pracę na dystansie minimum 100 metrów po światłowodzie jednomodowym (standard 10G-LRM). 5. Wkładki muszą pochodzić od tego samego dostawcy co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.
4.	Wymagania dodatkowe	1. Wsparcie dla technologii Universal Power Over Ethernet (UPOE) z zachowaniem kompatybilności ze starszymi standardami PoE. 2. Wsparcie dla EEE (IEEE 802.3az). 3. Obsługa co najmniej 128,000 wpisów NetFlow ze wsparciem sprzętowym. 4. Port konsolowy i zarządzający 10/100/1000 RJ-45. 5. Tablica musi posiadać minimum: a. 64 000 wpisów dla IPv4, b. 32 000 wpisów dla IPv6. 6. Wsparcie sprzętowe dla technologii IPv6, zapewniające działanie sieci IPv6 oraz wsparcie dla dual-stack z pełna wydajnością urządzenia.
5.	Gwarancja	Co najmniej 36 miesięcy gwarancji, usługa serwisowa świadczona na miejscu instalacji urządzenia, przyjmowanie zgłoszenia musi być możliwe przez 24h na dobę, siedem dni w tygodniu, czas reakcji następny dzień roboczy w przypadku wystąpienia awarii. Maksymalny czas rozwiązania w przypadku awarii pięć dni.

Tabela 2.2.3. Osprzęt sieciowy (typ 5) – 2 sztuki

l.p.	cecha	wartość
1.	Informacje ogólne	Przedmiotem zamówienia są dwie karty liniowe z 48 portami 10/100/1000 pracującymi bez nadsubskrypcji względem matrycy przełączającej.
2.	Wymagania podstawowe	Zamawiający posiada obecnie wdrożony w infrastrukturze sieciowej przełącznik Cisco Catalyst 4507RE, który zamierza rozbudować o dwie dodatkowe karty liniowe wyposażone w 48 portów. Z uwagi na specyfikę prowadzonej działalności, która obsługiwana jest przez przedmiotowy segment sieci należy dostarczyć moduły Cisco oznaczone symbolem WS-X4748-RJ45-E.

3.	Gwarancja	Co najmniej 36 miesięcy gwarancji świadczonej w miejscu montażu dostarczonych urządzeń.

Tabela 2.2.4. Osprzęt sieciowy (typ 6) – 20 sztuk

l.p.	cecha	wartość
1.	Informacje ogólne	Wkładki optyczne będące rozszerzeniem obecnie posiadanych wkładek przez Zamawiającego do sprzętu będącego w posiadaniu Zamawiającego, wdrożonego w infrastrukturze sieciowej. Wkładki w standardzie SFP SR. Obecnie posiadane to Cisco SFP-10G-SR.
2.	Wymagania podstawowe	Oferowane moduły interfejsów muszą pochodzić od tego samego producenta co urządzenia sieciowe, w których będą instalowane. Moduły muszą podlegać wsparciu serwisowemu bazującemu na kontraktach serwisowych producenta sprzętu przypisanych dla urządzeń, w których będą instalowane.
3.	Gwarancja	Co najmniej 36 miesięcy gwarancji.

Tabela 2.2.5. Osprzęt sieciowy (typ 7) – 14 sztuk

l.p.	cecha	wartość
1.	Informacje ogólne	Wkładki optyczne będące rozszerzeniem obecnie posiadanych wkładek przez Zamawiającego do sprzętu będącego w posiadaniu Zamawiającego, wdrożonego w infrastrukturze sieciowej. Wkładki w standardzie SFP MMD. Obecnie posiadane to Cisco GLC-SX-MMD.
2.	Wymagania podstawowe	Oferowane moduły interfejsów muszą pochodzić od tego samego producenta co urządzenia sieciowe, w których będą instalowane. Moduły muszą podlegać wsparciu serwisowemu bazującemu na kontraktach serwisowych producenta sprzętu przypisanych dla urządzeń, w których będą instalowane.
3.	Gwarancja	Co najmniej 36 miesięcy gwarancji.

Tabela 2.2.6. Osprzęt sieciowy (typ 8) – 4 sztuki

l.p.	cecha	wartość
1.	Informacje ogólne	Wkładki optyczne będące rozszerzeniem obecnie posiadanych wkładek przez Zamawiającego do sprzętu będącego w posiadaniu Zamawiającego, wdrożonego w infrastrukturze sieciowej. Wkładki w standardzie SFP LRM. Obecnie posiadane to Cisco SFP-10G-LRM.
2.	Wymagania podstawowe	Oferowane moduły interfejsów muszą pochodzić od tego samego producenta co urządzenia sieciowe, w których będą instalowane. Moduły muszą podlegać wsparciu serwisowemu bazującemu na kontraktach serwisowych producenta sprzętu przypisanych dla urządzeń, w których będą instalowane.
3.	Gwarancja	Co najmniej 36 miesięcy gwarancji.

Tabela 2.2.7. Osprzęt sieciowy (typ 9) – 10 sztuk

l.p.	cecha	wartość
1.	Informacje ogólne	Wkładki optyczne będące rozszerzeniem obecnie posiadanych wkładek przez Zamawiającego do sprzętu będącego w posiadaniu Zamawiającego, wdrożonego w infrastrukturze sieciowej. Wkładki w standardzie SFP GE-T. Obecnie posiadane to Cisco SFP-GE-T.
2.	Wymagania podstawowe	Oferowane moduły interfejsów muszą pochodzić od tego samego producenta co urządzenia sieciowe, w których będą instalowane. Moduły muszą podlegać wsparciu serwisowemu bazującemu na kontraktach serwisowych producenta sprzętu przypisanych dla urządzeń, w których będą instalowane.
3.	Gwarancja	Co najmniej 36 miesięcy gwarancji.

Tabela 2.2.8. Osprzęt sieciowy (typ 10) – 16 sztuk

l.p.	cecha	wartość
1.	Informacja ogólna	Kable połączeniowe 10GBase zakończone na obydwu końcach męskimi złączami SFP+.
2.	Długość	1,5 metra – 8 sztuk, 2,0 metra – 8 sztuk

Tabela 2.2.9. Osprzęt sieciowy (typ 11) – 14 sztuk

l.p.	cecha	wartość
1.	Informacja ogólna	Okablowanie strukturalne światłowodowe w trzech długościach służące jako kable połączeniowe do patchpaneli światłowodowych, które Zamawiający otrzymał w wyniku realizacji i wdrożenia postępowania z dnia 20.03.2014.
2.	Długość	35 metrów – 2 sztuki, 40 metrów – 2 sztuki, 25 metrów – 10 sztuk
3.	Ilość włókien	Dostarczone okablowanie musi posiadać dokładnie 12 włókien (12J).
4.	Średnica kabla	Nie więcej niż 4mm.
5.	Złącza	Musi być zakończony po obu stronach pojedynczym złączem MPO/MTP. Złącze z każdej strony kabla musi terminować wszystkie 12J.
6.	Kompatybilność	Kompatybilne z już posiadanymi patchpanelemi światłowodowymi GBC Photonics GPxWDM-4DRACK

Tabela 2.2.10. Osprzęt serwerowy (typ 4) – 16 sztuk

l.p.	cecha	wartość
1.	Informacja ogólna	Rozszerzenie pamięci do posiadanych przez Zamawiającego dwóch serwerów Cisco UCS-SP6-C220E oraz wsparcia serwisowego.
2.	Pełne oznaczenia serwera	UCS-SP6-C220E: UCS SP C220 SFF ENTRY w/2xE5-2609 32GB 5709 NIC SAS 2008M
3.	Pamięć (rozszerzenie)	8 modułów o pojemności 16GB, DDR3, DIMM 240-pin, 1600 MHz (PC3-12800), ECC, registered. 8 modułów o pojemności 8GB, DDR3, DIMM 240-pin, 1600 MHz (PC3-12800), ECC, registered.
4.	Gwarancja	Co najmniej 36 miesięcy gwarancji na dostarczone moduły pamięci. Co najmniej 36 miesięcy gwarancji na posiadane przez Zamawiającego dwa serwery UCS-SP6-C220E (SN: FCH1822V14G, FCH1822V18V).

Tabela 2.2.11. Osprzęt inny (typ 1) – 3 sztuki

l.p.	cecha	wartość
1.	Informacje ogólne	Biblioteka taśmowa (3 zestawy) wraz z taśmami. Zamawiający dysponuje obecnie biblioteką taśmową HP MSL8096 (nr seryjny DEC12801M9) oraz oprogramowaniem zarządzającym obejmującym licencję na 250 slotów na taśmy.
2.	Napędy taśmowe	Biblioteka musi być wyposażona w: Zestaw nr 1: minimum dwa napędy LTO Ultrium-6 FC o wydajności, co najmniej 160MB/s. Zestaw nr 2 i 3: minimum cztery napędy LTO Ultrium-6 FC o wydajności, co najmniej 160MB/s. Każdy napęd musi być wyposażony w dwa interfejsy FC 8Gb/s. Każdy napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie, co najmniej 55-160MB/s.
3.	Pojemność	Biblioteka musi zawierać minimum 80 slotów na taśmy LTO Ultrium-6 oraz co najmniej 10 tzw. „mail slots" umożliwiających wymianę pojedynczej taśmy bez konieczności wyjmowania z modułu całego magazynka z taśmami. Możliwość rozbudowy oferowanej biblioteki do 42 napędów LTO Ultrium-6 i 560 slotów wewnętrznych na taśmy LTO Ultrium-6, poprzez dołączenie dodatkowego modułu w celu utworzenia jednej, większej biblioteki taśmowej ze wspólnym robotem i modułem zarządzania.

4.	Montaż	Wysokość oferowanej (pojedynczego zestawu) biblioteki taśmowej nie może przekraczać 6U. Biblioteka musi być przystosowana do montażu w szafie rack 19”. Urządzenie musi być dostarczone wraz z kompletem elementów montażowych.
5.	Wyposażenie	Biblioteka musi być wyposażona w: Zestaw nr 1: 20 szt. taśm LTO Ultrium-6 RW (o pojemności pojedynczej taśmy, co najmniej 2500GB - bez uwzględniania kompresji danych) wraz z etykietami oraz 2 szt. taśm czyszczących. Zestaw nr 2 i 3: 80 szt. taśm LTO Ultrium-6 RW (o pojemności pojedynczej taśmy, co najmniej 2500GB - bez uwzględniania kompresji danych) wraz z etykietami oraz 2 szt. taśm czyszczących. Dodatkowo należy dostarczyć 20 szt. taśm LTO Ultrium-5 RW o pojemności co najmniej 1500 GB bez kompresji danych.
6.	Zarządzanie	Każda dostarczona biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej.
7.	Wysoka dostępność	Każda dostarczona biblioteka musi być wyposażona w redundantne zasilacze. MTBF musi wynosić, co najmniej 100 000 godzin. MSBF musi wynosić co najmniej 2000 000 pełnych cykli „załaduj/wyładuj”.
8.	Funkcjonalność	Napędy LTO Ultrium-6 muszą posiadać wsparcie dla taśm typu WORM i sprzętową enkrypcję AES 256-bit. Możliwość współpracy ze sprzętowym kluczem USB w celu przechowywania kluczy szyfrujących. Każda biblioteka musi umożliwiać konfigurację 20 odrębnych partycji sprzętowych.
9.	Gwarancja	Każda biblioteka taśmowa, musi być objęta gwarancją o długości co najmniej 36 miesięcy, świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 24 godzin. Dodatkowo obecnie posiadana biblioteka taśmowa zostanie objęta wsparciem serwisowym na 36 miesięcy, świadczonym w miejscu instalacji z gwarancją usunięcia awarii w ciągu 24 godzin.

Tabela 2.2.12. Oprogramowanie (typ 1) – 1 sztuka

l.p.	cecha	wartość
1.	Informacja ogólna	Oprogramowanie do wykonywania kopii zapasowych na dziesięciu napędach taśmowych będących przedmiotem postępowania oraz czterech napędów obecnie posiadanych przez Zamawiającego. Ponadto, Zamawiający posiada obecnie wdrożone oprogramowanie HP DataProtector dla czterech napędów taśmowych wraz z licencjami na 250 slotów na taśmy backupowe. Celem zamówienia jest rozbudowa już wykorzystywanego przez Zamawiającego systemu kopii zapasowych. Napędy taśmowe wraz z oprogramowaniem, licencjami i wdrożeniem Zamawiający otrzymał w wyniku realizacji postępowania przetargowego z dnia 22.06.2011.
2.	Wymagania podstawowe	Oprogramowanie ma zapewnić funkcjonalność scentralizowanego systemu wykonywania kopii backupowych w heterogenicznym (różne systemy operacyjne) środowisku sieci LAN i SAN. W szczególności oprogramowanie musi spełniać następujące wymagania: • Centralną kontrolę wykonywania kopii zapasowych rozproszonego, heterogenicznego systemu komputerowego. Wymagane zaoferowanie odpowiednich licencji. • Wewnętrzna baza danych oraz część systemu realizująca funkcję zarządzania sesjami kopii zapasowych (wraz z nazwami i wersjami zabezpieczanych plików), nośnikami i urządzeniami musi mieć możliwość instalacji na systemach operacyjnych Microsoft Windows oraz Linux. • Zarządzanie całym środowiskiem wykonywania kopii zapasowych z pojedynczej konsoli z wykorzystaniem interfejsu tekstowego CLI oraz graficznego GUI. • Automatyzacja procesu wykonywania kopii zapasowych zgodnie z zaplanowanym harmonogramem (kalendarzem).

		• System musi przechowywać informacje o wykonanych kopiach bezpieczeństwa, wykorzystanych nośnikach oraz urządzeniach w relacyjnej bazie danych. Wymagana jest funkcja wykonania kopii zapasowej bazy danych na taśmy i urządzenia dyskowe w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności. • Możliwość wykonywania różnych typów kopii (całościowa, przyrostowa, różnicowa). • Możliwość wykonywania kopii zapasowych z wykorzystaniem sieci LAN oraz SAN. Wymagane jest zaoferowanie co najmniej 2 licencji typu Klient oraz Media dla wykonywania kopii zapasowych przez sieć LAN oraz SAN. • Możliwość wykonywania kopii zapasowych dla wiodących rozwiązań klastrowych takich jak: Microsoft Cluster Server, HP MC Service Guard, Veritas Cluster, RedHat Cluster, SLES Cluster. • Możliwość wykonywania kopii na różnych nośnikach takich jak taśmy magnetyczne, napędy dyskowe. • Możliwość wykonywania kopii zapasowych w trybie on-line (bez przerywania dostępu do aplikacji) dla pakietów oprogramowania SAP R/3, Oracle, Sybase, Informix, MS Exchange 2010, MS Exchange 2013, MS SQL Server 2008, MS SQL Server 2012, MS Sharepoint 2010, MS SharePoint Fundation 2013, DB2; SAP/ERP2004, Lotus Domino 8.5. • Możliwość wykonywania kopii otwartych plików dla platformy Windows. • Po wykonaniu kopii zapasowej środowiska MS Exchange musi być możliwość odtwarzania pojedynczych obiektów (Granular Recovery) takich jak listy elektroniczne (email), wpisy do kalendarza i kontakty. • Po wykonaniu kopii zapasowej środowiska MS Sharepoint musi być możliwość odtwarzania pojedynczych obiektów (Granular Recovery) takich jak kalendarz, zadania, dokumenty (pliki). • Możliwość odtworzenia pojedynczej skrzynki pocztowej danego użytkownika dla Lotus Domino. • Możliwość wykonywania kopii zapasowych środowisk: Vmware, VMware vCloud Director, Citrix XenServer, Microsoft Virtual Server, Microsoft Hyper-V Server 2012, Sun Solaris Zone, HP Integrity VMs, RedHat KVM. • Możliwość wykonania kopi zapasowej maszyn wirtualnych Vmware ESXi 5.x za pomocą technologii vStorage APIs for Data Protection (VADP). • Po wykonaniu kopii zapasowej maszyn wirtualnych Vmware za pomocą technologii VADP musi być możliwość odtworzenia pojedynczych plików dla zwirtualizowanych systemów MS Windows (Granular Recovery). Operacja odtwarzania plików musi być automatyczna oraz zintegrowana z interfejsem oprogramowania VMware vCenter Server. • Funkcjonalność odtworzenia pojedynczych plików w środowisku Vmware musi być realizowana jednoprzebiegowo. Oznacza to jedną sesję na wykonanie kopii maszyny wirtualnej oraz jedną sesję na odtworzenie plików z urządzenia docelowego.
3.	Funkcjonalności	• Możliwość wykonania kopii zapasowej maszyn wirtualnych Vmware z wykorzystaniem technologii kopii migawkowych macierzy dyskowych (snapshots). Po wykonaniu kopii zapasowej maszyny wirtualnej musi być możliwość odtwarzania z niej pojedynczych plików (Granular Recovery) bezpośrednio z kopii migawkowej wykonanej na macierzy dyskowej (snapshot). • Możliwość wykonania kopi zapasowej środowiska Hyper-V, za pomocą agenta zainstalowanego na systemie Windows z wykorzystaniem technologii kopii migawkowych (snapshots). • Możliwość obsługi bibliotek taśmowych pochodzących od wiodących na świecie producentów. • Efektywne przeszukiwanie nośników z kopiami zapasowymi. • Mechanizmy kompresji i szyfrowania danych przesyłanych siecią

		LAN/WAN. • Możliwość szyfrowania danych na poziomie oprogramowania klienta oraz wsparcie dla szyfrowania sprzętowego w napędach LTO Ultrium 4, LTO Ultrium 5. • Zarządzanie kluczami szyfrującymi dla szyfrowania programowego (klient) oraz sprzętowego (LTO 4, LTO 5) – tworzenie i przechowywanie kluczy; wykorzystywanie przechowywanych kluczy w procesie odtwarzania danych. • Przesyłanie danych kontrolnych oraz metadanych pomiędzy agentami a systemem centralnym musi być szyfrowana w oparciu o protokół Secure Socket Layer (SSL). • Możliwość backupu i odzyskiwania danych zainstalowanych na dyskach skonfigurowanych jako znakowe (raw-devices). • Wsparcie dla technologii NDMP. • Wsparcie dla interfejsu Volume Shadow Copy Services (VSS) na platformie Microsoft Windows. • Wsparcie dla mechanizmu Microsoft Windows Change Journal • Możliwość automatycznego i bezobsługowego odtwarzania danych (Disaster Recovery) w przypadku awarii systemu Windows. Wymagane zaoferowanie odpowiednich licencji, co najmniej 150 klientów/serwerów. • Wsparcie dla różnych metod odtwarzania systemu w przypadku uszkodzenia całej maszyny. Możliwość odtwarzania na dedykowanym serwerze (Windows i UNIX) pełnego obrazu uszkodzonego dysku serwera produkcyjnego na nowym napędzie dyskowym. Nowy dysk może być następnie przewieziony do innej lokalizacji i natychmiast uruchomiony w serwerze, który uległ uszkodzeniu. Wymagane zaoferowanie odpowiedniej licencji, co najmniej 2 klientów/serwerów. • Możliwość współdzielenia zasobów pojedynczej biblioteki taśmowej poprzez wielu klientów/serwery w sieci SAN. Wymagane zaoferowanie odpowiedniej licencji, co najmniej dla 150 klientów/serwerów. • Możliwość współdzielenia robotyki biblioteki taśmowej poprzez wszystkich klientów/serwery w sieci SAN. Wymagane zaoferowanie odpowiedniej licencji. • Możliwość równoległego zapisu tych samych danych (kopii zapasowej) na wiele napędów taśmowych (lub innych mediów). Wymagane zaoferowanie odpowiedniej licencji. • Możliwość jednoczesnego zapisywania wielu strumieni danych na pojedynczym napędzie taśmowym (tzw. multipleksowanie) – min. 32 strumienie. Wymagane zaoferowanie odpowiedniej licencji. • Możliwość migracji kopii danych pomiędzy różnymi typami nośników. Wymagane zaoferowanie odpowiedniej licencji. • Optymalizacja wykorzystania przestrzeni nośników poprzez możliwość usunięcia nieaktualnych kopii danych. Wymagane zaoferowanie odpowiedniej licencji. • Możliwość wykonywania kopii zapasowych poprzez firewall. • Możliwość wygenerowania nośnika z kopiami dla konkretnego klienta/serwera (de-multipleksowania). Wymagane zaoferowanie odpowiedniej licencji. • Dostępna funkcjonalność realizacji zaawansowanego backup'u wielostopniowego typu disk-to-disk-to-tape (D2D2T) • Obsługa technologii deduplikacji danych realizowanej na poziomie agentów (klientów) oferowanego oprogramowania. Dla powyższej funkcjonalności wymagane jest, aby w procesie wykonywania backup'u na przestrzeń dyskową składowane były na niej wyłącznie unikalne bloki danych w skali całego kopiowanego środowiska danej lokalizacji. Bloki są rozumiane, jako podzielone na mniejsze fragmenty dane. System dzieląc

		dane na bloki musi traktować każdy blok, a nie każdą daną indywidualnie, a więc w przypadku modyfikacji, np. z zabezpieczonego serwera pliku (rozumianego jako dana), zachowane przez system mają być wyłącznie te bloki, które są nowe lub uległy zmianie, zamiast całego pliku. • Deduplikacja danych realizowana na poziomie agentów (klientów) oferowanego oprogramowania musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych i dzielić otrzymany strumień danych na bloki o różnej długości. • Obsługa technologii deduplikacji danych realizowana na poziomie urządzenia docelowego, które jest stworzone programowo i przechowuje backup'owane dane na udostępnionych poprzez protokół SCSI zasobach dyskowych. • Wykorzystana technologia deduplikacji realizowana na poziomie agentów musi być taka sama jak w oferowanym urządzeniu docelowym typu biblioteka wirtualna, na którym są przechowywane kopie bezpieczeństwa. Agenci oprogramowania oraz urządzenie fizyczne muszą wykorzystywać ten sam algorytm deduplikacji oraz dane muszą być zapisywane w tym samym formacie. • Obsługa interfejsu programowania aplikacji (API - Application Programming Interface) udostępnianego przez urządzenia docelowe, przechowujące kopie bezpieczeństwa, które wykorzystują ten sam algorytm deduplikacji, co oferowane oprogramowanie. Możliwość wykorzystania API do zarządzania danymi sesji backup przechowywanymi na urządzeniach docelowych, w szczególności wykonanie kopi obiektów pomiędzy urządzeniami używając technologii deduplikacji. • Możliwość integracji z mechanizmami macierzy dyskowych do wykonywania wewnętrznych kopii danych w celu minimalizacji czasu odtworzenia zasobów aplikacji. • Wsparcie dla technologii Zero Downtime Backup (ZDB). Możliwość wykonania kopii bezpieczeństwa danych aplikacji z wykorzystaniem technologii replikacji danych mechanizmami macierzy dyskowej. Wymagane jest, aby oprogramowanie do wykonywania kopii bezpieczeństwa w pełni zarządzało całym procesem ZDB - zarządzało macierzą poprzez uruchomienie kopii migawkowych lub klonów, kontrolowało pracę aplikacji. • Możliwość zautomatyzowanego kopiowania taśm w obrębie jednej biblioteki taśmowej, jak i pomiędzy różnymi bibliotekami taśmowymi. Wymagane zaoferowanie odpowiedniej licencji. • Dostępny moduł zarządzania i kontroli składowania nośników usuwanych z biblioteki (z funkcją automatycznego transportu do portów wymiany, drukowaniem listy usuwanych nośników, monitorowaniem czasu retencji). • Definiowanie uprawnień dla poszczególnych klas użytkowników (co najmniej 3) korzystających z systemu backupów. • Możliwość definiowania różnych strategii wykonywania kopii zapasowych dla poszczególnych obiektów podlegających backupowi. • Możliwość zdefiniowania zarówno automatycznego wykonywania backupów, jak i na żądanie administratora. • Mechanizmy definiowania czasu ochrony nośników. • Możliwość dołączania własnych poleceń przed i po wykonaniu backupu. • Możliwość automatycznego generowania raportów i wysyłania poczty elektronicznej o wykonaniu danej sesji backupowej.
4.	Wymagane licencje	Wymagane jest dostarczenie licencji pozwalających na: • Obsługę dodatkowych dziesięciu napędów LTO udostępnionych w sieci SAN dla wszystkich serwerów podlegających procesowi wykonania kopii

		bezpieczeństwa (wraz z czterema napędami na które Zamawiający obecnie posiada już licencje i oprogramowanie). • Wykonanie kopii bezpieczeństwa online (bez przerywania dostępu do systemu i jego danych) dla trzech systemów środowiska kopii zapasowych. Przez system rozumie się aplikację wspieraną przez oprogramowanie lub serwer fizyczny, na którym uruchomione są maszyny wirtualne Vmware lub MS Hyper-V. Dla systemów Vmware i MS Hyper-V wymagane jest wykonywanie nieograniczonej ilości kopii maszyn wirtualnych bez przerywania ich pracy. Licencja musi uwzględniać liczbę co najmniej 16 rdzeni zainstalowanych w każdym serwerze, na którym jest zainstalowana aplikacja lub środowisko wirtualne. • Wykonanie kopii bezpieczeństwa w technologii disk-to-disk-to-tape (D2D2T) oraz deduplikacji, z wykorzystaniem dyskowych urządzeniach docelowych o sumarycznej pojemności 22TB i możliwości emulacji 150 napędów taśmowych.

Zadanie 3. Infrastruktura przestrzeni dyskowej

Specyfikacja sprzętu i oprogramowania dla zadania nr 3

Tabela 2.3.1. Storage (typ 1) – 1 sztuka

l.p.	cecha	wartość
1.	Wymagana przestrzeń dyskowa	Dostarczona macierz musi być wyposażona w min. 16 dysków o pojemności co najmniej 600GB 2.5” 6G SAS o prędkości co najmniej 15k RPM, minimum 8 dysków o pojemności co najmniej 1.92TB 2.5” 6G SAS SSD cMLC oraz co najmniej 8 dysków o pojemności 6TB 3.5” 6G SAS 7.2k RPM NL.
2.	Architektura	Dostarczona macierz musi być złożona, z co najmniej 2 kontrolerów dyskowych z możliwością rozbudowy bez wymiany kontrolerów obsługujących ruch blokowy (bez stosowania dodatkowych przełączników lub koncentratorów FC / LAN). Wymagane jest, aby możliwość posiadania, co najmniej 4 kontrolerów obsługujących ruch blokowy była cechą oferowanej macierzy.
3.	Obsługa dysków	Dostarczona macierz dyskowa musi umożliwiać obsługę, co najmniej następujących typów dysków instalowanych w ramach macierzy dyskowej: • NL-SAS: 1TB, 2TB, 3TB, 4TB, 6TB • SAS: 300GB 15K RPM, 450GB 10K RPM, 600GB 10K RPM, 900GB 10K RPM, 1,2TB 10K RPM • SSD w technologii SLC, eMLC lub cMLC - 200GB, 400GB, 480GB, 980GB, 1,92TB
4.	Pamięć podręczna	Macierz musi być wyposażona, w co najmniej 96GB pamięci cache. Pojedynczy kontroler musi być wyposażony, w co najmniej 48GB pamięci cache. Jeśli oferowane rozwiązanie zabezpiecza kopią typu „mirror” pamięć „read cache”, wymagane jest, aby zaoferowane było, co najmniej 384GB pamięci cache. Pojemność pamięci cache nie może być osiągnięta poprzez wykorzystanie przestrzeni na dyskach SSD lub dodatkowych kartach z pamięcią flash. Pamięć cache musi mieć możliwość dynamicznej alokacji w zakresie 50 -100% dla odczytów (odpowiednio 50-0% dla zapisów).
5.	Mechanizm oszczędzania przestrzeni dyskowej	Macierz musi zapewnić mechanizm deduplikacji pozwalający na eliminacji powtarzających się bloków danych. Sam proces deduplikacji musi odbywać się na bieżąco, w trakcie działania macierzy (on-line) i nie wpływać negatywnie na wydajność macierzy. W przypadku posiadania odrębnej licencji na wymaganą funkcjonalność licencja musi obejmować całą dostarczoną pojemności macierzy.
6.	Liczba portów zewnętrznych	Macierz musi posiadać minimum 4 portów FC 8 Gb/s (wszystkie z możliwością obsługi zdalnej replikacji danych do macierzy zapasowej). Macierz musi posiadać możliwość rozbudowy do minimum 24 portów FC

		(bez stosowania dodatkowych przełączników lub koncentratorów FC). Macierz musi posiadać możliwość instalacji min. 4 portów FCoE/iSCSI. Macierz musi mieć możliwość instalacji minimum 8 portów 1/10GbE do obsługi funkcjonalności plikowej NFS/CIFS bez stosowania dodatkowych urządzeń zewnętrznych typu Główka/Gateway.
7.	Ochrona danych	Macierz musi obsługiwać mechanizmy RAID w konfiguracji: RAID-1, RAID-5, RAID-6, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i wykorzystaniem wszystkich typów dysków twardych, w tym flash/SSD. Wymagane jest, aby oferowana macierz pozwalała na tworzenie i istnienie w tym samym czasie dysków logicznych zabezpieczonych różnymi poziomami RAID na tych samych dyskach fizycznych. Dopuszcza się rozwiązania, które nie umożliwiają tej funkcjonalności, w takim przypadku wymagane jest dostarczenie dodatkowo 30% przestrzeni dyskowej opisanej w punkcie „Wymagana przestrzeń dyskowa" wraz z niezbędnymi licencjami.
8.	Wysoka dostępność	Macierz musi być odporna na awarię pamięci cache i zapewniać zrzut zawartości pamięci cache na pamięć nieulotną (Flash/SSD) w razie utraty zasilania.
9.	Wysoka dostępność	Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez zauważalnego zanikania ścieżek dostępu do zasobów dyskowych macierzy.
10.	Wysoka dostępność	Macierz musi mieć zdublowane płyty pamięci cache (podział pamięci cache, na co najmniej dwie redundantne karty, zasilane dwoma obwodami zasilania), płyty interfejsów FC (podział interfejsów FC, na co najmniej dwie redundantne karty, zasilane dwoma obwodami zasilania), kontrolery macierzowe oraz zasilacze/wentylatory (odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy).
11.	Skalowalność	Macierz musi posiadać możliwość rozbudowy do co najmniej 500 dysków. Macierz musi posiadać możliwość rozbudowy za pomocą nowych dysków o większych pojemnościach oraz możliwość rozbudowy do min. 200 dysków typu flash/SSD o pojemności, co najmniej 1,9TB.
12.	Wolumeny logiczne	Macierz musi wspierać kreowanie wolumenów logicznych w rozmiarach, co najmniej 16TB.
13.	Mechanizmy Thin Provisioning	Macierz musi mieć możliwość udostępniania zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu "Thin Provisioning". Dla wolumenów tego typu musi istnieć możliwość automatycznej, ciągłej reklamacji zwalnianej przestrzeni poprzez wykrywanie zer. Jest wymagane dostarczenie licencji dla tej funkcjonalności dla całej dostarczanej pojemności macierzy.
14.	Zarządzanie grupami dyskowymi i dyskami logicznymi	Macierz musi zapewniać możliwość dynamicznego zwiększania pojemności woluminów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych. Musi być możliwość zdefiniowania, co najmniej 8000 woluminów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego dysku/woluminu logicznego na wszystkie dyski fizyczne macierzy, bez konieczności łączenia wielu różnych dysków logicznych w jeden większy (tzw. wide striping).
15.	Możliwość migracji danych w obrębie macierzy	Macierz musi umożliwiać migrację danych, bez przerywania do nich dostępu, pomiędzy różnymi warstwami technologii dyskowych: flash/SSD, SAS, Nearline SAS/SATA oraz różnych poziomów RAID na poziomie całych woluminów logicznych. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jest wymagane dostarczenie licencji dla tej funkcjonalności dla całej dostarczanej pojemności macierzy.
16.	Możliwość migracji danych w obrębie macierzy	Macierz musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych: Flash/SSD, SAS/FC, Nearline SAS/SATA na poziomie części woluminów logicznych (ang. Sub

		LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach/warstwach dysków obsługiwanych przez macierz (Flash/SSD, SAS, NL SAS/SATA), a jego części będą automatycznie i transparentnie dla korzystającego z tego LUNa hosta/hostów realokowane w trybie online na podstawie analizy ruchu. Macierz musi umożliwiać relokację bloków danych, w trybie real-time (z pominięciem interwałów czasowych), pomiędzy minimum dwoma warstwami dyskowymi: 1) dyski SSD/Flash, 2) dyski SAS/NL. Jest wymagane dostarczenie licencji dla tej funkcjonalności dla całej dostarczanej pojemności macierzy.
17.	Wewnętrzne kopie danych	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 500 kopii migawkowych per wolumen logiczny i minimum 4000 wszystkich kopii migawkowych. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wykonana kopia danych musi mieć możliwość zabezpieczenia innym poziomem RAID. Musi być możliwość wykonania kopii w innej grupie dyskowej niż dane oryginalne. Aktualnie nie jest wymagane dostarczenie licencji dla tej funkcjonalności. Możliwość aktywowania za pomocą licencji w przyszłości.
18.	Wewnętrzne kopie danych	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wykonana kopia danych musi mieć możliwość zabezpieczenia innym poziomem RAID. Musi być możliwość wykonania kopii w innej grupie dyskowej niż dane oryginalne. Jest wymagane dostarczenie licencji dla tej funkcjonalności dla całej dostarczanej pojemności macierzy.
19.	Zdalna replikacja danych	Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń zewnętrznych i bez obciążania serwerów podłączonych do macierzy. Musi istnieć możliwość jednoczesnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem różnych infrastruktur (FC, sieci IP). Macierz musi umożliwiać replikację zdalną w następujących trybach: jeden do jednego, jeden do wielu, wiele do jednego, replikację jednego wolumenu logicznego (tych samych danych) do dwóch innych, niezależnych ośrodków za pomocą replikacji synchronicznej i asynchronicznej. Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zamiany ról oryginału i kopii (dla określonej pary dysków logicznych LUN macierzy) z poziomu interfejsu administratora. Musi być możliwość integracji z klastrami geograficznymi, co najmniej MSCS oraz VMware SRM. Macierz musi znajdować się na aktualnej liście VMware Compatibility Guide – SAN/Storage dla rozwiązania FC Metro Cluster Storage. Aktualnie nie jest wymagane dostarczenie licencji dla tej funkcjonalności. Możliwość aktywowania za pomocą licencji w przyszłości
20.	Wydajność	Macierz musi umożliwiać ograniczenie wydajności wybranych wolumenów/ grup wolumenów na poziomie max IOPS i max MB/s.

		Jest wymagane dostarczenie licencji dla tej funkcjonalności dla całej dostarczanej pojemności macierzy.
21.	Administracja	Zarządzanie macierzą musi być możliwe z poziomu pojedynczego interfejsu graficznego i interfejsu znakowego. Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz możliwość konfigurowania jej zasobów dyskowych. Wymagane jest również monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, wewnętrznych, grup dyskowych, dysków logicznych (LUN), pojedynczych napędów dyskowych oraz kontrolerów. Konieczne jest gromadzenie historycznych danych wydajnościowych. Oprogramowanie zarządzające musi umożliwiać reakcje na zdarzenia, np. wysłanie powiadomienia do administratora lub uruchomienie skryptu.
22.	Obsługa wielu ścieżek	Macierz musi obsługiwać wiele kanałów I/O (Multipathing). Musi być zapewnione automatyczne przełączanie kanału I/O w wypadku awarii ścieżki dostępu serwerów do macierzy z utrzymaniem ciągłości dostępu do danych i bez zauważalnej reakcji ze strony mechanizmów MPIO na systemach operacyjnych korzystających z zasobów macierzy serwerów. Musi być zapewnione przełączanie kanałów I/O oparte o natywne mechanizmy systemów operacyjnych wspieranych przez macierz. Wymagana jest również obsługa równoważenia obciążenia (load balancing) pomiędzy kanałami macierzy. W szczególności musi istnieć możliwość równomiernego rozłożenia obciążenia pojedynczego LUN na wszystkie interfejsy macierzy. Wymagane jest dostarczenie odpowiednich licencji do obsługi ww. funkcjonalności dla nielimitowanej liczby serwerów.
23.	Gwarancja	36 miesięcy świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 6 godzin.

Tabela 2.3.1. Osprzęt sieciowy (typ 12) – 2 sztuki

l.p.	cecha	wartość
1.	Wymagania podstawowe	• Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. • W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. • W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. • Przełącznik FC musi być wyposażony, w co najmniej 24 aktywne porty FC obsadzone wkładkami SFP 8Gb/s. • Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC. • Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 768 Gb/s end-to-end full duplex. • Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 700ns. • Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.
2.	Montaż	Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość

		montażu w szafie 19”. Wraz z urządzeniem należy dostarczyć komplet elementów montażowych do szafy rack 19” umożliwiających bezpieczny montaż urządzenia.
3.	Pobór mocy	Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 wkładki SFP 16Gb/s nie może przekroczyć 80W.
4.	Zasilanie i chłodzenie	Przełącznik FC musi posiadać przynajmniej 2 nadmiarowe zasilacze i co najmniej 2 wentylatory, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika.
5.	Firmware	Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.
6.	Agregacja połączeń	Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.
7.	Balans ruchu	Przełącznik FC musi wspierać mechanizm balansowania ruchu, pomiędzy co najmniej 3 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.
8.	Przepustowość	Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Jednoczesne wykorzystanie obu mechanizmów powinno zapewnić dla dowolnej pary komunikujących się urządzeń końcowych uzyskanie kanału komunikacyjnego o zagregowanej przepustowości 384Gb/s half duplex.
9.	Zoning	Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
10.	Bezpieczeństwo	Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: • mechanizm szyfrowania i kompresji wybranych połączeń ISL wspierany, na co najmniej 2 portach przełącznika FC. Symetryczny klucz szyfrujący nie może być krótszy niż 256-bitów, • mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric, • uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP, • uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP, • szyfrowanie połączenia z konsolą administracyjną, wsparcie dla SSHv2, • definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control), • definiowane kont administratorów w środowisku RADIUS i LDAP, • szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS, • obsługa SNMP v1 oraz v3, • IP Filter dla portu administracyjnego przełącznika, • wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP, • wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP.
11.	Zarządzanie	Przełącznik FC musi mieć możliwość konfiguracji przez: • polecenia tekstowe w interfejsie znakowym konsoli terminala,

		• przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, port szeregowy (RJ-45) oraz inband IP-over-FC. Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S.
12.	Narzędzia diagnostyczne	Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC: • logowanie zdarzeń poprzez mechanizm „syslog”, • monitoring wydajności end-to-end umożliwiający pomiar przepustowości między wybranymi parami komunikujących się urządzeń, • monitorowanie połączeń fizycznych i połączeń typu „trunk, • ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administrator musi być możliwe za pomocą wysyłania wiadomości e-mail. Dostarczenie licencji aktywującej tę funkcjonalność nie jest wymagane, • port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla wkładek SFP 16Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric, • FCping, • FC traceroute, • kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika.
13.	Rozbudowa	Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 8Gb/s.
14.	Kategoryzacja ruchu	Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie.
15.	Wymagania dodatkowe	• Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. • Przełącznik musi być wyposażony w mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy. • Przełącznik musi być wyposażony w mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe.
16.	Gwarancja	Gwarancja i wsparcie: 36 miesięcy świadczona w miejscu instalacji z gwarancją usunięcia awarii w ciągu 6 godzin.

Zadanie 4. Infrastruktura przestrzeni dyskowej

Specyfikacja sprzętu i oprogramowania dla zadania nr 4

Tabela 2.4.1. Storage (typ 2) – 2 sztuki

l.p.	cecha	wartość
1.	Wymagania funkcjonalne	1. Pojemność całkowita użyteczna oferowanego rozwiązania pamięci dyskowej na dane użytkowników musi wynosić nie mniej niż 125TB w

		obrębie jednego systemu plików po sformatowaniu przy zachowaniu dostępu do danych w przypadku awarii co najmniej trzech dowolnych dysków jednocześnie w jednej zabezpieczonej grupie dysków lub jednego węzła czy półki dyskowej wraz z dyskami, które zawiera dana półka. 2. Dla maksymalizacji gęstości w przechowywaniu danych, półka dyskowa lub węzeł stanowiący element rozwiązania pamięci dyskowej musi zawierać nie mniej niż 36 dysków typu NL-SAS w obudowie o wysokości nie większej niż 4U. 3. Pojemność użyteczna oferowanego rozwiązania pamięci dyskowej na dane użytkowników musi wynosić nie mniej niż 60% całkowitej pojemności. 4. Oferowane rozwiązanie pamięci dyskowej musi udostępniać całkowitą dostępną przestrzeń w ramach jednego systemu plików. 5. Oferowane rozwiązanie pamięci dyskowej musi zapewniać dostępną łączną pojemność pamięci cache typu RAM nie mniejszą niż 144 GB. Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci na dodatkowych kartach rozszerzeń lub dyskach SSD. 6. Oferowane rozwiązanie pamięci dyskowej musi posiadać nie mniej niż 6 CPU, a każdy CPU powinien zawierać nie mniej niż 4 rdzenie. 7. Oferowane rozwiązanie pamięci dyskowej musi powinno zapewniać dostęp do danych wykorzystując jednocześnie porty typu 1 Gigabit Ethernet i 10 Gigabit Ethernet. 8. Oferowane rozwiązanie pamięci dyskowej musi posiadać nie mniej niż 6 portów 1 Gigabit Ethernet oraz nie mniej niż 6 portów typu 10 Gigabit Ethernet. Sumaryczna wydajność portów zapewniających dostęp do danych (od strony serwerów i sieci LAN) musi być nie mniejsza niż 60 Gbps. 9. Oferowane rozwiązanie pamięci dyskowej do komunikacji półek dyskowych lub węzłów musi posiadać dodatkowe dedykowane porty w liczbie co najmniej 6 lub więcej o łącznej przepustowości nie mniejszej niż 120 Gbps. Wymagane jest zastosowanie dedykowanych dodatkowych przełączników (nie mniej niż 2 przełączniki) zapewniających komunikację między półkami dyskowymi lub węzłami.
2.	Wymagania dot. niezawodności	1. Oferowane rozwiązanie pamięci dyskowej musi być całkowicie dostępne (on-line) i wszystkie dane w pełni dostępne w przypadku awarii, która ma wpływ na minimalnie jeden kontroler/jedną półkę dyskową . 2. Oferowane rozwiązanie pamięci dyskowej musi zapewniać zabezpieczenie danych w przypadku utraty do czterech dysków lub kontrolerów jednocześnie. 3. Oferowane rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych.
3.	Oprogramowanie	1. Oferowane rozwiązanie pamięci dyskowej musi być w stanie zarządzać dyskami SAS, SATA oraz SSD w jednym systemie plików. 2. Oferowane rozwiązanie pamięci dyskowej musi zapewniać automatyczne rozszerzanie pojemności systemu plików bez konieczności modyfikacji już zainstalowanych kontrolerów, restartu systemu oraz ręcznej migracji/dystrybucji danych na nowe dyski system, w oparciu o całą pojemność fizyczną dodawaną do klastra bez warstwy wirtualizacyjnej systemu. System plików zawarty w oferowanym rozwiązaniu musi być skalowalny do co najmniej 30 PB powierzchni netto. 3. Oferowane rozwiązanie pamięci dyskowej musi realizować replikację asynchroniczną danych na poziomie pojedynczego katalogu celem dystrybucji treści i zapewnienia kopii danych w ośrodku zapasowym. 4. Oferowane rozwiązanie pamięci dyskowej musi pozwalać na rozbudowę o funkcjonalność wykonywania kopii migawkowych (snapshot'ów) dla wybranych folderów w interwałach czasowych i czasach retencji definiowanych przez administratora systemu. 5. Oferowane rozwiązanie pamięci dyskowej musi mieć możliwość

		rozbudowy o wykonywanie co najmniej 1000 kopi migawkowych (snapshotów) per katalog/share oraz pozwalać na nielimitowaną ilość snapshotów dla całego filesystemu w celu zapewnienia lokalnej ochrony danych. 6. Każdy z systemów pamięci masowej musi wspierać integracje kopi migawkowych z usługą VSS firmy Microsoft. 7. Oferowane rozwiązanie pamięci dyskowej musi posiadać możliwość rozbudowy o funkcjonalność tworzenia limitów na przechowywanie danych dla wybranych użytkowników lub grup użytkowników (tzw. quoty). Zamawiający nie dopuszcza wykorzystania oprogramowania firm zewnętrznych czy OEM. 8. Oferowane rozwiązanie pamięci dyskowej musi zapewniać możliwość obsługi deduplikacji na poziomie bloków o wielkości 8kb dla wyznaczonych katalogów. Zamawiający nie dopuszcza wykorzystania oprogramowania firm zewnętrznych czy OEM. 9. Oferowane rozwiązanie musi zapewniać możliwość zastosowania technologii szyfrowania typu SED lub równoważnej na wszystkich napędach dyskowych. 10. Oferowane rozwiązanie pamięci dyskowej musi obsługiwać RAN APIs (RESTful Access to Namespace) lub równoważne dla aplikacji zewnętrznych. 11. Oferowane rozwiązanie pamięci dyskowej musi zapewniać możliwość rozbudowy o technologię migracji danych między warstwami dysków (tiers) w ramach jednego systemu plików i przestrzeni nazw. 12. Oferowane rozwiązanie pamięci dyskowej musi mieć możliwość zastosowania mechanizmu WORM oraz być zgodne ze standardem regulacji SEC 17a-4. 13. Administracja systemem musi odbywać się poprzez Web GUI oraz Command Line Interface. 14. Monitorowanie SNMP musi być włączone i obsługiwane w systemie.
4.	Dostęp do danych	1. Oferowane rozwiązanie pamięci dyskowej musi łączyć się do wszystkich sieci klientów bez konieczności instalowania jakiegokolwiek oprogramowania na klientach. 2. Oferowane rozwiązanie pamięci dyskowej musi umożliwiać rozbudowę o funkcjonalność load balancingu połączeń bez stosowania dodatkowej aplikacji na stacji klienckiej lub zewnętrznych urządzeń równoważących obciążenie. oraz pozwalać na ustawienie różnej przepustowości dla różnych klientów aby spełnić szczególne wymagania wydajnościowe. 3. Rozwiązanie powinno zapewnić dostęp do zasobów z różnych systemów operacyjnych (Mac, Linux, Windows) przy użyciu następujących protokołów udostępniania plików co najmniej: NFS, CIFS, HTTP, oraz FTP Rozwiązanie powinno obejmować wszystkie usługi protokołu bez dodatkowych licencji i sprzętu. 4. Rozwiązanie musi zapewnić dostęp do zasobów z różnych systemów operacyjnych (Mac, Linux, Windows) przy użyciu protokołu HDFS bez rozbudowy sprzętowej
5.	Integralność danych, ochrona i dostępność	1. Każdy z systemów pamięci masowej musi zapewnić gwarantowaną ochronę przed „cichym uszkodzeniem dysków” (silent data corruption) podczas korzystania z wszystkich typów dysków twardych (w tym SATA). 2. Oferowane rozwiązanie pamięci dyskowej musi być w pełni dostępny dla hostów w sieci LAN i wszystkie dane w pełni dostępne w przypadku awarii, która ma wpływ na jeden kontroler lub dwa dyski w systemie. 3. Oferowane rozwiązanie pamięci dyskowej musi być w pełni on-line i wszystkie dane w pełni dostępne w przypadku awarii dowolnej półki dyskowej. 4. Oferowane rozwiązanie pamięci dyskowej musi obsługiwać protokół NDMP w wersji 3 oraz 4 dla kopii zapasowych na taśmach z jakiegokolwiek obszaru systemu plików

6.	Skalowalność, pojemność i wydajność	1. Oferowane rozwiązanie pamięci dyskowej musi być skalowalne do co najmniej 250 CPU przy wykorzystaniu 1000 rdzeni. 2. Oferowane rozwiązanie pamięci dyskowej musi być skalowalne do 6TB (6144GB) pamięci RAM, nie dopuszcza się realizacji pamięci na dodatkowych kartach rozszerzeń lub dyskach SSD. 3. Oferowane rozwiązanie pamięci dyskowej musi dawać możliwość rozbudowy do 1.25PB w jednej 19-calowej szafie montażowej RACK o głębokości 1200 mm. 4. Oferowane rozwiązanie powinno umożliwiać zwiększenie wydajności i pojemności. Rozszerzenie wydajności musi być możliwe do poziomu co najmniej 6GB/sec przepustowości zarówno dla operacji odczytu i zapisu oraz przynajmniej 30PB netto pojemności w obrębie jednego systemu plików. 5. Oferowane rozwiązanie pamięci dyskowej musi umożliwiać zwiększenie dwukrotne pojemności i wydajności bez wprowadzania zmian do zaproponowanych kontrolerów. 6. Oferowane rozwiązanie pamięci dyskowej musi mieć możliwość skalowania zachowując pełny dostęp do danych przy dodawaniu kolejnych węzłów.
7.	Gwarancja i serwis	1. Serwis gwarancyjny producenta na całość oferowanego rozwiązania na okres nie krótszy niż 3 lata. Serwis gwarancyjny powinien być świadczony przez 24 h na dobę 365 dni w roku. Czas dostawy części zamiennych: najpóźniej następny dzień roboczy. W przypadku awarii wymagających wizyty inżyniera Dostawcy w miejscu instalacji: czas rozpoczęcia pracy w miejscu instalacji najpóźniej następny dzień roboczy. Czas usunięcia awarii: nie dłużej niż 14 dni kalendarzowych. Serwis gwarancyjny powinien umożliwiać pobieranie aktualizacji oprogramowania. 2. Dostawca przeprowadzi instruktaż dla pracowników Zamawiającego z zakresu zarządzania i administracji oferowanej macierzy dyskowej autoryzowany przez producenta tej macierzy. 3. Wszystkie uszkodzone dyski w czasie trwania gwarancji pozostają u Zamawiającego.
8.	Zarządzanie	1. Rozwiązanie musi obsługiwać uwierzytelnianie użytkowników i administratorów co najmniej z NIS, LDAP i Active Directory. 2. Oferowane rozwiązanie pamięci dyskowej musi obsługiwać mechanizm wielodostępowy zarówno dla protokołu CIFS jak i NFS. 3. Oferowane rozwiązanie pamięci dyskowej musi zapewnić obsługę alertów i mieć możliwość monitorowania za pomocą protokołu SNMP. 4. Oferowane rozwiązanie pamięci dyskowej powinno umożliwiać przegląd historii wydajności pamięci masowej. 5. Oferowane rozwiązanie pamięci dyskowej musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. 6. Każde z urządzeń proponowanego rozwiązania musi zapewniać możliwość montażu w 19-calowych szafach montażowych RACK o głębokości 1200 mm. Do każdego oferowanego urządzenia należy dołączyć komplet elementów montażowych do 19 calowej szafy RACK o głębokości 1200 mm zapewniających pełne wysunięcie każdego urządzenia z szafy RACK bez konieczności odłączania okablowania i kompletu kabli zasilających (C13-C14 lub C19-C20).

Zadanie 5. Infrastruktura przestrzeni dyskowej

Specyfikacja sprzętu i oprogramowania dla zadania nr 5

Tabela 2.5.1. Storage (typ 3) – 1 sztuka

l.p.	cecha	wartość

1.	Wymagania podstawowe	1) Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. 2) Macierz musi być wyposażona w co najmniej 2 kontrolery pracujące w trybie Active/Active zajmujących się obsługą dostępu do dysków, z możliwością wsparcia dla protokołów blokowych: FC, FCoE i iSCSI. 3) Kontrolery macierzy obsługujące przestrzeń dyskową powinny być wyposażone w pamięć cache o pojemności, co najmniej 256 GB do buforowania operacji zapisu i odczytu dla wszystkich wolumenów macierzy, również po rozbudowie o dowolny typ dysku wymieniony w pkt 52. Wymagana wartość pojemności jest wartością netto po uwzględnieniu wymaganych zabezpieczeń za pomocą kopii lustrzanej. Pamięć cache (do odczytu i zapisu) musi mieć możliwość rozbudowy do 512GB. 4) Macierz musi być odporna na awarię pamięci cache, w szczególności pamięci cache przeznaczonej do zapisu (ang. Write cache) i zapewniać w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez nieograniczony czas. Pamięć cache do zapisu powinna być zabezpieczona za pomocą funkcjonalności kopii lustrzanej (mirror). Cała macierz musi być zabezpieczona przez nieograniczony czas przed utratą danych w przypadku awarii zasilania. Macierz musi być wyposażona w wewnętrzny system podtrzymywania bateryjnego, pozwalający, w przypadku utraty zasilania wykonanie zapisu danych z pamięci cache na dyski twarde (opróżnienie buforu zapisania) i bezpieczne wyłącznie macierzy. Jeśli oferowana macierz nie posiada takiej opcji Zamawiający dopuszcza dostarczenie oddzielnego modułu UPS wraz z oprogramowaniem/skryptami automatyzującymi zrzut danych w przypadku braku dostępu do zasilania. Producent UPS i/lub skryptów musi zagwarantować kompatybilność rozwiązania. 5) Urządzenie powinno być wyposażone w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwalność pracy i utrzymanie funkcjonalności macierzy w szczególności działania pamięci cache w przypadku awarii jednego ze źródeł zasilania. 6) Biorąc pod uwagę możliwość przyszłej rozbudowy środowiska wymagane jest aby pojedynczy port FC miał możliwość obsługi przynajmniej 255 host inicjatorów a cała macierz obsługiwała 2048 host inicjatorów. 7) Oferowane urządzenie musi być wyposażone w co najmniej 8 portów FC typu 8Gbps. Wszystkie porty FC muszą być wyposażone w niezbędne moduły SFC lub inne oraz patchcordy do podłączenia do przełącznika sieci SAN, wyposażonego w porty FC pracujące z prędkością 8/16Gb. Macierz powinna mieć możliwość rozbudowy do 16 portów FC 8Gbps bez dokładania dodatkowych kontrolerów (modułów odpowiedzialnych za obsługę zarządzanej przestrzeni dyskowej, jej konfigurację, liczenie RAID oraz wyposażonych w pamięć cache do obsługi buforowania operacji odczytu i zapisu). 8) Macierz musi pozwalać na obsługę dysku logicznego przez wszystkie kontrolery macierzy jednocześnie, w sposób symetryczny. 9) Macierz dyskowa musi umożliwiać stosowanie w niej dysków SSD, HDD 15k, HDD 10k i HDD 7,2k rpm wyposażonych w interfejsy SAS 6Gbps (SAS, NL-SAS) lub FC 4Gbps (FC, SATA), zarówno 2,5" jak i 3,5". 10) Macierz musi być wyposażona w dyski posiadające podwójne interfejsy. 11) Macierz musi być wyposażona w globalne dyski zapasowe dla dysków danych w liczbie wynikającej z udokumentowanych zaleceń producenta

		macierzy. 12) Macierz musi mieć możliwość instalacji dysków SSD, SAS, NL-SAS w tej samej półce dyskowej. 13) Macierz musi umożliwiać rozbudowę do 240 napędów dyskowych w obrębie pojedynczego urządzenia jedynie poprzez dołożenie dodatkowych półek dyskowych. 14) Oferowana macierz musi zostać wyposażona, w przynajmniej: a. 10 dysków typu SSD o pojemności co najmniej 200 GB każdy, b. 48 dysków typu SAS/FC o pojemności co najmniej 900 GB każdy, o prędkości obrotowej co najmniej 10 tys RPM c. 29 dysków NL-SAS/FC o pojemności co najmniej 4000 GB każdy, o prędkości obrotowej co najmniej 7,2 tys RPM d. oraz niezbędne dyski zapasowe (tzw. hot-spare) zgodnie z zaleceniami producenta macierzy (jednak nie mniej niż 4 sztuki) w tym: 1xSSD, 2x900GB/SAS , 1x4TB/NL-SAS, 15) Połączenia między dyskami a kontrolerami powinny być wykonane w technologii SAS 6Gbps. 16) Rozwiązanie musi pozwalać w przyszłości na rozbudowę, do co najmniej 1000 napędów dyskowych. 17) Ze względu na ograniczoną ilość miejsca w szafie RACK, wymaga się aby oferowane rozwiązanie umożliwiało zastosowanie półek dyskowych o większej gęstości upakowania na poziomie 60 dysków 3.5” w półce o wysokości nie większej niż 4U. 18) Wymagana jest obsługa min 24 dysków 2,5" w półce o wysokości max 2U oraz możliwość obsługi 12 dysków 3,5" w obrębie jednej półki o wysokości max 3U. 19) Macierz musi umożliwiać równoczesną obsługę wielu poziomów RAID. Ze względu na zakładane przeznaczenie niniejszego urządzenia zamawiający wymaga, by obsługiwało ono, co najmniej RAID 0, 1, 5, 6. 20) Macierz musi umożliwiać deduplikację na poziomie blokowym. Wymaga się dostarczenia licencji na całą oferowaną pojemność. 21) Blokowa deduplikacja danych musi działać globalnie, t.j. deduplikować bloki znajdujące się na różnych wolumenach (LUN-ach). 22) Blokowa deduplikacja danych musi obejmować dane znajdujące się w pamięci cache kontrolerów macierzy. 23) Macierz musi umożliwiać blokową deduplikację danych na wolumenach objętych autotieringiem. 24) Macierz musi posiadać możliwość włączenia kompresji udostępnianych obszarów. Niezbędne jest dostarczenie odpowiedniej licencji na tą funkcjonalność na pełną pojemność macierzy dla wszystkich wymaganych protokołów udostępniania danych. 25) Macierz musi obsługiwać lun masking, lun mapping i inicjowanie startu systemów operacyjnych. Należy dostarczyć licencje dla maksymalnej wspieranej liczby serwerów podłączonych do macierzy. 26) Macierz musi umożliwiać migrację dysków logicznych na i z macierzy dyskowych innych producentów z wykorzystaniem wewnętrznych mechanizmów macierzy. Wymagane jest dostarczenie licencji na całą

		oferowaną pojemność macierzy. 27) Macierz musi umożliwiać przenoszenie całych dysków logicznych (LUN) udostępnionych do hostów pomiędzy poszczególnymi obszarami macierzy dyskowej bez przerywania dostępu do danych i pracy aplikacji korzystających z tych dysków.
2.	Oprogramowanie	28) Oprogramowanie powinno umożliwiać monitorowanie i raportowanie (w zakresie dostarczanych macierzy dyskowych) zasobów blokowych. Wymagana jest funkcjonalność raportowania (generacji raportów), co najmniej w zakresie: a) przestrzeni macierzy - całościowa, wolna, wykorzystywana, skonfigurowana-nieprzydzielona dla aplikacji, b) przestrzeni macierzy jw. z podziałem na poszczególne grupy RAID/storage pool'e/wolumeny logiczne, c) wydajności - mierzonej w IOPS oraz MB/s dla zasobów blokowych, d) utylizacji kontrolerów części blokowej macierzy, e) raportów capacity planning - prezentujących trendy czasowe w zakresie przestrzeni oraz wydajności macierzy (dla obszarów parametrów podanych powyżej - w punktach a i b), f) raporty inwentarzowe, prezentujące skonsolidowane zestawienia zasobów fizycznych macierzy, wolumenów logicznych, pul dyskowych, podłączonych hostów, wraz z odpowiednimi szczegółami dla poszczególnych kategorii, g) raporty dla zasobów korzystających z mechanizmu "Thin Provisioningu", zawierające szczegóły dotyczące wykorzystania zasobów, over-subskrypcji oraz trendów/prognoz konsumpcji zasobów. 29) Oprogramowanie powinno posiadać funkcjonalność rozliczania wykorzystywanych zasobów storage, tzw. chargeback. 30) Dostarczone oprogramowanie powinno umożliwiać tworzenie i generowanie własnych raportów (tzw. custom reports) - w zakresie raportowania wydajności i pojemności (capacity). 31) Oprogramowanie powinno umożliwiać eksportowanie generowanych raportów (mechanizmami wbudowanymi) do zewnętrznych, ogólnie stosowanych formatów plikowych - wymagane co najmniej formaty PDF, XLS oraz CSV, oraz możliwość automatycznego wysyłania wygenerowanych raportów pocztą elektroniczną. 32) Macierz musi być wyposażona w funkcjonalność zarządzania poziomem usług (ang. Quality of Service) poprzez możliwość określania wartości „nie większej niż” oraz „wymagane” dla następujących parametrów dostępu do dysku logicznego: a. Ilość operacji na sekundę (IOPS), b. Przepustowość (MB/s). 33) Macierz musi mieć możliwość rozbudowy o funkcjonalność automatycznego tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych, w zależności od stopnia wykorzystania danego obszaru przez aplikację – jeśli niniejsza funkcjonalność wymagałaby zakupu dodatkowej licencji w przyszłości, wtenczas Zamawiający wymaga zaoferowania jej w niniejszym postępowaniu. Migracje muszą być wykonywane automatycznie bez udziału administratora. Pojedynczy migrowany obszar nie może być większy niż

		256MB. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji. Funkcjonalność tieringu musi być możliwa pomiędzy wszystkimi typami stosowanych dysków (SSD, SAS/FC, NLSAS/SATA). 34) Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych. 35) Macierz musi zapewniać mechanizm Thin Provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała przydzielonej pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy. 36) Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (ang. Space reclamation). 37) Macierz musi oferować integrację z platformą Microsoft w zakresie wsparcia dla SCVMM, SCO, SCOM w wersji 2012R2 oraz musi oferować integrację z platformą VMware vSphere (ESX) w ramach vStorage API.
3.	SLA	38) Macierz musi oferować funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy. 39) Oferowane urządzenie musi być objęte co najmniej 3-letnim wsparciem i gwarancją producenta sprzętu w trybie NBD w miejscu instalacji sprzętu. Nie dopuszcza się ograniczeń gwarancji związanych z ilością zapisów do dysków SSD. Uszkodzone dyski pozostają u Zamawiającego.
4.	Wymagania dodatkowe	40) Oferowane urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 2 miesiące przed dostawą i pochodzić z autoryzowanego kanału dystrybucji producenta w Polsce. 41) Urządzenia oraz ich oprogramowanie wewnętrzne musi być objęte opieką serwisową producenta przez okres 3 lat. W okresie opieki wymagany jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii w trybie NBD oraz dostęp do wszystkich nowszych wersji oprogramowania. 42) Oprogramowanie (wbudowane) macierzy musi wspierać szyfrowanie danych na obsługiwanych woluminach z wykorzystaniem algorytmu szyfrującego o długości klucza minimum 256-bitów. 43) Oprogramowanie macierzy musi wspierać zabezpieczenie danych przed lokalnymi uszkodzeniami, przerwami w zasilaniu, fizycznymi uszkodzeniami 44) Oferowana macierz powinna posiadać odpowiednie okablowanie i moduły wymagane do uruchomienia w środowisku sieci SAN. 45) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik nie wymagający stosowania zasilania zewnętrznego lub bateryjnego. 46) Kontrolery muszą posiadać możliwość ich wymiany bez konieczności wyłączania zasilania całego urządzenia – dotyczy konfiguracji z dwoma kontrolerami RAID. 47) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę

		WWW oraz w trybie tekstowym. Pełne zdalne zarządzanie macierzą powinno być możliwe bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora. Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW. 48) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego i kontrolerów RAID bez konieczności wyłączania macierzy lub bez konieczności wyłączania ścieżek logicznych FC/iSCSI/FCoE dla podłączonych stacji/serwerów. Macierz musi umożliwiać dokonywanie w trybie on-line(tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji: - zmiana rozmiaru woluminu, - migracja woluminu na grupę dyskową z innym poziomem RAID, - migracja woluminu na grupę dyskową z dyskami innej technologii, - dodawanie nowych dysków do istniejącej grupy dyskowej 49) Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej bez konieczności dedykowania oddzielnego serwera do obsługi tego oprogramowania. 50) Macierz musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server 2012R2, RedHat Linux, HP-UNIX, VMWare 5.0/5.5 51) Macierz musi obsługiwać woluminy logiczne o maksymalnej pojemności min. 60TB. 52) Macierz dyskowa musi umożliwiać obsługę co najmniej następujących typów dysków instalowanych w ramach macierzy dyskowej: – NL-SAS: 1TB, 2TB, 3TB i 4TB, – SAS: 300GB, 600GB, 900GB i 1,2TB, – SSD: minimum 200GB, 400GB, 800GB.

Zadanie 6. Infrastruktura wsparcia procesów zarządzania

Specyfikacja sprzętu i oprogramowania dla zadania nr 6

Tabela 2.6.1. Storage (typ 4) – 1 sztuka

l.p.	cecha	wartość
1.	Informacje ogólne	Rozwiązanie klasy NAS, budżetowe do zadań niekrytycznych, wymagających przestrzeni dyskowej o pojemności co najmniej 20TB netto
2.	Wymiary	Obudowa o wysokości maksymalnie 2U (szafa rack 19”). Z urządzeniem należy dostarczyć komplet elementów montażowych pozwalających na bezpieczne zamocowanie urządzenia w szafie rack 19”.
3.	Ilość dysków	Co najmniej 12 miejsc na dyski twarde w standardzie minimum SATA 2.5”/3.5”
4.	Komunikacja	Co najmniej 4 karty sieciowe o prędkości co najmniej 1 GbE z możliwością przełączania awaryjnego oraz agregacji łączy
5.	Zabezpieczenie	Urządzenie musi obsługiwać poziomy RAID co najmniej 0, 1, 10, 5, 6
6.	Interfejsy zewnętrzne	Co najmniej 2 porty USB 3.0 oraz co najmniej 2 porty USB 2.0
7.	Pamięć	Co najmniej 2GB DDR3 z możliwością rozbudowy do co najmniej 4GB

8.	Gwarancja	Co najmniej 3 lata gwarancji producenta na całe urządzenie oraz dyski. Uszkodzone dyski w trakcie trwania gwarancji pozostają u Zamawiającego. Dostarczone urządzenia muszą być nowe i nieużywane wcześniej.
9.	Zasilanie	Co najmniej 2 zasilacze pracujące w trybie redundantnym.
10.	Dyski	Urządzenie musi zostać dostarczone z co najmniej 8 dyskami o pojemności co najmniej 4TB o prędkości co najmniej 7200 obrotów na minutę oraz z co najmniej 64MB cache.

Tabela 2.6.2. Serwer (typ 4) – 2 sztuki

l.p.	cecha	wartość
1.	Procesor	Co najmniej 1 procesor, osiągający w teście Passmark nie mniej niż 14 tyś punktów o częstotliwości taktowania nie mniejszej niż 2,6GHz, ilości fizycznych rdzeni co najmniej 8 oraz poborze prądu nie większym niż 100W.
2.	Pamięć	Co najmniej 64GB RAM DDR3 lub szybszych
3.	Dysk twardy	Co najmniej 4 dyski twarde o pojemności co najmniej 600GB o prędkości co najmniej 10000 obrotów na minutę każdy, interfejs co najmniej SAS 6G
4.	Kontroler RAID	Co najmniej 1 kontroler RAID sprzętowy z pamięcią cache co najmniej 512MB ze wsparciem sprzętowym co najmniej dla poziomów RAID 5 i 6.
5.	Karta sieciowa	Co najmniej 2 karty sieciowe o prędkości co najmniej 1 GbE.
6.	Montaż	Urządzenia muszą zostać dostarczone z kompletem elementów montażowych do szaf rack 19” wraz z organizerem kabli.
7.	Zarządzanie	Urządzenia muszą posiadać niezależny od innych interfejsów fizyczny port/interfejs zarządzający
8.	Gwarancja	Co najmniej 3 lata gwarancji w systemie NBD. Wszystkie uszkodzone dyski w trakcie trwania gwarancji pozostają u Zamawiającego.
9.	Oprogramowanie	Z uwagi na posiadane przez Zamawiającego oprogramowanie BMS dostarczone w wyniku realizacji przetargu z dnia , które będzie instalowane na serwerach, każdy serwer musi być wyposażony w system operacyjny Windows Server 2012 R2 EN lub nowszy.

Zadanie 7. Infrastruktura przestrzeni dyskowej

Specyfikacja sprzętu i oprogramowania dla zadania nr 7

Tabela 2.7.1. Serwer (typ 5) – 2 sztuki

l.p.	cecha	wartość
1.	Pojemność	• Serwer musi zapewnić dostępną pojemność użyteczną nie mniejszą niż 100 GB po skonfigurowaniu sprzętowego RAID1. • Serwer musi posiadać możliwość konfiguracji sprzętowego RAID 1. • Serwerów musi posiadać co najmniej dwa dyski SAS co najmniej 10k rpm.
2.	Wydajność	Serwer musi posiadać co najmniej 2 procesory o łącznej ocenie co najmniej 20 000 punktów (per serwer) w teście PassMark (na podstawie wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php). Zużycie energii per procesor nie może być większe niż 100 W. Serwer musi posiadać nie mniej niż 64 GB RAM.
3.	Komunikacja	Oferowane urządzenia powinny wspierać połączenia 1 Gigabit Ethernet. Pojedynczy serwer powinien posiadać liczbę portów 1 Gigabit Ethernet nie mniejszą niż 4 na co najmniej 2 kartach sieciowych (nie wliczając w to interfejsu administracyjnego z punktu 2.7.1.5.).
4.	Niezawodność i bezpieczeństwo danych	Oferowane urządzenia (serwery) muszą posiadać po dwa redundantne zasilacze oraz zapewniać ich wymianę bez zatrzymywania urządzenia oraz systemu. Oferowane urządzenia (serwery) muszą być wyposażone w obsługę wszystkich dostarczonych dysków twardych oraz zapewniać ich wymianę bez

		zatrzymywania urządzenia oraz systemu.
5.	Zarządzanie i monitorowanie	Administracja pojedynczym serwerem musi odbywać się poprzez przeglądarkę internetową (Web GUI) w wersji maksymalnej dostępnej dla danego urządzenia. Serwery muszą zapewniać obsługę alertów i mieć możliwość monitorowania za pomocą protokołu SNMP.
6.	Montaż	Serwery muszą zapewniać montaż w 19-calowych szafach montażowych RACK o głębokości 1200 mm. Do urządzenia należy dołączyć komplet elementów montażowych do 19 calowej szafy RACK o głębokości 1200 mm zapewniających pełne wysunięcie urządzenia z szafy RACK bez konieczności odłączania okablowania i komplet kabli zasilających (C13-C14 lub C19-C20).
7.	Gwarancja i wsparcie techniczne	• Gwarancja producenta urządzenia na minimum 3 lata na wszystkie elementy serwera. Serwis musi być świadczony przez 24 h na dobę 365 dni w roku. Czas reakcji: najpóźniej następny dzień roboczy, czas usunięcia awarii: nie dłużej niż 14 dni kalendarzowych. • Producent oferowanego urządzenia musi posiadać zespół inżynierów serwisowych w Polsce i zapewniać obsługę zgłoszeń 24 godz. na dobę, 365 dni w roku. • Producent oferowanego urządzenia w trakcie trwania kontraktu serwisowego zapewni bezpłatną wymianę uszkodzonych części, dostęp do wszystkich nowych wersji oprogramowania systemu (w zakresie zakupionych funkcjonalności licencji systemu). • Producent oferowanego urządzenia pozostawi u zamawiającego uszkodzone części, w szczególności dyski bez obowiązku ich zwrotu.
8.	Wymagania dodatkowe	Dostawa urządzeń do siedziby zamawiającego na koszt dostawcy.

Tabela 2.7.2. Serwer (typ 6) – 8 sztuk

l.p.	cecha	wartość
1.	Pojemność	Serwer musi posiadać co najmniej dwanaście dysków o pojemności co najmniej 4 TB SATA co najmniej 7.2k rpm.
2.	Wydajność	• Serwer musi posiadać co najmniej 2 procesory o łącznej ocenie co najmniej 15 000 punktów (per serwer) w teście PassMark (na podstawie wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php). Zużycie energii per procesor nie może być większe niż 80 W. • Serwer musi posiadać nie mniej niż 32 GB RAM.
3.	Komunikacja	Oferowane urządzenia powinny wspierać połączenia 1 Gigabit Ethernet. Serwer powinien posiadać liczbę portów 1 Gigabit Ethernet nie mniejszą niż 4 na co najmniej 2 kartach sieciowych (nie wliczając w to interfejsu administracyjnego z punktu 5).
4.	Niezawodność i bezpieczeństwo danych	• Oferowane urządzenia (serwery) muszą posiadać po dwa redundantne zasilacze oraz zapewniać ich wymianę bez zatrzymywania urządzenia oraz systemu. • Oferowane urządzenia (serwery) muszą być wyposażone w obsługę wszystkich dostarczonych dysków twardych oraz zapewniać ich wymianę bez zatrzymywania urządzenia oraz systemu.
5.	Zarządzanie i monitorowanie	• Administracja pojedynczym serwerem musi odbywać się poprzez przeglądarkę internetową (Web GUI) w wersji maksymalnej dostępnej dla danego urządzenia. • Serwery muszą zapewniać obsługę alertów i mieć możliwość monitorowania za pomocą protokołu SNMP.
6.	Montaż	Serwery muszą zapewniać montaż w 19-calowych szafach montażowych RACK o głębokości 1200 mm. Do urządzenia należy dołączyć komplet elementów montażowych do 19 calowej szafy RACK o głębokości 1200 mm zapewniających pełne wysunięcie urządzenia z szafy RACK bez konieczności odłączania okablowania i komplet kabli zasilających (C13-C14 lub C19-C20).

7.	Gwarancja i wsparcie techniczne	• Gwarancja producenta urządzenia na minimum 3 lata na wszystkie elementy serwera. Serwis będzie świadczony przez 24 h na dobę 365 dni w roku. Czas reakcji: najpóźniej następny dzień roboczy, czas usunięcia awarii: nie dłużej niż 14 dni kalendarzowych. • Producent oferowanego urządzenia musi posiadać zespół inżynierów serwisowych w Polsce i zapewniać obsługę zgłoszeń 24 godz. na dobę, 365 dni w roku. • Producent oferowanego urządzenia w trakcie trwania kontraktu serwisowego zapewni bezpłatną wymianę uszkodzonych części, dostęp do wszystkich nowych wersji oprogramowania systemu (w zakresie zakupionych funkcjonalności licencji systemu). • Producent oferowanego urządzenia pozostawi u zamawiającego uszkodzone części, w szczególności dyski bez obowiązku ich zwrotu.
8.	Wymagania dodatkowe	Dostawa urządzeń do siedziby zamawiającego na koszt dostawcy.

Zadanie 8. Infrastruktura wsparcia procesów bezpieczeństwa

Specyfikacja sprzętu i oprogramowania dla zadania nr 8

Tabela 2.8.1. Serwer (typ 7) – 3 sztuki

l.p.	cecha	wartość
1.	Obudowa	Serwer stelażowy 2U do instalacji w szafie standardowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie 19”, w tym szyny montażowe z ramieniem do organizacji kabli)
2.	Procesor	Co najmniej dwa procesory co najmniej ośmiordzeniowe, każdy o częstotliwości pracy wynoszącej minimum 2.4GHz przy wszystkich rdzeniach aktywnych, zgodny z x86 - 64 bity, osiągające w testach SPECint®_rate2006 wynik nie gorszy niż 692 punktów. Wynik testu musi być opublikowany na stronie www.spec.org najpóźniej w dniu złożenia oferty. Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów.
3.	Liczba procesorów	Co najmniej 2
4.	Pamięć operacyjna	Co najmniej 128 GB, z możliwością rozbudowy do co najmniej 768GB. Minimum 24 sloty na pamięć.
5.	Sloty rozszerzeń	Co najmniej 3 sloty PCI-Express Generacji 3 w tym co najmniej dwa sloty x8 (szybkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy co najmniej o kolejne 3 sloty, z których: - co najmniej 1 slot będzie działał z szybkością x16 (Bus Width); - co najmniej 2 sloty będą pełnej wysokości.
6.	Dysk twardy	Możliwość zainstalowania co najmniej 16 dysków typu Hot Swap (Hot Plug), SAS/SATA/SSD, 2,5”. Wraz z urządzeniem muszą zostać dostarczone do każdego urządzenia co najmniej 2 dyski o pojemności co najmniej 300GB prędkości obrotowej co najmniej 10k rpm SAS
7.	Kontroler	Kontroler macierzowy SAS 12Gb z co najmniej 2GB pamięci cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę co najmniej 16 napędów dyskowych SAS (dopuszcza się zastosowanie tzw. expandera) oraz obsługujący co najmniej poziomy: RAID 0/1/1+0/5/5+0/6/6+0.
8.	Interfejsy sieciowe	Co najmniej 4 porty Ethernet 1000 Mb/s z funkcją Wake-On-LAN, wsparciem dla PXE, interfejsami RJ-45, mechanizmami odciążania CPU Large Send Offload (LSO) oraz Checksum Offload. Porty te nie mogą zajmować slotów PCIe. Dopuszcza się rozwiązania równoważne, w którym zajmują sloty PCIe, o ile ilość wolnych slotów PCIe w serwerze nie będzie mniejsza niż 1.
9.	Interfejsy HBA FC	Co najmniej dwie karty jednoportowe o prędkości co najmniej 8Gb FC z wkładkami co najmniej 8Gb SW.
10.	Karta graficzna	Zintegrowana karta graficzna

11.	Napęd DVD	Opcjonalny wewnętrzny napęd DVD-RW
12.	Porty	- co najmniej 3x USB z możliwością rozbudowy do 5 portów - co najmniej 1x VGA (z tyłu) - co najmniej 1x port szeregowy z tyłu obudowy - wewnętrzny slot na kartę SD lub port uSSD. - opcjonalny dodatkowy port VGA dostępny z przodu serwera, - opcjonalny moduł TPM.
13.	Zabezpieczenie dostępu do dysków twardych	Serwer musi posiadać możliwość zabezpieczenia przed dostępem do dysków w formie panelu zamykanego na kluczyk i uniemożliwiającego wyjęcie dysków twardych z serwera.
14.	Panel diagnostyczny	Panel diagnostyczny LCD lub LED informujący co najmniej o stanie procesorów, pamięci, wentylatorów oraz temperaturze.
15.	Zasilacz	Minimum 2 szt., typ hot-plug, redundantne.
16.	Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) co najmniej pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej, nagrywania sesji graficznych i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Zarządzanie musi zabezpieczać przed możliwością jednoczesnego logowania się tego samego użytkownika więcej niż raz. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI. Wymagane jest dostarczenie odpowiedniej licencji.
17.	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Co najmniej dla Microsoft Windows Server 2012 R2, Canonical Ubuntu LTS 14.04, Red Hat Enterprise Linux (RHEL) w wersji 7, SUSE Linux Enterprise Server (SLES) w wersji 12, VMware 5.5 U2, Citrix XenServer 6.5
18.	Wsparcie techniczne	3 lata z czasem reakcji w następnym dniu roboczym i możliwością zgłaszania awarii w dni robocze od 8:00 do 17:00. W ramach usługi wsparcia technicznego wymagane jest również zapewnienie: - priorytetowej obsługi problemów o znaczeniu krytycznym; - zdalnej diagnostyki problemu i pomocy technicznej; - zdalnego wykrywania i diagnostyki incydentów; - tworzenia raportów incydentów i trendów (4 razy w roku); - bezpośredniego dostępu do specjalistów z Centrum Zaawansowanych Rozwiązań; - zdalnej asysty podczas instalacji aktualizacji (sterowników/mikrokodów); - zdalnej obsługi Technicznego Opiekuna Klienta (TAM); - zdalnej obsługi Specjalisty ds. Rozwiązań Technicznych (TSS). - zdalnego doradztwa technicznego; - zdalnej analizy konfiguracji i rekomendacji zmian w zakresie bezpieczeństwa, wydajności i wysokiej dostępności (2 razy do roku); - zdalnej analizy i rekomendacji dla aktualizacji systemu operacyjnego, oprogramowania wirtualizacyjnego oraz oprogramowania wbudowanego i sterowników. Wszystkie uszkodzone dyski w okresie trwania gwarancji pozostają u Zamawiającego.

Tabela 2.8.2. Serwer (typ 8) – 1 sztuka

l.p.	cecha	wartość
1.	Obudowa	Serwer stelażowy 2U do instalacji w szafie standardowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie, w tym szyny montażowe z ramieniem do organizacji kabli)
2.	Procesor	Co najmniej dwa procesory sześciordzeniowe, każdy o częstotliwości pracy wynoszącej co najmniej 2.4GHz przy wszystkich rdzeniach aktywnych, x86 -

		64 bity, osiągające w testach SPECint®_rate2006 wynik nie gorszy niż 520 punktów. Wynik testu musi być opublikowany na stronie www.spec.org najpóźniej w dniu złożenia oferty. Zamawiający nie wymaga złożenia wraz z ofertą wyników w/w testów.
3.	Liczba procesorów	Co najmniej 2
4.	Pamięć operacyjna	Co najmniej 128 GB, z możliwością rozbudowy do co najmniej 768GB. Co najmniej 24 sloty na pamięć.
5.	Sloty rozszerzeń	Co najmniej 3 sloty PCI-Express Generacji 3 w tym co najmniej dwa sloty x8 (szybkość slotu – bus width) pełnej wysokości (full height). Możliwość rozbudowy o kolejne 3 sloty, z których: - co najmniej 1 slot będzie działał z szybkością x16 (Bus Width); - co najmniej 2 sloty będą pełnej wysokości.
6.	Dysk twardy	Możliwość zainstalowania co najmniej 16 dysków typu Hot Swap (Hot Plug), SAS/SATA/SSD, 2,5". Wraz z urządzeniem należy dostarczyć co najmniej 5 dysków o pojemności co najmniej 600GB i prędkości co najmniej 10k rpm SAS
7.	Kontroler	Kontroler macierzowy SAS 12Gb z co najmniej 2GB pamięci cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę co najmniej 16 napędów dyskowych SAS (dopuszcza się zastosowanie tzw. expandera) oraz obsługujący co najmniej poziomy: RAID 0/1/1+0/5/5+0/6/6+0.
8.	Interfejsy sieciowe	Co najmniej 4 porty Ethernet 1000 Mb/s z funkcją Wake-On-LAN, wsparciem dla PXE, interfejsami RJ-45, mechanizmami odciążania CPU Large Send Offload (LSO) oraz Checksum Offload. Porty te nie mogą zajmować slotów PCIe. Dopuszcza się rozwiązania równoważne, w którym zajmują sloty PCIe, o ile ilość wolnych slotów PCIe w serwerze nie będzie mniejsza niż 1.
9.	Interfejsy HBA FC	Co najmniej dwie karty jednoportowe o prędkości co najmniej 8Gb FC z wkładkami co najmniej 8Gb SW.
10.	Karta graficzna	Zintegrowana karta graficzna
11.	Napęd DVD	Opcjonalny wewnętrzny napęd DVD-RW
12.	Porty	- co najmniej 3x USB z możliwością rozbudowy do 5 portów - co najmniej 1x VGA (z tyłu) - wewnętrzny slot na kartę SD lub port uSSD. - opcjonalny dodatkowy port VGA dostępny z przodu serwera, - opcjonalny moduł TPM.
13.	Zabezpieczenie dostępu do dysków twardych	Serwer musi posiadać możliwość zabezpieczenia przed dostępem do dysków w formie panelu zamykanego na kluczyk i uniemożliwiającego wyjęcie dysków twardych z serwera.
14.	Panel diagnostyczny	Panel diagnostyczny LCD lub LED informujący o stanie procesorów, pamięci, wentylatorów, temperaturze, itp.
15.	Zasilacz	Minimum 2 szt., typ hot-plug, redundantne.
16.	Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej co najmniej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej, nagrywania sesji graficznych i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Zarządzanie musi zabezpieczać przed możliwością jednoczesnego logowania się tego samego użytkownika więcej niż raz. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI. Wymagane jest dostarczenie odpowiedniej licencji.
17.	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Obsługa co najmniej Microsoft Windows Server 2012 R2, Canonical Ubuntu LTS 14.04, Red Hat Enterprise Linux (RHEL) w wersji 7, SUSE Linux Enterprise Server (SLES) w wersji 12, VMware 5.5 U2, Citrix XenServer 6.5

18.	Wsparcie techniczne	3 lata z czasem reakcji w następnym dniu roboczym i możliwością zgłaszania awarii w dni robocze od 8:00 do 17:00. W ramach usługi wsparcia technicznego wymagane jest również zapewnienie: - priorytetowej obsługi problemów o znaczeniu krytycznym; - zdalnej diagnostyki problemu i pomocy technicznej; - zdalnego wykrywania i diagnostyki incydentów; - tworzenia raportów incydentów i trendów (4 razy w roku); - bezpośredniego dostępu do specjalistów z Centrum Zaawansowanych Rozwiązań; - zdalnej asysty podczas instalacji aktualizacji (sterowników/mikrokodów); - zdalnej obsługi Technicznego Opiekuna Klienta (TAM); - zdalnej obsługi Specjalisty ds. Rozwiązań Technicznych (TSS). - zdalnego doradztwa technicznego; - zdalnej analizy konfiguracji i rekomendacji zmian w zakresie bezpieczeństwa, wydajności i wysokiej dostępności (2 razy do roku); - zdalnej analizy i rekomendacji dla aktualizacji systemu operacyjnego, oprogramowania wirtualizacyjnego oraz oprogramowania wbudowanego i sterowników. Wszystkie uszkodzone dyski w trakcie trwania gwarancji pozostają u Zamawiającego.

Zadanie 9. Infrastruktura sieciowa

Specyfikacja sprzętu i oprogramowania dla zadania nr 9

Tabela 2.9.1. Osprzęt sieciowy (typ 13) – 1 sztuka

l.p.	cecha	wartość
1.	Informacje ogólne	Przełącznik o konstrukcji modularnej min. 7-slotowy, w tym min. 5 slotów na karty liniowe.
2.	Wyposażenie	Wymagane jest, aby w momencie dostawy przełącznik był wyposażony w: a. Co najmniej dwa moduły zarządzające (switch fabric), b. Co najmniej 2 porty TenGigabitEthernet definiowane przez moduły SFP+, c. Co najmniej 96-portów 10/100/1000Base-T pracujących bez nadsubskrypcji względem matrycy przełączającej, d. Co najmniej 96-portów 10/100/1000Base-T pracujących bez nadsubskrypcji względem matrycy przełączającej, wspierających standard PoE - 802.3at, e. Co najmniej 2 zasilacze redundantne zapewniające poprawną pracę urządzenia, o mocy co najmniej 2800W każdy.
3.	Wydajność/porty	1. Porty SFP+ urządzenia muszą umożliwiać instalacje zarówno transceiverów 10GE jak i GE. 2. Urządzenie musi zapewnić wydajność na poziomie co najmniej 520Gbps 3. Urządzenie musi zapewniać pasmo minimum 48Gb/s per slot. Szybkość przełączania/routingu min. 225Mpps dla IPv4 i 100Mpps dla IPv6.
4.	LAN	Urządzenie musi zapewniać obsługę: a. min. 4 000 aktywnych sieci VLAN, interfejsów SVI, instancji Spanning Tree, b. min. 50 000 adresów MAC, c. sprzętową dla QoS i ACL - minimum 64 000 wpisów sprzętowych.
5.	Pamięć	Urządzenie musi posiadać min. 2GB pamięci DRAM.
6.	Ramki	Przełącznik musi obsługiwać ramki Jumbo (do min. 9216 bajtów).
7.	Ciągłość pracy sieci	Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: a. 802.1w Rapid Spanning Tree, b. 802.1s Multi-Instance Spanning Tree,

		c. Możliwość grupowania portów zgodnie ze specyfikacją IEEE 802.3ad (LACP) z wykorzystaniem portów pochodzących z różnych kart liniowych, d. Możliwość instalacji “na gorąco” zasilaczy oraz kart liniowych.
8.	L2/L3	Urządzenie musi umożliwiać przełączanie w warstwie 2 i 3. Wymagane jest wsparcie dla routingu statycznego i dynamicznego (min. dla protokołu RIPv2 i RIPng), routingu multicast IPv4 i IPv6 (PIM-SM, PIM-SSM) i protokołu redundancji bramy VRRP lub równoważnego. Urządzenie musi umożliwiać rozszerzenie funkcjonalności (poprzez upgrade oprogramowania lub zakup odpowiedniej licencji) o zaawansowane protokoły routingu warstwy 3 dla ruchu IPv4 i IPv6 (OSPFv2 i v3, IS-IS dla IPv4 i IPv6, BGPv4, MBGP, Policy Based Routing). Jeżeli oprogramowanie, lub licencja jest wymagana do opisanej funkcjonalności należy ją dostarczyć w ramach tego projektu.
9.	Tablica routingu	Tablica routingu urządzenia musi posiadać minimum: a. 64 000 wpisów dla IPv4, b. 32 000 wpisów dla IPv6, c. 30 000 wpisów dla ruchu multicast.
10.	Jakość usług	Urządzenie musi wspierać co najmniej następujące mechanizmy związane z zapewnieniem jakości usług w sieci: a. Obsługa 8 kolejek sprzętowych per port dla różnego rodzaju ruchu, b. Obsługa co najmniej jednej kolejki ze statusem strict priority, c. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, d. Możliwość “re-kolorowania” pakietów przez urządzenie – pakiet przychodzący do urządzenia przed przesłaniem na port wyjściowy może mieć zmienione pola 802.1p (CoS) oraz IP ToS/DSCP. e. Kontrola sztormów dla ruchu boradcast i multicast, f. Mechanizm AutoQoS lub równoważny.
11.	Dodatkowe funkcjonalności	Obsługa protokołu LLDP i LLD-MED. Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
12.	Bezpieczeństwo	Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a. Min. 5 poziomów dostępu administracyjnego poprzez konsolę, b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL, c. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, d. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC , e. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, f. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie, g. Urządzenie musi umożliwiać wymuszenie ponownego uwierzytelniania portu dostępowego oraz zdalnego restartu portu (zgodnie z RFC 5176), h. Wszystkie porty urządzenia muszą zapewniać możliwość szyfrowania ruchu zgodnie ze standardem IEEE 802.1AE (MACSec), i. Możliwość uzyskania dostępu do urządzenia przez SNMPv3 i SSHv2, j. Obsługa list kontroli dostępu (ACL) dla IPv4 i IPv6, k. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, l. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed

		rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), m. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny oraz 802.1X) do serwerów RADIUS lub TACACS+, n. Funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym.
13.	Monitoring	• Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie (mechanizmy SPAN i RSPAN) – wymagana jest obsługa min. 8 sesji SPAN/RSPAN na przełączniku. • Funkcjonalność traceroute dla warstwy 2 umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC. • Urządzenie musi posiadać wbudowany analizator pakietów. • Urządzenie musi posiadać funkcjonalność umożliwiającą monitorowanie parametrów usług dla ruchu IP (IP SLA), w tym również dla usług wideo (urządzenie musi posiadać wbudowany symulator ruchu wideo). Wymagana jest możliwość monitorowania parametrów takich jak opóźnienie, jitter, utrata pakietów. • Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie. • Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 128 000 (wymagane jest wsparcie sprzętowe).
14.	Konfiguracja	Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.
15.	Montaż	Obudowa przystosowana do montażu w szafie 19”. Wysokość nie większa niż 11RU. Urządzenie musi zostać dostarczone wraz z kompletem elementów montażowych producenta urządzenia pozwalające na montaż w szafie 19”.
16.	Wymagania dodatkowe	Zamawiający wymaga, aby dostarczone urządzenie zapewniało możliwość stworzenia wirtualnego przełącznika z drugim urządzeniem o analogicznej konfiguracji. Pod pojęciem wirtualnego przełącznika Zamawiający rozumie możliwość: a. Konfiguracji obydwu urządzeń z jednego punktu, b. Terminowania połączeń link aggregation (z wykorzystaniem protokołu IEEE 802.3ad LACP) z innych urządzeń sieciowych w taki sposób, aby jedno łącze było terminowane na jednym przełączniku, a drugie łącze na drugim przełączniku (tzw. multi-chassis link aggregation).
17.	Wkładki SFP/SFP+	1. 4 wkładki umożliwiającymi pracę na dystansie minimum 100 metrów po światłowodzie jednomodowym (standard 10G-LRM) 2. 4 wkładki umożliwiające pracę na dystansie minimum 100 metrów po światłowodzie wielomodowym (standard 10G-SR), 3. Wkładki muszą pochodzić od tego samego dostawcy co oferowany przełącznik celem uniknięcia problemów z utrzymaniem sieci i serwisowaniem urządzeń.
18.	Gwarancja	Co najmniej 36 miesięcy gwarancji, usługa serwisowa świadczona na miejscu instalacji urządzenia, przyjmowanie zgłoszenia musi być możliwe przez 24h na dobę, siedem dni w tygodniu, czas reakcji następny dzień roboczy w przypadku wystąpienia awarii. Maksymalny czas rozwiązania w przypadku

		awarii pięć dni.

Tabela 2.9.2. Osprzęt sieciowy (typ 14) – 2 sztuki

l.p.	cecha	wartość
1.	Informacje ogólne	Przełącznik sieciowy połączony ze szkieletem sieci portami 10GE
2.	Porty	Typ i liczba portów: a. minimum 48 portów 10/100/1000 PoE+ zgodne z IEEE 802.3at, b. minimum 2 dodatkowe porty uplink 10 Gigabit Ethernet SFP+, zapewniające również zgodność z modułami Gigabit Ethernet SFP, c. porty SFP+ muszą umożliwiać ich obsadzanie wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz Gigabit Ethernet – minimum 1000Base-SX, 1000Base-LX/LH, 1000Base-BX-D/U oraz modułami CWDM zależnie od potrzeb Zamawiającego. Wymagane jest, aby wszystkie porty dostępowe 10/100/1000 obsługiwały standard zasilania poprzez sieć LAN (Power over Ethernet) zgodnie z IEEE 802.3at. Zasilacz urządzenia musi być tak dobrany, aby zapewnić minimum 740W dla portów PoE/PoE+.
3.	LAN	Urządzenie musi obsługiwać minimum jednocześnie aktywnych 1000 sieci VLAN. Urządzenie musi obsługiwać minimum 16000 adresów MAC.
4.	Pamięć	Urządzenie musi posiadać min. 512MB pamięci DRAM i 128MB pamięci flash.
5.	Montaż	Parametry fizyczne – wysokość nie większa niż 1RU, montaż w szafie 19”. Dostarczone urządzenia muszą posiadać komplet elementów montażowych do szafy rack 19”.
6.	Wydajność	Wydajność przełączania minimum 130Mpps dla pakietów 64-bajtowych. Przepustowość przełącznika minimum 108Gb/s (216Gb/s full duplex). Urządzenie musi zapewniać możliwość łączenia w stos z zachowaniem następującej parametrów: • do min. 8 jednostek w stosie, • magistrala stackująca o przepustowości co najmniej 80Gb/s, • długość kabli połączeniowych w stosie powinna wynosić co najmniej 50 cm, • możliwość tworzenia połączeń EtherChannel zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (Cross-stack EtherChannel), • jeżeli realizacja funkcji stackowania wymaga dodatkowych modułów/kabli/licencji itp. ich dostarczenie w ramach tego postępowania jest wymagane. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów
7.	Energooszczędność	Wbudowane funkcje zarządzania energią: d. zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet), e. możliwość hibernowania przełącznika w określonych godzinach celem dodatkowego oszczędzania energii.
8.	Trasy routingu	Musi zapewniać obsługę min. 16 statycznych tras dla routingu IPv4.
9.	Protokoły i funkcjonalności	• Obsługa protokołu NTP. • Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping. • Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 128 instancji protokołu STP. • Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server. • Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.

		• Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów bezpieczeństwa typu Port Security i IP Source Guard na interfejsach link aggregation. • Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP).
10.	Bezpieczeństwo	Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa: a. minimum 5 poziomów dostępu administracyjnego poprzez konsolę, b. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL, c. obsługa funkcji Guest VLAN , d. możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, e. możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X , f. przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www, g. wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie, h. możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, i. możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6, j. obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6, k. obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, l. funkcjonalność Protected Port, m. zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard) oraz ochronę przed fałszowaniem źródłowych adresów IPv6 (IPv6 Source Guard), n. obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne).
11.	Jakość usług	Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, • Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek, • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi. Wymagana jest możliwość skonfigurowania minimum 256 różnych ograniczeń.
12.	Monitoring i zarządzanie	- Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np.

		telefon IP). - Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB. - Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN). - Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych.
13.	Zasilanie	Zasilanie 230V AC, możliwość zastosowania redundantnego zasilacza (dopuszczalne rozwiązania zewnętrzne).
14.	Gwarancja	Co najmniej 36 miesięcy gwarancji, usługa serwisowa świadczona na miejscu instalacji urządzenia, przyjmowanie zgłoszenia musi być możliwe przez 24h na dobę, siedem dni w tygodniu, czas reakcji następny dzień roboczy w przypadku wystąpienia awarii. Maksymalny czas rozwiązania w przypadku awarii pięć dni.

Zadanie 10. Infrastruktura sieci bezprzewodowej

Specyfikacja sprzętu i oprogramowania dla zadania nr 10

Tabela 2.10.1. Osprzęt sieciowy (typ 15) – 2 sztuki

l.p.	cecha	wartość
1.	Informacje ogólne	Kontrolery sieci WLAN obsługujące co najmniej 27 punktów dostępowych (AP). 1. Urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego: a. zarządzanie politykami bezpieczeństwa, b. wykrywanie intruzji nieuprawnionych dostępów, c. zarządzanie pasmem radiowym, d. zarządzanie mobilnością, e. zarządzanie jakością transmisji, f. zgodnie z protokołem CAPWAP (RFC 5415). 2. Obsługa 27 punktów dostępowych z możliwością rozszerzenia do min. 75 (kratowe lub klasyczne).
2.	Interfejsy	Min. 4 interfejsy 10/100/1000Base-T.
3.	Pasmo radiowe	Zarządzanie pasmem radiowym punktów dostępowych: a. automatyczna adaptacja do zmian w czasie rzeczywistym, b. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia), c. dynamiczne przydzielanie kanałów radiowych, d. wykrywanie, eliminacja i unikanie interferencji, e. równoważenie obciążenia punktów dostępowych, f. tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych, g. automatyczna dystrybucja klientów pomiędzy punkty dostępowe,

		h. mechanizmy wspomagające nastawę priorytetu dla zakresu 5GHz na potrzeby klientów dwuzakresowych.
4.	Obsługa SSID	Mapowanie SSID do segmentów VLAN w sieci przewodowej: a. 1:1 b. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty), c. możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID).
5.	Sieci kratowe	Obsługa sieci kratowych: a. komunikacja między punktami dostępowymi bez medium kablowego, b. separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi z możliwością tworzenia wyjątków), c. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo), d. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji), autoryzacja punktów dostępowych w oparciu o certyfikaty X.509, adresy MAC.
6.	Bezpieczeństwo	Obsługa mechanizmów bezpieczeństwa: a. 802.11i, WPA2, WPA, WEP, b. 802.1x z EAP (PEAP, EAP-TLS, EAP-FAST, EAP-TTLS), c. DTLS, d. obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, LDAP, wbudowana lokalna baza użytkowników (min. 2.000 wpisów), e. możliwość kreowania różnych polityk bezpieczeństwa w ramach pojedynczego SSID, f. możliwość profilowania użytkowników: • przydział sieci VLAN, • przydział list kontroli dostępu (ACL), g. uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 (wykrywanie podszywania się punktów dostępowych użytkowników pod adresy infrastruktury) – 802.11w lub podobny, h. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty X.509, i. obsługa list kontroli dostępu (ACL), j. wykrywanie i dezaktywacja obcych punktów dostępowych, k. wbudowany system IDS wykrywający typowe ataki na sieci bezprzewodowe (fake AP, netstumbler, deathentication flood itp.), l. współpraca z systemami IDS/IPS, m. ochrona kryptograficzna (DTLS lub równoważny) ruchu kontrolnego i ruchu użytkowników CAPWAP, n. DHCP proxy.
7.	Multicast/unicast	Obsługa ruchu unicast IPv4 i IPv6. Obsługa ruchu multicast IPv4 i IPv6 a. IGMP / MLD snooping, b. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym, obsługa konwersji ruchu multicast do unicast.

8.	Roaming	Obsługa mobilności (roamingu) użytkowników (L2 i L3 – IPv4 i IPv6, w ramach i pomiędzy kontrolerami).
9.	QoS	Obsługa mechanizmów QoS a. 802.1p, b. WMM, TSpec, c. ograniczanie pasma per użytkownik, d. Call Admission Control – ze statyczną definicją pasma i dynamiczna w oparciu o analizę profili ruchu, e. U-APSD.
10.	Dostęp dla gości	Obsługa dostępu gościnnego (IPv4 i IPv6): a. przekierowanie użytkowników określonych SSID do strony logowania (z możliwością personalizacji strony), b. możliwość kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta.
11.	Wymagania dodatkowe	Współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych. Możliwość redundancji rozwiązania (N+1). Mechanizmy pozwalające na dezaktywację modułów radiowych w określonych godzinach w celu redukcji poboru energii przez system. Zarządzanie przez HTTPS, SNMPv3, SSH, port konsoli szeregowej. Niezbędna obsługa posiadanych przez Zamawiającego dwóch punktów dostępu Cisco AP 1140 oraz punktów kontroli dostępu „Access Point" będących przedmiotem zamówienia.
12.	Gwarancja	Co najmniej 36 miesięcy gwarancji, usługa serwisowa świadczona na miejscu instalacji urządzenia, przyjmowanie zgłoszenia musi być możliwe przez 24h na dobę, siedem dni w tygodniu, czas reakcji następny dzień roboczy w przypadku wystąpienia awarii. Maksymalny czas rozwiązania w przypadku awarii pięć dni.

Tabela 2.10.2. Osprzęt sieciowy (typ 16) – 25 sztuk

l.p.	cecha	wartość
1.	Informacja ogólna	Punkt kontroli dostępu „Access Point", współpracujący z kontrolerami sieci WLAN będącymi przedmiotem zamówienia.
2.	802.11a/b/g/n	Obsługa standardów 802.11a/b/g/n a. obsługa MIMO – min. 3x4 b. obsługa trzech strumieni przestrzennych c. obsługa kanałów 20 i 40 MHz d. obsługa prędkości PHY do 450 Mbps e. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) f. obsługa TxBF (transmitbeamforming) dla klientów 802.11a/g/n/ac
3.	802.11ac	Obsługa standardu 802.11ac a. obsługa MIMO – min. 3x4 b. obsługa trzech strumieni przestrzennych c. obsługa kanałów 20, 40 i 80 MHz d. obsługa prędkości PHY do 1.3Gbps e. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) f. obsługa TxBF (transmitbeamforming)
4.	Obsługa zakresu kanałów radiowych	Obsługa szerokiego zakresu kanałów radiowych: a. dla zakresu 2.4GHz: min. 13 kanałów b. dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów c. dla zakresu 5GHz (extended UNII-2): min. 8 kanałów
5.	Moc nadajnika	Konfigurowalna moc nadajnika a. dla zakresu 2.4GHz do 160 mW

		b. dla zakresu 5GHz do 200 mW
6.	Optymalizacja pasma radiowego	Optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany), a. obsługa min. 16 BSSID, b. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID, c. współpraca z systemami IDS/IPS, d. uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – funkcjonalność 802.11w lub równoważna, e. obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN), f. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN i lokalną autoryzacją użytkowników (lokalny serwer RADIUS, skrócona baza danych użytkowników na poziomie AP) – przełączenie nie może powodować zerwania sesji użytkowników, g. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IPS), h. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h, i. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – funkcjonalność 802.11r lub równoważna, j. obsługa mechanizmów QoS: • shaping/ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik • obsługa WMM, TSPEC, U-APSD k. współpraca z urządzeniami o oprogramowaniem , l. współpraca z urządzeniami o oprogramowaniem realizującym usługi lokalizacyjne, m. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury sieciowej.
7.	Tryb kratowy	Możliwość pracy w trybie kratowym (część AP dołączona do sieci kablowej, pozostałe formujące sieć w oparciu o medium radiowe): a. komunikacja między punktami dostępowymi bez medium kablowego, b. autoryzacja punktów dostępowych w oparciu o certyfikaty X.509, adresy MAC, c. separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi) z możliwością konfiguracji wyjątków (asocjacji użytkowników w zakresie przeznaczonym do komunikacji między AP oraz komunikacji między AP w zakresie przeznaczonym do obsługi użytkowników, d. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo), e. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji), f. automatyczna ochrona kryptograficzna (AES) ruchu pomiędzy AP, g. mechanizm kompatybilny dla wszystkich oferowanych modeli AP.
8.	Analizator widma częstotliwościowego	Zintegrowany moduł analizatora widma częstotliwościowego (dotyczy zakresów 2.4GHz i 5GHz): a. dokładność analizy (kwant próbkowania) max. 200 kHz,

		b. zakres częstotliwościowy zgodny z zakresem pracy modułów radiowych, c. automatyczne wykrywanie i klasyfikacja źródeł interferencji (bluetooth, DECT, urządzenia mikrofalowe, urządzenia transmisji audio wideo, urządzenia zakłócające itp.), d. możliwość wizualizacji wyników analizy na stacji roboczej klasy PC (FFT, gęstość widma, spektrogram, zajętość kanałów, poziom mocy sygnałów) w czasie rzeczywistym.
9.	Interfejsy	Interfejs Gigabit Ethernet (10/100/1000Base-T). Wbudowany port konsolowy (RJ-45).
10.	Wymagania dodatkowe	Zróżnicowane możliwości zasilania: a. zasilacz sieciowy 230V AC, b. zasilanie PoE+ (802.3at) w sposób zapewniający ich pełną wydajność. Anteny dookólne wewnętrzne (zintegrowane) o wzmocnieniu 4 dBi dla częstotliwości 2,4 GHz, oraz 6 dBi dla częstotliwości 5 GHz. Obudowa przystosowana do warunków pracy w pomieszczeniach biurowych (0 – 40°C), o niskim profilu (nie więcej niż 5,5 cm). Diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji. Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z automatycznym wykrywaniem kontrolera i konfiguracją poprzez sieć LAN.
11.	Gwarancja	Co najmniej 36 miesięcy gwarancji, usługa serwisowa świadczona na miejscu instalacji urządzenia, przyjmowanie zgłoszenia musi być możliwe przez 24h na dobę, siedem dni w tygodniu, czas reakcji następny dzień roboczy w przypadku wystąpienia awarii. Maksymalny czas rozwiązania w przypadku awarii pięć dni.

Tabela 2.10.3. Osprzęt inny (typ 2) – 3 sztuki

l.p.	cecha	wartość
1.	Informacje ogólne	Zasilacz zewnętrzny dla punktu kontroli dostępu „Access Point”
2.	Wymagania	1. Urządzenie musi zasilać punkty kontroli dostępu „Access Point” będące przedmiotem zamówienia; 2. Urządzenie musi obsługiwać charakterystykę prądu wejścia 230V / 50Hz zgodnie z polską normą PN-IEC 60038; 3. Urządzenie musi występować w formie „power injector” umożliwiające podanie do urządzenia zasilania w oparciu o technologię PoE oraz zawierać w komplecie przewód zasilający umożliwiający podłączenie do gniazda elektrycznego typu E.
3.	Gwarancja	Gwarancja producenta co najmniej 24 miesiące. Dostarczone urządzenie musi być nowe i nieużywane.

Zadanie 11. Infrastruktura sieciowa dostępowa

Specyfikacja sprzętu i oprogramowania dla zadania nr 11

Tabela 2.11.1. Osprzęt sieciowy (typ 17) – 2 sztuki

l.p.	cecha	wartość
1.	Informacje ogólne	Koncentrator VPN z licencjami dla 100 użytkowników
2.	Wymagania podstawowe	1. Urządzenie będzie pełnić rolę ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji. 2. Urządzenie pozwalające na uzyskanie funkcji firewall oraz VPN (sprzętowe wsparcie szyfrowania). 3. Urządzenie musi umożliwiać realizację wysokiej dostępności dla ruchu IPv4 i IPv6 poprzez mechanizmy: • failover active-standby, • failover active-active,

		• wsparcie dla routingu asymetrycznego w trybie active-active. 4. Urządzenie musi zapewniać możliwość podziału na co najmniej 5 odseparowanych urządzeń wirtualnych (domen/kontekstów). W ramach dostawy wymagane jest dostarczenie licencji zapewniających uruchomienie na urządzeniu 2 wirtualnych instancji. 5. W celu zachowania jednorodności aplikacyjnej dla użytkowników VPN urządzenie musi być kompatybilne z wykorzystywanym w środowisku zamawiającego na stacjach roboczych oprogramowaniem Cisco AnyConnect VPN w wersji co najmniej 3.1 służącym do zestawiania tunelu VPN między stacją roboczą, a posiadanym już koncentratorem VPN. 6. Urządzenie musi zostać dostarczone z permanentnymi licencjami pozwalającymi na zestawienie tuneli IPSec VPN dla co najmniej 100 użytkowników z komputerów PC lub urządzeń mobilnych.
3.	Interfejsy	1. Urządzenie musi posiadać minimum 6 interfejsów Gigabit Ethernet 10/100/1000. 2. Urządzenie musi zostać dostarczone z 4 wkładkami 1000Base-T Copper SFP ze wsparciem autonegocjacji 10/100/1000Mbps oraz auto MDI/MDIX. Oferowane wkładki muszą pochodzić od tego samego producenta co urządzenia sieciowe, w których będą instalowane. Wkładki muszą podlegać wsparciu serwisowemu bazującemu na kontraktach serwisowych producenta sprzętu przypisanych dla urządzeń, w których będą instalowane. 3. Urządzenie musi posiadać możliwość rozbudowy o dodatkowy moduł rozszerzeń posiadający przynajmniej 6 interfejsów GigabitEthernet 10/100/1000Base-T lub 6 interfejsów SFP 1000Base-SX/1000Base-LH/LX. 4. Urządzenie musi posiadać minimum dwa dedykowane dla zarządzania porty RJ-45: console (konsolowy) oraz management (port zarządzający 10/100/1000).
4.	VLAN	1. Urządzenie musi wspierać przynajmniej 100 VLANów per kontekst w trybie pracy jako firewall warstwy 3 (routed) dla protokołu IPv4 i IPv6. 2. Urządzenie musi wspierać przynajmniej 8 grup po 4 VLANy per kontekst w trybie pracy jako firewall warstwy 2 (transparent) dla protokołu IPv4 i IPv6.
5.	Bezpieczeństwo	1. Urządzenie musi posiadać zintegrowane sprzętowe wsparcie dla szyfrowania algorytmami DES i AES. 2. Urządzenie musi zapewniać 250 Mbps maksymalnej wydajności dla szyfrowanego symetrycznymi algorytmami 3DES/AES. 3. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. 4. Ze względów bezpieczeństwa, urządzenie musi pracować w oparciu o dedykowany 64-bitowy system operacyjny. Nie dopuszcza się rozwiązań gdzie platformą systemową jest otwarty system operacyjny np. UNIX (Linux, FreeBSD etc.) lub jego modyfikacje. 5. Urządzenie musi mieć możliwość operowania jako transparentna ściana ogniowa warstwy drugiej ISO OSI.
6.	Parametry fizyczne	1. Urządzenie musi posiadać przynajmniej 8 GB pamięci RAM oraz przynajmniej 8GB pamięci flash. 2. Urządzenie musi posiadać obudowę o wysokości 1U i zapewniać możliwość instalacji w szafie 19”.
7.	Przepustowość i wydajność	1. Urządzenie musi obsługiwać co najmniej 250 000 jednoczesnych sesji/połączeń z prędkością 15 000 połączeń na sekundę. 2. Urządzenie musi oferować co najmniej 1,2 Gbps maksymalnej wydajności dla ruchu IPv4 i IPv6.
8.	Wymagania dodatkowe	1. Urządzenie musi mieć możliwość routingu pakietów zgodnie z

		protokołami RIP, OSPF. 2. Urządzenie musi obsługiwać mechanizmy związane z obsługą ruchu multicast. 3. Urządzenie musi obsługiwać protokół NTP. 4. Urządzenie musi funkcjonalność Network Address Translation (NAT) . 5. Urządzenie musi obsługiwać mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu. 6. Urządzenie musi wspierać ramki Ethernet typu Jumbo wielkości do 9216 bajtów. 7. Urządzenie musi posiadać możliwość komunikacji z serwerami uwierzytelnienia • RADIUS, • TACACS+, • SNMP 1, 2c oraz v3. 8. Dostęp do urządzenia musi być możliwy przez SSH. 9. Urządzenie musi umożliwiać terminowanie co najmniej 250 jednoczesnych tuneli IPSec VPN site-to-site.
9.	Gwarancja	Co najmniej 36 miesięcy gwarancji, usługa serwisowa świadczona na miejscu instalacji urządzenia, przyjmowanie zgłoszenia musi być możliwe przez 24h na dobę, siedem dni w tygodniu, czas reakcji następny dzień roboczy w przypadku wystąpienia awarii. Maksymalny czas rozwiązania w przypadku awarii czternaście dni.

Zadanie 12. Oprogramowanie wspierające procesy utrzymania

Specyfikacja sprzętu i oprogramowania dla zadania nr 12

Tabela 2.12.1. Oprogramowanie (typ 2) – 1 sztuka

l.p.	cecha	wartość
1.	Tworzenie części i złożeń	▪ Możliwość modelowania bryłowego, powierzchniowego oraz hybrydowego zarówno prostych geometrii 3D jak i bardzo skomplikowanych, wymagających specjalistycznych narzędzi: skręcenia, odciśnięcia, kopuły, swobodnego formowania, powierzchni według granic, helis o zmiennym skoku, itp.: • Środowisko wieloobiektowe umożliwiające łączenie, operacje lokalne, modelowanie symetrii, przecięcie obiektów, zapis struktury części wielobryłowej do pliku złożenia przy zachowaniu asocjatywności z plikiem źródłowym, zapis pliku złożenia do pliku części wieloobiektowej ▪ Modelowanie arkuszy blach i konstrukcji spawanych w środowisku wieloobiektowym ▪ Narzędzia wspomagające projektowanie form ▪ Zaawansowane operacje na powierzchniach: • Tworzenie i edycja złożonej geometrii powierzchni i brył • Możliwość swobodnego formatowania powierzchni w oparciu o krzywe kontroli i punkty kontroli • Zaawansowane funkcje spłaszczania powierzchni
2.	Skrócenie czasu tworzenia złożeń i wspieranie standaryzacji	• Automatyczne łączenia, dopasowywanie rozmiarów • Automatyczne tworzenie otworów znormalizowanych • Automatyczne dopasowywanie elementów do istniejących otworów
3.	Rysunki 2D	• Możliwość generowania zautomatyzowanej listy materiałów z odnośnikami: ○ Aktualizacja odnośników wraz ze zmianami modelu ○ Eksport zestawienia materiałów ze złożenia lub rysunku do wydruku, lub do importu do systemu ERP/MRP ○ Aktualizacja listy materiałów w związku ze zmianą struktury złożenia

		• Możliwość edycji wymiarów części lub złożenia na asocjatywnym rysunku zapewniająca przebudowę obiektów 3D i zaktualizowanie dokumentacji • Możliwość sprawdzenia norm: o Zapewnienie spójności przez porównanie rysunków z normami obowiązującymi w firmie • Możliwość sprawdzenia rysunków – graficzne sprawdzenie wersji i porównanie rysunków w celu znalezienia różnic
4.	Obliczenia i symulacje	• Zintegrowana w programie możliwość przeprowadzenia wstępnej oceny wpływu projektu na środowisko i optymalny dobór materiałów, geometrii części i miejsc zaopatrzenia/wykonania • Zintegrowana w programie możliwość przeprowadzenia wstępnej symulacji wytrzymałościowej części z zastosowaniem Metody Elementów Skończonych • Zintegrowana w programie możliwość przeprowadzenia wstępnej symulacji przepływów płynów z zastosowaniem Metody Objętości Skończonych • Zintegrowane w programie wstępne sprawdzenie możliwości wyprodukowania modelu części pod kątem technologicznym • Zintegrowana w programie możliwość przeprowadzenia zaawansowanej symulacji wytrzymałościowej w zakresie liniowej analizy statycznej (siatka bryłowa, powierzchniowa i belkowa, analiza części i złożeń) • Zintegrowana w programie możliwość przeprowadzenia zaawansowanej symulacji kinematycznej dla części i złożeń • Funkcja automatycznego szacowanie kosztów produkcji części • Analiza stosu tolerancji • Szacowanie oddziaływania projektu na środowisko naturalne – Sustainability na poziomie części i złożeń modelu • Zintegrowana w programie CAD3D możliwość przeprowadzania zaawansowanych obliczeń wytrzymałościowych w tym: o Typ geometrii: Części i Złożenia, Modele bryłowe, powierzchniowe, belkowe i kratownice, Komponenty sztywne i Wirtualne ściany, Masa skupiona o Typy analiz: Statyczne naprężenia i przemieszczenia z kontaktem, Częstotliwości drgań własnych, Wyboczenia i utrata stabilności, Wymiana ciepła – stacjonarna i niestacjonarna, Zmęczenie / Trwałość, Test upadku, Obciążenia mieszane dla Badania zbiorników ciśnieniowych, Materiały nieliniowe, Duże przemieszczenia, Analiza niestacjonarna, Dynamika liniowa – Historia modalna, Harmoniczna, Drgania losowe o Własności materiałów: Liniowy sprężysty izotropowy & ortotropowy zależny od temperatury, Nieliniowy plastyczny von Mises, Nieliniowy sprężysty, Hipersprężysty Mooney-Rivlin & Ogden, Nieliniowy wiskoelastyczny (pełzanie), Nitinol, Kompozyty – laminaty o Narzędzia projektowe: Badania wielotokowe / scenariusz „Co jeśli”, Tabela danych wejściowych dla scenariusza dowolnych kombinacji, Doradca symulacji, Sensory z alarmem ograniczeń projektowych, Metody adaptacyjny siatki elementów skończonych dla zbieżności, Optymalizacja i wgląd w projekt oraz Śledzenie trendu o Środowisko (obciążenia/umocowania): Normalne i kierunkowe ciśnienie i siła, Nierównomierny rozkład ciśnienia i siły, Grawitacja, Siła odśrodkowa, Przyspieszenie liniowe i obrotowe, Sztywna i Rozprowadzona masa, Obciążenie łożyskiem, Obciążenie temperaturą dla rozkładu termicznego, Import obciążeń z symulacji kinematycznych, Symetria i Symetria kołowa, Geometria odniesienia (nieruchoma, cylindryczna, sferyczna, płaska, Przesuwne podpory /

		Nieruchome, Umocowanie łożyskiem kulowym, Temperatura, Konwekcja, Radiacja, Moc cieplna, Strumień ciepła, Import temperatur do Badania statycznego z Badania termicznego, Import wyników przepływu jako obciążeń w Statycznym i Termicznym Badaniu o Połączenia komponentów: Kontakt Część-Do-Części z poślizgiem i tarciem, Kontakt wiązany stykających ścian części, Pasowanie skurczowe, Sprężyna, Śruba, Sworzeń i Spoina Punktowa, Opór termiczny o Narzędzia wyświetlania wyników: Wypadkowa i składowe przemieszczenia z deformacją, Naprężenia vonMises, Naprężenia główne, składowe naprężenia, Odkształcenia główne, Składowe odkształcenia, Gęstość energii odkształcenia, Kryterium vonMises, Tresca, Mohr-Coulomb dla współczynnika bezpieczeństw, Współczynnik bezpieczeństwa śrub i kołków, Sonda i lokalne wyświetlanie, Dynamiczne przekroje, Porównanie wyników z wielu badań, Zdeformowana geometria (zapis jako część do programu CAD3D),Trwałość i uszkodzenie, Kształt modów częstotliwości rezonansowych z animacją, Kształt wyboczenia, Rozkład temperatury i strumienia ciepła, Naprężenie zlinearyzowane dla badania zbiornika ciśnieniowego, Odpowiedź w funkcji czasu dla Badania upadku, Odpowiedź w funkcji przyrostu obciążenia, Odpowiedź w funkcji czasu lub częstotliwości dla Analizy dynamicznej z PSD o Współpraca i wymiana danych: Raporty HTML i DOC, Zapis wykresów do BMP, JPEG, VRML, XGL czy AVI, Biblioteka / Szablony, Eksport do innych aplikacji MES
5.	Możliwość pracy z projektem bez konieczności rozumienia szczegółów oprogramowania	• Narzędzia rozwiązujące konflikty w predefiniowanych szkicach i proponujące zestawy rozwiązań • Narzędzie zarządzające tworzywem i modyfikacją pochyleń • Narzędzie zarządzające interakcjami pomiędzy operacjami zaokrąglania i pochylenia • Narzędzie do identyfikacji problemów dotyczących wiązań w złożeniach.
6.	Obsługa formatów plików	Obsługa popularnych formatów plików CAD, w tym: DWG, DXF, PRT, ASM, IPT, IAM, SLDDRW, SLDPRT, SLDASM, SAT, STEP, IGS, STL, Parasolid
7.	Zapis dokumentacji	• Możliwość zapisania z poziomu aplikacji CAD dokumentacji (część/złożenie/rysunek płaski wraz z modelem 3D, z którego został wykonany) do pliku wykonywalnego EXE niewymagającego od odbiorcy instalowania jakichkolwiek dodatkowych aplikacji. • Możliwość dodawania znaczników, odnośników i notatek do przeglądanego pliku • Możliwość mierzenia, dodawania przekrojów i sprawdzania właściwości masy pliku • Możliwość ochrony pliku poprzez hasło
8.	Model licencjonowania	• Możliwość instalacji oprogramowania na wielu stacjach (liczba większa od posiadanych kluczy licencyjnych). • Możliwość uruchomienia programu w tym samym czasie w ilości zgodnej z liczbą posiadanych kluczy. • Możliwość manualnego przenoszenia aktywnej licencji programu z komputera na komputer.
9.	Subskrypcja	• Roczne wsparcie techniczne z aktualizacjami do najnowszej wersji • Możliwość otrzymania pomocy technicznej kanałami: poczta email, zdalny pulpit, portal www „HelpDesk”, telefon, wizyta bezpośrednia.
10.	Firma wdrażająca	Firma wdrażająca musi zagwarantować obecność w swej kadrze pracowników z odpowiednim doświadczeniem potwierdzonym zdaniem niezbędnych egzaminów i posiadaniem pełnej certyfikacji producenta

		oprogramowania.
11.	Wymaganie dodatkowe	• Bezproblemowa praca (widoczna i edytowalna historia operacji) na istniejącej dokumentacji CAD3D (SLDDRW, SLDPRT, SLDASM). • Możliwość przeprowadzenia wizualizacji i renderingu modelu bezpośrednio z poziomu aplikacji projektowej. • Dostęp do biblioteki elementów znormalizowanych. • Możliwość otwierania i obróbki plików zawierających chmury punktów lub siatki ze skanerów 3D i maszyn pomiarowych. • Import i eksport obwodów drukowanych PCB z popularnych aplikacji ECAD. • Zintegrowane narzędzie do zarządzania plikami projektowymi w ramach grupy konstruktorów. • Automatyzacja często wykonywanych operacji tj. konwersja pomiędzy formatami pliku, generowanie rysunków na bazie modeli 3D, aktualizacja plików, renderowanie. • Możliwość tworzenia konfiguracji części i złożeń oraz zapisywania typoszeregów w pojedynczym pliku. • Współpraca z arkuszem kalkulacyjnym w celu automatyzacji tworzenia konfiguracji. • Automatyzacja projektowania instalacji rurowych i okablowania. • Wizualne planowanie, tworzenie, edytowanie i wyświetlanie struktury złożenia.

Zadanie 13. Infrastruktura sieciowa

Specyfikacja sprzętu i oprogramowania dla zadania nr 13

Tabela 2.13.1. Osprzęt sieciowy (typ 18) – 2 sztuki

l.p.	cecha	wartość
1.	Informacja ogólna	Urządzenia związane z równoważeniem obciążenia ruchu sieciowego o dużym wolumenie, pracujące w układzie redundancji dla wielu sieci.
2.	Pamięć i dysk	Pamięć co najmniej 32GB, dysk co najmniej 380GB SSD lub szybszy.
3.	Procesor	Co najmniej 4 rdzeniowa jednostka (rdzenie fizyczne).
4.	Przetwarzanie ruchu	Urządzenie musi obsługiwać co najmniej 1,6 miliona rozkazów L7 na sekundę, co najmniej 770 tysięcy połączeń L4, co najmniej 7 milionów zapytań http L4 na sekundę, co najmniej 24 miliony jednoczesnych połączeń L4. Przepustowość co najmniej 40Gbps dla L4 i co najmniej 20Gbps dla L7
5.	FIPS SSL	Urządzenie musi spełniać co najmniej standard FIPS 140-2 Poziom 2 lub wyższy, co najmniej 9000 TPS (transakcji na sekundę) przy 2k kluczach, obsługa co najmniej 18Gbps ruchu szyfrowanego.
6.	Architektura oprogramowania układowego	64-bit
7.	Kompresja sprzętowa	Co najmniej 18Gbps
8.	Sprzętowe zabezpieczenie DDOS	Co najmniej 40 milionów SYN cookies na sekundę
9.	Porty	Co najmniej 4 porty miedziane 1GE, co najmniej 8 portów 10GE SFP+ w tym co najmniej 2 porty wyposażone we wkładki SR
10.	Zasilanie	Co najmniej dwa zasilacze wbudowane w urządzenie.
11.	Montaż i wymiary	Urządzenie musi mieć wymiary pozwalające na montaż w szafie rack 19”. Wraz z urządzeniem należy dostarczyć komplet elementów montażowych pozwalających na montaż w szafie rack.
12.	Gwarancja	Co najmniej 36 miesięcy gwarancji, serwis świadczony w miejscu montażu urządzenia, czas usunięcia awarii nie dłuższy niż 14 dni kalendarzowych, czas reakcji na awarię następny dzień roboczy.

Tabela 2.13.2. Osprzęt sieciowy (typ 19) – 2 sztuki

l.p.	cecha	wartość
1.	Informacje ogólne	Serwer konsolowy wraz z okablowaniem.
2.	Interfejsy	1. Urządzenie musi posiadać co najmniej 16 portów konsolowych (RJ-45). 2. Urządzenie musi posiadać przynajmniej dwa porty sieciowe RJ-45 Gigabit Ethernet 10/100/1000BT. 3. Urządzenie musi posiadać przynajmniej jeden port konfiguracyjny (Console Setup) RJ-45 (RS-232). 4. Urządzenie musi posiadać przynajmniej jeden port USB w wersji co najmniej 2.0.
3.	Zarządzanie konsolą	Urządzenie musi charakteryzować się co najmniej obsługą następujących funkcjonalności względem zarządzania konsolą: a) Obsługa break przez SSH, b) Zapisywanie daty i godziny logowanych zdarzeń, c) Zdalne lub lokalne składowanie logów, d) Sun Break-safe, e) Nielimitowana ilość jednoczesnych sesji, f) Konfigurowalne powiadamianie o zdarzeniach (co najmniej SNMP trap),
4.	Bezpieczeństwo	Urządzenie musi charakteryzować się co najmniej obsługą następujących funkcjonalności względem bezpieczeństwa: a) Predefiniowane profile bezpieczeństwa oraz możliwość tworzenia własnych profili, b) Obsługa standardu SSHv1 oraz v2, c) Autoryzacja grupowa: TACACS+, RADIUS, LDAP, d) Uwierzytelnianie lokalne: RADIUS, TACACS+, LDAP/AD, NIS, Kerberos, RSA SecureID, e) Definiowana lista dostępowa na każdym porcie RS-232, f) Syslog, g) Wbudowany moduł kryptograficzny, h) Obsługa IPSec oraz NAT, i) Filtrowanie pakietów IP, j) Obsługa IP Forwarding.
5.	Dodatkowe funkcjonalności	1. Urządzenie musi posiadać przynajmniej jeden zasilacz 10-240 VAC. 2. Urządzenie musi posiadać przynajmniej jeden wbudowany czujnik temperatury. 3. Wszystkie porty RS-232 muszą mieć możliwość podłączenia do listew iPDU. 4. Urządzenie musi być dostarczone z fabrycznie nowymi kablami konsolowymi typu „rollover” w następującej ilości: 10 kabli o długości 2m oraz 4 kable o długości 10m.
6.	Gwarancja	Urządzenie musi być nowe i objęte co najmniej dwuletnią gwarancją producenta.

Zadanie 14. Oprogramowanie warstwy zarządzającej

Specyfikacja sprzętu i oprogramowania dla zadania nr 14

Tabela 2.14.1. Oprogramowanie (typ 3) – 1 pakiet

l.p.	cecha	wartość
1.	Informacje ogólne	Pakiet oprogramowania rozszerzający obecnie posiadane przez Zamawiającego licencje i środowiska oraz zapewniający szersze wykorzystanie obecnie posiadanych licencji. W wyniku realizacji zadań ujętych w przetargu z dnia 22.06.2011 Zamawiający otrzymał licencje i wdrożył rozwiązania bazujące na oprogramowaniu firmy Microsoft. W szczególności dotyczy to środowiska

		opartego o rozwiązania VMware oraz przede wszystkim środowisko deweloperskie, usługowe (platforma do sprzedaży usług cloud computing, serwer IIS, serwer Active Directory, serwer bazodanowy MS SQL) oraz środowisko testowe, backoffice, monitorujące oraz serwisowe. W wyniku realizacji zadań ujętych w przetargu z dnia 07.10.2011 Zamawiający wdrożył i wykorzystuje system zarządzania budynkiem BMS, system kart kontroli dostępu, system kamer przemysłowych które do poprawnego działania wymagają środowiska opartego o oprogramowanie Microsoft. W wyniku realizacji zadań ujętych w przetargu z dnia 20.03.2014 Zamawiający wdrożył i wykorzystuje oprogramowanie do monitorowania ruchu sieciowego, który do poprawnego działania wymaga środowiska opartego o oprogramowanie Microsoft. Oprogramowanie będące przedmiotem niniejszego zadania, ma służyć rozbudowie wszystkich wyżej wymienionych środowisk, zwiększeniu ich bezpieczeństwa poprzez dodanie elementów redundantnych oraz zwiększeniu ich potencjału rozwojowego w celu pełniejszego wykorzystania do zadań realizowanych przez Zamawiającego.
2.	Warstwa zarządzająca	1. Windows Server DataCenter 2012 R2 x64 EN 2 CPU lub równoważne – 3 licencje z gwarancją wersji na co najmniej 36 miesięcy. Przez równoważny dla pozycji 1. Zamawiający rozumie oprogramowanie spełniające warunki, zależności I funkcjonalności opisane w punkcie 1 i 7 tabeli 2.14.1. 2. System Center 2012 R2 DataCenter Edition 2 CPU lub równoważne - 3 licencje z gwarancją wersji na co najmniej 36 miesięcy. Przez równoważny dla pozycji 2. Zamawiający rozumie oprogramowanie spełniające warunki, zależności I funkcjonalności opisane w punkcie 1 i 8 tabeli 2.14.1.
3.	Warstwa backoffice	1. Exchange Server Standard 2013 EN lub równoważne - 2 licencje. Przez równoważne Zamawiający rozumie oprogramowanie spełniające zapisy punktu 1 i 9 tabeli 2.14.1. 2. SharePoint Server 2013 EN - 1 licencja. Przez równoważne Zamawiający rozumie oprogramowanie spełniające zapisy punktu 1 i 10 tabeli 2.14.1. 3. Lync Server 2013 EN - 2 licencje. Przez równoważne Zamawiający rozumie oprogramowanie spełniające zapisy punktu 1 i 11 tabeli 2.14.1. 4. SQL Server Standard Core 2014 Edition EN 2 Licenses – 4 licencje. 5. Project Server 2013 Single – 1 licencja. 6. Project Server CAL 2013 Device – 10 licencji.
4.	Licencje dostępowe	Enterprise CAL Suite EN - 75 licencji. Przez równoważne Zamawiający rozumie oprogramowanie spełniające zapisy punktu 1 i 12 tabeli 2.14.1.
5.	Warstwa rozwoju oprogramowania	1. Visual Studio Team Foundation Server 2013 – 1 licencja. 2. Visual Studio Team Foundation Server CAL 2013 Device – 5 licencji.
6.	Wymagania dodatkowe	Licencje muszą być nowe, nie używane, pochodzić z legalnego kanału sprzedaży. Licencje muszą umożliwiać Zamawiającemu trwałe w czasie wykorzystywanie licencji. Licencje muszą umożliwiać Zamawiającemu zapewnienie dostępu do najnowszej wersji oferowanego oprogramowania, poprawek krytycznych i opcjonalnych przez co najmniej 36 miesięcy. Licencje muszą być przenaszalne, bezterminowe oraz muszą dawać możliwość sublicencjonowania na podmioty stowarzyszone.

7.	Wymagania systemu operacyjnego dla serwerów	Licencja na serwerowy system operacyjny musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do: uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym, nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji na serwerze fizycznym. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 6 fizycznych procesorów co najmniej 8 rdzeniowych oraz co najmniej 1 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 48 procesorów wirtualnych oraz 256MB pamięci RAM i dysku o pojemności do 8TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 6 węzłów, z możliwością uruchamiania 100 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 kontroli dostępu dla określonych grup użytkowników. 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 opartych o iOS i Windows 8.1. 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 100 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.
8.	Wymagania dla oprogramowania do zarządzania środowiskami	Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego procesora fizycznego na serwerze zarządzanym. Oprogramowanie musi być licencjonowane na minimum 2 fizyczne

	serwerowymi	procesory każdego z 3 serwerów zarządzających. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do zarządzania dowolną liczbą środowisk systemu operacyjnego na tym serwerze. Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach: • System zarządzania infrastrukturą i oprogramowaniem • System zarządzania komponentami • System zarządzania środowiskami wirtualnym • System tworzenia kopii zapasowych • System automatyzacji zarządzania środowisk IT • System zarządzania incydentami i problemami • Ochrona antymalware System zarządzania infrastrukturą i oprogramowaniem System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji. 1. Inwentaryzacja i zarządzanie zasobami: a. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania b. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu c. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp…) d. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta e. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera 1. Użytkowane oprogramowanie – pomiar wykorzystania a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego. 2. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych. 3. Definiowanie i sprawdzanie standardu serwera: a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być

		określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej, b. Reguły powinny sprawdzać następujące elementy systemy komputerowego: - stan usługi (Windows Service) - obecność poprawek (Hotfix) - WMI - rejestr systemowy - system plików - Active Directory - SQL (query) - Metabase 4. Raportowanie, prezentacja danych: a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services c. System powinien posiadać predefiniowane raport w następujących kategoriach: - Sprzęt (inwentaryzacja) - Oprogramowanie (inwentaryzacja) - Oprogramowanie (wykorzystanie) - Oprogramowanie (aktualizacje, w tym system operacyjny) d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu 5. Analiza działania systemu, logi, komponenty a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym. System zarządzania komponentami System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania: 1. Architektura a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji. b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług. c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być

		pobierane z usług katalogowych. d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny. e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych. f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany. g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN). h. Wsparcie dla protokołu IPv6. i. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta. 2. Audyt zdarzeń bezpieczeństwa System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować: a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących). b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji. c. Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów. 3. Konfiguracja i monitorowanie System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym: a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z: - rejestru - WMI - OLEDB - LDAP - skrypty (uruchamiane w celu wykrycia atrybutów obiektu), W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi. b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp… c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane

		w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla: - Windows Server 2003/2008/2008R2 - Active Directory 2003/2008 - Exchange 2003/2007/2010 - Microsoft SharePoint 2003/2007/2010 - Microsoft SharePoint Services 3.0 - Microsoft SharePoint Foundation 2010 - SQL 2005/2008/2008R2 (x86/x64/ia64) - Windows Client OS (XP/Vista/7) - Information Worker (Office, IExplorer, Outlook, itp…) - IIS 6.0/7.0/7.5 - HP-UX 11i v2/v3 - Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86) - Red Hat Enterprise Linux 4/5/6 (x86/x64) Server - Novell SUSE Linux Enterprise Server 9/10SP1/11 - IBM AIX v5.3 i v6.1/v7.1 (POWER) d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego. e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji: - interfejsy sieciowe - porty - sieci wirtualne (VLAN) - grupy Hot Standby Router Protocol (HSRP) f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych: - SNMP (trap, probe) - WMI Performance Counters - Log Files (text, text CSV) - Windows Events (logi systemowe) - Windows Services - Windows Performance Counters (perflib) - WMI Events - Scripts (wyniki skryptów, np.: WSH, JSH) - Unix/Linux Service - Unix/Linux Log g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów 4. Tworzenie reguł a. w systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych: - Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event) - Performance based (SNMP performance, WMI performance, Windows performance)

		- Probe based (scripts: event, performance) b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia. c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości: - na ilość takich samych próbek o takiej samej wartości - na procentową zmianę od ostatniej wartości próbki. d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia" się monitorowanego parametru w zakresie przebiegu bazowego „baseline" w zadanym okresie czasu. e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji. f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym: - ASP .Net Application - ASP .Net Web Service - OLE DB - TCP Port - Web Application - Windows Service - Unix/Linux Service - Process Monitoring Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji. h. Z każdym elementem monitorującym (w szczególności monitor, reguła, alarm) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu). i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych. j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla: monitora (dostepność), i licznika wydajności (z agregacją dla wartości – min, max, avg). 5. Przechowywanie i dostęp do informacji a. Wszystkie informacje operacyjne (w szczególności zdarzenia, liczniki wydajności, informacje o obiektach, alarmy) powinny być przechowywane w

		bazie danych operacyjnych. b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane. c. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy). d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności. e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych. f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów: - XML - CSV - TIFF - PDF - XLS - Web archive 6. Konsola systemu zarządzania a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli. b. System powinien udostępniać dwa rodzaje konsoli: - w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna) - w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa). c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach: - Alerts - Events - State - Performance - Diagram - Task Status - Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu). d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie. e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (w szczególności po typie, ważności, typach obiektów), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych". f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.

		g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym: - opcji definiowania ról użytkowników - opcji definiowania widoków - opcji definiowania i generowania raportów - opcji definiowania powiadomień - opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących - opcji instalacji/deinstalacji klienta h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostepu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego). 7. Wymagania dodatkowe a. System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający w szczególności na: - Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo), - Wykonywanie operacji w systemie z poziomu linii poleceń, - Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania, - Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie, System zarządzania środowiskami wirtualnym System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy: 1. Architektura a. System zarządzania środowiskiem wirtualnym powinien składać się z: - serwera zarządzającego, - relacyjnej bazy danych przechowującej informacje o zarządzanych elementach, - konsoli, instalowanej na komputerach operatorów, - portalu self-service (konsoli webowej) dla operatorów „departamentowych”, - biblioteki, przechowującej komponenenty niezbędne do budowy maszyn wirtualnych, - agenta instalowanego na zarządzanych hostach wirtualizacyjnych, - „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych. b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over). c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców. 2. Interfejs użytkownika a. Konsola musi umożliwiać wykonywanie codziennych zadań związnych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny. b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień

		posczególnym operatorom do grup hostów. c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy w szczególności maszyny wyłączone, maszyny z systemem operacyjnym X, d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit. e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań. 3. Scenariusze i zadania a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach: 1. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny, 2. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych: - profilu sprzętowego - profilu systemu operacyjnego, - przygotowanych dysków twardych, b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania. c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami: - w trybie migracji „on-line” – bez przerywania pracy, - w trybie migracji „off-line – z zapisem stanu maszyny d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami. e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta. f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance” w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu. g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej. h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji. 4. Wymagania dodatkowe a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę. b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania. c. System musi kreować raporty z działania zarządzanego środowiska, w tym:

		- utylizacja poszczególnych hostów, - trend w utylizacji hostów, - alokacja zasobów na centra kosztów, - utylizacja poszczególnych maszyn wirtualnych, - komputery-kandydaci do wirtualizacji d. System musi umożliwiać skorzystanie z szablonów: - wirtualnych maszyn - usług oraz profili dla: - aplikacji - serwera SQL - hosta - sprzętu - systemu operacyjnego gościa e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów). f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej. g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją) System tworzenia kopii zapasowych System tworzenia i odtwarzania kopii zapasowych danych (backup) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać następujące wymagania: 1. System musi składać się z: a. serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych b. agentów kopii zapasowych instalowanych na komputerach zdalnych c. konsoli zarządzającej d. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach e. wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną f. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service) 2. System kopii zapasowych musi umożliwiać: a. zapis danych na puli magazynowej złożonej z dysków twardych b. zapis danych na bibliotekach taśmowych 3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej. 4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe. 5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej. 6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania. 7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej

		pełnej kopii. 8. System kopii zapasowych powinien umożliwiać przywrócenie: a. danych plikowych b. danych aplikacyjnych c. stanu systemu (Systemstate) d. obrazu systemu operacyjnego (tzw. Bare Metal Restore) 9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych 10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości 11. Agenci systemu kopii zapasowych muszą posiadać konfiguracje dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy 12. System kopii zapasowych musi rozpoznawać aplikacje: a. ze względu na tworzone logi transakcyjne: - Microsoft Exchange Server - Microsoft Office Sharepoint Server - Microsoft SQL Server b. ze względu na zapewnienie nieprzerwalności pracy - Microsoft Virtual Server 2005 - Microsoft Hyper-V server 13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach 14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach 15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów 16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń 17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki „Poprzednie wersje” 18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych 19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych 20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.). 21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku 22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat 23. System kopii zapasowych musi umożliwiać synchronizacje przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie te muszą być tworzone w

		ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób. 24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe. 25. System kopii zapasowych musi umożliwiać odtworzenie danych do: a. lokalizacji oryginalnej b. lokalizacji alternatywnej c. w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych System automatyzacji zarządzania środowisk IT System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk. 1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie. 2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT. 3. System musi wspomagać planowanie i automatyzację wdrażania poprawek. 4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych. 5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania worklow. 6. Wbudowane konektory zapewniające integrację narzędzi Microsoft System Center, HP OpenView, IBM Tivoli i BMC Patrol do zarządzania oprogramowaniem i sprzętem. 7. Wbudowane (gotowe) workflow, takie jak: - Active Directory Password Reset - Microsoft Cluster Patching - Microsoft SQL Server Cluster Patching - Microsoft SQL: Server Dump Copy Load - Operations Manager Event Remediation - Operations Manager Event Remediation and Enrichment - Operations Manager Service Alert Testing - VM Provisioning - Working with FTP - Operations Manager Tool Integration - Operations Manager: Manager of Managers - Operations Manager: Maintenance Windows - Active Directory: New Employee Onboarding - Operations Manager: Multi-Service Desk Integration System zarządzania incydentami i problemami System zarządzania incydentami i problemami musi spełniać następujące wymagania: 1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna) 2. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np.

		MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą. 3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami. 4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie. 5. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać: - Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką, - Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia, - Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu, - Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania, - Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniu systemu w przypadku incydentów, - Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej, - Tworzenie baz wiedzy na temat rozwiązywania problemów, - Automatyzację działań w przypadku znanych i opisanych problemów, - Wykrywanie odchyleń od założonych standardów ustalonych dla systemu. Ochrona antymalware Oprogramowanie antymalware musi spełniać następujące wymagania: 1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day. 2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem 3. Centralne zarządzanie politykami ochrony. 4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony. 5. Mechanizmy wspomagające masową instalację. 6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów", skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego. 7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie

		oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania. 8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia. 9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (w szczególności ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa"). 10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania. 11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.
9.	Wymagania dla oprogramowania serwera systemu pocztowego	Serwer systemu poczty elektronicznej musi charakteryzować się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich: 1. Funkcjonalność podstawowa: a. Odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych. b. Mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata. c. Tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami. d. Zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia. e. Wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości. f. Pełne wsparcie dla klienta poczty elektronicznej MS Outlook 2007 i nowszych wersji. 2. Funkcjonalność wspierająca pracę grupową: a. Możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. b. Możliwość określenia terminu wygaśnięcia wiadomości. c. Udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu. d. Podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze. e. Mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone. f. Mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania. g. Tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań.

		h. Mechanizm udostępniania współdzielonych skrzynek pocztowych. i. Obsługa list i grup dystrybucyjnych. j. Dostęp ze skrzynki do poczty elektronicznej, poczty głosowej, wiadomości błyskawicznych i SMS-ów. k. Możliwość informowania zewnętrznych użytkowników poczty elektronicznej o dostępności lub niedostępności. l. Możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności. m. Widok rozmowy, automatycznie organizujący wątki wiadomości w oparciu o przebieg wymiany wiadomości między stronami. n. Konfigurowalna funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności. o. Transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie oznaczanie priorytetu wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego. p. Możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej. q. Telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów. r. Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby wsparcia ze strony informatyków. s. Mechanizm automatycznego dostosowywania się funkcji wyszukiwania kontaktów do najczęstszych działań użytkownika skutkujący ustawieniem priorytetu wyników wyszukiwania. t. Możliwość wyszukiwania i łączenia danych (zgodnie z nadanymi uprawnieniami) z systemu poczty elektronicznej oraz innych systemów w organizacji (portali wielofunkcyjnych, komunikacji wielokanałowej i serwerów plików). u. Możliwość dostępu do poczty elektronicznej i dokumentów przechowywanych w portalu wielofunkcyjnym z poziomu jednego interfejsu zarządzanego przez serwer poczty elektronicznej. 3. Funkcjonalność wspierająca zarządzanie systemem poczty: a. Oparcie się o profile użytkowników usługi katalogowej Active Directory. b. Wielofunkcyjna konsola administracyjna umożliwiająca zarządzanie systemem poczty oraz dostęp do statystyk i logów użytkowników. c. Definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. d. Możliwość definiowania różnych limitów pojemności skrzynek dla różnych grup użytkowników. e. Możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer. f. Możliwość korzystania interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną. g. Narzędzia kreowania, wdrażania i zarządzania politykami nazewnictwa grup dystrybucyjnych. 4. Utrzymanie bezpieczeństwa informacji a. Centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym: śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, oraz archiwizacja danych.

		b. Możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych. c. Mechanizm zapobiegania wycieku danych ograniczający możliwość wysyłania danych poufnych do nieuprawnionych osób poprzez konfigurowalne funkcje monitoringu i analizy treści, bazujący na ustalonych politykach bezpieczeństwa. d. Możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości. e. Możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych zapytań przez pracowników działu lub osoby odpowiedzialne za zgodność z uregulowaniami. f. Integracja z usługami zarządzania dostępem do treści pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania. Wymagana jest możliwość użycia 2048-bitowych kluczy RSA, 256-bitowych kluczy SHA-1 oraz algorytmu SHA-2. g. Odbieranie wiadomości zabezpieczonych funkcją IRM przez zewnętrznych użytkowników oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS. h. Przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji. i. Wbudowane filtrowanie oprogramowania złośliwego, wirusów i oprogramowania szpiegującego zawartego w wiadomościach wraz z konfigurowalnymi mechanizmami powiadamiania o wykryciu i usunięciu takiego oprogramowania. j. Mechanizm audytu dostępu do skrzynek pocztowych z kreowaniem raportów z audytów. 5. Wsparcie dla użytkowników mobilnych: a. Możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu. Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem b. Możliwość „lekkiej” synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.) c. Możliwość korzystania z usług systemu pocztowego w podstawowym zakresie przy pomocy urządzeń mobilnych typu smartphone. d. Możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej. e. Umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej. f. Obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak

		Internet Explorer, Apple Safari i Mozilla Firefox. 6. Funkcje związane z niezawodnością systemu: a. Zapewnienie pełnej redundancji serwerów poczty elektronicznej bez konieczności wdrażania klastrów oraz niezależnych produktów do replikacji danych. b. Automatyzacja replikacji bazy danych i przełączania awaryjnego już dla dwóch serwerów poczty, a także w wypadku centrów danych rozproszonych geograficznie. c. Utrzymanie dostępności i uzyskanie możliwości szybkiego odzyskiwania po awarii dzięki możliwości konfiguracji wielu replik każdej bazy danych skrzynki pocztowej. d. Automatyczne odtwarzanie redundancji poprzez tworzenie kopii zapasowych w miejsce kopii na uszkodzonych dyskach według zadanego schematu. e. Ograniczenie zakłócenia pracy użytkowników podczas przenoszenia skrzynek pocztowych między serwerami, pozwalające na przeprowadzanie migracji i konserwacji w dowolnym czasie – nawet w godzinach pracy biurowej. f. Zapewnienie ochrony przed utratą e-maili spowodowaną uaktualnianiem lub awarią roli serwera transportu poprzez zapewnienie redundancji i inteligentne przekierowywanie poczty na inną dostępną ścieżkę.
10.	Wymagania dla oprogramowania serwera portalu wielofunkcyjnego	Serwer portalu wielofunkcyjnego, który posiada następujące cechy dostępne bezpośrednio: a. Publikację dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych i zewnętrznych. b. Tworzenie wspólnej infrastruktury wszystkich stron dla całej organizacji w oparciu o farmę serwerów portalu. c. Zarządzanie strukturą portalu i treściami WWW. d. Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści. e. Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej. f. Udostępnienie formularzy elektronicznych. g. Tworzenie repozytoriów dokumentów oraz wzorów dokumentów. h. Wspólną, bezpieczną pracę nad dokumentami. i. Wersjonowanie dokumentów (dla wersji roboczych (0.1,0.2) i głównych (1.0,2.0)). j. Organizację pracy grupowej. k. Wyszukiwanie treści. l. Dostęp do danych w relacyjnych bazach danych. m. Analizy danych wraz z graficzną prezentacją danych, (w tym drążenie danych oraz drzewo dekompozycji dostępne z poziomu przeglądarki). n. Możliwość wykorzystanie mechanizmów portalu do budowy systemu zarządzania e-szkoleniami (e-learning). o. Możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie. p. Możliwość zaimplementowania procesów przepływu dokumentów i spraw oraz zapewnienie dostępu do informacji niezbędnych do realizacji założonych celów i procesów. 1. Interfejs użytkownika: a. Praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w

		specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu). b. Wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0 c. Praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów d. Tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego e. Możliwość pracy off-line z plikami przechowywanymi w repozytoriach portalu f. Umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych. 2. Uwierzytelnianie – wbudowane mechanizmy wspierające uwierzytelnianie na bazie: a) Oświadczeń (claim-based authentication) z wykorzystaniem: ▪ Open Authorization 2.0 dla uwierzytelniania aplikacji, ▪ Uwierzytelniania w trybie server-to-server, ▪ SAML ▪ Windows claims b) Pojedynczego logowania domenowego (single-sign on), c) Na bazie formularzy (Form-based). 3. Projektowanie stron a) Wbudowane narzędzia projektowania wyglądu stron, b) Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML, c) Wsparcie dla ASP.NET, Apache, C#, Java i PHP, d) Możliwość osadzania elementów iFrame w polach HTML na stronie. 4. Integracja z pozostałymi modułami rozwiązania oraz innymi systemami: a) Wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili b) Dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów c) Możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili d) Integracja z systemem obsługującym serwis WWW w zakresie publikacji treści z repozytoriów wewnętrznych firmy na zewnętrzne strony serwisu WWW (pliki, strony) e) Integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego f) Wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services g) Mechanizm jednokrotnej identyfikacji (single sign-on) pozwalający na autoryzację użytkowników portalu i dostęp do danych w innych systemach biznesowych, niezintegrowanych z systemem LDAP. h) Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

		i) Integracja z pakietem biurowym w zakresie wyświetlania oraz edycji metryk dokumentu z poziomu pakietu biurowego. j) Integracja z pakietem biurowym w zakresie tworzenia i modyfikacji formularzy elektronicznych bez potrzeby znajomości HTML przez użytkownika końcowego. k) Integracja z mechanizmami relacyjnej bazy danych poprzez dostępność narzędzi wizualizacji analiz biznesowych dostępnych serwerze bazodanowym. 5. Zarządzanie treścią i wyglądem portalu powinno opierać się o narzędzia umożliwiające prostą i intuicyjną publikację treści w formacie HTML w trybie WYSIWYG, bez konieczności znajomości języka HTML i innej wiedzy technicznej przez autorów treści: a) Możliwość formatowania tekstu w zakresie zmiany czcionki, rozmiaru, koloru, pogrubienia, wyrównania do prawej oraz lewej strony, wyśrodkowania, wyjustowania. b) Proste osadzenie i formatowanie plików graficznych, łącz (linków) różnych typów, tabel, paragrafów, wypunktowań itp. w treści artykułów publikowanych w intranecie (stron HTML) c) Spójne zarządzanie wyglądem stron intranetu, głównie pod kątem formatowania tekstu: możliwość globalnego zdefiniowania krojów tekstu, które mogą być wykorzystywane przez edytorów treści, możliwość wklejania treści przy publikacji stron intranetu z plików tekstowych lub edytorów tekstu (np. MS Word) z zachowaniem lub z usunięciem formatowania oryginalnego d) Zarządzanie galeriami zasobów elektronicznych (pliki graficzne, filmy video, dokumenty), wykorzystywanymi przy tworzeniu stron intranetu i przechowywanymi w intranetowym repozytorium treści. Możliwość współdzielenia tych zasobów na potrzeby stron umiejscowionych w różnych obszarach portalu intranetowego. Podstawowe funkcjonalności związane z wersjonowaniem i wyszukiwaniem tych zasobów e) Definiowanie szablonów dla układów stron (tzw. layout'ów), określających ogólny układ stron intranetu oraz elementy wspólne dla stron opartych na tym samym szablonie. Możliwość stworzenia wielu szablonów na potrzeby różnych układów stron w zależności od potrzeb funkcjonalnych w różnych częściach intranetu. Możliwość generalnej zmiany wyglądu utworzonych już stron poprzez modyfikację szablonu, na którym zostały oparte f) Możliwość wielokrotnego wykorzystania elementów zawartości intranetu (części treści publikowanych na stronach) w różnych częściach portalu, tzn. modyfikacja zawartości w jednym miejscu powoduje jej faktyczną zmianę na wszystkich stronach intranetu, gdzie dana treść została opublikowana g) Możliwość odwzorowania w systemie CMS przyjętej wizualizacji portalu intranetowego (projekt graficzny i funkcjonalny). h) Możliwość osadzania na stronach narzędzia do odtwarzania materiałów audio i wideo, 6. Organizacja i publikacja treści: a) Wersjonowanie treści stron intranetu, działające automatycznie przy wprowadzaniu kolejnych modyfikacji przez edytorów treści. b) Zastosowanie procesów zatwierdzania zawartości przez publikacją, tzn. Udostępnieniem jej dla szerokiego grona pracowników. Możliwość zdefiniowania przynajmniej dwóch poziomów uprawnień edytorów (edytor i recenzent), przy czym treści publikowane przez edytorów muszą uzyskać pozytywną akceptację recenzenta przed Udostępnieniem jej wszystkim użytkownikom intranetu. c) Możliwość budowania hierarchicznej struktury stron portalu z

		prostym przenoszeniem stron i sekcji w ramach struktury nawigacji. d) Automatyczne tworzenie nawigacji na stronach intranetu, odwzorowujące obecną hierarchię. e) Automatyczne generowanie mapy stron portalu. f) Możliwość definiowania nawigacji w oparciu o centralne zarządzanie metadanymi. g) Umożliwienie zarządzania poszczególnymi obszarami portalu osobom nietechnicznym, pełniącym rolę edytorów bądź administratorów merytorycznych. Istotne jest nieangażowanie zespołu IT w proces zarządzania treścią intranetu. h) Definiowanie uprawnień użytkowników niezależnie do poszczególnych sekcji i stron intranetu, np. do obszarów poszczególnych spółek, dywizji, biur. Dotyczy to zarówno uprawnień do odczytu zawartości, jak i edycji oraz publikacji (różni edytorzy zawartości intranetu w zależności od jego części). Definiowanie uprawnień powinno być dostępne dla administratorów merytorycznych poszczególnych obszarów portalu w sposób niezależny od pracowników działu IT. i) Automatyczne dołączanie do publikowanych stron informacji o autorze (edytorze) i dacie publikacji. j) Możliwość personalizacji i filtrowania treści w intranecie w zależności od roli lub innych atrybutów pracownika (np. stanowiska, działu, pionu lub spółki). Funkcjonalność ta ma być niezależna od mechanizmów zarządzania uprawnieniami użytkownika do zawartości, i ma mieć na celu dostarczenie pracownikowi adekwatnych, skierowanych do niego informacji. k) Wsparcie dla obsługi różnych wersji językowych wybranych zawartości intranetu oraz zapewnienie automatycznego tłumaczenia na wybrane języki. 7. Repozytoria dokumentów: a) Możliwość prostej publikacji dokumentów w intranecie przez edytorów portalu. Prosty sposób publikacji dokumentów, funkcjonalny dostęp użytkowników intranetu do opublikowanych dokumentów. b) Wykorzystanie do publikacji, edycji i przeglądania dokumentów w repozytorium narzędzi znanych użytkownikom np. pakiety biurowe czy przeglądarka internetowa. c) Możliwość tworzenia wielu tematycznych repozytoriów dokumentów w różnych częściach intranetu. d) Możliwość publikacji plików w strukturze katalogów. e) Możliwość publikacji materiałów wideo oraz audio. f) Możliwość definiowania metryki dokumentu, wypełnianej przez edytora przy publikacji pliku. g) Możliwość nawigacji po repozytorium dokumentów (lub całym portalu) w oparciu o metadane z metryk dokumentów. h) Prosty, elastyczny i niezależny od działu IT mechanizm zarządzania uprawnieniami do publikowanych dokumentów w ramach istniejących uprawnień. Możliwość definiowania różnych poziomów uprawnień przez administratorów merytorycznych, np. uprawnienia do odczytu, publikacji, usuwania. i) Zarządzanie wersjonowaniem dokumentów: obsługa głównych oraz roboczych wersji (np.: 1.0, 1.1, 1.x… 2.0), automatyczna kontrola wersji przy publikacji dokumentów. j) Możliwość zdefiniowania w systemie procesu zatwierdzania nowych lub modyfikowanych dokumentów. System informuje użytkowników recenzujących materiały o oczekujących na nich elementach do zatwierdzenia i pozwala podjąć decyzję o ich publikacji lub

		odrzuceniu. k) Możliwość tworzenia specjalnych repozytoriów lub katalogów przeznaczonych do przechowywania specyficznych rodzajów treści, np. galerie obrazów dla plików graficznych. l) Możliwość definiowania polityk cyklu życia dokumentu oraz retencji dokumentów. m) Możliwość tworzenia specjalnych repozytoriów przeznaczonych na raporty osadzone w arkuszach kalkulacyjnych w formacie ISO/IEC 29500:2008. Serwer powinien generować na podstawie tych arkuszy kalkulacyjnych raporty dostępne do oglądania przez przeglądarkę Internetową bez zainstalowanych innych narzędzi klienckich. n) Możliwość automatyzacji usuwania duplikatów dokumentów. o) Możliwość prezentacji dostosowanych przez użytkowników końcowych formularzy z poziomu przeglądarki dzięki użyciu serwera formularzy. 8. Wyszukiwanie treści: a) Pełno tekstowe indeksowanie zawartości intranetu w zakresie różnych typów treści publikowanych w portalu, tj. stron portalu, dokumentów tekstowych (w szczególności dokumentów XML), innych baz danych oraz danych dostępnych przez webservice. b) Centralny mechanizm wyszukiwania treści dostępny dla użytkowników intranetu c) Opcja wyszukiwania zaawansowanego, np. wyszukiwanie wg typów treści, autorów, oraz zakresów dat publikacji d) Możliwość budowania wielu wyszukiwarek w różnych częściach portalu, służących do przeszukiwania określonych obszarów intranetu wg zadanych kryteriów, np. wg typów dokumentów e) Możliwość definiowania słownika słów wykluczonych (często używanych) f) Podświetlanie w wynikach wyszukiwania odnalezionych słów kluczowych zadanych w zapytaniu. g) Przedstawianie w wynikach duplikatów plików h) Statystyki wyszukiwanych fraz 9. Administracja intranetem i inne funkcje: a) Możliwość definiowania ról / grup uprawnień, w ramach których definiowane będą uprawnienia i funkcje użytkowników. Przypisywanie użytkowników do ról w oparciu o ich konta w LDAP lub poprzez grupy domenowe. Funkcjonalność zarządzania uprawnieniami dostępna dla administratorów merytorycznych intranetu, niewymagająca szczególnych kompetencji technicznych b) Możliwość określania uprawnień do poszczególnych elementów zawartości intranetu tj. sekcja, pojedyncza strona, repozytorium dokumentów, katalogu dokumentów, pojedynczego dokumentu c) Generowanie powiadomień pocztą elektroniczną dla użytkowników intranetu z informacją o publikacji najbardziej istotnych treści d) Definiowanie metryk opisujących dokumenty w poszczególnych repozytoriach portalu oraz centralnie zarządzanego zbioru metadanych z wyznaczonym administratorem merytorycznym. e) Możliwość definiowania zewnętrznych źródeł danych takich jak bazy danych i webservice oraz wykorzystywania ich do opisywania dokumentów, f) Konfigurowanie procesów zatwierdzania publikowanych stron i dokumentów. Możliwość odrębnej konfiguracji w poszczególnych częściach portalu tj. definiowanie różnych edytorów i recenzentów w ramach różnych obszarów intranetu g) Statystyki odwiedzin poszczególnych części i stron intranetu – analiza liczby odsłon w czasie. Opcjonalnie zaawansowane statystyki i analizy

		h) Funkcjonalności wspierające pracę grupową - do wykorzystania na najniższym poziomie intranetu do celów pracy działów i zespołów zadaniowych. Funkcjonalności wspierające gromadzenie dokumentów, wsparcie komunikacji, planowanie zadań i wydarzeń i) Funkcjonalność serwera formularzy - publikowania na portalu formularzy elektronicznych pozwalających tworzyć dokumenty w formacie XML i przetwarzanych na aplikację webową dostępną dla użytkowników przez przeglądarkę Internetową. Dane z wypełnionego formularza mają być zapisywane w formacie XML zgodnie z definicją formularza. j) Mechanizmy wspierające przepływy pracy (workflow) wraz z funkcjonalnością definiowania procesów obiegu dokumentów, integracji przepływów z web-services, wywoływania web-services z poziomu workflow bez konieczności kodowania przy wykorzystaniu prostych w obsłudze narzędzi portalu.
11.	Wymagania dla oprogramowania serwera komunikacji wielokanałowej	Serwer komunikacji wielokanałowej (SKW) wspomagający wewnętrzną komunikację Zamawiającego ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy: 1. Prostą, efektywną kosztowo, niezawodną i bezpieczną komunikację głosową oraz video 2. Przesyłanie wiadomości błyskawicznych (tekstowych) z komputerów klasy PC wyposażonych w klienta SKW lub przeglądarkę. 3. Możliwość organizowania telekonferencji. Wymagana jest funkcjonalność polegająca na umożliwieniu współpracy wykorzystującej integrację poczty elektronicznej, kalendarzy, wiadomości błyskawicznych, konferencji w sieci Web, audio i wideokonferencji. Serwer SKW ma zapewniać integrację z komponentami portalu wielofunkcyjnego i poczty elektronicznej. Ponadto SKW będzie wykorzystywała mechanizm pojedynczego logowania (single sign-on), uprawnień użytkowników i ich grup, bazując na komponencie posiadanych usług katalogowych (Active Directory). Wynikiem takiej integracji mają być następujące cechy systemu: 1. Ujednolicenie komunikacji biznesowej a. Dostęp z dowolnego miejsca do komunikacji w czasie rzeczywistym i asynchronicznej. b. Możliwość ujednolicenia i współdziałania poczty głosowej, e-mail, kontaktów, kalendarzy, wiadomości błyskawicznych (IM) i danych o obecności. c. Dostępność aplikacji klienckiej udostepniającej komunikację głosową, video i tekstową, organizowanie konferencji planowanych i ad-hoc. d. Dostępność aplikacji klienckiej dla uczestników telekonferencji nieposiadających licencji dostępowej do serwerów SKW z funkcjonalnością: a. Dołączania do telekonferencji b. Szczegółowej listy uczestników c. Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu. d. Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli e. Głosowania f. Udostępniania plików g. Możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji e. Dostępność funkcjonalności text-to-speech w języku polskim f. Integracja z aplikacjami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.

		g. Wbudowane mechanizmy dostępu mobilnego i bezprzewodowego. h. Rozszerzalna platforma integracji narzędzi współpracy z pakietem biurowym. i. Usługi bezpieczeństwa umożliwiające chronioną komunikację wewnątrz organizacji. j. Aplikacje biznesowe dostępne bezpośrednio na urządzeniach mobilnych. k. Mobilny dostęp do ludzi i danych firmowych. l. Obniżone koszty dzięki zdalnej administracji i zarządzaniu urządzeniami. m. Niższe koszty usług telefonicznych i komunikacji między odległymi lokalizacjami. n. Funkcje statusu obecności, IM i konferencji (głosowych i video) bezpośrednio wbudowane w portale i obszary robocze zespołów i dostępne z poziomu klienta poczty elektronicznej. o. Możliwość wspólnej pracy zespołów z różnych lokalizacji, wewnątrz i spoza ram organizacyjnych, także z wykorzystaniem przez użytkowników zewnętrznych bezpłatnych aplikacji klienckich. 2. W związku z tak postawionymi założeniami SKW ma zapewnić: a. Efektywną wymianę informacji z możliwością wyboru formy i kanału komunikacji i niezależnie od lokalizacji pracowników. b. Ulepszoną komunikację poprzez wykorzystanie statusu obecności i konferencje w czasie rzeczywistym. c. Zarządzanie, sortowanie i pracę z różnymi typami wiadomości, bez konieczności przełączania się pomiędzy aplikacjami czy systemami. d. Dostęp z dowolnego miejsca poprzez dostęp do usług komunikacyjnych z poziomu pulpitu, przeglądarki sieci Web i urządzeń mobilnych. 3. SKW ma zapewnić obsługę następujących funkcjonalności: a. Status obecności – informacja o statusie dostępności użytkowników (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej, zintegrowana z usługą katalogową i kalendarzem, a dostępna w interfejsach poczty elektronicznej, komunikatora i portalu wielofunkcyjnego. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności. b. Krótkie wiadomości tekstowe – Możliwość komunikacji typu chat. Możliwość grupowania kontaktów, możliwość konwersacji typu jeden-do-jednego, jeden-do-wielu, możliwość rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat. Możliwość komunikacji z darmowymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu. Możliwość administracyjnego zarządzania treściami przesyłanymi w formie komunikatów tekstowych. c. Obsługa komunikacji głosowej – Możliwość realizowania połączeń głosowych między użytkownikami lokalnymi, możliwość realizacji połączeń głosowych do i z sieci PSTN (publicznej sieci telefonicznej). Możliwość realizacji funkcjonalności RCC (Remote Call Controll) tj. zarządzania telefonem stacjonarnym firm trzecich z poziomu komunikatora. d. Obsługa komunikacji wideo – Możliwość zestawiania połączeń wideo-telefonicznych. e. Obsługa konferencji wirtualnych – Możliwość realizacji konferencji wirtualnych z wykorzystaniem głosu i wideo. Możliwość współdzielenia aplikacji jak również całego pulpitu. f. Możliwość dostępu do telekonferencji użytkownikom wykorzystujących urządzenia z systemami Android, Apple iOS,

		Windows, Windows Phone. g. Możliwość nagrywania konferencji na centralnym serwerze jak również lokalnie przez uczestników. h. Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie z poziomu serwera WWW. i. Automatyzacja planowania konferencji - zaproszenia rozsyłane są automatycznie w postaci poczty elektronicznej. j. Wsparcie dla funkcjonalności single sign-on – po zalogowaniu w systemie operacyjnym użytkownik nie musi ponownie podawać ponownie nazwy użytkownika i hasła. k. Wbudowane funkcjonalności: SIP Proxy l. Wbudowana funkcjonalność mostka konferencyjnego MCU m. Obsługa standardów: CSTA, TLS, SIP over TCP n. Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów, o. Kodowanie video H.264, p. Wsparcie dla adresacji IPv6, q. Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności, r. Wykorzystanie wyłącznie 64 bitowej platformy serwerowego systemu operacyjnego s. Możliwość instalacji w układzie klastra niezawodnościowego. t. Dostępność wspieranego przez SKW sprzętu peryferyjnego. W tym telefonów IP pochodzących od różnych producentów. 4. Wymagania w zakresie administracji i zarządzania serwerem: a. Mechanizm pozwalający na przełączenie serwera w tryb off-line (np. w celach dokonania czynności administracyjnych) bez utraty usług serwera dla zalogowanych użytkowników, a jednocześnie blokujący dostęp nowych użytkowników b. Możliwość administrowania z wiersza poleceń c. Możliwość administrowania za pomocą interfejsu Web d. Mechanizm gotowych kreatorów (wizard) umożliwiających planowanie i zmiany topologii serwerów SKW e. Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników, 5. Dodatkowe wymagania: a. Możliwość instalacji w układzie klastra typu load-balancing, b. DNS load balancing balansujący ruch sieciowy dla serwerów SKW, na przykład w zakresie ruchu SIP lub mediów, c. Możliwość instalacji bazy danych serwera komunikacji wielokanałowej na oddzielnym serwerze, d. Możliwość wydzielenia na niezależnym serwerze roli serwera konferencji audio i video.
12.	Wymagania dla pakietu licencji dostępowych do oprogramowania serwerowego	Pakiet licencji dostępowych musi zapewnić w zgodzie z wymaganiami licencyjnymi producenta możliwość wykorzystania przez użytkowników funkcjonalności serwerów: 1. Serwerowych systemów operacyjnych, 2. Podstawowej funkcjonalności serwerów portali wielofunkcyjnych intranet, 3. Podstawowej funkcjonalności serwerów poczty e-mail, 4. Serwerów systemu zarządzania infrastrukturą i oprogramowaniem, 5. Podstawowej funkcjonalności serwerów komunikacji wielokanałowej, 6. Licencje dostępowe rozszerzające zakres funkcji dostępnych posiadaczom licencji dostępowych serwera komunikacji wielokanałowej, pozwalające dodatkowo wykorzystać funkcjonalność serwera komunikacji wielokanałowej w zakresie: a. Łączności głosowej i video z wieloma (więcej niż dwoma)

		uczestnikami konferencji, b. Zarządzania połączeniami telefonicznymi i głosowymi c. Współdzielenia aplikacji. 7. Serwerów zarządzania, monitorowania, składowania danych i zarządzania maszynami wirtualnymi, 8. Serwerów poczty e-mail w zakresie uzupełniającym pakiet podstawowych licencji dostępowych, zapewniających (w zgodzie z wymaganiami licencyjnymi producenta) możliwość wykorzystania przez użytkowników zaawansowanych narzędzi archiwizacyjnych, ochrony informacji oraz narzędzi poczty głosowej. 9. Licencje umożliwiające użytkownikom wykorzystanie pełnej funkcjonalności serwera portalu wielofunkcyjnego, uwzględniające dostęp do usług serwera formularzy, narzędzi wizualizacji analiz biznesowych, wspólnej infrastruktury wszystkich stron w organizacji.