OPIS PRZEDMIOTU ZAMÓWIENIA

wraz ze wskazaniem wymagań technicznych , użytkowych i jakościowych

odnoszących się do głównych elementów składających się na przedmiot zamówienia

NAZWA ZAMÓWIENIA:

DOSTAWA I WDROŻENIE INFRASTRUKTURY SERWEROWEJ, SIECIOWEJ

I SYSTEMÓW BEZPIECZEŃSTWA IT

W WARSZAWSKIM ROLNO-SPOŻYWCZYM RYNKU HURTOWYM S.A.

ZAMAWIAJĄCY :

Warszawski Rolno-Spożywczy Rynek Hurtowy S.A. z siedzibą w Broniszach
ul. Poznańska 98
05-850 Ożarów Mazowiecki

Spis treści

1. Warunki wstępne 3
2. Specyfikacja sprzętu i oprogramowania 5
2.1 Serwer produkcyjny 6
2.2 Serwer do wykonywania kopii zapasowych 10
2.3 Oprogramowanie do wykonywania kopii zapasowych 15
2.4 UTM 21
2.5 Przełącznik Core 24
2.6 Przełącznik dostępowy 25
2.7 Macierz dyskowa – typ I 27
2.8 Macierz dyskowa – typ II 30
2.9 UPS 34
2.10 Szafa serwerowa 35
2.11 Konsola KVM 35
3. Wymagania wdrożenia sprzętu i oprogramowania 36
3.1 Serwer produkcyjny 36
3.2 Serwer do wykonywania kopii zapasowych 37
3.3 Oprogramowanie do wykonywania kopii zapasowych 38
3.4 UTM 38
3.5 Przełącznik Core 38
3.6 Przełącznik dostępowy 39
3.7 Macierz dyskowa – typ I 39
3.8 Macierz dyskowa – typ II 39
3.9 UPS 40
3.10 ZABBIX 40
3.11 Greylog 40
4. Dokumentacja wdrożenia 41
5. Szkolenia 41
6. Zobowiązanie Zamawiającego 41

1. Warunki wstępne

1. Wykonawca jest zobowiązany dostarczyć przedmiot zamówienia bezpośrednio do siedziby Zamawiającego: Warszawski Rolno-Spożywczy Rynek Hurtowy S.A. z siedzibą w Broniszach, ul. Poznańska 98, 05-850 Ożarów Mazowiecki.
2. Wykonawca zobowiązany będzie zrealizować dostawy objęte przedmiotem zamówienia z należytą starannością, zgodnie z obowiązującymi przepisami prawa, standardami oraz postanowieniami umowy, z uwzględnieniem wymogów bhp.
3. Wykonawca zabezpieczy we własnym zakresie i na własny koszt, wszystkie materiały niezbędne do prawidłowej realizacji przedmiotu zamówienia.
4. Wszystkie urządzenia, na dzień składania oferty przez Wykonawcę, nie mogą być przeznaczone przez producenta tego sprzętu do wycofania z produkcji lub sprzedaży w okresie minimum 6 miesięcy od dnia składania ofert.
5. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001 lub równoważną tj. równoważne inne zaświadczenie niezależnego podmiotu zajmującego się poświadczaniem zgodności działań producentów z normami jakościowymi.
6. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
7. Urządzenia muszą być dostarczone do lokalizacji wskazanych w niniejszym OPZ w oryginalnych opakowaniach fabrycznych, bez śladów ich otwierania.
8. Oferowane urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, a gwarancja musi pochodzić od producenta i być świadczona przez producenta na terenie Polski lub partnera z autoryzacją serwisową.
9. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: kabli zasilających, kabli Ethernet, kabli DAC, kabli AOC, kabli optycznych oraz innych akcesoriów, niezbędnych do przeprowadzenia prawidłowej instalacji urządzeń.
10. Wkładki, kable DAC, kable SOC, kable Splitter, patchcordy muszą być na liście kompatybilności oferowanych urządzeń (jeśli dotyczy i są elementem dostawy).
11. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz, jedno lub trzy fazowo i być wyposażone w przewody zasilające.
12. Wszystkie oferowane urządzenia muszą działać pod kontrolą oprogramowania, które jest publiczną wersją, udostępnianą na rynku przez producenta oferowanych urządzeń. Zamawiający nie dopuszcza stosowania oprogramowania dedykowanego, stworzonego na potrzeby niniejszego zamówienia, dla zaoferowanych urządzeń.
13. Wszystkie oferowane urządzenia muszą być publicznie dostępne. Zamawiający nie dopuszcza stosowania urządzeń dedykowanych, stworzonych na potrzeby niniejszego zamówienia.
14. Infrastruktura sprzętowa stanowiąca przedmiot Zamówienia musi być fabrycznie nowa (tj. nieregenerowana, nienaprawiana, niefabrykowana, nieużywana we wcześniejszych wdrożeniach), kompletna (w szczególności ze wszystkimi podzespołami, częściami, materiałami niezbędnymi do uruchomienia i użytkowania).

15. Wszędzie, gdzie w opisie przedmiotu zamówienia Zamawiający wskazuje znaki towarowe, patenty lub pochodzenie, źródła lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę – Zamawiający, dopuszcza oferowanie rozwiązań równoważnych. Wykonawca, który powoła się na rozwiązania równoważne do opisanych przez Zamawiającego, jest zobowiązany wskazać w ofercie rozwiązania przyjęte do wyceny i zastosowania przy realizacji zamówienia oraz wykazać przy użyciu dowolnych przedmiotowych środków dowodowych (złożonych wraz z ofertą), że zaproponowane przez niego rozwiązania równoważne spełniają wymagania określone przez Zamawiającego. Niewykazanie równoważności skutkować będzie odrzuceniem oferty, jako niezgodnej z warunkami zamówienia. W przypadku niewskazania przez Wykonawcę w ofercie rozwiązania równoważnego Zamawiający uzna, iż Wykonawca będzie realizował przedmiot zamówienia zgodnie z rozwiązaniami wskazanymi w SWZ i jej załącznikach. W sytuacji gdy w opisie przedmiotu zamówienia zawarto odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a odniesieniu takiemu w domyśle towarzyszą wyrazy „lub równoważne".

    Ponadto, w przypadku gdy opis przedmiotu zamówienia odnosi się do:

    – norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, Zamawiający nie może odrzucić oferty tylko dlatego, że oferowane roboty budowlane, dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem, że Wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia;
    – wymagań dotyczących wydajności lub funkcjonalności, Zamawiający nie może odrzucić oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez Zamawiającego, pod warunkiem że Wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, że obiekt budowlany, dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez Zamawiającego.

16. Zakres instalacji i konfiguracji przeprowadzonej przez Wykonawcę musi obejmować co najmniej:
    a. rozpakowanie i rozmieszczenie sprzętu we wskazanej przez Zamawiającego lokalizacji, sprawdzenie czy nie wystąpiły uszkodzenia;

b. montaż sprzętu we wskazanych miejscach, podpięcie wszystkich kabli połączeniowych;
c. sprawdzenie stanu zabezpieczeń zasilaczy i podłączenie sprzętu do sieci energetycznej;
d. uruchomienie sprzętu;
e. instalację i konfigurację oprogramowania niezbędnego do pracy danego urządzenia;
f. włączenie sprzętu do istniejącej infrastruktury sprzętowej, w tym podłączenie do sieci. Po przeprowadzeniu prac instalacyjnych i konfiguracyjnych sprzęt musi działać jako integralna część infrastruktury sprzętowej Zamawiającego;
g. wykonanie testów połączeń i wydajności urządzeń. Pozytywny wynik testów będzie podstawą podpisania protokołu odbioru;
h. zebranie opakowań i dokumentacji i przekazanie ich Zamawiającemu;

17. W przypadku wymagań producenta sprzętu odnośnie do posiadania uprawnień lub certyfikatów przez osoby dokonujące instalacji i konfiguracji (np. w celu zachowania gwarancji producenta), Wykonawca jest zobowiązany przedstawić potwierdzenia posiadania ich przez osoby wyznaczone do tego zadania.
18. W przypadku konieczności wykorzystania dodatkowych licencji lub oprogramowania Wykonawca zobowiązany jest do zapewnienia ich na czas trwania Umowy.

2. Specyfikacja sprzętu i oprogramowania

W ramach realizacji przedmiotowego zamówienia, Wykonawca zobowiązany jest dostarczyć i wdrożyć:

1. Serwer produkcyjny - 3szt.
2. Serwer do wykonywania kopii zapasowych – 1szt.
3. Oprogramowanie do wykonywania kopii zapasowych – 1 szt.
4. UTM – 1 szt.
5. Przełącznik Core – 2szt.
6. Przełącznik dostępowy – 4 szt.
7. Macierz dyskowa – typ I – 1 szt.
8. Macierz dyskowa – typ II – 1 szt.
9. UPS – 1 szt.

2.1 Serwer produkcyjny

Komponent	Minimalne wymagania dla sprzętu
Obudowa	Obudowa Rack 19” o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM.
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej: 1. SPECrate2017_int_base wynik min. 169pkt 2. SPECrate2017_fp_base wynik min. 246pkt Maksymalny TDP dla procesora 125W Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty. Do oferty należy załączyć wyniki testów - dołączyć do oferty jako przedmiotowy środek dowodowy.
RAM	Minimum 256GB
Gniazda PCI	Minimum 5 slotów PCIe x16 generacji 4
Interfejsy sieciowe/	2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT 2 interfejsy sieciowe 10/28Gb SFP28 obsadzone wkładkami 10Gb MM SR LC
Kontroler SAS HBA	Zainstalowana 4 portowa karta SAS HBA umożliwiająca podłączenie oferowanej macierzy jak i bibliotek taśmowej
Dyski twarde	Zainstalowane 2 dyski M.2 NVMe SSDs o pojemności min. 480GB z możliwością konfiguracji RAID 1. Dopuszcza się zastosowanie dysków SATA SSD.
Wbudowane porty	3 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1900x1200
Zasilacze	Redundantne, Hot-Plug, Klasy Titanium
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Moduł TPM 2.0 Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
Diagnostyka	Serwer musi być wyposażony w panel LCD lub panel z diodami LED umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, zasilaniu oraz temperaturze. Panel LCD lub panel z diodami LED to w rozumieniu Zamawiającego jeden dedykowany wyświetlacz (wskaźnik) na który widoczne są do odczytania przytoczone parametry.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;

	• wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • integracja z Active Directory; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość zarządzania min. 3 serwerami bezpośrednio z konsoli karty zarządzającej pojedynczego serwera (funkcjonalność może zostać osiągnięta poprzez dodatkowe oprogramowanie producenta serwera, jeżeli wymaga dodatkowych licencji należy je dostarczyć z serwerem
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 - dołączyć do oferty jako przedmiotowy środek dowodowy. Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy.
System operacyjny	Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w postaci 8 wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji w klastrze HA. Wykonawca dostarczy zgodne z system operacyjnym licencje dla użytkowników końcowych w ilość 65 sztuk (na całe rozwiązanie). Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta. SSO musi posiadać następujące, wbudowane cechy: a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,

	III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów

	operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, Zamawiający wymaga dostarczenia nośnika downgreade jedną wersje wcześniejszej oferowanego Systemu operacyjnego wraz z kluczem aktywacyjnym jeśli jest wymagany do poprawnej pracy systemu.
Warunki gwarancji	1. Okres gwarancji zgodny z ofertą wykonawcy lecz nie krótszy niż 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.

	6. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. 9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 10. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 11. Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny dokument np. certyfikat lub deklaracją producenta, potwierdzającą autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku gdy dany producent nie posiada takiego ogólnodostępnego dokumentu, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe.

2.2 Serwer do wykonywania kopii zapasowych

Komponent	Minimalne wymagania dla sprzętu
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji 8 dysków 2,5”, Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	Zainstalowany jeden procesor minimum 8-rdzeniowy, min. 2.8GHz częstotliwości nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocesorowej: 1. SPECrate2017_int_base wynik min. 89pkt 2. SPECrate2017_fp_base wynik min. 105pkt Wynik testu musi być opublikowany na stronie www.spec.org w dniu złożenia oferty. Należy załączyć do oferty wydruk ze strony www.spec.org potwierdzające powyższe wymagania.
Pamięć RAM	Min. 64GB
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wbudowane porty	min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy, 1 port VGA na tylnym panelu
Interfejsy sieciowe	2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ obsadzone wkładkami 10GB SFP+ MM SR
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający: 1. Min. 8GB nieulotnej pamięci cache 2. Możliwość konfiguracji poziomów RAID: 1, 5, 6, 10, 50, 60. 3. Wsparcie dla dysków samoszyfrujących
Kontroler HBA	Zainstalowana karta SAS HBA 4 portowa umożliwiająca podłacznie biblioteki taśmowej LTO i oferowanej macierzy

Dyski twarde	Zainstalowane: 1. 2 dyski min. 480TB SSD SATA, typu ReadIntensive DWPD>=1, Hot-Plug skonfigurowane RAID 1 2. 6 dysków min. 2,4TB SAS 12Gb 10k RPM Hot-Plug skonfigurowane w RAID 6 Możliwość doinstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Zasilacze	Redundantne, hot-plug, klasy Titanium
Bezpieczeństwo	1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. 2. Moduł TPM 2.0 3. Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust)
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: 1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; 4. możliwość podmontowania zdalnych wirtualnych napędów; 5. wirtualną konsolę z dostępem do myszy, klawiatury; 6. wsparcie dla IPv6; 7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; 10. integracja z Active Directory; 11. możliwość obsługi przez dwóch administratorów jednocześnie; 12. wsparcie dla dynamic DNS; 13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 14. możliwość zarządzania min. 3 serwerami bezpośrednio z konsoli karty zarządzającej pojedynczego serwera (funkcjonalność może zostać osiągnięta poprzez dodatkowe oprogramowanie producenta serwera, jeżeli wymaga dodatkowych licencji należy je dostarczyć z serwerem
Certyfikaty	1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 - dołączyć do oferty jako przedmiotowy środek dowodowy. 2. Serwer musi posiadać deklarację CE - dołączyć do oferty jako przedmiotowy środek dowodowy.
System operacyjny	1. Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 2. Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta. 3. SSO musi posiadać następujące, wbudowane cechy:

	a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: o pozwalają na zmianę rozmiaru w czasie pracy systemu, o umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, o umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, o umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2 l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,

	u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: o podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, o usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, 3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, o zdalna dystrybucja oprogramowania na stacje robocze, o praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, o centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, o szyfrowanie plików i folderów, o szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), o możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, o serwis udostępniania stron WWW, o wsparcie dla protokołu IP w wersji 6 (IPv6), o wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,

	6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. Zamawiający wymaga dostarczenia nośnika downgrade jedną wersje wcześniejszej oferowanego Systemu operacyjnego wraz z kluczem aktywacyjnym jeśli jest wymagany do poprawnej pracy systemu.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	1. Okres gwarancji zgodny z ofertą wykonawcy lecz nie krótszy niż 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta. 6. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

	7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. 9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 10. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 11. Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny dokument np. certyfikat lub deklaracją producenta, potwierdzającą autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku gdy dany producent nie posiada takiego ogólnodostępnego dokumentu, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe.

2.3 Oprogramowanie do wykonywania kopii zapasowych

Komponent	Minimalne wymagania dla oprogramowania backupowego
Wymagania ogólne	Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Funkcjonalności	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 mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji. 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 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 tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

	Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (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 posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora). Oprogramowanie musi posiadać integracje z systemami zarządania kluczami szyfrującymi (KMS). Oprogramowanie musi posiadać integracje z systemami typu SIEM. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
Wymagania RPO	Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. 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 z dokładnością do pojedynczego datastoru. 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. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 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 asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. 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 wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).
Wymagania RTO	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, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV 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 pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. 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, Amazon EC2 oraz Google Cloud Platform. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień 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 natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

	Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. 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 wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.
Ograniczenie ryzyka	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna). Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz 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 umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania. Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Środowiska fizyczne	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.

	Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE. Rozwiązanie musi wspierać system operacyjny macOS. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą). Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów. Rozwiązanie musi wspierać backup podłączonych dysków USB. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury). Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone. Rozwiązanie musi wspierać kontrolę pasma sieciowego. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft. Rozwiązanie musi wspierać technologię BitLocker. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. Rozwiązanie musi wspierać szyfrowanie. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.
Monitoring	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.

	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard). System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
Raportowanie	System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.

	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych. System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots). System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.
Wsparcie techniczne i aktualizacyjne	Powyższe funkcjonalność mają działać w środowisku wirtualnym i/lub fizycznym. Wymagane jest dostarczenie licencji dla zabezpieczenie minimum 15 sztuk wirtualnych lub fizycznych serwerów. Wraz z oprogramowanie wymagane jest dostarczenie wsparcia producenta oprogramowania na okres co najmniej 36 miesięcy.

2.4 UTM

Komponent	Minimalne wymagania dla sprzętu
Wymagania ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych
Interfejsy, Dysk, Zasilanie	1. Urządzenie dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 22 portami Gigabit Ethernet RJ-45, • 8 gniazdami SFP 1 Gbps • 2 gniazdami SFP+ 10 Gbps

	2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB. 5. System jest wyposażony w zasilanie 2xAC
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 1,5 mln. jednoczesnych połączeń oraz 56 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11.3 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps
Funkcje Systemu Bezpieczeństwa	1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

	4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

	3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Gwarancja	System jest objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Serwisy i licencje,	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy.

2.5 Przełącznik Core

Komponent	Minimalne wymagania dla sprzętu
Obudowa, zasilanie	Wymiary urządzeń powinny pozwalać na montaż w szafie rack 19", łączna wysokość wszystkich urządzeń nie powinna być wyższa niż 2U, redundantne zasilanie 230V
Interfejsy sieciowe	System urządzeń musi składać się z dwóch tożsamych rozwiązań technicznych (każde wysokości 1U), z których każde urządzenie posiada co najmniej: 24 porty 10G/1G SFP+/SFP 2 porty 100G/40G QSFP28/QSFP+
Zarządzanie	• dedykowany interfejs do zarządzania GE – RJ-45 • port konsoli szeregowej • Zarządzanie przez konsolę szeregową (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę • Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami NGFW (Next Generation Firewall) • Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem. • Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników

	• Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).
Wydajność	• przepustowość urządzenia - min. 880 Gbps, min. 1300 Mpps • możliwość zapamiętania co najmniej 64.000 adresów MAC • Opóźnienie - poniżej 1 mikrosekund • Bufor pakietów: min. 8 MB • Pamięć DRAM: min. 8 GB

Funkcjonalność	• możliwość automatycznej negocjacji prędkości i duplexu dla połączeń
	• obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree), ilość instancji min 15
	• możliwość agregacji portów zgodna z 802.3ad, ilość grup min. 48, ilość portów w grupie: min. 48
	• obsługa co najmniej 4000 VLANów, zgodna z 802.1Q
	• możliwość wykonywania routingu statycznego
	• możliwość wykonywania routingu dynamicznego (OSPFv2, RIPv2) – jeżeli funkcjonalność wymaga dodatkowej licencji, to nie jest ona wymagana do dostarczenia
	• wsparcie dla ECMP (Equal-cost multi-path routing) oraz BFD (Bidirectional Forwarding Detection)
	• funkcjonalność DHCP Relay, DHCP Snooping, Dynamic ARP Inspection, IGMP Snooping
	• port-mirroring
	• obsługa sFlow
	• obsługa list kontrolnych ACL, min. 2000 wpisów
	• wsparcie dla protokołu wysokiej dostępności MCLAG (multi-chassis link aggregation)
	• kontrola dostępu na poziomie portu w oparciu o standard 802.1x (port oraz MAC-based), możliwość uwierzytelniania w oparciu o bazę Radius
	• zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS
	• Wspracie dla SNTP, LLDP (w trybie odbioru)
	• wsparcie dla SNMP w wersjach 1 – 3
	• możliwość zarządzania przez interfejs graficzny i tekstowy
	• możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI
	• wsparcie dla HTTP REST API dla konfiguracji i monitoringu
	• możliwość integracji z systemem bezpieczeństwa NGFW (Next Generation Firewall) polegającej na przekierowaniu całego ruchu w obrębie tego samego VLAN-u przez urządzenie NGFW i filtracja tego ruchu z wykorzystaniem mechanizmów NGFW, np. IPS, AV.
	• możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:
	  ○ możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników
	  ○ obsługa białych i czarnych list MAC
	  ○ stateful firewall, umożliwiający kontrolę dostępu do sieci
	  ○ routing statyczny i dynamiczny, co najmniej OSPF.

Gwarancja	System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości

2.6 Przełącznik dostępowy

Komponent	Minimalne wymagania dla sprzętu

Parametry fizyczne platformy	Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V.
Interfejsy sieciowe - wymagania minimalne	Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: 48 porty GE RJ-45 i 4 porty 10 GE SFP+.
Zarządzanie	1. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 2. Wsparcie dla SNMP w wersjach 1-3 3. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 4. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 5. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 6. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 7. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 8. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 9. Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	1. Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. 2. Tablica adresów MAC o pojemności co najmniej 32k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Obsługa Jumbo Frames. 3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). 4. Agregacja portów zgodna ze standardem 802.3ad. 5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. 6. Port-mirroring. 7. Uwierzytelnianie 802.1x na poziomie portu. 8. Uwierzytelnianie 802.1x w oparciu o adres MAC. 9. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). 10. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. 11. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC	1. Przełącznik musi wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: a. centralne zarządzanie konfiguracją urządzenia b. aktualizacja oprogramowania realizowana z systemu centralnego zarządzania c. centralne zarządzanie sieciami vlan. d. blokowanie ruchu pomiędzy klientami w ramach jednego vlan'u e. rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.

	f. przenoszenie zidentyfikowanych urządzeń do właściwych stref. w przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. g. integrację z systemem kontroli dostępu. urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. h. automatyczna detekcja i rekomendacje konfiguracji. i. przesyłanie logów na zewnętrzny serwer syslog. j. funkcja uruchomienia captive portalu w celu identyfikacji użytkowników. k. obsługa białych i czarnych list adresów mac. l. wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	1. Przełącznik musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. 2. Przełącznik musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Okablowanie	Dla każdego przełącznika należy dostarczyć: 15 x patchcord kat. 5e RJ45 0.25m – zielony 15 x patchcord kat. 5e RJ45 0.5m – zielony 4 x patchcord światłowodowy LC-UPC/ LC-UPC – 1m 4 x patchcord kat. 5e RJ45 2m - czerwony
Gwarancja oraz wsparcie	Przełącznik musi być objęty serwisem gwarancyjnym producenta polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości, przez okres zgodny ze złożoną ofertą, lecz nie krótszy niż 36 miesięcy. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania.

2.7 Macierz dyskowa – typ I

Komponent	Minimalne wymagania dla sprzętu
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, w oferowanej konfiguracji o wysokość maksymalnie 2U.
Przestrzeń dyskowa	Zainstalowane: 13 dysków SSD 1.92TB SSD SAS Read Intensive Hot-Plug
Możliwość rozbudowy	Macierz musi obsługiwać (bez wymiany kontrolerów macierzy), co najmniej 264 dyski twarde.
Obsługa dysków	1. Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. 2. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	1. Macierz musi obsługiwać mechanizmy RAID zgodne RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). 2. Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. 3. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do

	zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). 4. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	1. Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe.
Pamięć cache	1. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. 2. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.
Rozbudowa pamięci cache	1. Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. 2. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów 12Gb SAS (4 porty na kontroler),
Zarządzanie	1. Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. 2. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	1. Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. 2. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.
Thin Provisioning	1. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. 2. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).
Tiering	1. Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. 2. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. 3. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	1. Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. 2. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. 3. Macierz musi wspierać minimum 1012 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	1. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.
Migracja danych w obrębie macierzy	1. Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy.

	2. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	1. Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. 2. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	1. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). 2. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. 3. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.
Redundancja	1. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. 2. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. 3. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
Warunki gwarancji	1. Okres gwarancji zgodny z ofertą wykonawcy lecz nie krótszy niż 36 miesiące gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta. 6. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.

	7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. 9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 10. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 11. Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny dokument np. certyfikat lub deklaracją producenta, potwierdzającą autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku gdy dany producent nie posiada takiego ogólnodostępnego dokumentu, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe.

2.8 Macierz dyskowa – typ II

Minimalne wymagania dla sprzętu
Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji.
Dostarczone urządzenie powinno umożliwiać rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla AWS oraz Microsoft Azure. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 64TB netto dla warstwy CLOUD.
1. Oferowane urządzenie musi posiadać minimum 4 porty 10GB SFP+ obsadzone wkładkami 10Gb SR MM 2. Wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle.
Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: 1. CIFS, NFS. 2. Zapewniającym deduplikację na źródle, 3. VTL (min. 10 jednocześnie).
Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, dedupliakacja na źródle, VTL do oferowanej pojemności urządzenia
Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 10 TB/h (dane podawane przez producenta) oraz co najmniej 20 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).
3. Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie: a) zapis danych minimum 150 strumieniami, b) odczyt danych minimum 50 strumieniami, c) replikacja minimum 50 strumieniami pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie. 4. Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia. 5. Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.

Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych StorageTek L180 lub IBM TS 3500
Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7.
Urządzenie musi umożliwiać (w przypadku VTL'a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów.
Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
1. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB. 2. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. 3. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.
1. Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. 2. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A", nie może zostać ponownie zapisany, jeśli trafi do innej wirtualnej biblioteki „B" w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.
1. Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. 2. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. 3. Wymaganie nie będzie spełnione, jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup'ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu'owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup'owej również muszą być deduplikowane w sposób in-line
Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)
Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane, dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu, a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych.
1. Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Veeam Backup and Replication, RMAN, Microsoft SQL Server Management Studio. 2. Urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. 3. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu.
1. W przypadku przyjmowania backupów z Veeam Backup and Replication, Oracle RMAN oraz Microsoft MSSQL (przy wykorzystaniu Microsoft SQL Server Management Studio), urządzenie musi umożliwiać

deduplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC. 2. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
Oferowane urządzenie powinno umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych.
Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów wykorzystywanych przez aplikację backupową.
Wymagane wsparcie dla backupów typu Virtual Synthetics.
W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych: 1) Windows, 2) Linux (RedHat, SuSE).
1. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: a) jeden do jednego, b) wiele do jednego, c) jeden do wielu, d) kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C). 2. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację nie jest przedmiotem postępowania.
Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Microsoft SQL Server Management Studio, muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: 1) replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących 2) replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu 3) replikacja zarządzana jest z poziomu wymaganej aplikacji 4) aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej.
1. Oferowane urządzenie musi pozwalać na realizację oraz przechowywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. 2. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów).

Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia).
Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia.
Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia jako niezależnego urządzenia dostępnego za pośrednictwem: 1) CIFS 2) NFS 3) VTL 4) deduplikacja na źródle
1. Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. 2. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): a) Możliwość zdjęcia blokady przed upływem ważności danych b) Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) lub ISO Standard 15489-1 w zakresie ochrony danych 3. Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem. 4. Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).
Urządzenie musi mieć możliwość przechowywania danych niezmienialnych: 1) video 2) grafika 3) nagrania dźwiękowe 4) pliki pdf na udziałach CIFS/NFS.
1. Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. 2. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).
Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.
Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólno dostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności)

Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta).
Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni.
Urządzenie musi mieć możliwość zarządzania poprzez: 1. Interfejs graficzny dostępny z przeglądarki internetowej. 2. Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell).
Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu deduplikacyjnym.
Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade'ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.
1. Okres gwarancji zgodny z ofertą wykonawcy lecz nie krótszy niż 36 miesiące gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. 2. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. 5. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta. 6. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. 7. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 8. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. 9. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. 10. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe. 11. Wskazana firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny dokument np. certyfikat lub deklaracją producenta, potwierdzającą autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku gdy dany producent nie posiada takiego ogólnodostępnego dokumentu, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty jako przedmiotowe środki dowodowe.

2.9 UPS

Komponent	Minimalne wymagania dla sprzętu

Minimalne wymagania techniczne dla jednostki UPS	• Moc znamionowa jednostki nie mniej 10 kVA 10000 W • Jednostka samodzielna, stojąca • Technologia Podwójnej konwersji (online) • Klasa IEC 62040-1, IEC 62040-2, IEC 62040-3 • Wysokość n.p.m. podczas pracy 0-2000metry • Hałas słyszalny w odległości 1 m od powierzchni urządzenia 54,0dBA • Klasa ochrony IP 20 • Bypass zewnętrzny serwisowy
Parametry mocy	• Nominalne napięcie wejściowe minimalne $220V_{AC}$ • Nominalne napięcie wejściowe $415V_{AC}$ • Częstotliwość wejściowa 50–60 Hz (wykrywanie automatyczne) • Liczba faz wejściowych: 3 • Liczba faz wyjściowych: 3
Akumulatory i czas podtrzymania	• Typ akumulatora bezobsługowy 9Ah, 12V (maksymalnie 192 sztuki) • Oczekiwana żywotność akumulatora (lata) 5 • Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów • Baterie wymieniane na gorąco
Komunikacja i zarządzanie	• Karta WEB/SNMP- Smart Slot x1 RJ45 • Port uniwersalny do podłączenia np. czujnika temperatury (jeden czujnik temperatury dostarczyć w komplecie z UPS) • Porty komunikacyjne: RJ45 Serial, Smart-Slot, USB • Wielofunkcyjna konsola sterownicza i informacyjna LCD • Alarm dźwiękowy Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia • Awaryjny wyłącznik zasilania (EPO) • Darmowe oprogramowanie do zamykania systemów operacyjnych
Certyfikaty, zgodności oraz gwarancja	• min. 36 miesięcy gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulatory z możliwością przedłużenia o 3 lata.

2.10 Szafa serwerowa

Komponent	Minimalne wymagania dla sprzętu
Wysokość	min. 42U, szerokość min. 800mm, głębokość 1000mm
Funkcjonalność	możliwość zestawienia szaf w zespoły możliwość ustawiania szafy na stopkach, kółkach i cokołach doprowadzenie kabli do szafy możliwe z każdej strony otwory kablowe o szerokości min. 70 mm w płycie dolnej i górnej, pozwalające na wprowadzenie kabli zasilających z wtyczkami trójfazowymi
Drzwi	przednie/tylne blaszane, jednoskrzydłowe z perforacją o prześwicie 80%, z zamkiem trzypunktowym z klamką na klucz, osłony boczne pełne z zamkami jednopunktowymi, kąt otwarcia drzwi: min. 120 stopni
Kolor	RAL 9005
Dodatkowe wyposażenie	1 x listwa zarządzalna pionowa, wtyk IEC 60309 32A/400V, gniazda 18xC13 10A/250V, 6xC19 16A/250V

2.11 Konsola KVM

Komponent	Minimalne wymagania dla sprzętu
Zastosowanie	Konsola KVM do zdalnego zarządzania za pośrednictwem protokołu TCP/IP wraz z przełącznikiem , wysokość konsoli 1U, wysokość przełącznika 1U

Ilość obsługiwanych hostów	8
Ekran	18,5” TFT-LCD, 16,7 mln kolorów, obsługa rozdzielczości do 1366 x 768 przy 60Hz dla lokalnej konsoli, do 1920x1200 przy 60Hz dla zdalnego połączenia, kąt widzenia 170° (w poziomie) i 160° (w pionie)
Konstrukcja	Do montażu w szafie rackowej, urządzenie po złożeniu nie wyższe łącznie niż 1U, ekran z klawiaturą QWERTY i touchpadem,

3. Wymagania wdrożenia sprzętu i oprogramowania

1. Wykonawca przygotuje i omówi koncepcję instalacji i konfiguracji z administratorem sieci Zamawiającego.
2. Wykonawca będzie uzgadniał z Zamawiającym harmonogramy dostawy i montażu.
3. Wdrożenie nowych urządzeń musi uwzględniać aspekt współpracy/integracji z innymi systemami i urządzeniami (typu UTMy, przełączniki, UPSy, Active Directory) będących w posiadaniu Zamawiającego. Dodatkowo każda zmiana w koncepcji musi być każdorazowo uzgadniana z Administratorem sieci.
4. Wykonawca zamontuje urządzenia będące przedmiotem dostawy w serwerowni głównej Zamawiającego uwzględniając wszelkie aspekty związanie z montażem tego typu urządzeń przewidzianych przez producenta dostarczanych rozwiązań.
5. Prace, które będą powodować przerwy w segmentach sieci w dostępności do usług dla pracowników Zamawiającego winny być wykonywane poza godzinami pracy Spółki. Możliwe jest również wykonywanie prac w dni wolne od pracy Spółki po wcześniejszym uzgodnieniu z Zamawiającym.
6. Wykonawca zapewni kompletność i poprawność działania nowego środowiska sieciowego w środowisku Zamawiającego. Wszystkie urządzenia sieciowe dostarczone muszą w pełni współpracować ze środowiskiem sieciowym obecnie użytkowanym przez Zamawiającego. Wykonawca przed przystąpieniem do testów funkcjonalnych nowego środowiska przedstawi Zamawiającemu proponowaną metodologię testów wraz z ich opisem funkcjonalnym, a następnie, po uzyskaniu pisemnej akceptacji zakresu i terminarza testów, przystąpi do wykonania testów
7. Na zakończenie prac Wykonawca przekaże Zamawiającemu dokumentację uwzględniającą co najmniej:
    a) Schemat topologii sieci
    b) Schemat ideowy szafy w serwerowni głównej uwzględniający zamontowany sprzęt
    c) Adresację wdrożonych urządzeń uwzględniającą IP / VLAN ID
    d) Schemat połączeń sieciowych
    e) Karty katalogowe urządzeń.

3.1 Serwer produkcyjny

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Instalacja urządzeń w szafie RACK w miejscu wyznaczonym przez Zamawiającego,
2. Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
3. Okablowanie sieciowe urządzeń,
4. Uruchomienie i weryfikacja poprawności działania urządzeń,
5. Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,

6. Konfiguracja adresacji IP interfejsów zarządzania,
7. Konfiguracja protokołu synchronizacji czasu NTP,
8. Konfiguracja protokołu rozwiązywania nazw DNS,
9. Podpisanie certyfikatem wygenerowanym przy pomocy Active Directory Certificate Services,
10. Konfiguracja sieci zarządzania wirtualizatora w tym IPv4, NTP, DNS,
11. Uruchomienie kreatora konfiguracji klastra w menedżerze serwerów na jednym z węzłów.
12. Dodanie pozostałych węzłów klastra do konfiguracji.
13. Konfiguracja ustawień klastra, takie jak nazwa klastra, adresy IP i konfiguracja przechowywania współdzielonego,
14. Włączenie funkcji wysokiej dostępności dla maszyn wirtualnych na klastrze.
15. Konfiguracja ustawień zapasowych dla klastra, aby zapewnić ochronę przed awariami węzłów,
16. Utworzenie nowych maszyn wirtualnych na klastrze z wykorzystaniem oprogramowania do wirtualizacji.
17. Konfiguracja ustawień maszyn wirtualnych, takich jak liczba procesorów, ilość pamięci i przypisywanie zasobów sieciowych.
18. Zarządzanie maszynami wirtualnymi, monitorowanie ich wydajności i wykonywanie niezbędnych operacji konserwacyjnych jest kluczowe w zapewnieniu prawidłowo funkcjonującego środowiska wirtualnego uruchomionego w klastrze.
19. Migracja danych i systemów na nowe serwery
20. Zaprojektowanie polityk realizowania kopii zapasowej,
21. Wdrożenie polityk kopii zapasowej,
22. Wykonanie testów akceptacyjnych dla polityk kopii zapasowej,
23. Integracja z dostarczaną macierzą dyskową
24. Zaprojektowanie przestrzeni dyskowej, na dostarczanej macierzy dyskowej typ I,
25. Konfiguracja przestrzeni dyskowej na dostarczanej macierzy dyskowej,
26. Wdrożenie snapshotów na skonfigurowanej przestrzeni dyskowej,
27. Integracja z usługami chmurowymi producenta

3.2 Serwer do wykonywania kopii zapasowych

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Instalacja urządzeń w szafie RACK w miejscu wyznaczonym przez Zamawiającego,
2. Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
3. Okablowanie sieciowe urządzeń,
4. Uruchomienie i weryfikacja poprawności działania urządzeń,
5. Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
6. Konfiguracja adresacji IP interfejsów zarządzania,
7. Konfiguracja protokołu synchronizacji czasu NTP,
8. Konfiguracja protokołu rozwiązywania nazw DNS,
9. Podpisanie certyfikatem wygenerowanym przy pomocy Active Directory Certificate Services,
10. Konfiguracja sieci zarządzania wirtualizatora w tym IPv4, NTP, DNS,
11. Migracja danych i systemów na nowe serwery

12. Zaprojektowanie polityk realizowania kopii zapasowej,
13. Wdrożenie polityk kopii zapasowej,
14. Wykonanie testów akceptacyjnych dla polityk kopii zapasowej,
15. Integracja z dostarczaną biblioteką taśmową.

3.3 Oprogramowanie do wykonywania kopii zapasowych

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Instalacja oprogramowania do realizowania backupu (na serwerze do kopii zapasowych jako maszyna wirtualna)
2. Zaprojektowanie architektury systemu backupu i wdrożenie nowych komponentów systemu kopi zapasowej,
3. Konfiguracja środowiska kopii zapasowych w zakresie min. konfiguracji zasobów dyskowych dostarczonego serwerów backupu, instalacji i konfiguracji biblioteki taśmowej, pul nośników oraz zadań kopii danych na taśmy,
4. Weryfikacja poprawności działania kopii zapasowej oraz jej odtwarzania,
5. Weryfikacja poprawności działania replikacji,
6. Przygotowanie procedury na wypadek odzyskiwania kopii zapasowej w przypadku awarii.

3.4 UTM

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego szafie rack
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych
3. Upgrade oprogramowania układowego jest wymagane.
4. Konfiguracja protokołu synchronizacji czasu NTP, DNS
5. Konfiguracja połączeń z siecią operatora
6. Uruchomienie wszystkich silników skanujących
7. Konfiguracja powiadomień i alaramów
8. Integracja z domeną Microsoft Active Directory
9. Konfiguracja security group w domenie Microsoft Active Directory
10. Konfiguracja usługi SSL-VPN, pozwalającej autoryzować użytkowników w zdefiniowanej security group Active Directory
11. Podpisanie certyfikatem wygenerowanym przy pomocy Active Directory Certificate Services
12. Migracja konfiguracja polityk bezpieczeństwa z obecnego UTM
13. Analiza wdrożonych polityk bezpieczeństwa
14. Konfiguracja deszyfracji ruchu szyfrowanego
15. Konfiguracja sieci VLAN
16. Konfiguracja ochrony DNS.

3.5 Przełącznik Core

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego szafie rack

2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych
3. Upgrade oprogramowania układowego jest wymagane.
4. Konfiguracja protokołu synchronizacji czasu NTP, DNS
5. Konfiguracja wirtualnych sieci VLAN,
6. Konfiguracja połączeń agregowanych,
7. Konfiguracja parametrów drzewa rozpinającego.

3.6 Przełącznik dostępowy

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego szafie rack
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych
3. Upgrade oprogramowania układowego jest wymagane.
4. Konfiguracja protokołu synchronizacji czasu NTP, DNS
5. Konfiguracja wirtualnych sieci VLAN,
6. Konfiguracja połączeń agregowanych,
7. Konfiguracja parametrów drzewa rozpinającego.

3.7 Macierz dyskowa – typ I

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Instalacja urządzenia w szafie RACK w miejscu wyznaczonym przez Zamawiającego
2. Okablowanie sieciowe urządzeń (sieć LAN oraz SAS) i podłączenie do serwerów produkcyjnych
3. Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
4. Uruchomienie i weryfikacja poprawności działania urządzeń
5. Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
6. Konfiguracja adresacji IP interfejsów zarządzania
7. Konfiguracja protokołu synchronizacji czasu NTP
8. Konfiguracja protokołu rozwiązywania nazw DNS
9. Weryfikacja poprawności działania połączeń LAN
10. Konfiguracja pul przestrzeni dyskowych
11. Uruchomienie storage'u dla klastra HA

3.8 Macierz dyskowa – typ II

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Instalacja urządzenia w szafie RACK w miejscu wyznaczonym przez Zamawiającego
2. Okablowanie sieciowe urządzeń (sieć LAN oraz SFP+)
3. Podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
4. Uruchomienie i weryfikacja poprawności działania urządzeń
5. Aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
6. Konfiguracja adresacji IP interfejsów zarządzania

7. Konfiguracja protokołu synchronizacji czasu NTP
8. Konfiguracja protokołu rozwiązywania nazw DNS
9. Weryfikacja poprawności działania połączeń LAN
10. Aktywacja niezbędnych licencji wg wytycznych producenta
11. Konfiguracja urządzenia z oprogramowaniem Sewera do wykonywania kopii zapasowych

3.9 UPS

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia w pomieszczeniu serwerowni
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych
3. Konfiguracja protokołu synchronizacji czasu NTP, DNS
4. Upgrade oprogramowania układowego jest wymagane.
5. Konfiguracja oprogramowania do zarządzania zasilaczem, w tym powiadomień
6. Konfiguracja poszczególnych portów zasilania z opisem urządzeń, które zasilają
7. Konfiguracja polityk zdalnego zarządzania fizycznymi serwerami, które to UPS będzie zasilać

3.10 ZABBIX

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Instalacja i konfiguracja oprogramowania jako maszyna virtualna w klastrze HA
2. Adresacja portów interfejsów
3. Inwetaryzacja środowiska Zamawiającego w systemie (hosty fizyczne, virtualne, przełączniki, router)
4. Utworzenie reguł dla poszczególnych grup agentów (hosty fizyczne, virtualne, windows, linux)
5. Instalacja agentów na wdrożonym środowisku
6. Konfiguracja dashboard'u wedle wymagań Zamawiającego.
7. Instalacja klienta na jednym komputerze na potrzeby szkolenia.

3.11 Greylog

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Instalacja i konfiguracja oprogramowania jako maszyna virtualna w klastrze HA
2. Adresacja portów interfejsów
3. Inwetaryzacja środowiska Zamawiającego w systemie (hosty fizyczne, virtualne, przełączniki, router)
4. Utworzenie reguł dla poszczególnych grup agentów (hosty fizyczne, virtualne, windows, linux)
5. Instalacja agentów na wdrożonym środowisku.
6. Konfiguracja dashboard'u wedle wymagań Zamawiającego.

4. Dokumentacja wdrożenia

1. Wykonawca zobowiązany jest do wytworzenia i dostarczenia dokumentacji powykonawczej, która będzie podlegała odbiorom. Dostarczona dokumentacja musi być dostępna w wersji papierowej i elektronicznej w języku polskim. Dopuszcza się język angielski w dokumentacji technicznej elementów, które nie są dziełem Wykonawcy, a dokumentacja producenta w języku polskim nie jest dostępna.
2. Dokumentacja powykonawcza musi zawierać co najmniej:
    a) opis instalacji i konfigurowania wszystkich dostarczonych komponentów,
    b) opis integracji z innymi systemami,
    c) numery części (part number), numery seryjne, etc. wszystkich urządzeń dostarczonych przez Wykonawcę,
    d) opis wraz ze schematami umiejscowienia oferowanego rozwiązania w topologii sieci zamawiającego w warstwie fizycznej i logicznej zawierający przynajmniej informacje o użytej adresacji,
    e) konfiguracja interface'ów sieciowych, etc.,
    f) schemat logiczny i fizyczny sieci oraz zainstalowanych urządzeń,
    g) opis licencji, numery i klucze aktywacyjne i numery licencji,
    h) okres wsparcia producenta.

5. Szkolenia

1. Wykonawca przygotuje i zaproponuje program osobnych szkoleń stanowiskowych dla dwóch osób w zakresie:
    a) szkolenie w zakresie obsługi dostarczonych serwerów, macierzy dyskowych poprzez kartę zarządzającą / kontrolery,
    b) szkolenie w zakresie zarządzania rozwiązaniem do wirtualizacji,
    c) szkolenie w zakresie oprogramowania do wykonywania kopii zapasowych i odtwarzania danych,
    d) szkolenie w zakresie obsługi bieżącej – macierzy dyskowej – typ II,
    e) szkolenie w zakresie obsługi UPS,
    f) szkolenie w zakresie obsługi UTM.
    g) szkolenie w zakresie systemu ZABBIX,
    h) szkolenie w zakresie systemu Graylog.
2. Wykonawca będzie uzgadniał z Zamawiającym harmonogramy poszczególnych szkoleń.
3. Szkolenia będą przeprowadzone w siedzibie Zamawiającego w godzinach pracy Zamawiającego, lub alternatywnie online po uprzednim uzgodnieniu stron.

6. Zobowiązanie Zamawiającego

Zamawiający w ramach realizacji przez Wykonawcę Przedmiotu Zamówienia zobowiązany jest do:

1. Udostępnienia wszelkich materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, które są niezbędne celem realizacji Przedmiotu Zamówienia.
2. Informowania Wykonawcy o wszelkich czynnościach, które mogą mieć wpływ na realizację Przedmiotu Zamówienia przez Wykonawcę.

3. Udostępnienia obiektów, sprzętu, oprogramowania i dokumentacji technicznej obiektów, które są niezbędne do realizacji Przedmiotu Zamówienia zgodnie z polityką bezpieczeństwa i regulacjami wewnętrznymi, obowiązującymi Zamawiającego.
4. Udostępnienia infrastruktury technicznej dla przeniesienia środowiska produkcyjnego.
5. Wykonawca przygotuje i omówi koncepcję instalacji i konfiguracji z administratorem sieci Zamawiającego.