Załącznik - Nr 5 - Część nr 1 **zamówienia – Zakup wraz z dostawą serwerów**
Serwer – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5” • Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	• Jeden procesor 8-rdzeniowy, min. 3.2GHz, umożliwiający osiągnięcie wyniku min. 68.1 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej. • Należy załączyć do oferty wydruk ze strony www.spec.org potwierdzające powyższe wymagania.
Pamięć RAM	• Minimum 2x16GB pamięci RAM ECC UDIMM o częstotliwości pracy min. 3200MT/s.
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, • 1 port RS232
Gniazda PCI	• Min. 3 sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT

Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający
	  ○ Min. 8GB nieulotnej pamięci cache,
	  ○ Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.
	• Wsparcie dla dysków samoszyfrujących

Dyski twarde	• Zainstalowane 2 dyski SAS o pojemności min. 2.4TB, 12Gb, Hot-Plug. • Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. • Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.

Diagnostyka	• Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Wentylatory	• Minimum 4 wentylatory
Zasilacze	• Redundantne, o mocy maks. 800W.
System operacyjny/dodatkowe oprogramowanie	• Zainstalowany Windows Server 2022 Standard lub równoważny. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 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. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. Wbudowane wsparcie instalacji i pracy na wolumenach, które: pozwalają na zmianę rozmiaru w czasie pracy systemu, umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, umożliwiają zdefiniowanie list kontroli dostępu (ACL). Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 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: Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. Zdalna dystrybucja oprogramowania na stacje robocze. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: Dystrybucję certyfikatów poprzez http Konsolidację CA dla wielu lasów domeny, Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. Szyfrowanie plików i folderów. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. Serwis udostępniania stron WWW. Wsparcie dla protokołu IP w wersji 6 (IPv6), Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 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: Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, Obsługi ramek typu jumbo frames dla maszyn wirtualnych. Obsługi 4-KB sektorów dysków Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

	Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) 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. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera oraz z możliwością rozszerzenia funkcjonalności o: o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane SSL o wsparcie dla IPv6; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o integracja z Active Directory; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera o możliwość obsługi przez sześciu użytkowników jednocześnie; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze

	○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

	• Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
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	• Gwarancji producenta: 24 miesiące • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • 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.

	• Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.
	• Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.
	• 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.
	• Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
	• Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
	• Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.
	• Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.
	• W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
	• Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
	• Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
	
	Możliwość rozszerzenia gwarancji o:
	• Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało:
	  o Monitorowanie zdarzeń w obrębie infrastruktury
	  o Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji
	• Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche)
	• Zdalne lub na miejscu wdrażanie poprawek - 2x w roku
	• Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie)

Serwer SQL – 1 **szt**.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5” • Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci

Chipset	• Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	• Jeden procesor 8-rdzeniowy, min. 3.2GHz, umożliwiający osiągnięcie wyniku min. 68.1 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej.
Pamięć RAM	• Min. 2x16GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s.
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, • 1 port RS232
Gniazda PCI	• Min. 3 sloty PCIe generacji 4
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający o Min. 8GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. • Wsparcie dla dysków samoszyfrujących
Dyski twarde	• Zainstalowane 3 dyski SAS o pojemności min. 2.4TB, 12Gb, Hot-Plug. • Zainstalowane 2 dyski SSD SATA o pojemności min. 480GB, 6Gb/s, Hot- Plug, do intensywnego odczytu. • Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. • Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Diagnostyka	• Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Wentylatory	• Minimum 4 wentylatory
Zasilacze	• Redundantne, o mocy maks. 800W.
System operacyjny/dodatkowe oprogramowanie	• Zainstalowany Windows Server 2022 Standard lub równoważny. • Microsoft SQL Server 2022 Standard, OEM – licencja oparta o USER CALs (30x USER CALs) • <u>Zamawiający dopuszcza zaoferowanie systemu równoważnego:</u> Microsoft Windows Server min. 2019 Standard lub równoważny. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Licencja zgodna z ilością fizycznych core procesorowych w serwerze Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej

	4 TB pamięci RAM w środowisku fizycznym. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 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. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. Wbudowane wsparcie instalacji i pracy na wolumenach, które: pozwalają na zmianę rozmiaru w czasie pracy systemu, umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, umożliwiają zdefiniowanie list kontroli dostępu (ACL). Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, 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: Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. Zdalna dystrybucja oprogramowania na stacje robocze.

	Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: Dystrybucję certyfikatów poprzez http, Konsolidację CA dla wielu lasów domeny, Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. Szyfrowanie plików i folderów. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. Serwis udostępniania stron WWW. Wsparcie dla protokołu IP w wersji 6 (IPv6), Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 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: Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, Obsługi ramek typu jumbo frames dla maszyn wirtualnych. Obsługi 4-KB sektorów dysków Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) 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. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji. • <u>Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego:</u> oprogramowanie równoważne musi być kompatybilne z wymienionym typem oprogramowania oraz posiadać wszystkie jego cechy funkcjonalne. oprogramowanie równoważne musi spełniać warunki opisane w punkcie - Kryteria równoważności. Oprogramowanie równoważne musi charakteryzować się cechami wskazanymi poniżej: Cechy równoważnego Oprogramowania typu Microsoft SQL Server Standard 1. Oferowane równoważne rozwiązanie musi być dostosowane do obsługi komponentów VMware vRealize Automation w wersji 7.6.0, który jest zainstalowany na platformie wirtualizacyjnej Zamawiającego. 2. System bazodanowy (SBD) licencjonowany na rdzenie procesora musi spełniać następujące wymagania poprzez wbudowane mechanizmy: 1) Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać

	serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL. 2) Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania. 3) Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem. 4) Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów. 5) Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania). 6) SBD musi umożliwiać tworzenie klastrów niezawodnościowych. 7) Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech: - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD), - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe), - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach, 8) Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych. 9) Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych. 10) Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji

	dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory. 11) Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność. 12) Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń: - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system), - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur), - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy). 13) Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci. 14) Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Wykonawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji. 15) Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi: - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,

	- udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD, - udostępniać język zapytań do struktur XML, - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML), - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań. 16) Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności: - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów, - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp., - obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD, - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja - punkt, seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.). 17) Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania. 18) Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny. 19) Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.

	20) Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych. 21) Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera. 22) System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.: - mechanizm debuggowania tworzonego rozwiązania, - mechanizm stawiania „pułapek” (breakpoints), - mechanizm logowania do pliku wykonywanych przez transformację operacji, - możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu), - możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo), - mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli), - mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach), - mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego, - mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.

	23) Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina. 24) Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail). 25) Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki). 26) Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych. 27) Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta). 28) Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli. 29) Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów,

	jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu. 30) System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać: - raporty parametryzowane, - cache raportów (generacja raportów bez dostępu do źródła danych), - cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów), - współdzielenie predefiniowanych zapytań do źródeł danych, - wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File), - możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport, - możliwość wizualizacji wskaźników KPI, - możliwość wizualizacji danych w postaci obiektów sparkline. 31) Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services). 32) Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF, PowerPoint. 33) SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów. 34) SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja). 35) Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT. 36) W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD. 37) System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie

	asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań. 38) W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit). 39) SBD musi posiadać wbudowane mechanizmy do obsług danych grafowych (struktur złożonych z węzłów i krawędzi - reprezentujących relacje między węzłami). System musi mieć wbudowane funkcje (dostępne z poziomu kodu SQL) do analizy powiązań między węzłami grafu oraz wyszukiwania najkrótszej ścieżki w grafie. 40) SBD musi posiadać mechanizmy klasyfikacji informacji przechowywanych w bazie danych w celu łatwej identyfikacji obszarów (obiektów) w bazie danych, gdzie składowane są dane wrażliwe. Mechanizm ten powinien umożliwiać przypisanie kolumnom w tabeli m.in. takich atrybutów jak: typ przechowywanych informacji oraz poziom wrażliwości danych. Dodatkowo SBD powinien udostępniać zestaw predefiniowanych raportów prezentujących m.in. listę sklasyfikowanych tabel i kolumn oraz liczbę tabel zawierających dane wrażliwe. Kryteria równoważności – ocena, zasady, wymagania, budowanie kompetencji 1. We wszystkich miejscach niniejszego dokumentu, w których użyto przykładowego znaku towarowego, patentu lub pochodzenia, jest to uzasadnione specyfiką przedmiotu zamówienia i Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń. 2. Wykonawca, który powoła się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać w ofercie, że oferowany przez niego przedmiot dostawy spełnia wymagania określone przez Zamawiającego. 3. Ciężar dowodowy w zakresie udowodnienia równoważności zaoferowanych rozwiązań z rozwiązaniami opisanymi poprzez wskazanie przykładowego znaku towarowego, patentu lub pochodzenia, spoczywa na Wykonawcy, składającym ofertę równoważną. 4. Zamawiający wymaga, aby zaoferowane przez Wykonawcę rozwiązania równoważne nie wiązały się z koniecznością wykonania dodatkowych prac integracyjnych, testowych czy migracyjnych po stronie Zamawiającego, tym samym poniesienia dodatkowych, niezaplanowanych kosztów. 5. W przypadku oferowania rozwiązania równoważnego, wykonawca zobowiązany jest wykazać,

	że oferowane przez niego rozwiązanie równoważne spełnia wymagania określone przez Zamawiającego, załączając do oferty dowody potwierdzające, że rozwiązanie równoważne spełnia wszystkie parametry równoważności. Dowody powinny zawierać informacje umożliwiające Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne poszczególnych parametrów równoważności. 6. Zaoferowane rozwiązanie równoważne musi być w pełni kompatybilne z istniejącymi rozwiązaniami w środowisku, w tym dedykowanymi ze względu na specyfikę aplikacjami, systemami, także w warstwie aplikacyjnej. 7. Zamawiający przygotuje środowisko testowe i scenariusze testowe w celach udowodnienia przez Wykonawcę spełnienia warunków równoważności. Koszty związane z przeprowadzenia jakichkolwiek prac związanych z wykonywaniem testów i przygotowaniem środowiska testowego w tym instalacji, konfiguracji i integracji dostarczonego produktu z systemami Zamawiającego, przy uwzględnieniu m.in. licencji, konsultacji specjalistów, przygotowania scenariuszy testowych, szkoleń ponosi w całości Wykonawca. 8. Wykonawca musi zapewnić oraz udowodnić że oprogramowanie charakteryzuje się cechami wymienionymi w punkcie - Cechy oprogramowania równoważnego. 9. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego. 10. Integracja dostarczonego równoważnego oprogramowania nie może wymuszać wykonania dodatkowych zmian programistycznych po stronie posiadanego przez Zamawiającego oprogramowania oraz musi umożliwiać integrację ze wszystkimi rozwiązaniami, które Zamawiający posiada w ramach istniejących środowisk. Wykonawca oddeleguje zespół posiadający ww. wymagania kompetencyjne oraz poświadczenia w celu przeprowadzenia migracji istniejących środowisk produkcyjnych. W przypadku wystąpienia jakichkolwiek trudności, które skutkować będą niepoprawną pracą bądź przerwami w ciągłości działania systemów i usług, które Zamawiający świadczy na rzecz innych podmiotów, na Wykonawcę mogą zostać przeniesione w całości wszelkie kary oraz zobowiązania, którymi Zamawiający zostanie obciążony przez te podmioty. 11. Zamawiający nie dopuszcza dostarczenia licencji dla produktów równoważnych w formie

	upgradu, licencji czasowej, OEM, z wyłączeniem, w którym Zamawiający określił taki warunek w opisie oprogramowania. 12. Licencje muszą pochodzić z autoryzowanego kanału dystrybucji. 13. Zamawiający nie dopuszcza zaoferowania oprogramowania i planów licencyjnych opartych o rozwiązania chmury oraz rozwiązań wymagających stałych opłat w okresie używania zakupionego produktu, z wyłączeniem, w którym Zamawiający określił taki warunek w opisie oprogramowania. 14. Oprogramowanie musi zostać dostarczone w najnowszej dostępnej wersji wydanej przez producenta oprogramowania z wyłączeniem sytuacji, w której Zamawiający określił taki warunek w opisie oprogramowania. 15. W przypadku zaoferowania przez Wykonawcę rozwiązań równoważnych, Wykonawca na swój koszt przeprowadzi szkolenia dla administratorów i użytkowników zespołu Zamawiającego. Dedykowane szkolenie w zależności od grupy docelowej będzie trwało min. 2 dni i będzie miało charakter warsztatowy, praktyczny. Liczba uczestników każdego ze szkoleń wynosi min. 10 osób. Szkolenie dla administratorów ma na celu pozyskanie kompetencji w zakresie administrowania dostarczonymi rozwiązaniami m.in. zarządzania użytkownikami, dostępami, zmian w konfiguracji, modyfikacji, integracji z zainstalowanymi rozwiązaniami w środowisku Zamawiającego. Szkolenie dla użytkowników ma na celu przećwiczenia funkcji oprogramowania, scenariuszy użycia. 16. Szkolenia powinny zostać przeprowadzone w terminie 14 dni od daty podpisania Umowy. 17. Wykonawca przedstawi do akceptacji plan i zakres szkoleń dla obu grup wraz z terminem. 18. Na wniosek Zamawiającego szkolenia, o których mowa w pkt 15-17 powyżej zostaną przeprowadzone w formie warsztatów w trybie online. Wykonawca zobowiązany jest zapewnić wszelkie niezbędne narzędzia do przeprowadzenia szkolenia online, w tym odpowiednią platformę. Do czasu szkolenia online nie dolicza się czasu kiedy nie mogło być prowadzone z przyczyn dotyczących Wykonawcy, oraz z powodów technicznych niedotyczących Stron, np. zakłóceń połączenia, awarii sprzętu lub oprogramowania. 19. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 5 minut.

	Migracja systemów zostanie zrealizowana w terminie maksymalnie 10 dni od daty podpisania Umowy. 20. Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania w terminie nie dłuższym niż 6 godzin od chwili wykrycia błędnego działania środowiska, a w przypadku braku takiej możliwości Wykonawca zobowiązany jest do przywrócenia stanu pierwotnego w terminie nie dłuższym niż 6 godzin od chwili wykrycia błędnego działania środowiska oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ w terminie nie dłuższym niż 24 godziny od chwili wykrycia błędnego działania środowiska.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0
Elementy montażowe	• Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego, karta zarządzająca, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera oraz z możliwością rozszerzenia funkcjonalności o: o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane SSL o wsparcie dla IPv6; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o integracja z Active Directory; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera o możliwość obsługi przez sześciu użytkowników jednocześnie; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

	○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart

	sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
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	• Gwarancji producenta: 24 miesiące • Możliwość rozszerzenia gwarancji przez producenta do 7 lat. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • 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. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. • 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. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. • Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. • W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń. • Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji o: • Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało: o Monitorowanie zdarzeń w obrębie infrastruktury o Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji • Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche) • Zdalne lub na miejscu wdrażanie poprawek - 2x w roku • Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie)

Załącznik - Nr 5 -Część nr 2 zamówienia – Zakup, dostawa oraz wdrożenie UTM

UTM – 2 szt.

Wymagania:	
Sekcja 1 — Interfejs	
1	Urządzenie musi posiadać interfejs WWW z poziomu, którego administrator może wykonać wszystkie czynności administracyjne
2	Rozwiązanie musi posiadać możliwość podpięcia rozwiązania do systemu centralnego zarządzania i zarządzania urządzeniem poprzez dedykowaną aplikacje.
3	Rozwiązanie musi posiadać możliwość zarządzania nim z poziomu chmurowego portalu centralnego zarządzania. Dostęp do portalu chmurowego musi być dostarczony w ramach podstawowej licencji.
4	Z poziomu interfejsu WWW administrator musi mieć możliwość szybkiego przeglądu stanu urządzenia widząc na pierwszej stronie minimum następujące informacje: - wersja oprogramowania układowego, - nazwa urządzenia, - adres sprzętowy urządzenia, - czas pracy urządzenia od ostatniego restartu, - status sieci internet, - status sieci wifi, - ostatnio wykryte urządzenia w sieci wraz z alertami, - aktywność sieci zawierającą wykres ilości pakietów i ilości danych przepływających w czasie rzeczywistym przez urządzenie.
5	Urządzenie musi możliwość wyświetlenie wszystkich aktywnych urządzeń pracujących w sieci, w postaci listy dostępnej bezpośrednio z interfejsu WWW.
6	Jeśli urządzenie posiada moduł sieci bezprzewodowej to musi umożliwiać wyświetlenie aktywnych urządzeń podłączonych do sieci bezprzewodowej, wraz z informacjami o jakości sygnału dla pojedynczych urządzeń.
7	Urządzenie musi umożliwiać generowanie raportów ogólnych zawierających status urządzenia minimum w odstępach: - ostatnia godzina, - ostatni dzień,
8	Urządzenie musi umożliwiać generowanie raportów z aktywności użytkowników i komputerów minimum w odstępach: - ostatnia godzina, - ostatni dzień, - ostatni tydzień, - ostatni miesiąc,
9	Urządzenie musi umożliwiać na wydruk raportów z aktywnością użytkowników bezpośrednio z poziomu interfejsu WWW rozwiązania.
10	Urządzenie musi umożliwiać przegląd i wyszukiwanie logów sieciowych bezpośrednio z interfejsu WWW.
11	Urządzenie musi umożliwiać przegląd i wyszukiwanie logów systemowych bezpośrednio z interfejsu WWW.
12	Jeśli urządzenie posiada moduł sieci bezprzewodowej to musi umożliwiać monitorowanie okolicznych sieci bezprzewodowych znajdujących się w zasięgu urządzenia, oraz pozwalać na ich przegląd bezpośrednio z interfejsu WWW.
13	Urządzenie musi mieć możliwość na wyświetlenia: - stanu zasobów sprzętowych, - tablicy routingu, - stanu połączenia z usługami chmurowymi, bezpośrednio z poziomu interfejsu WWW
14	Urządzenie musi posiadać funkcje pozwalające na wykonanie testów działania sieci dostępne bezpośrednio z interfejsu WWW. Wymagane są minom narzędzia takie jak: - ping, - traceroute, - dns lookup, - tcpdump,
15	Urządzenie musi umożliwiać wygenerowanie plików diagnostycznych z działania systemu urządzenia, bezpośrednio z interfejsu WWW.
16	Interfejs WWW musi umożliwiać zalogowanie się wielu administratorom jednocześnie.
Sekcja 2 — Funkcjonalności	
Numer	Wymaganie
1.	Urządzenie musi mieć możliwość pracy zarówno w trybie monitorowania, jak i w trybie inline.
2.	Urządzenie musi być minimalnie wyposażone w następujące moduły funkcjonalne: - Firewall, - Kontrola aplikacji i URL Filtering, - Rozpoznawanie użytkowników, - QoS, - IPS, - Anti-Virus,

	- Anti-Bot, - Emulacja zagrożeń (dodatkowo punktowane 20 pkt) - Antyspam, - VPN Site-to-Site, - VPN Client-to-Site,
3.	Urządzenie musi mieć możliwość monitorowania dostępu do internetu poprzez weryfikacje podanych przez administratora hostów. Urządzenie musi monitorować minimum następujące parametry sieciowe: - Utrata pakietów, - Średnie opóźnienie, - Minimalne opóźnienie, - Maksymalne opóźnienie, - Jitter,
4.	Urządzenie musi umożliwiać pełną rekonfigurację interfejsów wewnętrznych, wspierając m.in.: - Stworzenie wirtualnego switch z interfejsów, - Stworzenie interfejsów typu bridge, - Agregacji interfejsów m.in. za pomocą LACP.
5.	Urządzenie musi mieć możliwość filtrowania urządzeń poprzez filtrowanie adresów MAC.
6.	Urządzenie musi posiadać mechanizm DNS Proxy.
7.	Urządzenie musi posiadać możliwość ograniczenia dostępu administracyjnego tylko z konkretnych podsieci, oraz tylko z konkretnych stref.
8.	Urządzenie musi mieć możliwość synchronizacji czasu poprzez protokół NTP.
9.	Urządzenie musi mieć możliwość uruchomienia serwera NTP bezpośrednio na urządzeniu.
10.	Urządzenie musi wspierać serwisy DDNS, minimum: - DynDNS - no-ip.org
11.	Urządzenie musi posiadać funkcję pozwalającą na zarządzenie urządzeniem z sieci internet, nawet jeśli znajduje się za NATem. Funkcja ta nie może wymagać od administratora uruchomienia tunelu VPN do sieci wewnętrznej.
12.	Urządzenie musi mieć możliwość pracownia w klastrze wysokiej dostępności.
13.	Urządzenie musi posiadać predefiniowane profile pracy Firewalla, Kontroli aplikacji, URL Filteringu i modułu IPS.
14.	Urządzenie musi umożliwiać ręczne definiowanie reguł działających na: - firewallu, - module kontroli aplikacji i URL Filteringu, - module IPS,
15.	Urządzenie musi umożliwiać logowanie każdej sesji zezwolonej lub zablokowanej.
16.	Urządzenie musi posiadać dwa osobne zestawy reguł. Jeden dla połączeń wychodzących do internetu, drugi dla obsługi połączeń wewnętrznych.
17.	Urządzenie musi posiadać predefiniowaną politykę translacji adresów, pozwalającą na jej zastosowanie przy połączeniach wychodzących do internetu.
18.	Urządzenie musi wspierać filtrowanie protokołów VoIP, oraz pozwalać na konfiguracje filtrowania tych urządzeń za pomocą prostego kreatora konfiguracji.
19.	Urządzenie musi mieć możliwość integrowania się z usługami katalogowymi, minimum Microsoft Active Directory.
20.	Urządzenie musi mieć możliwość inspekcji ruchu SSL.
21.	Urządzenie musi mieć możliwość kategoryzowania stron HTTPS bez inspekcji ruchu SSL.
22.	Urządzenie musi posiadać interfejs, w którym administrator może znaleźć wszystkie zainfekowane urządzenia w sieci.
23.	Urządzenie musi mieć możliwość całkowitego wyłączenia modułu IPS i uruchomienia go tylko w trybie IDS.
24.	Urządzenie musi umożliwiać na stworzenie tuneli VPN typu client-2-site minimum w formie: - dedykowane klienta VPN dostarczanego przez producenta rozwiązania, - mobilnego klient VPN dostarczanego przez producenta rozwiązania, - portalu SSL VPN, - klienta wbudowanego w system Windows,
25.	Urządzenie musi posiadać moduł kontroli aplikacji zawierający ponad 9300 różnych aplikacji.
26.	Urządzenie musi umożliwiać inspekcje ponad 70 protokołów przemysłowych w tym minimum: - BACNet, - CIP, - DNP3, - IEC-60870-5-104, - IEC 60870-6 (ICCP), - IEC 61850, - MMS, - ModBus, - OPC DA & UA, - Profinet, - Step7 (Siemens)

27.	Urządzenie musi posiadać funkcjonalność tzw. Virtual Patchingu. Funkcja ta pozwala na zablokowanie ataków kierowanych na podatne urządzenie, które z różnych przyczyn nie mogą zostać zaktualizowane przez administratora.
28.	Lista wspieranych przez moduł kontroli aplikacji, aplikacji musi być publicznie dostępna i pozwalać na przeszukiwanie jej z wykorzystaniem różnych filtrów.
Sekcja 3 — Wydajność	
Numer	Wymaganie
1	Urządzenie musi być przystosowane do pracy w temperaturach od 0 stopni do 40 stopni Celsiusa.
2	Urządzenie musi posiadać następujące certyfikacje: CB 62368-1, CE, FCC IC Class B, VCCI, AS/NZS RCM EMC.
3	Urządzenie musi posiadać następujące porty: - LAN: 17 x 1GbE, - WAN: 1x1GbE - USB typ C do połączenia konsolowego, - 2 x Port USB 3.0, - wielkość pamięci nieulotnej 32 GB
4	Wymagane przepustowość urządzenia dla: - Ruchu NGTP: 1450 Mbps, - Ruchu NGFW: 3150 Mbps, - Ruchu IPS: 3450 Mbps, - Ruchu Firewall: min. 4800 Mbps, - Firewalla i pakietów UDP o wielkości 1518 bajtów: min. 8000 Mbps - VPN AES-128: min. 1300 Mbps, - Połączeń na sekundę: min. 54000 - Jednoczesnych połączeń: min. 245000
Sekcja 4 — Certyfikaty	
Numer	Wymaganie
1.	Oświadczenie producenta, iż oferent jest autoryzowanym przedstawicielem producenta rozwiązania UTM
Szkolenie: "Opis wymagań - Zakres szkolenia po wdrożeniowego. Tryby pracy urządzeń w sieci Użycie GUI i CLI do zadań konfiguracyjnych Omówienie zasad dostępu sieciowego do zabezpieczanych sieci za pomocą reguł zapory sieciowej. Omówienie funkcji przekierowywania portów, source NAT i destination NAT Uwierzytelnianie użytkowników za pomocą reguł zapory sieciowe Omówienie zagadnień związanych z szyfrowaniem i operacji opartych na certyfikatach Omówienie jak role i uprawnienia administracyjne wspomagają politykę zarządzania Omówienie wdrożeń i środowisk dla VPN typu Site-to-Site i zdalnego dostępu VPN Omówienie jak analizować i interpretować ruch VPN Omówienie praktyk wykonania okresowych zadań administratoraSzkolenie dla wyznaczonych pracowników Zamawiającego min. 2 Użytkowników.	

Usługa wdrożenia UTM – 1 szt.

Lp.	Usługa wdrożenia UTM
1.	Zamawiający planuje zainstalowanie dwóch urządzeń bezpieczeństwa - Firewall. Zostaną one uruchomione i skonfigurowane jako klaster Active-Standby, dzięki temu w momencie awarii urządzenia głównego, urządzenie zapasowe, będzie w stanie przejąć pracę urządzenia głównego, bez dodatkowej inicjatywy administratora. Klaster zostanie zaktualizowany do najnowszej, rekomendowanej przez producenta wersji w celu zapewnienia najwyższej możliwej na dany moment funkcjonalności i bezpieczeństwa. Konfiguracja sieciowa, w tym interfejsów lokalnych, WAN, routingu oraz protokołów komunikacyjnych zostanie odtworzona z obecnej konfiguracji Zamawiającego lub zostanie wykonana wg nowych wytycznych dostarczonych przez Zamawiającego. Zakończenie tego etapu poprzedzą testy komunikacyjne weryfikujące wszystkie uruchomione funkcjonalności oraz prawidłowe działanie samego klastra. Kolejnym krokiem będzie zapewnienie dostępu do urządzenia. Utworzone zostaną konta użytkowników lokalnych z zachowaniem polityk bezpieczeństwa i ograniczonego dostępu do pewnych funkcjonalności. Zostaną skonfigurowane połączenia VPN umożliwiające zdalny dostęp do klastra. Klasyfikacja użytkowników opierać się będzie o miejsca gdzie użytkownicy mogą się dostać oraz o poziom uprawnień dzielony na: • odczyt/zapis, • tylko odczyt, • dostęp zabroniony. Aby zapewnić bezpieczeństwo i kontrolę sieci utworzone zostaną polityki bezpieczeństwa. Powstaną na podstawie już istniejących polityk lub informacji dostarczonych bezpośrednio przez Zamawiającego. Zostanie utworzona baza obiektów wykorzystywanych w sieci Zamawiającego, które później posłużą jako obiekty źródłowe/docelowe przy kreowaniu polityk. Po

	odtworzeniu pełnej listy polityk wykonane zostaną testy komunikacyjne potwierdzające prawidłowe dostępy w sieci lub ich celowy brak. Ostatnim etapem będzie konfiguracja cyklicznego backupu konfiguracji i polityk w celu zabezpieczenia się przed utratą części lub całości danych. Zostanie sporządzona dokumentacja powykonawcza opisująca wdrożenie oraz wykorzystane funkcjonalności
2.	Zakres działań: 1.Analiza przedwdrożeniowa obejmująca weryfikację logicznej konfiguracji sieci Zamawiającego niezbędna do przygotowania projektu technicznego; analiza będzie obejmować spotkania robocze na których Zamawiający przedstawi infrastrukturę sieciową, systemową oraz aplikacyjną w zakresie niezbędnym do realizacji przedmiotu zamówienia. 2.Opracowanie projektu technicznego opisującego konfigurację urządzeń i oprogramowania niezbędnego do realizacji wdrożenia. 3.Instalacja sprzętu wraz z okablowaniem w serwerowni określonej w zaakceptowanym przez Zamawiającego projekcie technicznym, Wykonawca będzie zobowiązany do posprzątania miejsc instalacji urządzeń w siedzibie Zamawiającego, oraz pozostawienia tych miejsc w stanie nie gorszym od zastanego przed przystąpieniem do prac. 4.Opracowanie scenariuszy testowych potwierdzających zgodność dostarczonych rozwiązań z SIWZ, zatwierdzeniu scenariuszy przez Zamawiającego i przeprowadzenie testów zgodnie ze scenariuszami. 5.Przeprowadzenie testów. 6.Wykonanie dokumentacji powykonawczej opisującej szczegółową konfigurację wdrożonego rozwiązania.