UNIWERSYTET SZCZECIŃSKI
DZIAŁ ZAMÓWIEŃ PUBLICZNYCH
al. Papieża Jana Pawła II 31
70-453 Szczecin
tel. (0-91) 444 11 51, 444 12 02

Szczecin dn. 14.09.2020 r.

SZACOWANIE WARTOŚCI ZAMÓWIENIA

W związku z koniecznością dokonania szacowania wartości zamówienia pod nazwą: **zakup, dostawa, instalacja i uruchomienie zintegrowanej infrastruktury sieciowo-serwerowej niezbędnych dla wydajnej i bezpiecznej pracy platformy „Herbarium Pomeranicum" w trzech istniejących centrach danych** w ramach projektu „Zintegrowane wirtualne Herbarium Pomorza Herbarium Pomeranicum – digitalizacja i udostępnienie zbiorów herbariów jednostek akademickich Pomorza poprzez ich połączenie i udostępnienie cyfrowe" współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa 2014-2020" Uniwersytet Szczeciński, jako Zamawiający Upoważniony na podstawie Porozumienia zawartego na podstawie art. 16 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843), do przeprowadzenia wspólnego postępowania przetargowego i udzielenia zamówienia zwraca się z prośbą o oszacowanie kosztu realizacji zamówienia w odniesieniu do zakresu prac określonego poniżej:

zakup, dostawa, instalacja i uruchomienie zintegrowanej infrastruktury sieciowo-serwerowej niezbędnych dla wydajnej i bezpiecznej pracy platformy „Herbarium Pomeranicum" w trzech istniejących centrach danych

Opis przedmiotu zamówienia stanowiący podstawę wyceny:

Zastosowanie:
Zamówienie obejmuje: zakup, dostawę, instalację i uruchomienie zintegrowanej infrastruktury sieciowo-serwerowej niezbędnych dla wydajnej i bezpiecznej pracy platformy „Herbarium Pomeranicum", w trzech istniejących centra danych:

1. **Podstawowe Centrum Przetwarzania (PCP)** umieszczone w Akademii Pomorskiej w Słupsku, który będzie miało za zadanie gromadzenie wszystkich danych oraz obsługę edycji danych jak i ich przeglądanie przez interesariuszy,
2. **Awaryjne Centrum Przetwarzania (ACP)** centrum danych umieszczone na Uniwersytecie Gdańskim, które w razie wystąpienia awarii przejmie na siebie wszystkie funkcje głównego centrum,
3. **Zapasowe Centrum Przetwarzania (ZCP)** centrum danych na Uniwersytecie Szczecińskim przechowujące wersjonowane w określonym zakresie czasowym dane kopii bezpieczeństwa.

Każde Centrum Przetwarzania zostanie wyposażone w autonomiczny zestaw urządzeń i oprogramowania zapewniający możliwość wprowadzanie zeskanowanych danych.

W ramach przedmiotowego zamówienia, Zamawiający wymaga dostarczenia sprzętu oraz oprogramowania, którego parametry minimalne wskazane zostały w niniejszym dokumencie. Zamawiający akceptuje sprzęt oraz oprogramowanie o wyższych (lepszych) parametrach użytkowych lub wykonany w nowszej technologii pod warunkiem, że produkty zaoferowane przez Wykonawcę spełniają wszystkie parametry minimalne oraz:

- wszystkie oferowane urządzenia muszą być fabrycznie nowe. Przed dostawą sprzęt musi być zarejestrowany przez producenta bezpośrednio na Zamawiającego jako jedynego użytkownika po opuszczeniu fabryki. Jeśli producent nie prowadzi rejestracji sprzętu, to wymaga się deklaracji producenta, iż sprzęt jest fabrycznie nowy.
- w momencie oferowania wszystkie elementy oferowanego systemu muszą być dostępne (dostarczane przez producenta) w dacie złożenia oferty i nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
- urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
- urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych.
- do każdego urządzenia i oprogramowania musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku angielskim lub polskim.
- sprzęt musi pochodzić z autoryzowanego przez jej producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży i serwisu na rynku polskim.
- wszystkie urządzenia posiadają oznakowanie CE produktu albo spełniają normy równoważne.
- wszystkie urządzenia, jeśli nie podano inaczej, muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz.
- korzystanie przez Zamawiającego z dostarczonego produktu nie narusza majątkowych praw autorskich osób trzecich

Zamawiający zastrzega sobie:

- prawo do sprawdzenia legalności dostawy bezpośrednio u polskiego przedstawiciela producenta, w szczególności ważności i zakresu uprawnień licencyjnych oraz gwarancyjnych.
- żądanie dostarczenia przed dostawą dokumentu zawierającego listę numerów seryjnych dostarczanego sprzętu w celu weryfikacji spełnienia warunków gwarancyjnych.

Zamawiający wymaga kompleksowego uruchomienia i zainstalowania dostarczonego sprzętu oraz oprogramowania.

1. **Sprzęt**
   Zamawiający wymaga, aby wszystkie dostarczone urządzenia został uruchomione i umieszczone (zamontowane) w miejscach przeznaczenia, w uzgodnionym przez obie strony terminie. Sposób montażu powinien być dostosowany do technologii wykonania oraz ma być przeprowadzony zgonie z zaleceniami producenta dostarczonych rozwiązań.
2. **Oprogramowanie**
   Dostarczone systemy operacyjne, oprogramowanie aplikacyjne oraz wszystkie niezbędne oprogramowanie dodatkowe mają być kompletnie zainstalowane oraz aktywowane o ile jest to wymagane.

Przez sformułowania: „ma umożliwić, ma zapewnić" Zamawiający rozumie możliwość pełnego, zgodnego z opisem wymagań, wykorzystania danej funkcjonalności, bez konieczności zakupu dodatkowych licencji lub ponoszenia dodatkowych opłat.

Mając na uwadze nadrzędność celu jakim jest skuteczne uruchomienie planowanych rozwiązań Zamawiający zastrzega, że zadaniem Wykonawcy jest dostarczenie wszelkich niezbędnych elementów sprzętowych, oprogramowania, licencji oraz wykonanie wszystkich niezbędnych prac instalacyjnych, konfiguracyjnych i wdrożeniowych, które konieczne są do osiągnięcia zakładanego celu, nawet jeśli nie zostały one wymienione w dalszej części niniejszego dokumentu.

1.1 Elementy dostawy

W ramach zadania zaplanowano instalację następującego sprzętu teleinformatycznego w każdej serwerowni (szczegółowe wymagania dla wskazanych niżej elementów znajdują się w tabelach w dalszej części dokumentacji):

1. **Szafa Rack 19"** wraz z niezbędnymi akcesoriami zgodnymi ze specyfikacją szczegółową:
   a. Zasilacz awaryjny z modułami bateryjnymi umożliwiający utrzymanie zasilania urządzeń elektronicznych zainstalowanych w szafie w przypadku wystąpienia przerw lub nieprawidłowych parametrów zasilania sieci energetycznej. Pojemność baterii musi umożliwić bezpieczne wyłączenie pracujących urządzeń w ciągu 20 minut przy obciążeniu równym 40% nominalnej mocy podłączeniowej dostarczonych urządzeń.
   b. Redundantne listwy dystrybucji zasilania, zarządzane, z monitorowaniem parametrów środowiskowych wewnątrz szafy (temperatura, pobór prądu).
2. **Warstwę dedykowanych Serwerów Pamięci Masowej** z funkcjami wybiórczego szyfrowania, deduplikacji, kompresji, detekcji i usuwaniu zer oraz tzw. cienkich woluminów realizowanych w locie dla całej dostarczonej przestrzeni użytkowej netto (przestrzeń po uwzględnieniu oferowanego mechanizmu zabezpieczenia RAID oraz przestrzeni hotspare), liczonej bez uwzględnienia mechanizmów redukcji ilości przechowywanych danych w wymiarze **260TB** i wsparciem dla replikacji pomiędzy ośrodkami badawczymi w trybie synchronicznym i asynchronicznym opisanym powyżej.
3. Redundantną **Warstwę Sieciową Data Center** umożliwiającą podłączenie do 24 portów dostarczonych urządzeń o wydajności nie mniejszej niż 10GbE, w obudowie

przystosowanej oraz z zestawem producenta do montażu w dostarczonej szafie stelażowej 19".

4. Redundantną **Warstwę Sprzętowych Serwerów Wirtualizacji x86_64**, na potrzeby platformy SAHP, w obudowie przystosowanej oraz z zestawem producenta do montażu w dostarczonej szafie stelażowej 19".
5. **Warstwę Sprzętowych Firewall/UTM** umożliwiający podłączenie do infrastruktury sieciowej w danej lokalizacji, zapewniający minimalną przepustowość komunikacji szyfrowanej VPN 2750Mb/s, w obudowie przystosowanej oraz z zestawem producenta do montażu w dostarczonej szafie stelażowej 19".
6. **Urządzenia brzegowe** umożliwiające podłączenie zintegrowanej infrastruktury sieciowo-serwerowej do sieci Internet oraz połączenie wymienionych wyżej trzech centrów danych.
7. **Licencje oprogramowania wirtualizacyjnego** wymagane przez proponowane rozwiązanie w ilości wymaganej dla dostarczonych elementów infrastruktury.
8. **Certyfikowane Szkolenia** obejmujące komponenty dostarczonej platformy infrastrukturalnej oraz oprogramowania wirtualizacyjnego dla 6 osób.
9. **Dokumentację powykonawczą oraz 1-dniowe nieodpłatne warsztaty szkoleniowe** jako element zakończenia projektu i przekazania go do działu utrzymania.

Wszystkie urządzenia wymienione powyżej:

1. Powinny zostać dostarczone, w obudowie przystosowanej oraz z zestawem producenta do montażu w dostarczonej oraz standardowej szafie stelażowej 19".
2. Urządzenia dostarczone wraz z kompletem niezbędnych wkładek/kabli umożliwiających połączenie serwerów z przestrzenią dyskową lub jej nośnikiem, firewall'a, listw PDU i UPS'a oraz podłączenia do istniejącej sieci LAN kablami światłowodowymi o długości 7 metrów.
3. Być objęte wsparciem NBD (Next Business Day).
4. Oferent jest zobowiązany dostarczyć wszystkich innych zasobów niezbędnych do działania oferowanego rozwiązania zgodnie z dobrą praktyką w powyższej architekturze oraz po dokonaniu wizji lokalnej. Oferent jest zobowiązany do przedstawienia szczegółowego wykazu dostarczanych komponentów i ich konfiguracji, opisu architektury z uwzględnieniem realizacji wymaganych usług w celu i umożliwienia analizy rzetelności składanej oferty. Informacje te nie mogą podlegać utajnieniu w postępowaniu.

Specyfikacje i wymagania techniczne dla komponentów.

1.2 Szafa Rack 19"

Ilość: 3 sztuki - po jednej do każdej lokalizacji

Lp.	Opis wymagania / Element	Wymaganie / Wymagany parametr
1.	Wymiary szafy RACK 19"	Szafa stelażowa 19" 42U wewnętrznego miejsce do instalacji urządzeń. Wysokość szafy max 201cm. Szerokość szafy max. 60cm Głębokość szafy max. 112 cm pozwalająca na montaż urządzeń o dł. 1075mm
2.	Wyposażenie szafy RACK 19"	Szafa wyposażona w: a) Drzwi przednie perforowane (perforacja min. 80%), wyposażone w zamek b) Drzwi tylne, dzielone, wyposażone w zamek c) Obie ściany boczne zamykane na zamek. d) Każda ze ścian bocznych składająca się 2 elementów. e) Zaślepki montowane bez użycia narzędzi z przodu szafy, pozwalające na zamaskowanie miejsca o wysokości 30U; wysokość pojedynczej zaślepki równa 1U f) Element stabilizujący – podpora. g) Styk uziemiający h) 6 x wertykalnych listew PDU 3,6 kVA, każda wyposażona w: • 20 gniazd C12 • 2 gniazda C19.
3.	Standardy przemysłowe dla szafy RACK19"	Szafa RACK 19" zgodna ze standardami: a) EIA-310 b) WEEE c) RoHS compliant d) UL/CES Certification
4.	Awaryjne podtrzymanie zasilania	Systemy awaryjnego podtrzymania zasilania (UPS) o nominalnej mocy nie mniejszej niż 85% sumy nominalnych mocy wszystkich zasilaczy, dostarczonych w ramach zadania urządzeń. UPS musi posiadać moduł sieciowy (LAN) pozwalający na automatyczne zamknięcie wszystkich dostarczonych elementów infrastruktury w przypadku awarii zasilania. Pojemność dostarczonego UPS musi zapewniać 12 minutowe podtrzymanie zasilania przy obciążeniu 50% nominalnej mocy dostarczonego UPS. UPS musi być: a) Wyposażony w moduły zasilania formujące tzw. „pełną sinusoidę". b) wyposażony w 6 niezależnie zarządzanych sekcji zabezpieczonych własnym zabezpieczeniem prądowym (bezpiecznik). c) zasilany z 2 niezależnymi jednofazowymi źródłami prądu 240V.
5.	Inne	Możliwość instalacji sprzętu o wadze min. 1360kg (obciążenie statyczne). Dopuszczalne obciążenie podczas przemieszczania/przesuwania szafy 1100kg (obciążenie dynamiczne) bez użycia dodatkowych środków technicznych (wózek, platforma itp.)

1.3 Warstwa Serwerów Pamięci Masowej

Ilość: 3 sztuki - po jednej w każdej lokalizacji

Lp.	Parametr	Charakterystyka parametru
1.	Opis urządzenia	Zoptymalizowany pod kątem technologii *flash* hybrydowy serwer pamięci masowej z dostępem przez interfejsy 10GbE oraz wewnętrzną magistralą 12Gbps. Przez Serwer Pamięci Masowej Zamawiający rozumie zestaw nośników do składowania danych obsługiwanych przez dedykowane węzły (bez dodatkowych urządzeń pośrednich, serwerów wirtualizujących, oprogramowania wirtualizującego itp.). Spełnienie wymagań poniżej powinno być udokumentowane w ogólnodostępnych materiałach producenta.
2.	Wsparcie klastrów i systemów operacyjnych	Urządzenie musi być na listach wsparcia i wspierać główne systemy operacyjne i klastry, w tym: system operacyjny Windows Server 2012, Windows Server 2016, Windows Server 2019, VMware 6.7, Linux (Centos 7.x, SUSE12, Redhat 7.x) i Unix (Solaris, Aix, HP-UX). Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Preferowane jest rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. W przypadku stosowania rozwiązań firmowych/własnych – konieczna jest ich certyfikacja dla platform: Windows 2012 i nowsze, Linux RedHat 7.x+, Suse12+, VMware 5,5+. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów. Jeżeli dla realizacji powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów/pojemności obsługiwanych przez oferowane urządzenie.
3.	Partycjonowanie zasobów	Serwer pamięci masowych musi umożliwiać podział na minimum 8 odseparowanych urządzeń logicznych zarządzanych przez dedykowanych administratorów.
4.	Pojemność i skalowalność	Oferowane Urządzenie musi być wyposażone w co najmniej: a) Surową pojemność zbudowaną z $(1+W_2+W_4)*42$ nośników/dysków. b) Pojemność netto $(1+W_3+W_4)*260$TB (po odjęciu narzutu na RAID, przestrzenie/dyski *hotspare* oraz metadane). c) Dedykowaną pamięć *flash* zbudowaną z dysków SSD o pojemności użytecznej $(1+W_5)*26$TB zbudowaną z minimum 9 dysków SSD. oraz zapewniać rozbudowę: a) W trybie „scale-up" do $(1+W_2+W_4)*128$ nośników danych o łącznej przestrzeni surowej 504TB przez rozbudowę kontrolerów/dodanie dysków/półek dyskowych w trybie na gorąco. b) „scale-out" do 5PB przestrzeni surowej przez integrację do 8 kontrolerów w sposób zapewniający stworzenie pojedynczej, jednolitej puli dyskowej dla świadczonych serwisów z wykorzystaniem wbudowanego w macierz oprogramowania. Używane jednostki pojemności: a) $1TiB=1024GiB=240B$, $1GiB=1024MiB=2^{40}B$ b) $1TB=1000GB=1012B$, $1GB=1000MB=10^{12}B$

Lp.	Parametr	Charakterystyka parametru
5.	Bufor danych RAM	Każdy redundantny węzeł oferowanego urządzenia musi być wyposażony w minimum dwa procesory oraz 64GB pamięci RAM dedykowanej dla operacji odczytu i zapisu z zastrzeżeniem: a) Wyszczególniona pojemność musi być dedykowana na dane i informacje kontrolne. FW/OS musi posiadać własną dedykowaną pamięć operacyjną różną od wyspecyfikowanej powyżej. b) Pamięć zapisów musi być zabezpieczona dodatkową kopią zabezpieczającą przed awarią kontrolera i utratą zasilania (na drugi kontroler). c) Rozbudowa opisana w pkt 4, ppkt. d) musi pozwalać na zwiększenie RAM kontrolera do 128GB – oraz rozbudowę szybkiej przestrzeni flash do $(1+W_5)*50TB$
6.	Efektywność obsługi nośników danych	Zamawiający dla urządzeń zapewniających: a) wielokrotną redukcję wszystkich operacji zapisu przez grupowanie i sekwencyjny zrzut zdeduplikowanych oraz skompresowanych danych z bufora na wewnętrzne nośniki danych paskiem nie mniejszym niż 8MB b) ochronę RAID, zabezpieczającą przed jednoczesną awarią co najmniej 2 dysków pozwala na stosowanie dysków o pojemności do 12TB i dowolnej długości grupy RAID. Dla pozostałych (tradycyjnych) przypadków grup należy do wyceny stosować grupę RAID6 (4+2) i dyski o pojemności nie przekraczającej 6TB. Zamawiający przez „zrzut paskiem" rozumie sposób agregacji wszystkich bieżących zapisów (losowych i sekwencyjnych) dla wszystkich wystawianych LUN'ów w ciągły strumień danych zapisywanych jako pełen pasek grupy RAID (to jest wymagające jednokrotnego naliczenia i zapisu danych nadmiarowych), zapisywany sekwencyjnie na dyskach twardych bez konieczności odczytu istniejących danych. Architektura zapisu musi (w odróżnieniu od tradycyjnych architektur RAID5/6+, które dla realizacji pojedynczego zapisu losowego wymagają wykonania wielu operacji odczytu i zapisu), redukować kilkudziesięciokrotnie ilość fizycznych operacji na nośnikach. Efektywne wykorzystanie nośników typu HDD pozwala zredukować ilość nośników tradycyjnie wymaganych dla RAID6 w celu uzyskania wymaganej wydajności.
7.	Bufor Flash	Oferowane urządzenie musi zapewniać możliwość rozbudowy buforu flash do pojemności $(1+W_5)*50$ TB netto przez dodanie nośników SSD w trybie pracy zlecanym przez producenta (flash cache, SSD tier) a) Współczynnik $W_5=0$ należy stosować dla urządzeń przechowywujących w buforze flash zdeduplikowane i skompresowane dane. W pozostałych przypadkach $W_5=3$ Termin deduplikacja i kompresja odnosi się do urządzeń zapewniających deduplikację z granulacją 4kB oraz kompresję algorytmem lze realizowane w trybie w locie (inline), to jest przed zapisem na dyski/nośniki danych. Zamawiający dopuszcza, aby urządzenie, w celu zapewnienia wymaganej wydajności, dynamicznie redukowało algorytm kompresji na nie gorszy niż lz4 dla obciążenia kontrolera powyżej 70% pod warunkiem, że kompresja zawsze odbywa się w locie (inline).
8.	Brak pojedynczego punktu awarii	Oferowane urządzenie musi być wolne od Pojedynczych Punktów Awarii, czyli wszystkie komponenty węzły, kontrolery, bufor flash, wentylatory, zasilacze itp. muszą być nadmiarowe. Awaria pojedynczego komponentu w tym węzła nie może powodować spadku wydajności urządzenia poniżej wyspecyfikowanych w Zapytaniu parametrów wydajnościowych.

Lp.	Parametr	Charakterystyka parametru
9.	Wsparcie dysków i szyfrowania	Oferowane urządzenie musi wspierać dyski SSD o pojemnościach 240, 480, 960, 1920, 3840, 7680 GB na potrzeby bufora danych oraz dyski HDD 1, 2, 4, 6, 10TB dla przechowywania danych. Oferowane urządzenie musi wspierać certyfikowane szyfrowanie zgodne z AES-256 XTS FIPS z granulacją i dedykowanym kluczem dla każdego prezentowanego LUN.
10.	Woluminy: wspierana ilość i zabezpieczenie RAID	Oferowane Urządzenie (W_4=0) musi: a) zabezpieczać przed jednoczesną utratą dowolnych 2 dysków bez utraty danych i dostępu do nich w dowolnym ośrodku przetwarzania. b) zapewnić przestrzeń *distributed hot spare* w wymiarze nie mniejszym niż 1 dysk na każde 24 dyski c) Urządzenie udostępniające jednolitą, pojedynczą pulę złożoną ze wszystkich wewnętrznych dysków HDD na potrzeby udostępniania danych. d) Oferowane urządzenie musi wspierać udostępnianie nie mniej niż 10000 woluminów (LUN) per kontroler. e) Zamawiający dopuszcza Urządzenie wymagające dedykowanych pul dla migawek zabezpieczonych RAID6. W takim przypadku należy zastosować współczynnik ekwiwalentności W_4=0,5 *Distributed hotspare* to technologia, w której przestrzeń *hotspare* jest alokowana na wszystkich dyskach grupy RAID – zapewniając wielokrotnie szybszą rozbudowę w porównaniu do tradycyjnego rozwiązania z dedykowanymi dyskami *hotspare*.
11.	Dostępność	a) Urządzenie ma charakteryzować się udokumentowaną dostępnością 99,9999%. b) Być wolne od pojedynczych punktów awarii c) Zapewnić wydajność (1+W6)*90000 IOps dla obciążenia typu losowego, blokiem 4kB przy stosunku odczytów do zapisów 50/50 (dla oferowanej konfiguracji): • Przypadku awarii (niedostępności) jednego kontrolera • W trakcie procesów aktualizacji oprogramowania i poprawek kontrolerów, sterowników/firmware'u. • Przy zabezpieczeniu RAID/deduplikacji i kompresji zgodnych z deklarowanymi odpowiednio w punktach 6, 7, 10. • Dla konfiguracji z aktywnymi migawkami na każdym udostępnianym LUN

Lp.	Parametr	Charakterystyka parametru
12.	Raportowanie i zalecenia dla kierownictwa	Oferowane rozwiązanie musi zapewniać tworzenie raportów w następującym zakresie: a) Bieżące wykorzystanie przestrzeni w rozbiciu na: • przestrzeń danych wykorzystywanych przez serwery (przed technologiami redukcji danych) • redukcję zajętości dzięki kompresji • redukcję zajętości dzięki deduplikacji • redukcję zajętości z uwagi na migawki niewymagające pełnej kopi danych • przestrzeń danych faktycznie zajęta na Urządzenie y • współczynnik redukcji danych b) Ilość otwartych dla środowiska zgłoszeń serwisowych w rozbiciu na: • zgłoszenia, dla których natychmiastowo zalecono rozwiązanie • zgłoszenia wymagające interakcji z serwisem c) Raport RPO zasobów chronionych migawkami w podziale na grupy aplikacyjne d) Raport Retencji (RET) zasobów chronionych migawkami w podziale na grupy aplikacyjne e) Raport odporności na katastrofy zasobów replikowanych w podziale na grupy aplikacyjne f) Rekomendacje rozbudowy wraz ze wskazaniem przyczyn dla wszystkich posiadanych Urządzeń Raporty muszą być udostępniane w trybie online dla uprawnionych osób oraz wysyłane na listę odbiorców email.
13.	Chmurowy Monitoring i analityka	Oferowane rozwiązanie musi zapewniać monitoring w minimalnym zakresie: a) Zdarzeń związanych z Urządzeniem (błędów, procedur utrzymania itp.) w podziale na priorytety (co najmniej Ważny, Pilny, Krytyczny) i obszary (Pule, Urządzenie, grupy zasobów, migawki); b) Obciążenia Urządzenia z rozbiciem na obciążenie procesorów i buforu Urządzenia c) Zajętości urządzenia: historycznej i przewidywanych trendów z okresu 3-12 miesięcy w podziale na aplikacje np. serwery wirtualne, Exchange, Oracle, MS SQL, SPS, Docker, woluminy (z migawkami) oraz pule/grupy. d) Trendów pojemności udostępnianych zasobów (woluminy, pule/grupy) w przedziale 1-365 dni z granulacją odpowiednio 10min-24h. e) Trendów wydajności udostępnianych zasobów w przedziale 1-365 dni z granulacją odpowiednio 10min - 24h. f) Historii i bieżącego statusu zgłoszeń serwisowych,

Lp.	Parametr	Charakterystyka parametru
14.	Monitoring i zarządzanie środowiskami	Oferowane rozwiązanie musi zapewniać raportowanie analiz wydajności platformy wirtualizacji na poziomie: a) serwerów w klastrze • wykorzystanie CPU/RAM, wykorzystania Swap, funkcji baloon, ilość przeciążonych serwerów w klastrze, • średnia wartość oraz histogram obciążenia CPU/RAM serwerów zarządzanych przez wskazane centrum wirtualizacji w przedziałach czasowych od ostatniego dnia (granulacja: 10 minut) do 12 miesięcy wstecz (granulacja 24h) . • Trend: Top 10 „Virtual Machine" wykorzystujących CPU/RAM w przedziale 1-365 dni z granulacją odpowiednio 10min - 24h. b) Datastore w przedziale 1-365 dni z granulacją odpowiednio 10min - 24h. • listy maszyn wirtualnych (host, zaalokowana przestrzeń, śr. obciążenie vCPU, vMEM z ostatnich 24h • trendy zajętości: lista top 10 „Virtual Machine" w przedziałach 7-365 dni z granulacją 24h. • obciążenia IO oraz śr. czas realizacji IO • Trend Top 10 „Virtual Machine" obciążających data store c) maszyn wirtualnych w przedziale 1-365 dni z granulacją odpowiednio 10min -24h. • bieżące wykorzystanie zasobów: średnie: zajętość, wykorzystanie vCPU, vMEM, przepustowość MB/s oraz IO/s (w rozbiciu na zapisy i odczyty) w ciągu ostatnich 24h; histogramu wykorzystanej pojemności, czasu obsługi ze wskazaniem składowych generowanych na serwerze, sieci LAN/SAN, Urządzenie), • histogramu czasu realizacji IO • średniej sumarycznej przepustowości (MB/s) i ilości IOps • średniej przepustowości dysku wirtualnego (MB/s), czasu obsługi, ilości IOps z ostatnich 24h. • dysku wirtualnego (przepustowość MB/s oraz IO/s (w rozbiciu na zapisy i odczyty) Interfejs musi zapewniać dla danych liczbowych możliwość eksportu do pliku csv. Jako funkcjonalność równoważną Zamawiający dopuszcza dostarczenie licencji VMware vRealize Suite Enterprise dla co najmniej 12 CPU wraz z wymaganą do jego pracy infrastrukturą.
15.	Ochrona inwestycji	Oferowane urządzenie musi zapewniać możliwość uaktualnienia do nowej generacji kontrolerów (bez konieczności zakupu pojemności dyskowej) w nieprzerwanym trybie pracy. W przeciwnym przypadku należy zastosować współczynnik równoważności W_6=2.

Lp.	Parametr	Charakterystyka parametru
16.	Wsparcie	Urządzenie musi być certyfikowane i wspierać specyfikację VASA 3/VVOL2 w zakresie: a) sprzętowej realizacji migawki pojedynczych maszyn wirtualnych. b) natychmiastowe i automatyczne odzyskiwanie przestrzeni w przypadkach skasowania i/lub migracji maszyny wirtualnej c) automatycznej, sprzętowej realizacji funkcji „VVols array-based thin provisioning". d) sprzętowej realizacji funkcji „Thin deduplication" z granulacją na poziomie wybranych maszyn wirtualnych. e) sprzętowej realizacji funkcji QoS zarządzana przez „VM resource controls and Storage I/O Control" z granulacją na poziomie wybranych maszyn wirtualnych. f) sprzętowej realizacji funkcji „Storage based replication" Zamawiający dopuszcza Urządzenie wspierające VASA 2/VVOL 1 pod warunkiem zastosowania współczynnika W_3=1
17.	Wsparcie dla technologii kontenerów	Urządzenie musi wspierać i oferować integrację z Docker, Redhat Openshift, Kubernetes oraz MESOS. Urządzenie musi oferować ogólnodostępny sterownik CSI z możliwością definicji usług QoS oraz zintegrowany z dostarczonym systemem zarządzania kopiami zapasowymi.
18.	Porty udostępniające usługę	Urządzenie musi być wyposażone w minimum dwa redundantne węzły z minimalną łączną ilością portów: a) 4 x 10GbE-T b) 8 x 10GbE SFP+ do podłączenia Serwerów Wirtualizacji. W przypadku konieczności dedykowania portów dla realizacji zadań replikacji Zamawiający wymaga, aby doposażono dostarczone Urządzenia w ilość interfejsów zgodną z zaleceniami dobrej praktyki producenta w tym zakresie ni mniej niż 2 na każdy węzeł oferowanego rozwiązania (redundancja). Urządzenie musi pozwalać na rozbudowę do łącznie 24 portów udostępniających LUN'y (bez wymiany zainstalowanych modułów) działających z prędkością nie mniejszą niż 10Gb.
19.	Zarządzanie jakością usług	Urządzenie musi zapewniać kontrolę jakości usług (QoS) co najmniej w zakresie ograniczenia parametrów IOps i MBps z granularnością per LUN/VVol/zasób CSI.
20.	Technologia Thin oraz optymalizacja wykorzystania przestrzeni.	Urządzenie musi zapewniać możliwość granularnej (per LUN) aktywacji funkcji redukcji zajętości przestrzeni w nieprzerwanym trybie pracy (inline) na poziomie kontrolera: a) deduplikacji blokiem nie większym niż 16kB b) kompresji algorytmem nie gorszym LZ4 dla wszystkich oferowanych dysków HDD i SSD. Urządzenie musi umożliwiać równoczesne udostępnianie dowolnej kombinacji zdeduplikowanych, skompresowanych, niezdeduplikowanych i nieskompresowanych LUN.
21.	Migawki Urządzenie owe	Urządzenie musi wspierać tworzenie co najmniej 100 000 migawek per Urządzenie i 500 per LUN w technologii "redirect on write". Zamawiający dopuszcza Urządzenie używające technologii „copy on write" pod warunkiem zastosowania współczynnika równoważności W_1=0,5. Technologia migawek musi być zgodna i integrować się z oprogramowaniem np. MS SQL, VMware, Hyper-V, Oracle oraz Kontenerami (CSI) w celu tworzenia koherentnych aplikacyjnie kopii zapasowych w trybie na gorąca (online) z licencjami na pełną pojemność dostarczonego Urządzenia.

Lp.	Parametr	Charakterystyka parametru
22.	Zdalna replikacja	Urządzenie musi wspierać sprzętową replikację synchroniczną i periodyczną/asynchroniczną: a) danych z granularnością na poziomie pojedynczych LUN lub grup LUN przez sieć WAN pomiędzy ośrodkami przetwarzania b) migawek z wykorzystaniem polityk i harmonogramów Replikacji mają podlegać wyłącznie zmienione skompresowane sprzętowo bloki danych urządzeń LUN dla których zdefiniowano relacje replikacji pomiędzy Urządzeniami w 3 ośrodkach przetwarzania. Oferowane Urządzenia muszą wspierać Metro Cluster pomiędzy 2 Urządzeniami wykorzystując sieć LAN/WAN (IP4) oraz jednocześnie repikację asynchroniczną do drugiego ośrodka.
23.	Ochrona danych	Oferowane rozwiązanie musi zapewniać zarządzanie kopiami zapasowymi zintegrowanymi np. z Vmware VADP, VSS, w oferowanej konfiguracji HA/DR. Kopie zapasowe muszą być przechowywane z zastosowaniem deduplikacji i kompresji zmiennym blokiem o wielkości 4kB+. Oprogramowanie musi być w pełni zintegrowane z konsolą do zarządzania. Kopie zapasowe maszyn wirtualnych muszą być wykonywane koherentnie/zintegrowane z hypervisorem i nie mogą wymuszać instalacji agenta lub dodatkowych zasobów dostarczonej infrastruktury produkcyjnej poza opisaną przez Zamawiającego. System ma objąć usługami ochrony danych wszystkie dane na dostarczonych serwerach pamięci masowych i pozwalać na odtworzenie danych w każdym ośrodku przetwarzania. System musi być zintegrowany (to jest nie wymaga dodatkowych narzędzi, zasobów, skryptów) i w pełni chronić replikowane pomiędzy 3 ośrodkami dane. System zarządzania kopiami zapasowymi musi zapewnić jakość opisywaną parametrami RPO=RTO=BW<=15 minut dla pełnych kopii zasobu o poj. 250 TB, oraz umożliwiać zarządzanie retencją kopii zapasowych (RET) w zakresie nie mniejszym niż 32 dni (1 miesiąc). Pod określeniem - tryb DR, należy rozumieć taką konfigurację wskazanych zasobów pamięci masowych, w której dane produkcyjne i migawki są replikowane przez dostarczone Serwery Pamięci Masowych pomiędzy ośrodkami przez przesyłanie wyłącznie zmodyfikowanych bloków. Zamawiający traktuje rozwiązania, w których migawka tworzona jest w ośrodku zapasowym względem aktywnych danych produkcyjnych jako rozwiązanie tożsame z replikacją migawek. Zamawiający wymaga, aby dostarczone licencje nie miały ograniczeń czasowych w ramach wyspecyfikowanych funkcjonalności. Oferowane Urządzenie musi umożliwiać integrację zadań wykonania i odtworzenia (w tym granularnego) kopii zapasowych z migawkami Urządzenia z co najmniej dwoma systemami backupu z ćwiartki „Leader" bieżącego raportu firmy Gartner (Data Center Backup and Recovery Solutions). Zamawiający zastrzega, że migawki muszą być integralną częścią polityki przechowywania danych. Integracja nie może wymagać tworzenia, utrzymywania i/lub modyfikacji skryptów i ma być w pełni zarządzana z jednego GUI. Oferent musi dostarczyć linki do stron internetowych producenta potwierdzających taką integrację. Jeśli funkcjonalność integracji wymaga zakupu dodatkowych komponentów (w tym licencji) muszą być dostarczone w ilości umożliwiającej objęcie taką ochroną środowiska o pojemności nie mniej niż 800TB danych użytkowych i serwerów z 36 procesorami łącznie.
24.	Licencje	Urządzenie powinno być dostarczone z licencją na wszystkie krytyczne funkcjonalności do pełnej pojemności Urządzenia, w tym co najmniej: tworzenie migawek sprzętowych zarządzanych przez aplikację, klonów, replikacji, QoS, zarządzanie i monitoring. Wymagane są licencje stałe (bez subskrypcji).

Lp.	Parametr	Charakterystyka parametru
25.	Fizyczne wymiary rozwiązania	Oferowane urządzenie musi mieć możliwość instalacji w standardowej szafie stelażowej 19" o głębokości 1050 mm, i być wyposażonej w redundantne zasilanie 230V. Urządzenie nie może zajmować więcej niż 12U.
26.	Usługi serwisowe	Gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii przez 24 godziny na dobę. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z Urządzeniem oraz oprogramowania wewnętrznego Urządzenia. Nośniki SSD muszą być objęte usługami wsparcia i gwarancji przy nieograniczonej intensywności wykorzystania (bez względu na intensywność zapisów).
27.	Szkolenia	Oferent dostarczy **nieodpłatne** certyfikowane szkolenia dla 6 osób z zakresu: a) podstawowego i zaawanasowanego zarządzania Urządzeniem b) integracji z platformą wirtualizacji c) integracji poszczególnych z klastrów Microsoft Hyper-V/MSCS d) replikacji i procedur DR e) integracji z dostarczonymi urządzeniami deduplikacyjnymi Oferent wykona 1 dniowe warsztaty obsługi dostarczonego rozwiązania w ramach procedury przekazania.

1.4 Warstwa Sieciowa Data Center

Ilość: - 6 sztuk - po 2 w każdej lokalizacji

Lp	Cecha	Wymagania minimalne/opis
1.	Ilość i typ portów przełącznika (obudowa/chassis)	Przełącznik montowany w standardowej szafie 42U o głębokości nieprzekraczającej 1075mm, umożliwiający w oferowanej konfiguracji: a) podłączenie serwerów co najmniej 20 portami w standardzie 10 GbE. b) podłączenie do istniejących urządzeń sieciowych Zamawiającego 1x10GbE SR LC. c) opisane w niniejszym punkcie przełączniki rdzeniowe, w części serwerowej danego ośrodka muszą być połączone ze sobą poprzez link wewnętrzny o sumarycznej przepustowości wynoszącej co najmniej 4x10Gbps. d) Porty stack/breakout oraz porty wymagane do podłączenia serwera pamięci masowej nie mogą ograniczać ilości podpiętych urządzeń wyspecyfikowanych powyżej. e) Podłączenia oferowanych serwerów pamięci masowych. Wykonawca jest zobowiązany dostarczyć okablowanie/transceivery w ilości niezbędnej do podłączenia dostarczonych serwera pamięci masowej, serwerów z istniejącą infrastrukturą Centrum Przetwarzania Danych Zamawiającego.
2.	Interfejs użytkownika	Web oraz CLI (SSH lub bezpośrednio przez port urządzenia) CLI musi wspierać zredefiniowane tryby pozwalające na dostęp do wybranych grup/poziomów komend systemowych. Urządzenie musi zapewniać ograniczenie dostępu do interfejsów zarządzających do wskazanych fizycznych interfejsów Ethernet (ang. out-of-band (OOB))
3.	SNMP	Oferującej bazę MIB pozwalającej na monitoring na poziomach: modułu, urządzenia oraz sensora.
4.	Wsparcie usług sieciowych	NTP, Clock & Time Zones PTP (IEEE-1588)
5.	Zarządzanie konfiguracją	Zapis, załadowanie oraz reset do ustawień fabrycznych konfiguracji.
6.	Logowanie zdarzeń i debugging	Logowanie musi zapewniać kategoryzację zdarzeń na kilkanaście poziomów krytyczności oraz konfigurowalny czas przechowywania informacji o zdarzeniach. Urządzenie musi zapewniać możliwość uruchomienia tzw. „debug traces" dla modułów Ethernet oraz protokołów. W szczególności musi wspierać tzw. „Link Diagnostic" per każdy wskazany port pozwalający na wgląd i konfigurację fizycznych parametrów pracy portu w tym „bit error rate (BER)", tzw. „samplowanie" zajętości bufora i zmiany jego zajętości w czasie.
7.	Kontrola dostępu i bezpieczeństwo	Różne poziomy autoryzacji dostępu dla użytkowników i grup, wsparcie dla RADIUS, TACACS+ & LDAP. Implementacja zabezpieczeń zgodnych z FIPS 140-2 w zakresach: kryptografii (X.509, IPSec) i szyfrowania, konfiguracja generowanie i modyfikacja certyfikatów x.509 do wykorzystania przez urządzenie. Wsparcie dla protokołu 802.1x w zakresie autentykacji hostów (suplikantów) i definicji dostępnych połączeń pomiędzy nimi.

Lp	Cecha	Wymagania minimalne/opis
8.	Realizowane funkcje	a) Przełączanie Ethernet, izolacja/grupowanie interfejsów, w tym Link Aggregation Group (LAG) – z rozszerzeniem wspierającym agregację interfejsów wielu urządzeń/przełączników). b) VLANs (segmentacja na poziomie L2 z wykorzystaniem TAG) c) Wsparcie dla Rapid Spanning Tree Protocol (RSTP): BPDU Filter, BPDU Guard, Loop Guard, Root Guard, MSTP & RPVST d) VXLAN (Virtual eXtensible Local Area Network) w zakresie wirtualnych sieci (tenantów) na poziomach L2 i L3 pozwalającej na rozszerzenie domeny broadcastowej L2 przez sieć poziomu 3. e) IGMP Snooping f) Link Layer Discovery Protocol (LLDP) g) Quality of Service: QoS Classification, QoS ReWrite, Queuing and Scheduling, RED & ECN h) Access Control List (ACL) na poziomie obiektu w celu monitorowania lub filtrowania pakietów. i) Port Mirroring j) sFlow (ver. 5) k) RDMA over Converged Ethernet (RoCE) l) Priority Flow Control m) IP Routing (interfejsy: VLAN, Loopback, Router port) dla IPv4/IPv6 n) Open Shortest Path First (OSPF) o) BGP p) BFD Infrastructure q) Multicast (IGMP and PIM) r) VRRP s) DHCP Relay
9.		Wraz z przełącznikiem należy dostarczyć transceivery oraz kable do połączenia z istniejącą infrastrukturą sieciową, Serwerami Pamięci Masowych i Wirtualizacji

1.5 Warstwa Sprzętowych Serwerów Wirtualizacji x86_64

Ilość: - 6 sztuk - po 2 w każdej lokalizacji

LP	Cecha	Wymagania minimalne/opis
1.	Obudowa	Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi oraz ramieniem do zarządzania kablami.
2.	Procesor(y)	Minimum 16 rdzeni procesorowych łącznie, x86 - 64 bity, osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 116 punktów w oferowanej konfiguracji. Wynik testu musi być opublikowany na stronie http://spec.org w dniu złożenia oferty.
3.	Liczba procesorów	Zgodnie z określoną ilością rdzeni procesorowych powyżej
4.	Pamięć operacyjna	256GB RDIMM DDR4 2800 MHZ w konfiguracji DPC=1. Płyta główna z minimum 16 slotami na pamięć i umożliwiająca rozbudowę do minimum 640GB. Płyta główna z fabrycznym oznaczeniem logo producenta (dopuszcza się logo producenta na module zarządzania trwale zintegrowanym na płycie głównej).
5.	Sloty rozszerzeń	Serwer musi być wyposażony w: a) 2 aktywne gniazda PCI-Express generacji 3 lub nowsze gotowe do obsadzenia kartami sieciowymi, każde gniazdo x16 (bus width) Serwer musi mieć dodatkowo dedykowane dwa gniazda PCI-Express: a) jeden na kontroler dyskowy; b) drugi na kartę sieciową 10/25Gb Ethernet dwuportową.
6.	Dysk twardy	Zatoki dyskowe gotowe do zainstalowania 8 dysków typu Hot Swap, SAS/SATA/SSD, 2,5" Zainstalowane 2 dyski SSD o pojemności 480GB każdy, DWPD min.2
7.	Kontroler	Serwer wyposażony w sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 2GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
8.	Interfejsy sieciowe i FC	Serwer musi być wyposażony w dwa porty 10 Gb SFP+. Oferowane karty LAN muszą znajdować się na liście kart certyfikowanych z ESXi 6.7 lub nowszym i wspierać sprzętowe SRIOV oraz ROCE2.0.
9.	Karta graficzna	Zintegrowana karta graficzna
10.	Porty	a) 2 x USB 3.0 lub nowsze b) 1x VGA Możliwość rozbudowy o: a) port szeregowy typu DB9/DE-9 (9-pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się stosowania kart PCI.
11.	Zasilacze	2 szt., typu Hot-plug, nadmiarowe – o mocy zapewniającej prace serwera w przypadku awarii jednego zasilacza.
12.	Chłodzenie	Zestaw nadmiarowych wentylatorów typu „hot-plug"
13.	Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w gnieździe PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:

		a) monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe b) dostęp do karty zarządzającej poprzez c) dedykowany port RJ45 z tyłu serwera lub d) przez współdzielony port zintegrowanej karty sieciowej serwera e) dostęp do karty możliwy f) z poziomu przeglądarki webowej (GUI) g) z poziomu wiersza poleceń; h) poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) i) wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i i wirtualnych folderów j) monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji k) konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (*capping*) l) zdalna aktualizacja oprogramowania (firmware) m) wsparcie dla Microsoft Active Directory n) wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API o) możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) p) automatyczne wysyłanie zgłoszeń do serwisu Wymagane dodatkowe oprogramowanie umożliwiające centralne monitorowanie i zarządzanie serwerami w tym zarządzanie za pomocą profili serwerowych (sekwencja *bootowania* systemu, ustawienia BIOS, wersja oprogramowania układowego i sterowników (dla Windows, VMware i Red Hat);
14.	Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	a) Microsoft Windows Server 2016 b) Microsoft Windows Server 2019 c) Red Hat Enterprise Linux (RHEL) d) SUSE Linux Enterprise Server (SLES) 15 e) VMware ESXi 6.7 U3, 7.0
15.	Certyfikaty i standardy	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.

1.6 Warstwa Sprzętowych Firewall/UTM

Ilość: - 3 sztuk - po jednym w każdej lokalizacji

ARCHITEKTURA SYSTEMU OCHRONY	
Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Dopuszcza się, aby elementy wchodzące w skład systemu ochrony były zrealizowane przez odrębne moduły w postaci zamkniętych platform sprzętowych lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Typ systemu ochrony	Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge).
Wymagania	System ochrony powinien spełniać wymagania w niżej wymienionym zakresie:

systemowe	a) Obsługa nielimitowanej ilości hostów w sieci chronionej. b) Typ procesora: Intel lub AMD multi-core technology c) Pamięć RAM: nie mniej niż 12 GB d) Obudowa przeznaczona do montażu w szafie RACK. e) Minimalna liczba i typ interfejsów fizycznych: 8x 1GbE Base-T, 2x 1GbE SFP, 6x 10GbE SFP+ f) Minimalna liczba nowych połączeń na sekundę: 200 000 g) Minimalna liczba jednoczesnych połączeń: 17 500 000 h) Minimalna przepustowość Firewall: 28 000 Mbps i) Minimalna przepustowość IPS: 5 500 Mbps j) Minimalna przepustowość Web Proxy AV: 3 300 Mbps k) Minimalna przepustowość VPN: 2 750 Mbps l) Dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 150 GB.
	PODSTAWOWE FUNKCJE SYSTEMU OCHRONY
Zarządzanie i utrzymanie	a) Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI). b) Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup. c) Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. d) Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. e) Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. f) System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności. g) System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów, w zakresie minimalnej ilości znaków czy złożoności hasła. h) System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. i) Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). j) System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. k) Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. l) System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji. m) Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej. n) System powinien być wyposażony w mechanizm automatycznego

	powiadamiania za pośrednictwem protokołów SMTP lub SNMP. o) Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpowiednik). p) System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. q) System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym on-premise lub on-cloud. r) Wymagane jest, aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP lub via email. s) Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych np. codziennie, raz w tygodniu lub raz w miesiącu. t) Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. u) Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej. v) Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). w) System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.
Zapora sieciowa, konfiguracja sieciowa oraz routing	a) Wymagane jest, aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. b) Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas. c) System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. d) Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług. e) Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. f) System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN. g) Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. h) Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading. i) System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). j) System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking). k) System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). l) Rozwiązanie powinno zapewniać obsługę routingu statycznego. m) Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). n) Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).

	o) System powinien oferować wsparcie dla IGMP snooping. p) Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy). q) Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. r) Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). s) System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. t) System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP. u) Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. v) Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów. w) Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules. x) Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta. y) Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). z) System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP. aa) System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania. bb) Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).
Podstawowe kształtowanie pasma oraz limity ilości danych	a) System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników. b) Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. c) System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Bezpieczna sieć bezprzewodowa	a) System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. b) Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater. c) Wdrożenie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. d) Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. e) Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej. f) Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej. g) Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2

	Enterprise. h) Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication). i) Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). j) System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. k) Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. l) System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden. m) System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe. n) Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection).
Autoryzacja użytkowników	a) Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication. b) Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. c) System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+. d) Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. e) Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password). f) Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server. g) System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. h) Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. i) Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal.
Samoobsługowy portal dla użytkowników	a) Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci. b) Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). c) Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows. d) Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android. e) Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła. f) Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika. g) Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email.
Podstawowe opcje VPN	System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: a) Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza

	RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) b) Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
	OCHRONA SIECI
IPS	a) Dodatkowy moduł ochrony klasy IPS z bazą minimum 2500 sygnatur. b) Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS. c) Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. d) Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów. e) System powinien generować alerty w przypadku wykrycia ataku.
ATP	System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control.
Clientless VPN	Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5.
	OCHRONA I KONTORLA WEB ORAZ APLIKACJI
Ochrona i kontrola Web	a) Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. b) Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP). c) System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. d) System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego. e) Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups). f) Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch). g) Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów. h) System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma. i) System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. j) Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów, cookies. k) System powinien zapewniać możliwość emulacji skryptów JavaScript. l) Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. m) Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. n) Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS. o) Rozwiązanie powinno umożliwiać blokadę stron HTTPS. p) Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS. q) Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/ tygodniowe/ miesięczne/ roczne dla użytkowników i grup użytkowników. r) System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji.
Ochrona i kontrola	a) Rozwiązanie powinno oferować bazę danych opisująca co najmniej 1500

aplikacji	aplikacji. b) Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. c) Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. d) Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania. e) Rozwiązanie powinno umożliwiać blokowanie: › aplikacji, które pozwalają na transfer plików (np. P2P). › komunikatorów internetowych, przynajmniej Skype, Gadu-gadu. › proxy uruchamianych poprzez przeglądarki internetowe. › streaming media (radio internetowe, Youtube, Vimeo). f) Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo.
Kształtowanie pasma dla Web i Aplikacji	a) Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie. b) Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. c) Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared).
	OCHRONA SERWERÓW APLIKACYJNYCH WEB
WAF	a) Ochrona klasy Web Application Firewall. b) Funkcjonalność oparta o mechanizm Reverse Proxy. c) Rozwiązanie powinno oferować mechanizm URL hardening with deep-linking and directory traversal prevention. d) Rozwiązanie powinno oferować mechanizm Form hardening. e) Rozwiązanie powinno oferować ochronę przed SQL injection. f) Rozwiązanie powinno oferować ochronę przed Cross-site scripting. g) System powinien zapewniać inspekcję ruchu HTTP oraz HTTPS (SSL). h) System powinien pozwalać na podpisywanie plików cookies. i) Rozwiązanie powinno oferować wsparcie dla Path-based routing. j) Rozwiązanie powinno oferować wsparcie dla Outlook Anywhere. k) Mechanizm Reverse authentication z automatycznym dodawaniem prefixu lub suffixu w trakcie autoryzacji użytkownika. l) Rozwiązanie umożliwiające publikowanie aplikacji web w Internecie na zasadzie wirtualnych serwerów aplikacyjnych. m) Rozwiązanie powinno oferować mechanizm rozkładający ruch odwiedzających między rzeczywiste serwery aplikacyjne (Load Balancing). n) System powinien umożliwiać stosowania masek typu wildcard dla ścieżek dostępowych. o) System powinien umożliwiać stosowanie operatorów logicznych AND/OR.
	LOGOWANIE I RAPORTOWANIE
	a) System powinien umożliwiać składowanie oraz archiwizację logów. b) System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. c) System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali.

d) System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.
e) System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).
f) Rozwiązanie powinno umożliwiać wysyłanie raportów via email.
g) Rozwiązanie powinno generować raporty w PDF, HTML i XLS.
h) Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.
i) System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza
j) System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację
k) Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.
l) System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora.
m) System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji.

1.7 Urządzenia brzegowe

Umożliwiają podłączenie zintegrowanej infrastruktury sieciowo-serwerowej do sieci Internet oraz połączenie trzech centrów danych między sobą.

Nazwa urządzenia	sztuk
Uniwersytet Szczeciński (ZCP)	
Switch minimum **4x10Gb SFP+**	4
Switch minimum **8x10Gb SFP+** oraz 10 portów RJ45 x 1Gb	1
Wkładki SFP+ LC MM 10Gb (min. 800 m)	10 (5 kompletów)
Wkładki SFP+ LC SM WDM 10Gb (min. 10km)	16 (8 kompletów)
Uniwersytet Gdański (ACP)	
Switch minimum **8x10Gb SFP+** oraz 10 portów RJ45 x 1Gb	2
Wkładki SFP+ LC SM WDM 10Gb (min. 800 m)	16 (8 kompletów)
Akademia Pomorska w Słupsku (PCP)	
Switch minimum **8x10Gb SFP+** oraz 10 portów RJ45 x 1Gb	3
Wkładki SFP+ LC SM WDM 10Gb	16 (8 kompletów)

1.8 Licencje oprogramowania wirtualizującego

Zamawiający wymaga dostarczenia licencji wirtualizatora zgodnego z opisem:

Pożądane parametry oprogramowania wirtualizacji:

1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
4. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
5. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows, Linux.
6. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
7. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.

8. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach.
9. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
11. Rozwiązanie musi mieć możliwość przenoszenia maszyn i dysków wirtualnych w czasie ich pracy pomiędzy zasobami dyskowymi i serwerami fizycznymi.
12. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
13. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).

W przypadku np. licencji VMWARE proponuje się następującą konfiguracje:

1. vSphere Standard 1 Processor - w ilości zgodnej ilością procesorów serwerów przeznaczonych do wirtualizacji.
2. vCenter Server Standard for vSphere - w ilości zgodnej z ilością ośrodków przetwarzania (3 sztuki)

1.9 Certyfikowane Szkolenia (nieodpłatne)

W ramach oferowanej ceny, Zamawiający wymaga, przeprowadzenia / zapewnienia udziału w nieodpłatnych certyfikowanych szkoleniach prowadzonych przez podmiot posiadający uprawnienia nadane przez producenta do prowadzenia autoryzowanych szkoleń w jego imieniu, w zakresie:

1. **Serwery Pamięci Masowych na poziomie podstawowymi i zaawansowanym** – obejmującym rozległe klastry i replikację
2. **Oprogramowanie wirtualizacji** – Administracja

Liczba osób, które wezmą udział w szkoleniu: 6 osób.

1.10 Dokumentacja powykonawcza

Wykonawca dostarczy szczegółową dokumentacje powykonawczą zawierającą co najmniej opis konfiguracji oraz schematy połączeń dla każdej lokalizacji oraz pomiędzy lokalizacjami.

2 Włączenie Platformy w infrastrukturę centrów danych

Dostarczoną platformę należy włączyć, w istniejąca infrastrukturę Zamawiającego z wykorzystaniem dostarczonych urządzeń brzegowych. Opis zasobów, jakimi dysponuje Zamawiający w poszczególnych lokalizacjach zawarty jest PONIŻEJ:

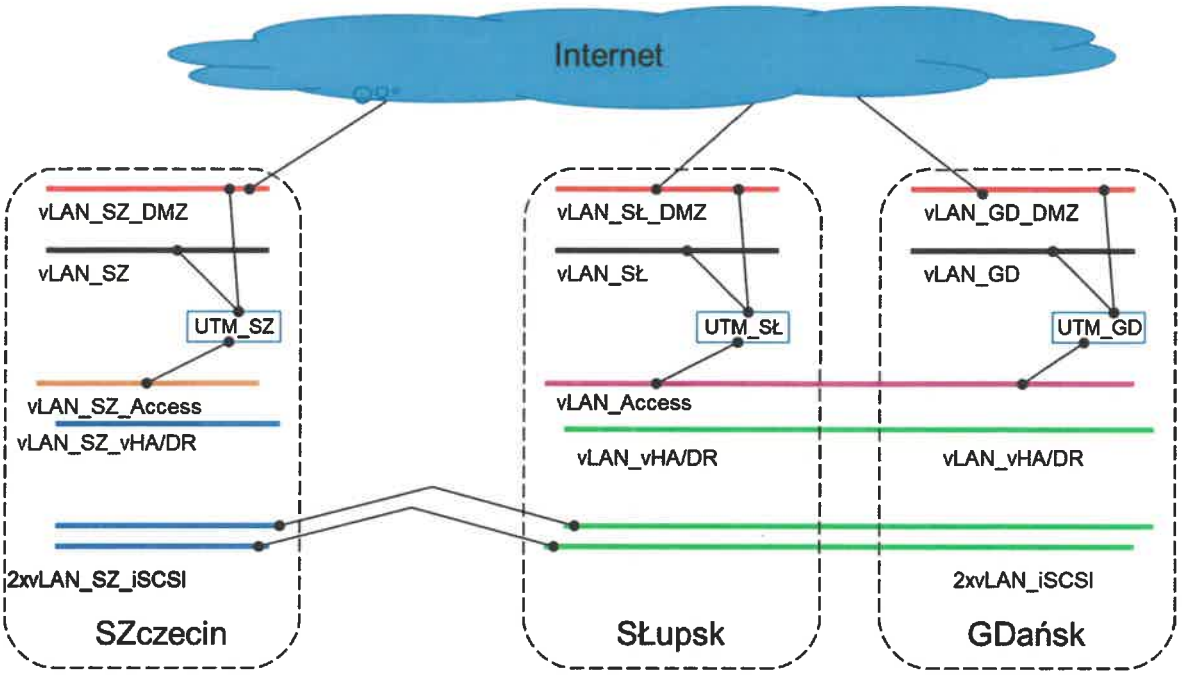
UWAGA:
Zamawiający, zobowiązuje się do udostępnienia w każdym ośrodku:

1. Przestrzeni na instalację szafy stelażowej 19" o wysokości 42U i wymiarach 600x1300.
2. Podłączenia dostarczonej infrastruktury do sieci energetycznej jednofazowej 4x 16A
3. Podłączenia dostarczonej platformy usługowej do istniejącej infrastruktury sieciowej LAN, w zależności od możliwości danego ośrodka, za pomocą jednego lub 2 portów 10GbE SR LC.
4. 10 portów 1GbE RJ45 (sieć zarządzająca)
5. Punktów podpięcia rozwiązań UTM/Firewall (wraz z dostosowaniem trybu ich pracy/strefy bezpieczeństwa/DMZ) w standardzie 1GbE RJ45 lub 10GbE SFP+.
6. Zamawiający zapewni wysokodostępne symetryczne łącza:
   a. pomiędzy ośrodkami PCP i ACP o przepustowości 10 Gbps
   b. pomiędzy ośrodkiem ZPC a ośrodkami PCP i ACP o przepustowości 10Gbps wspierające QinVNI funkcji VXLAN oraz Jumbo frames do 9200 B.

Rekomendowana konfiguracja logiczna segmentów sieciowych:

3. Segmenty sieciowe: vLAN_vHA/DR, vLAN_Access rozciągnięte pomiędzy ośrodkami **PCP i ACP** przy użyciu tunelowania QinVNI - funkcja VXLAN.
4. Podsieci vLAN_SZ_iSCSI_(1|2) oraz vLAN_ iSCSI_(1|2) połączone między sobą przy zastosowaniu routing'u (zamknięte podsieci obsługujące ruch techniczny – nie wymagają UTMa)
5. VLAN_SZ, VLAN_SŁ, VLAN_GD – segmenty sieciowe pozwalające na bezpośredni dostęp do platformy SAHP odpowiednio z sieci uczelnianych ośrodków **PCP, ACP oraz ZCP**.

Poglądowy schemat połączeń sieciowych dla planowanego rozwiązania przedstawia poniższy rysunek.



Rysunek 1: Schemat poglądowy połączeń sieciowych rozwiązania

3 Gwarancja i serwis

Dla każdej części zamówienia, o ile wymagania szczegółowe nie stanowią inaczej, Zamawiający wymaga udzielenia gwarancji na okres nie mniejszy niż 3 lata, zgodnie z warunkami podanymi poniżej.

3.1 Ogólne wymagania dotyczące sprzętu

1. Dostarczony sprzętu musi być objęta gwarancją zgodną z deklaracją Wykonawcy, zawartą w formularzy ofertowym.
2. Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów lub ich autoryzowanych, w zakresie serwisu, partnerów.
3. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.
4. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
5. Firma serwisująca musi posiadać autoryzacje producenta.
6. W przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, producent przejmie na siebie wszelkie zobowiązania związane z serwisem.
7. Wykonawca dostarczy wraz z towarem dokument gwarancji, jakości sprzętu wystawiony przez siebie lub producenta urządzenia, zobowiązujący wystawcę dokumentu (gwaranta) do usunięcia wady fizycznej towaru lub do dostarczenia towaru wolnego od wad, jeżeli wady te ujawnią się w ciągu terminu obowiązywania gwarancji.
8. Okres gwarancji, które Wykonawca udzieli Zamawiającemu, będzie zgodny z wymaganiami wyspecyfikowanymi dla poszczególnych urządzeń i oprogramowania.
9. Bieg okresów gwarancyjnych rozpoczyna się z dniem podpisania Protokołu Odbioru Końcowego bez uwag (zastrzeżeń).
10. Czas naprawy wyłączony będzie z okresu gwarancyjnego. Czas trwania gwarancji zostanie automatycznie wydłużony o czas trwania naprawy.

11. W okresie gwarancji, wszelkie koszty związane z usunięciem awarii, w tym dostarczenie uszkodzonego sprzętu do punktu serwisowego, obciążają wykonawcę.
12. Gwarancja obejmie wszystkie wykryte podczas eksploatacji sprzętu usterki i wady oraz uszkodzenia powstałe w czasie poprawnego zgodnego z instrukcją użytkowania.
13. Dla wszystkich urządzeń, które posiadają dyski twarde w razie awarii, Zamawiający wymaga, aby na czas naprawy dysk pozostał w siedzibie Zamawiającego.
14. Zasady eksploatacji i konserwacji urządzeń zostaną określone w przekazanej przez wykonawcę „Instrukcji użytkowania i eksploatacji urządzeń" wraz z wykazem urządzeń, które wymagają przeglądów serwisowych, które Wykonawca wykona na własny koszt.
15. W przypadku awarii sprzętu, która nie została usunięta w terminie 30 dni, Wykonawca zobowiązuje się do wymiany sprzętu na nowy o parametrach nie gorszych od sprzętu uszkodzonego. Wymiana sprzętu na nowy nastąpi najpóźniej w 35 dniu od zgłoszenia.
16. Wykonawca gwarantuje Zamawiającemu, że udzielając licencji na korzystanie z oprogramowania nie narusza żadnych praw osób trzecich oraz że nie zachodzą jakiekolwiek podstawy do zgłoszenia przez osoby trzecie roszczeń wobec tych praw. Wykonawca zabezpieczy Zamawiającego w zakresie zakupionych przez niego licencji przed roszczeniami osób trzecich. Wykonawca zobowiąże się do podjęcia na swój koszt i ryzyko wszelkich kroków prawnych zapewniających należytą ochronę przed roszczeniami osób trzecich oraz pokrycia wszelkich kosztów i strat z tym związanych, jak również związanych z naruszeniem przepisów Ustawy o prawie autorskim i prawach pokrewnych.
17. Wykonawca zapewni możliwość zgłaszania awarii sprzętu w okresie gwarancji telefonicznie, faksem oraz drogą mailową w godzinach od 8.00 do 17.00 od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy. Zgłoszenie awarii po godz. 17.00 będzie traktowane, jak zgłoszenie o godz. 8.00 następnego dnia roboczego.
18. Wykonawca, od momentu zgłoszenia, musi podjąć czynności serwisowych w czasie określonym dla poszczególnych urządzeń w tabelach powyżej.
19. W przypadku stwierdzenia wady ukrytej sprzętu (towaru) wykonawca musi wymienić go na nowy, w ciągu 14 dni roboczych od daty zgłoszenia tej wady.
20. Serwis gwarancyjny świadczony będzie w miejscu użytkowania sprzętu w godz. 7.30 -15.30.
21. W przypadku, kiedy Wykonawca uzna za konieczna naprawę sprzętu w serwisie, Wykonawca zapewni:
    a) odbiór na własny koszt wadliwego sprzętu (towaru) w terminie nieprzekraczającym 2 dni roboczych;
    b) dostawę naprawionego sprzętu na własny koszt w terminie nie przekraczającym 2 dni roboczych od dnia usunięcia awarii przez serwis, a w uzasadnionych przypadkach w terminie nie dłuższym niż 14 dni roboczych od odebrania sprzętu z siedziby zamawiającego
    c) w przypadku braku możliwości usunięcia awarii w terminie 14 dni roboczych od dnia odebrania wadliwego sprzętu (towaru) z siedziby zamawiającego, wykonawca zobowiąże się do bezpłatnego dostarczenia i uruchomienia nowego sprzętu zastępczego o parametrach równoważnych z oferowanymi. Podstawiony sprzęt będzie miał zainstalowany uzgodniony z Zamawiającym system operacyjny i wszystkie dodatkowe, standardowe poprawki niezbędne do jego poprawnej pracy.
22. Koszt dojazdu ekipy serwisowej w ramach napraw gwarancyjnych i koszty transportu sprzętu naprawianego w ramach gwarancji pokryje wykonawca.

3.2 Minimalne i wymagane okresy gwarancji

3.2.1 Szafa Rack 19"

- 5 lat gwarancji na systemy awaryjnego podtrzymania zasilania (UPS)

3.2.2 Warstwa Serwerów Pamięci Masowej

- 7-letnia gwarancja producenta w miejscu instalacji.
- Możliwość zgłoszenia awarii przez 24 godziny na dobę.
- W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z Urządzeniem oraz oprogramowania wewnętrznego Urządzenia.
- Nośniki SSD muszą być objęte usługami wsparcia i gwarancji przy nieograniczonej intensywności wykorzystania (bez względu na intensywność zapisów).

3.2.3 Warstwa Sieciowa Data Center

- 5 lat gwarancji i wsparcia w siedzibie klienta w trybie NBD

3.2.4 Warstwa Sprzętowych Serwerów Wirtualizacji x86_64

- 5-letnia gwarancja producenta serwera w miejscu instalacji świadczona w trybie NBD (9x5)
- Czas reakcji w miejscu instalacji to kolejny dzień roboczy.
- Wsparcie techniczne realizowane jest przez organizację serwisową producenta oferowanego serwera

3.2.5 Warstwa Sprzętowych Firewall/UTM

- Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 5 lat
- Gwarancja i wsparcie techniczne producenta w trybie 8x5 na okres nie krótszy niż 5 lat
- Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.

3.2.6 Urządzenia brzegowe

- 5 lat gwarancji i wsparcia w siedzibie klienta w trybie NBD

3.2.7 Licencje oprogramowania wirtualizującego

- Okres wsparcia licencji ma być równy czasowi wsparcia oferowanych Urządzeń, jednak nie krócej niż 5 lat

3.3 Opłaty utrzymaniowe

Zamawiający wymaga, aby cena ofertowa zawierała wszelkie opłaty serwisowe, utrzymaniowe (subskrypcje, aktualizacje, poprawki, dostęp do najnowszej wersji oprogramowania), licencyjne oraz wsparcia technicznego, w okresie zgodnym z deklaracją zawartą w formularzy ofertowym, jednak nie krótszym, o ile w tabelach powyżej nie wskazano inaczej, niż 5 lat od daty podpisania protokołu odbioru końcowego.

3.4 Oprogramowanie

1. O ile w tabelach powyżej nie wskazano inaczej, Wykonawca, zapewni wsparcie techniczne producenta oprogramowania na okres zgodny z deklaracją zawartą w formularzy ofertowym, jednak nie krótszą niż 5 lat.
2. Wsparcie techniczne obejmie co najmniej:
   a) aktualizacje,
   b) poprawki,
   c) dostęp do najnowszych wersji oprogramowania
3. Wykonawca zapewni możliwość dokonywania nielimitowanej liczby zgłoszeń oraz pomoc techniczną w trybie 24h/7 lub 9h/5;
4. Wsparcie techniczne producenta musi być świadczone w formie zgłoszeń telefonicznych lub przez stronę www producenta oprogramowania;
5. Usługi wsparcia technicznego i subskrypcji edycji muszą być świadczone przez producenta oprogramowania;

3.5 Inne

Oferowane przez Wykonawcę w dniu składania ofert rozwiązania, nie mogą być przeznaczone przez ich producenta do wycofania z produkcji, sprzedaży lub z wsparcia technicznego.
Zamawiający wymaga, aby dostarczone wraz ze sprzętem oprogramowanie było oprogramowaniem w wersji aktualnej na dzień składania ofert.

UWAGA:
Zamawiający informuje, iż Infrastruktura będąca przedmiotem niniejszego oszacowania gwarantować musi skuteczne uruchomienie planowanych rozwiązań informatycznych – środowiska Platformy Herbarium Pomeranicum. Zamawiający pomocniczo przekazuje, celem należytego doboru oferowanych rozwiązań opracowanie pt.: Projekt wykonawczy Platformy Herbarium Pomeranicum.

Wycenę prosimy przesłać wykorzystując do tego celu formularz oferty zamieszczony na platformie zakupowej https://platformazakupowa.pl/pn/usz w terminie do dnia **22.09.2020 r. do godz. 15.00**
Dopuszcza się możliwość ewentualnej zmiany parametrów oferowanych urządzeń – w przypadku, gdy Wykonawca dostrzega potrzebę zmiany konkretnego parametru, proszony jest o przesłanie za pomocą platformy zakupowej https://platformazakupowa.pl/pn/usz odpowiedniego wniosku.
Dopuszcza się także – w przypadku braku możliwości przedstawienia wyceny dotyczącej wszystkich urządzeń – wycenę poszczególnych pozycji zawartych w formularzu.

UWAGA:
Niniejsze Rozeznanie nie stanowi oferty w rozumieniu przepisów ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2019 r. poz. 1145), jak również nie jest ogłoszeniem w rozumieniu przepisów ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 ze zm.).

KIEROWNIK Działu Zamówień Publicznych mgr Wojciech Bieszko

KANCLERZ mgr inż. Andrzej Jabłoński 14.09.2020