Cześć nr 1 zamówienia

1. **Serwer do wirtualizacji – 1 szt.**

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi) Serwer wyposażony w zdejmowany panel przedni oraz czujnik otwarcia obudowy współpracujący z BIOS/UEFI.
Procesor	Dwa procesory ośmiordzeniowe, x86 - 64 bity, Intel Xeon Silver 4309Y lub równoważne procesory ośmiordzeniowe pracujące z częstotliwością bazową min. 2.8GHz i osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 133 punktów, dla testu oferowanego modelu serwera z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org Zamawiający posiada działający klaster vSphere HA oparty o serwery z procesorami Intel. Nowo dostarczony serwer ma zapewniać włączenie serwera do klastra. Płyta główna wspierająca zastosowanie procesorów od 4 do 40 rdzeni, mocy do min. 270W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 2 procesory
Pamięć operacyjna	Min. 128GB RDIMM DDR4 3200 MT/s w modułach pamięci o pojemności 16 GB każdy Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB. Zapewnia obsługę pamięci typu Intel Optane Persistent Memory, lub równoważny chipset jeśli potwierdza możliwość instalowania pamięci Intel Optane DC Persistent Memory.
Sloty rozszerzeń	Min. 3 aktywnych gniazd PCI-Express generacji 4, x16 (szybkość slotu – bus width). Jedno gniazdo pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi.
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min. 8 dysków SFF typu Hot Swap, SAS/SATA/SSD 2,5”. Opcja rozbudowy/rekonfiguracji serwera o dodatkowe 2 dyski typu Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy. W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 10 zatoki dyskowe SFF gotowe do instalacji dysków SAS/SATA/SSD 2,5”typu Hot Swap. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Zainstalowane min. 2szt. dysków M.2 NVMe SSD 480GB z realizacją RAID1 sprzętowo. Rozwiązanie wspierane minimum przez system operacyjny Esxi 7.x.
Kontroler	Możliwość instalacji kontrolera sprzętowego wyposażony w min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę napędów dyskowych SSD/SATA/SAS/NVMe.

Interfejsy sieciowe	Minimum 4 porty 1G Base-T (karta nie powinna zajmować slotów PCI-e i musi być zainstalowana w dedykowanym złączu dla karty sieciowej) Minimum 2 porty 10Gb SFP+ SR wraz z modułami optycznymi SFP+ SR Minimum 2 porty 16Gb FC wraz z modułami optycznymi 16Gb SW 4 kable światłowodowe OM3 LC-LC 3m 1 kabel do połączenia karty zarządzającej 3m
Karta graficzna	Zintegrowana karta graficzna
Porty	5 x USB 3.0 (w tym 2 porty wewnętrzne) 1x VGA 1x slot na kartę microSD Możliwość rozbudowy/rekonfiguracji o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express - cyfrowy port video (Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Diagnostyka	Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0 oraz czujnik otwarcia obudowy.
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników

	• przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power capping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Serwer jest dostarczany bez Systemu operacyjnego Zapewnia wsparcie dla: Microsoft Windows Server 2016, 2019, 2022 Ubuntu 20.04 LTS Red Hat Enterprise Linux (RHEL) 7.9 oraz 8.2 SUSE Linux Enterprise Server (SLES) 12 SP5 oraz 15 SP2 VMware ESXi 6.7 U3, 7.0 U2/U3
System operacyjny	Serwer dostarczony z systemem operacyjnym Windows Server 2022 16 core umożliwiającym uruchomienie 4 maszyn wirtualnych z Windows Server w ramach tego hosta.
Wsparcie techniczne	Minimum 3-letnia gwarancja producenta 9x5 w miejscu instalacji typu On-Site z 2-godzinnym czasem reakcji i przybyciem na miejsce najpóźniej na następny dzień roboczy. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń.
Inne	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.

	Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Dodatkowe wyposażenie	Dwie karty sieciowe 10Gb dwuportowe SFP+ z wkładkami optycznymi SFP+ SR. Karty kompatybilne z serwerami HPE DL360 Gen10 Dwie karty FC 16GB dwuportowe z wkładkami FC 16Gb SW. Karty kompatybilne z serwerami HPE DL360 gen10. 4 kable światłowodowe OM3 LC-LC 3m
Wdrożenie	a) Instalacja serwera w szafie i konfiguracja serwera do wirtualizacji. b) Okablowanie LAN i SAN w taki sposób aby awaria pojedynczego interfejsu nie powodował przerwy w dostępie maszyn wirtualnych do LAN i SAN. c) Instalacja systemu ESXi i włączenie do klastra vSphere HA. Zagwarantowanie działania HA i vMotion. d) Migracja części maszyn wirtualnych na nowy serwer e) Instalacja dostarczonych kart LAN i FC w dwóch hostach ESXi. Serwery to HPE DL360 Gen10. Rekonfiguracja LAN po stronie systemów w taki sposób aby komunikacja zapewniona była poprzez interfejsy 10Gb do dostarczonych przełączników.

2. Licencja do backupu do nowego serwera– 1 szt.

Wymagania minimalne
• Oprogramowanie musi byś dostarczone dla 15 maszyn wirtualnych. Okres wsparcia 24/7 minimum na 3 lata. • Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków • Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental) • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji

- Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
- Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
- Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
- Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
- Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
- Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
- Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
- Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
- Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
- Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
- Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
- Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
- Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
- Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
- Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
- Oprogramowanie musi oferować ten mechanizm z dokładnością do datastoru
- Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
- Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
- Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

- Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
- Oprogramowanie musi posiadać wsparcie dla NDMP
- Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
- Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
- Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
- Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
- Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
- Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
- Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
- Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
- Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
- Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
- Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)
- Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
- Dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
- Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
- Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
- Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
- Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
- Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

- Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
    - **Linux**
        - ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
    - **BSD**
        - UFS, UFS2
    - **Solaris**
        - ZFS, UFS
    - **Mac**
        - HFS, HFS+
    - **Windows**
        - NTFS, FAT, FAT32, ReFS
    - **Novell OES**
        - NSS
- Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
- Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
- Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.
- Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
- Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
- Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
- Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
- Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
- Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
- Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
- Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
- Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

• Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

3. Macierz dyskowa – 1 szt.

Wymagania minimalne
1. Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu.
2. Minimum dwa kontrolery pracujące w trybie Symmetrical Active-Active (SAN-only), to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery muszą pozwalać na udostępnianie zasobów protokołem FC, iSCSI w zależności od zastosowanych kart komunikacyjnych.
3. Komunikacja pomiędzy parą kontrolerów (synchronizacja cache) macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband.
4. Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze wielu kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego.
5. Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 2 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązanie oparte o wirtualizator.
6. Macierz musi umożliwiać rozbudowę do co najmniej 6 par kontrolerów dyskowych tworzących jedna logiczną macierz, bez konieczności wymiany zaoferowanej pary kontrolerów.
7. Macierz musi być skonstruowana wyłącznie do obsługi modułów pamięci SSD i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych.
8. Całkowita pojemność brutto (fizyczna) urządzenia musi wynosić minimum 30 TB i musi być zbudowana wyłącznie w oparciu o moduły pamięci SSD. Rozmiar pojedynczego modułu nie może być większy niż 4 TB.
9. Macierz musi umożliwiać rozbudowę do co najmniej 70 sztuk oferowanego typu modułów pamięci, bez wymiany kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. (tylko poprzez dodawanie półek i modułów SSD)
10. Kontrolery łącznie muszą być wyposażone w procesory o sumarycznej ilości min. 48 rdzeni (ang.: core).
11. Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 192GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin.
12. Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.

13. Macierz musi posiadać minimum 4 porty 10Gb/s obsługujące protokół iSCSI na każdy kontroler. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), wymaga się ich dostarczenia wraz z urządzeniem.
14. Macierz musi posiadać minimum 8 portów 16Gb/s FC w ramach zaoferowanej ilości kontrolerów oraz możliwość podłączania serwerów bezpośrednio do tych portów macierzy bez użycia przełączników.
15. Urządzenie musi obsługiwać poziomy RAID5 i RAID6 (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare) lub równoważne poziomy RAID zabezpieczające przed awarią dwóch dysków jednocześnie.
16. Macierz musi umożliwiać skonfigurowanie poziomu RAID zapewniającego odporność na jednoczesną awarię 3 dysków w grupie RAID.
17. Brak pojedynczego punktu awarii. Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy.
18. Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap.
19. Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania
20. Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów SSD. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI co najmniej 1 rok wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożlwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
21. Urządzenie musi umożliwiać utworzenie 800 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 5000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
22. Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii).
23. Tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
24. Macierz musi mieć możliwość włączenia funkcjonalności deduplikacji i kompresji danych w trybie in-line, a ponadto musi ona umożliwiać: • włączenie deduplikacji dla poszczególnych wolumenów, • wyłączenie deduplikacji dla poszczególnych wolumenów na których wcześniej deduplikacja była włączona, • włączenie kompresji dla poszczególnych wolumenów,

• wyłączenie kompresji dla poszczególnych wolumenów na których wcześniej kompresja była włączona, • uruchomienia jednocześnie deduplikacji i kompresji dla dowolnego wolumenu, Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
25. Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
26. Model oferowanej macierzy musi znajdować się na oficjalnej liście zgodności VMware (dostępnej na stronie https://www.vmware.com/resources/compatibility/search.php) dla kryterium wyszukiwania "Site Recovery Manager (SRM) for SRA" i produktu "SRM 8.3" lub jego nowszej dostępnej aktualizacji.
27. Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym pojęciem „wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności", musi wspierać klastrownie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności" musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności" musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności" musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
28. Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
29. Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows, Vmware, Linux, których używa Zamawiający.
30. Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Windows Server 2016/2019,Vmware 6.7, Vmware 7.0, których używa Zamawiający

31. Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.
32. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP.
33. Macierz dyskowa musi zostać objęta minimum 3-letnim okresem gwarancji producenta on-site z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.
34. Zgłoszenia usterek muszą być akceptowane zarówno drogą email jak również drogą telefoniczną.
35. Usługi gwarancyjne świadczone przez wykonawcę/producenta sprzętu posiadającego certyfikat ISO co najmniej 9001:2008 lub równoważny na świadczenie usług serwisowych lub podmiot posiadający autoryzację producenta sprzętu oraz posiadający certyfikat ISO co najmniej 9001:2008 lub równoważny.
36. Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków: – bezpłatna możliwość aktualizacje firmware; – dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń; – dostęp do centrum pomocy technicznej producenta; – otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware; – otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy. – uszkodzony dysk zostaje u zamawiającego
37. Wdrożenie: • Instalacja macierzy w szafie we wskazanym miejscu • Okablowanie SAN i zarządzanie • Inicjalizacja i konfiguracja w sposób redundantny po FC • Podłączenie do 3 hostów Esxi w sposób zapewniający dostęp do zasobów dyskowych macierzy dwoma niezależnymi ścieżkami FC • Migracja maszyn wirtualnych ze starej macierzy

4. Przełącznik sieciowy – 4 szt.

Wymagania minimalne
1. Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy
2. Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy
3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika
4. Wydajność: minimum 130 Mp/s
5. Bufor pakietów: minimum 7.5 MB
6. Minimum 8GB pamięci operacyjnej
7. Minimum 15GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9. Dedykowany port konsoli USB
10. Port USB 2.0 (niezależny od portu konsoli USB)
11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)
12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Dostępne metody łączenia przełączników muszą umożliwiać realizację stosów na odległość co najmniej 300m
13. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie
14. Pobór mocy nie może być większy niż 70W
15. Wielkość tablicy routingu: minimum 2000 wpisów IPv4, 1000 wpisów IPv6
16. Wielkość tablicy ARP co najmniej 8000 wpisów, wielkość tablicy ND co najmniej 8000 wpisów
17. Tablica adresów MAC o wielkości minimum 16000 pozycji
18. Obsługa Jumbo Frames
19. Obsługa sFlow lub Netflow
20. Obsługa skryptów w języku Python
21. Obsługa REST API
22. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty
23. Obsługa RMON (minimum grupy 1,2,3 i 9)
24. Obsługa 4094 tagów IEEE 802.1Q oraz 2000 jednoczesnych sieci VLAN
25. Obsługa standardu 802.1v
26. Obsługa protokołu MVRP
27. Wsparcie dla VXLAN
28. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
29. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
30. Obsługa Secure FTP lub SCP
31. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)

32. Obsługa SNTPv4 lub NTP
33. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
34. Obsługa protokołów rutingu: ruting statyczny, OSPF, OSPFv3
35. Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 1000 grup), MLD (co najmniej 1000 grup)
36. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
37. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
38. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
39. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
40. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
41. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera
42. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
43. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
44. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
45. Wbudowany serwer DHCP
46. Obsługa blokowania nieautoryzowanych serwerów DHCP
47. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
48. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
49. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Co najmniej 5000 wpisów typu ingress i 2000 wpisów typu egress dla IPv4 i MAC
50. Wbudowana sonda IP SLA
51. Zakres pracy od 0 do 45°C
52. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
53. Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 35 cm
54. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji
55. Minimum 3-letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu
56. Wdrożenie **a) Rekonfiguracja portów na LACP (posiadanego FG60E) z redundantnym podłączeniem do nowych switchy poprzez RJ45 np. 4 linkami** **b) Konfiguracja stosów przełączników** - konfiguracja przełącznika „master” - podłączenie pozostałych przełączników do stosu - aktualizacja oprogramowania (jeśli wymagana) - konfiguracja L2 – LACP, VLANy - konfiguracja L3 – IP

- konfiguracja mechanizmów bezpieczeństwa – loop-protect, STP, dhcp-snooping, arp-protect
- konfiguracja połączenia z istniejącą infrastrukturą
- konfiguracja połączeń z serwerami
- konfiguracja dostępu

5. Zasilacz awaryjny UPS z dodatkowym modułem bateryjnym do drugiej lokalizacji - 1 szt.

Element konfiguracji	Wymagania minimalne
Moc pozorna	3000 VA
Moc rzeczywista	3000 W
Współczynnik mocy	1
Topologia (klasyfikacja IEC 62040-3)	line-interactive
Typ obudowy UPS	Uniwersalna tower/rack 2U
Liczba, typ gniazd wyjściowych, możliwość sterowania	8 x C13 (w tym 2 grupy po 2 gniazda C13 z możliwością sterowania), 2 x C19
Typ gniazda wejściowego	Gniazdo C20
Czas podtrzymania dla 100% obciążenia	17 minut
Napięcie znamionowe	230 V
Tolerancja napięcia prostownika	160 - 294 V
Częstotliwość znamionowa	50/60 Hz autodetekcja
Tolerancja częstotliwości	47 - 70 Hz (system 50 Hz); 56,5 - 70 Hz (system 60 Hz); 40 Hz w trybie niskiej czułości
Napięcie znamionowe wyjściowe	230 V (domyślnie) / 200/208/220/240 V
Częstotliwość wyjściowa	50/60 Hz
Baterie wymieniane przez użytkownika "na gorąco"	Tak
Ochrona przed przeładowaniem	Tak
Ochrona przed głębokim rozładowaniem	Tak
Okresowy automatyczny test baterii	Tak
Zimny start	Tak
System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
Interfejs komunikacyjny	• USB
	• RS232 DB-9 żeński
	• miniport wyłącznik awaryjny RPO
	• miniport wyłącznik ON/OFF
	• listwa zaciskowa dla przekaźnika wyjściowego

Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS'a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh)
	• Poziomy rząd przycisków sterowania
	• Poziomy rząd wskaźników stanu: trybu normalnego (zielony), trybu bateryjnego (żółty), usterki (czerwony)
	• Pasek LED sygnalizujący stan
Przyciski sterujące i wskaźniki diodowe LED	• sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie)
	• przycisk Escape (anulowanie)
	• przyciski funkcyjne (przewijanie w górę i w dół)
	• przycisk Enter (potwierdzający)
Wyposażenie	• instrukcja obsługi, instrukcja bezpieczeństwa
	• przewód zasilający
	• kabel RS232
	• kabel USB
	• karta SNMP
	• uchwyty kablowe
	• podstawki do montażu pionowego (wieża)
	• 2 przewody IEC C13-C14 10 A
	• zestaw szyn montażowych do szafy 19"
Karta SNMP	• cyberbezpieczeństwo (certyfikaty UL 2900-2-2/IEC62443/HTTPS/MQTT/ /RNDIS/LDAP/NVD/SSH/PKI, pakiet szyfrów TLS 1.2 z minimum SHA256)
	• certyfikaty CA i PKl
	• prędkość gigabitowa (half-duplex, full-duplex)
	• różne poziomy nadawania dostępu do konta administratora lub użytkownika
Dołączone oprogramowanie	Oprogramowanie do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii. Oprogramowanie kompatybilne ze wszystkimi głównymi OS.
Max. wymiary UPS (szer. x gł. x wys. w mm)	438 x 603 x 85,5
Max. wymiary dodatkowego modułu bateryjnego (szer. x gł. x wys. w mm)	438 x 603 x 85,5
Poziom hałasu w odl. 1m	< 45 dBA
Zgodność z normami UE	Deklaracja zgodności producenta CE
Dodatkowe cetyfikaty	ISO 9001 producenta urządzenia
Gwarancja producenta	36 miesięcy dla elektroniki, 24 miesięcy dla baterii
Dodatkowe wyposażenie	**Listwa zasilająca – 3 szt.** Do montażu w szfie Rack. Wejście: IEC C20, wyjście 12 szt. IEC C13, 1 szt. C19. 2 grupy gniazd C13 (po 6 sztuk) każda z osobnym zabezpieczeniem nadprądowym. Zabezpieczenie przed przypadkowym wypięciem kabli. W zestawie z kablami zasilającymi: IEC C19-C20 oraz IEC C19-C14. **Przewód zasilający - 2 szt.** Kabel zasilający 16A, IEC 320 Schuko - C19, o długości min. 2,5 m

Wdrożenie	a) Dostawa oraz montaż urządzeń w szafie Rack. b) Podłączenie do prądu i uruchomienie. c) Konfiguracja zasilacza awaryjnego oraz karty SNMP. d) Szkolenie z obsługi dostarczonego zasilacza awaryjnego.

6. Serwer backupu– 1 szt.

Element konfiguracji	Wymagania minimalne
Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi) Serwer wyposażony w zdejmowany panel przedni zamkiem chroniącym przed nieuprawionym dostępem do dysków oraz czujnikiem otwarcia obudowy współpracującym z BIOS/UEFI.
Procesor	Jeden procesor ośmiordzeniowy, x86 - 64 bity, Intel Xeon Silver 4309Y lub równoważny procesor ośmiordzeniowy pracujący z częstotliwością bazową min. 2.8GHz i osiągające w testach SPECrate2017_int_base wynik nie gorszy niż 133 punktów, dla testu oferowanego modelu serwera z 2 procesorami. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org Płyta główna wspierająca zastosowanie procesorów od 4 do 40 rdzeni, mocy do min. 270W i taktowaniu CPU do min. 3.6GHz.
Liczba procesorów	Min. 1 procesor
Pamięć operacyjna	Min. 64GB RDIMM DDR4 3200 MT/s w modułach pamięci o pojemności 16 GB każdy Płyta główna z minimum 32 slotami na pamięć i umożliwiająca instalację do minimum 8TB. Zapewnia obsługę pamięci typu Intel Optane Persistent Memory, lub równoważny chipset jeśli potwierdza możliwość instalowania pamięci Intel Optane DC Persistent Memory.
Sloty rozszerzeń	Min. 3 aktywnych gniazd PCI-Express generacji 4, gniazda pełnej wysokości (full height) gotowe do obsadzenia kartami z portami zewnętrznymi, w tym min. 1 slot x16 (szybkość slotu – bus width).
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min. 16 dysków SFF typu Hot Swap, SAS/SATA/SSD/NVMe, 2,5”. Opcja rozbudowy/rekonfiguracji serwera o dodatkowe 8 dysków typu Hot Swap, SAS/SATA/SSD/NVMe, 2,5” montowane z przodu obudowy. W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 24 zatoki dyskowe SFF gotowe do instalacji dysków SAS/SATA/SSD/NVMe 2,5”typu Hot Swap i odpowiednią ilość kontrolerów do obsługi tych zatok. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. Zainstalowane min. 2 dyski 480GB SATA 6G SSD SFF oraz 14 dysków NL-SAS 2TB SAS 12G SFF 7200.
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 4GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, min.16 portowy (16 dedykowanych linii SAS do podłączenia dysków SAS), obsługujący poziomy: RAID

	0, 1, 5, 6, 10, 50, 60. Kontroler wraz z niezbędnymi elementami zapewniający obsługę min. 16 napędów dyskowych SSD/SATA/SAS/NVMe Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie.
Interfejsy sieciowe	Minimum 4 porty 1G Base-T (karta nie powinna zajmować slotów PCI-e i musi być zainstalowana w dedykowanym złączu dla karty sieciowej) Minimum 2 porty 10Gb SFP+ SR wraz z modułami optycznymi SFP+ SR 2 kable światłowodowe OM3 LC-LC 3m 1 kabel do połączenia karty zarządzającej 3m
Karta graficzna	Zintegrowana karta graficzna
Porty	5 x USB 3.0 (w tym 2 porty wewnętrzne) 1x VGA Wewnętrzny slot na kartę micro SD. Możliwość rozbudowy/rekonfiguracji o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express - cyfrowy port video (Display Port lub HDMI), bez użycia przejściówek z portu VGA lub USB
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Diagnostyka	Możliwość zainstalowania elektronicznego panelu diagnostycznego dostępnego z przodu serwera pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, zasilaczy, temperaturze.
Bezpieczeństwo	Serwer wyposażony w moduł TPM 2.0 i czujnik otwarcia obudowy
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • praca w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy - z poziomu przeglądarki webowej (GUI) - z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) - z poziomu skryptu (XML/Perl) - poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie

	• wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remote syslog) • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: - tworzenie i konfiguracja grup serwerów - sterowanie zasilaniem (wł/wył) - ograniczenie poboru mocy dla grupy (power capping) - aktualizacja oprogramowania (firmware) - wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparcie dla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Serwer jest dostarczany bez Systemu operacyjnego Zapewnia wsparcie dla: Microsoft Windows Server 2016, 2019, 2022 Ubuntu 20.04 LTS Red Hat Enterprise Linux (RHEL) 7.9 oraz 8.2 SUSE Linux Enterprise Server (SLES) 12 SP5 oraz 15 SP2 VMware ESXi 6.7 U3, 7.0 U2/U3
Wsparcie techniczne	Minimum 3-letnia gwarancja producenta 9x5 w miejscu instalacji typu On-Site z 2-godzinnym czasem reakcji i przybyciem na miejsce najpóźniej na następny dzień roboczy. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń. Uszkodzone dyski pozostają u Zamawiającego.
Inne	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.

	Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Wdrożenie	a) Instalacja serwera w szafie we wskazanym miejscu i konfiguracja pod system backup. b) Okablowanie LAN i konfiguracja w taki sposób aby awaria pojedynczego interfejsu nie powodował przerwy w dostępie do systemu operacyjnego. c) Instalacja systemu Linux i konfiguracja systemu oraz zasobów dyskowych. Konfiguracja dysków SSD pod system w RAID1 i dysków NL-SAS pod repozytorium backup RAID6. d) Konfiguracja serwera jako repozytorium w systemie Veeam Backup&Replication jako Hardened Repository z funkcją Immutability. Konfiguracja i zabezpieczenie serwera i systemu według zaleceń producenta systemu Veeam.

7. Przełącznik sieciowy POE – 1 szt.

Wymagania minimalne
1. Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy ze wsparciem dla protokołu 802.3at (PoE+)
2. Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy
3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 130 Mp/s
5. Bufor pakietów: minimum 7.5 MB
6. Minimum 8GB pamięci operacyjnej
7. Minimum 15GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9. Dedykowany port konsoli USB
10. Port USB 2.0 (niezależny od portu konsoli USB)
11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)
12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Dostępne metody łączenia przełączników muszą umożliwiać realizację stosów na odległość co najmniej 300m.
13. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie
14. Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W. Pobór mocy (bez PoE) nie może być większy niż 80W.
15. Wielkość tablicy routingu: minimum 2000 wpisów IPv4, 1000 wpisów IPv6
16. Wielkość tablicy ARP co najmniej 8000 wpisów, wielkość tablicy ND co najmniej 8000 wpisów
17. Tablica adresów MAC o wielkości minimum 16000 pozycji

18. Obsługa Jumbo Frames 19. Obsługa sFlow lub Netflow
20. Obsługa skryptów w języku Python
21. Obsługa REST API
22. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.
23. Obsługa RMON (minimum grupy 1,2,3 i 9)
24. Obsługa 4094 tagów IEEE 802.1Q oraz 2000 jednoczesnych sieci VLAN
25. Obsługa standardu 802.1v
26. Obsługa protokołu MVRP
27. Wsparcie dla VXLAN
28. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
29. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
30. Obsługa Secure FTP lub SCP
31. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
32. Obsługa SNTPv4 lub NTP
33. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
34. Obsługa protokołów rutingu: ruting statyczny, OSPF, OSPFv3
35. Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 1000 grup), MLD (co najmniej 1000 grup)
36. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
37. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
38. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
39. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
40. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
41. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera
42. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
43. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
44. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
45. Wbudowany serwer DHCP
46. Obsługa blokowania nieautoryzowanych serwerów DHCP
47. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
48. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
49. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Co najmniej 5000 wpisów typu ingress i 2000 wpisów typu egress dla IPv4 i MAC
50. Wbudowana sonda IP SLA
51. Zakres pracy od 0 do 45°C
52. Przełącznik w obudowie 19”. Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 35 cm.

53. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
54. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji
55. Minimum 3- letnia gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu.
56. Dodatkowe wyposażenie: • 4 szt - Wkładki SFP+ LR 10km • 4 szt - Wkładki DWDM SFP+ LR 10km • 8 szt - Wkładki SFP+ SR • 8 szt - Patchcord LC-SC single-mode 1m • 8 szt - Patchcord LC-LC multi-mode 3m • 4 szt - Patchcord RJ45 1m • 4 szt - Patchcord RJ45 2m • 7 szt – Kabel DAC 10G SFP+ to SFP+ 1m • 1 szt – Kabel DAC 10G SFP+ to SFP+ 3m
Wdrożenie: 1. Konfiguracja przełącznika wyniesionego 2. aktualizacja oprogramowania (jeśli wymagana) 3. konfiguracja L2 – LACP, VLANy 4. konfiguracja L3 – IP 5. konfiguracja mechanizmów bezpieczeństwa – loop-protect, STP, dhcp-snooping, arp-protect 6. konfiguracja połączenia z istniejącą infrastrukturą

8. System ochrony poczty – 1 szt.

Element konfiguracji	Wymagania minimalne
Wymagania ogólne	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

	Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: 1. Tryb Gateway. 2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
Parametry fizyczne systemu antyspamowego	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB
Ogólne funkcje systemu ochrony poczty	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: 1. Wsparcie dla co najmniej 20 domen pocztowych. 2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę. 3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all). 4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP. 5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości). 6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie. 7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej. 8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów. 9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP. 10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika. 11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. 12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. 13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. 14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. 15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu. 16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. 17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika

Kontrola antywirusowa i ochrona przed malware	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Skanowanie antywirusowe wiadomości SMTP. 2. Kwarantannę dla zainfekowanych plików. 3. Skanowanie załączników skompresowanych. 4. Definiowanie komunikatów powiadomień w języku polskim. 5. Blokowanie załączników w oparciu o typ pliku. 6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej. 7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. 8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. 9. Ochronę typu wirus outbrake
Kontrola antyspamowa	System musi zapewniać poniższe funkcje i metody filtrowania spamu: 1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta. 2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania. 3. Szczegółowa kontrola nagłówka wiadomości. 4. Analiza Heurystyczna. 5. Współpraca z zewnętrznymi serwerami RBL, SURBL. 6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen. 7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników. 8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF. 9. Kontrola w oparciu o Greylisting oraz SPF. 10. Filtrowanie treści wiadomości i załączników. 11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości. 12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej. 13. Ochrona typu outbrake. 14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking). 15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora
Ochrona przed atakami na usługę poczty	System musi zapewniać poniższe funkcje i metody filtrowania: 1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).

	2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu. 3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu. **4.** Kontrola Reverse DNS (ochrona przed Anty-Spoofing). **5.** Weryfikacja poprawności adresu e-mail nadawcy.
Funkcje logowania i raportowania	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Logowanie do zewnętrznego serwera SYSLOG. 2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku. 3. Logowanie informacji na temat spamu oraz niedozwolonych załączników. 4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych. 5. Możliwość analizy przebiegu sesji SMTP. 6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. 7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu. 8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.
Funkcje pracy w trybie wysokiej dostępności (HA)	System ochrony poczty musi umożliwiać poniższe funkcje: 1. Konfigurację HA w każdym z trybów: gateway, transparent. 2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP. 3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu. 4. Monitorowanie stanu pracy klastra.
Aktualizacje sygnatur, dostęp do bazy spamu	W tym zakresie dostarczony system ochrony poczty musi zapewniać: 1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. 2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
Zarządzanie	System ochrony poczty musi zapewniać poniższe funkcje: 1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH. 2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy. 3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
Certyfikaty	Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified
Serwisy i licencje	System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania

	funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres 12 miesięcy
Gwarancja oraz wsparcie	System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7
Dokumenty	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
Wdrożenie	- Pobranie software i instalacja obrazu na maszynie wirtualnej w środowisku VMWare - Wstępna konfiguracja systemu: a) konfiguracja interfejsów oraz adresacji b) konfiguracja routingu c) konfiguracja czasu d) konfiguracja ustawień głównych takich jak nazwa hosta domena główna e) konfiguracja domeny oraz subdomen f) Wstępna konfiguracja profili Anty Spam g) Wstępna konfiguracji profili Anty Virus h) Wstępna konfiguracja profili Content z blokowaniem plików typu exe i) Konfiguracja profili Resources j) Konfiguracja i podłączenie z AD po LDAP k) Konfiguracja polityk typu Access Control z kontrolą użytkowników po LDAP l) Konfiguracja polityk IP m) Konfiguracja polityki Recipient n) Konfiguracja ograniczenia wielkości plików oraz wielkości wiadomości oraz czarnych i białych list - Przepięcie ruchu mailowego na nowy system - Dalsze granularne ustawienia i konfiguracje:

	a) dokonfigurowanie limitu sesji b) dokonfigurowanie profilu Anty Spam c) dokonfigurowanie profilu Contentu - Poprawki / awarie - Dokumentacja/Szkolenie

Część nr 2 zamówienia

1. **Jednostki centralne – 4 szt.**

Nazwa komponentu	Wymagane parametry techniczne komputerów
Typ	Komputer stacjonarny. Fabrycznie nowy. Nieużywany
Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
Procesor	Procesor osiągający w teście PassMark CPU Mark, w kategorii Average CPU Mark wynik co najmniej 8,550 pkt. według wyników opublikowanych na stronie http://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	8GB DDR4
Pamięć masowa	Dysk m.in 500GB M.2
Karta graficzna	Zintegrowana karta graficzna.
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, wewnętrzny głośnik w obudowie komputera. Na przednim panelu: port słuchawek i mikrofonu
Obudowa	• Middle Tower, umożliwiająca montaż wewnątrz obudowy wewnętrznych dysków/napędów min. 3 x 2,5" 2 x 3,5" • Wymiary: nie większe niż: wysokość :415 mm; Szerokość: 191 mm; Głębokość:368 mm **Dodatkowe informacje:** • System aranżowania kabli, otwór wspomagający montaż chłodzenia na procesor, • Filtry antykurzowe, • Możliwość montażu chłodzenia wodnego, • Kensington Lock **Zasilacz zewnętrzy** o mocy min. 500W
Płyta główna	**Wewnętrzne złącza:** • SATA III (6 Gb/s) • PCIe 3.0 x16 • PCIe 3.0 x1 • Front Panel Audio • Złącze wentylatora **Zewnętrzne złącza** • VGA (D-Sub) • HDMI • RJ45 (LAN) • USB 3.2 Gen. • USB 2.0

System operacyjny	Zainstalowany system operacyjny Windows 10 Pro 64-bit w wersji polskiej. Licencja powinna być potwierdzona etykietą potwierdzającą legalność systemu
Zasilacz	500 W standard ATX
Wentylator	zintegrowany
Warunki gwarancji	Minimum 24 miesiące

2. **Monitory – 4 szt.**

Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą IPS 23,8” - fabrycznie nowy , nieużywany
Rozmiar plamki (maksymalnie)	0,274 x 0,274 mm
Jasność (typowa)	250 cd/m2
Kontrast (typowy)	1000:1
Kąty widzenia (pion/poziom)	178/178 stopni (typowo)
Czas reakcji matrycy (maksymalnie)	• 1 ms (gray to gray) w trybie Szybkim • 5 ms (gray to gray) w trybie Normalnym
Rozdzielczość maksymalna	1920 x 1080 przy 75 Hz
Format obrazu	16:9
Liczba wyświetlanych kolorów	16,7 mln
Powłoka powierzchni ekranu	Antyodblaskowa
Zużycie energii	Maksymalne 18W, czuwanie maksymalnie 0.3W
Bezpieczeństwo	Monitor musi być wyposażony dedykowany slot na linkę zabezpieczającą
Waga	Maksymalnie 3,3 kg
Złącze	• VGA (D-sub) - 1 szt. • HDMI - 1 szt. • DisplayPort 1.4 - 1 szt. • Wyjście słuchawkowe - 1 szt.

	• DC-in (wejście zasilania) - 1 szt.
Inne	• Zasilacz • Kabel HDMI
Warunki gwarancji	Minimum 24 miesiące