RG-PZI.271.6.2023 **Załącznik nr 1**

OPIS PRZEDMIOTU ZAMÓWIENIA

Dotyczy zamówienia publicznego pn.:

„Zwiększenie cyberbezpieczeństwa i rozwój e-usług w Gminie Łobżenica w ramach projektu „Cyfrowa Gmina”

I. Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Dostarczany sprzęt i oprogramowanie muszą pochodzić z oficjalnego kanału dystrybucyjnego w UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.
7. Materiały lub urządzenia, oprogramowania pochodzące od konkretnych producentów określają minimalne parametry jakościowe, cechy użytkowe jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby spełnione zostały wymagania stawiane przez Zamawiającego. Materiały i urządzenia pochodzące od konkretnych producentów stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia.
8. Pod pojęciem „minimalne parametry jakościowe i cechy użytkowe” Zamawiający rozumie wymagania dotyczące materiałów lub urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami produktów/producentów ma wyłącznie charakter przykładowy. Zamawiający wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt w opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach użytkowych i cechach jakościowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.

9. W każdym przypadku gdy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza rozwiązania równoważne opisywanym.

II. Zestawienie rzeczowo – ilościowe

Lp.	Nazwa	jednostka
1.	Doposażenie serwerowni –zakup serwera z licencją	1 sztuka
2.	Doposażenie serwerowni – zakup serwera z licencją	1 sztuka
3.	Doposażenie serwerowni – zakup serwera NAS	1 sztuka
4.	Doposażenie serwerowni – zakup routera UTM	1 sztuka

III. Opis przedmiotu zamówienia

Serwer z licencją (I)

LP	Parametr lub warunek	Minimalne wymagania
1	Obudowa	-Typu Rack, wysokość maksimum 1U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack; -Możliwość instalacji ramienia porządkującego ułożenie przewodów; -Możliwość montażu ramki na froncie obudowy serwera zabezpieczającej dyski przed nieuprawnionym wysunięciem;
2	Płyta główna	-Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych; -wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa do 4000GB pamięci RAM DDR4 3200 MHz i do 10000GB pamięci RAM DDR4 i Optane PMem -Minimum 4 złącza PCI Express generacji 4, w tym minimum 3 złącza o prędkości x16; -Wszystkie złącza PCI Express muszą być aktywne; -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;
3	Procesory	Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86, osiągające wynik w testach wydajności SPECrate2017_int_base min. 123 pkt. przy konfiguracji z dwoma procesorami dla dowolnej platformy dwuprocesorowej producenta serwera, który jest oferowany w postępowaniu przez oferenta. Wymagamy aby był załączony PDF ze strony spec.org i poświadczony przez producenta serwera oferowanego w postępowaniu; Nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych;
4	Pamięć RAM	-Zainstalowane 128 GB pamięci RAM typu DDR4 Registered, 3200Mhz w kościach o pojemności 32GB; -Wsparcie dla technologii zabezpieczania pamięci ECC, Memory Scrubbing, SDDC lub równoważnej; -Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM (memory mirror);
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 3.0 obsługujący poziomy RAID 0,1,5,10
6	Dyski twarde	-Zainstalowane 4 dyski SAS 12 Gb o pojemności 1,2 TB 10K RPM -Minimum 8 wnęk dla dysków Hotplug 2,5 cala;
7	Inne napędy zintegrowane	-Możliwość wyposażenia serwera w wewnętrzny napęd optyczny;
8	Kontrolery LAN	-Karta sieciowa wyposażona w 2 porty 10 Gbit/s Base-T -Dodatkowa osobna karta sieciowa LAN, 4x1Gbit/s RJ-45, niezajmująca slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express); -Możliwość instalacji dodatkowej karty sieciowej niezajmującej slotu PCI Express;
9	Kontrolery I/O FC/SAS/Inne	-Brak
10	Porty	-zintegrowana karta graficzna ze złączem VGA z tyłu serwera; -2x USB 3.0 dostępne na froncie obudowy -2x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;
11	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug o mocy maksymalnej 500W każdy, o sprawności 94% (tzw klasa Platinum); -Redundantne wentylatory hotplug; -Serwer dostarczony wraz z dwoma kablami C13-C14 o długości min. 4m każdy;
12	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system

przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zarządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera. Wymaga się aby system rozpoznawania awarii był niezależny od zasilania i działał (wskazywał uszkodzony element) po odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym).

-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
- Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
- Dostęp poprzez przeglądarkę Web
- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
- Zarządzanie alarmami (zdarzenia poprzez SNMP)
- Możliwość przejęcia konsoli tekstowej
- Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
- Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera)
- Możliwość pobrania darmowego oprogramowania zarządzającego i diagnostycznego wyprodukowanego przez producenta serwera, umożliwiającego konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).
- Zainstalowana, dedykowana dla potrzeb karty zarządzającej pamięć flash o pojemności minimum 16 GB;
- Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB);
- Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania;
- Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
- Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji;
- Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń);
- Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny

		od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; • karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera;
13	Wspieranie OS	- Windows Server 2016, Windows Server 2019, Windows Server 2022, Oracle Linux 7.9, Oracle Linux 8.4, RedHat 7.9, RedHat 8.5, Suse 15 SP3, VMWare 6.7 U3, VMware 7.0 U2;

14	Gwarancja	-3 lat gwarancji producenta serwera w trybie onsite z czasem reakcji w miejscu instalacji serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki; -Dostępność części zamiennych co najmniej przez 5 lat od momentu zakupu serwera; -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji; -Wymagana możliwość automatycznego powiadamiania o awarii serwera centrum serwisowego producenta. Jeżeli funkcja taka jest płatna należy ten koszt uwzględnić w ofercie.
15	Dokumentacja, inne	-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dostarczone przed odbiorem). -Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Unii Europejskiej. Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg; -Oferent zobowiązany jest dostarczyć przed odbiorem kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu w języku polskim lub angielskim; -Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801,) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne; -Wymagane jest oświadczenie dostawcy oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez dostawcy serwera na potrzeby oferty w niniejszym postępowaniu; -Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; -Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia. Zamawiający nie dopuszcza dostosowywania funkcji na potrzeby niniejszego postępowania. - Wszystkie parametry i funkcje oferowanego serwera ogólnodostępnej producenta. Wraz z serwerem należy dostarczyć licencję na OS Windows w wersji 2022 pozwalająca uruchomić taki OS na serwerze z powyżej specyfikacji.

Serwerowy system operacyjny

Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.
Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.
2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych.
4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9) Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    - 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).
10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji
12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15) Dostępne dwa rodzaje graficznego interfejsu użytkownika:

- Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
- Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18) Mechanizmy logowania w oparciu o:
    - Login i hasło,
    - Karty z certyfikatami (smartcard),
    - Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych
20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - Podłączenie 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.
        - Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
    c) Zdalna dystrybucja oprogramowania na stacje robocze.
    d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji robocze

e) 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,
   - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f) Szyfrowanie plików i folderów
g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i) Serwis udostępniania stron WWW.
j) Wsparcie dla protokołu IP w wersji 6 (IPv6),
k) Wsparcie dla algorytmów Suite B (RFC 4869),
l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 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:

   i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   iii. Obsługi 4-KB sektorów dysków
   iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet

27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
31) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim
32) Serwerowy system operacyjny w najnowszej wersji producenta oprogramowania dostępnej na rynku.

Serwer NAS

Specyfikacja sprzętowa	
Procesor	Procesor 64 bit x86 o takowaniu nie mniejszym niż
Procesor liczba rdzeni	2.2 GHz Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB
Pamieć RAM liczba slotów	Minimum 2 sloty
Pamięć RAM - możliwość	Nie mniej niż do 64GB
rozszerzenia Pamięć Flash	Nie mniej niż 5 GB
Liczba zatok na dyski	Minimum 4 zatoki 3,5"
Obsugiwane dyski	3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5"
Wbudowane w urządzenie interfejsy na dyski M2	SATA SSD Wymagane min. 2 x M2 PCIe Gen3x1
Możliwość stosowania dysków twardych o	do 18TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2
Porty LAN 2,5 GbE	Minimum 2 RJ-45
Diody LED	Minimum Status, LAN, HDD
Porty USB 3.2 Gen2	Minimum 3
Port PCiE	Tak, minimum 2 Gen3x4

Przyciski	Reset, Zasilanie
Typ obudowy	Tower
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna	5-95% R.H.
Zasilanie	Max. 250 W

Specyfikacja oprogramowania	
Obsługa dwóch systemów operacyjnych	Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS
Wymagania dla systemu operacyjnego opartego o system plików EXT4	
Agregacja łączy Obsługiwane	Tak
systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32,
Możliwość podłączenia karty WLAN	HFS+, exFAT Tak
na USB Szyfrowanie udziałów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN

Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP, OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP

	Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata

Do w/w sprzętu należy dostarczyć cztery dyski o min. następujących parametrach:

1. Pojemność: min. 6TB
2. Prędkość obrotowa: min. 5400 RPM
3. MTBF: min. 1 mln h
4. Gwarancja: min. 3 lata (w ramach gwarancji uszkodzony dysk pozostaje własnością Zamawiającego i nie podlega zwrotowi. Wykonawca dostarczy sprawny dysk w czasie trwania gwarancji).

Router UTM

Nazwa	Opis przedmiotu zamówienia
Wymagania Ogólne	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	- W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. - Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. - Monitoring stanu realizowanych połączeń VPN. - System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, **Zasilanie:**	1. System realizujący funkcję Firewall musi dysponować minimum:10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q 4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:	1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 GbpS 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 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 1.4 Gbp 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – min. 700 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSl dla ruchu http – min. 600 Mbps.
Funkcje Systemu Bezpieczeństwa:	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 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 – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 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. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone 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. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a. Translację jeden do jeden oraz jeden do wielu. b. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

	3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. a. Amazon Web Services (AWS). b. Microsoft Azure c. Google Cloud Platform (GCP). d. OpenStack Vmware NSX
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: a. Wsparcie dla IKE v1 oraz v2. b. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). c. Obsługa protokołu Diffie-Hellman grup 19 i 20 d. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. e. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. i. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: a. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. b. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. c. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN	1. W zakresie routingu rozwiązanie powinno zapewniać obsługę: a. Routingu statycznego. b. Policy Based Routingu. c. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

	3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

	2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: a. ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	1. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a. Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
Gwarancja oraz wsparcie	1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych	1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. Ww. dokumenty wymagane będą najpóźniej w dniu dostarczenia sprzętu

Serwer z licencją (II)

LP	Parametr lub warunek	Minimalne wymagania
1	**Obudowa**	1.Typu Tower; 4U; 2.Obudowa musi umożliwiać konwersję do rack jedynie poprzez dodanie elementów fabrycznych producenta serwera (np. szyny rack czy tzw. „conversion-kit”; 3.Maksymalna wysokość serwera po konwersji do rack - 4U; 4.Obudowa musi posiadać fabryczne zabezpieczenie klatek z dyskami oraz napędami przed nieautoryzowanym dostępem (zamek);
2	**Płyta główna**	1.Wyprodukowana i zaprojektowana przez producenta serwera; 2.Minimum 4 złącza PCI Express w tym minimum 2 złącza PCI Express 4.0 x8; 3.Minimum 2 sloty dla dysków M.2 na płycie głównej nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slocie M.2 bez zajmowania klatek dyskowych serwera) 4.Zainstalowany moduł TPM 2.0.
3	**Procesory**	1.Zainstalowany procesor 8-rdzeniowy w architekturze x86 osiągający w oferowanym serwerze w testach wydajności SPECrate2017_int_base min. 69 pkt; 2.Wymagane dołączenie do oferty pełnego protokołu testów SPEC dla oferowanego modelu serwera wyposażonego w oferowany procesor, protokół poświadczony przez producenta serwera;

4	**Pamięć RAM**	1.Zainstalowane 32 GB pamięci RAM DDR4 3200Mhz w kościach o wielkości 16GB; 2.Wsparcie dla technologii zabezpieczania pamięci ECC; 3.Minimum 4 gniazda pamięci RAM, obsługa minimum 128GB pamięci RAM;
5	**Kontrolery dyskowe, I/O**	1.Zainstalowany kontroler RAID SATA (Software) obsługujący poziom RAID 0,1,10; 2.Oferowany model serwera musi umożliwiać opcjonalną instalację wewnętrznego napędu LTO SAS zamiast napędu optycznego)
6	**Dyski twarde**	-Zainstalowane 2 dyski SATA 6G o pojemności 2 TB każdy,7,2k RPM 3,5”, dyski Hotplug; -Minimum 4 wnęki dla dysków twardych Hotplug 3,5” w dostarczonej konfiguracji; -Możliwość rozbudowy serwera do obsługi co najmniej 8 dysków twardych Hotplug 3,5”
7	**Inne napędy zintegrowane**	-Zainstalowany wewnętrzny napęd DVD-RW -Możliwość instalacji wewnętrznego streamera LTO;
8	**Kontrolery LAN**	2x 1Gb/s LAN, ze wsparciem iSCSI, RJ-45;
10	**Porty**	-.zintegrowana karta graficzna ze złączem VGA lub Display port; -10x USB, w tym minimum 3 złącz w standardzie USB 3.2 Gen2x1 TYP A (2 na panelu tylnym); -Możliwość wyposażenia w port RS-232-C;
11	**Zasilanie**	1.Zainstalowany jeden zasilacz hotplug o sprawności 94% (tzw klasa Platinium) o mocy minimalnej 500W; 2.Możliwość wyposażenia serwera w drugi zasilacz zapewniający redundancje.
12	**Zarządzanie**	1.Wbudowane diody informacyjne informujące o stanie serwera – minimum sygnalizacja (poprawna praca/usterka) dla komponentów jak: procesor, wentylatory, dyski twarde, temperatura wewnątrz obudowy, pamięci, zasilaczy; sygnalizacja pracy (zasilania), sygnalizacja identyfikacji (włączana zdalnie) 2.Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Opcjonalne przekierowania konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
13	**Wspierane OS**	1.Windows Server 2019, 2022, 2.SUSE Linux Enterprise Server 15 SP3, 15 SP4,

		3.RHEL 8.4, 8.5, 8.6
14	**System Operacjny**	1.Wraz z serwerem nalezy dostraczyć Windows Server 2022 Essentials 10-Core.
15	**Gwarancja**	1. 1 rok gwarancji producenta serwera w trybie onsite 2. Dostępność części zamiennych przez 5 lat od momentu zakupu serwera; 3.Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera– jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji; 4. Zgłoszenia serwisowe w języku polskim na dedykowany nr infolinii serwisowej producenta serwera; 5. w ofercie należy zamieścić stronę www producenta serwera (link), pod którą Zamawiający odnajdzie: nr tel. zgłoszeń serwisowych, adres email zgłoszeń serwisowych, formularz online zgłoszeń serwisowych producenta serwera. Nie dopuszcza się stron www podmiotów trzecich oraz nr kontaktowych/email/formularzy podmiotów trzecich. 6.Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera
15	**Dokumentacja, inne**	1. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie dostawcy serwera potwierdzające spełnienie wymagań dołączone do oferty). 2. Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu;

Opracował: