Załącznik nr 1 do SWZ
Opis Przedmiotu Zamówienia

Dostawa sprzętu komputerowego i oprogramowania dla Gminy Lubin w ramach grantu pn. „Wzmocnienie systemu bezpieczeństwa informacji w jednostkach administracji samorządowej Gminy Lubin"

1 PRZEDMIOT ZAMÓWIENIA

1.1 Tytuł zamówienia

„Dostawa sprzętu komputerowego i oprogramowania dla Gminy Lubin w ramach grantu pn. „Wzmocnienie systemu bezpieczeństwa informacji w jednostkach administracji samorządowej Gminy Lubin"

1.2 Podstawowe informacje dotyczące przedmiotu zamówienia

1. Zamówienie stanowi realizację grantu pn. „Wzmocnienie systemu bezpieczeństwa informacji w jednostkach administracji samorządowej Gminy Lubin" współfinansowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23".
2. Zamawiającym jest Gmina Lubin.
3. Zamówienie jest udzielane w dwóch częściach.
   3.1. Cześć I zamówienia „Dostawa dla Urzędu Gminy Lubin" obejmuje:
      3.1.1. Dostawę: serwera sprzętowego - 1 sztuka, macierzy dyskowej – 1 sztuka, przełączników sieciowych klasy A – 3 sztuki przełączników sieciowych klasy B – 2 sztuki, oprogramowania systemowego – licencji systemu operacyjnego;
      3.1.2. Przekazanie dokumentacji technicznej producenta sprzętu komputerowego oraz oprogramowania będącego przedmiotem zamówienia;
      3.1.3. Przeprowadzenie czynności montażu oraz wewnętrznych testów diagnostycznych dostarczonego sprzętu komputerowego celem dokonania odbioru ilościowego oraz potwierdzenia poprawności technicznej przedmiotu dostawy, iż nie posiada ono wady fizycznej;
      3.1.4. Udzielenie gwarancji dla przedmiotu dostawy, co obejmuje udzielenie gwarancji Producenta dla dostarczanego sprzętu komputerowego na warunkach Producenta zgodnie z wymaganiami niniejszej specyfikacji (Opisu Przedmiotu Zamówienia skrót OPZ) oraz zapewnienie asysty technicznej dla dostarczanego oprogramowania.
      3.1.5. Dla kluczowej infrastruktury technicznej tj. serwera sprzętowego oraz macierzy dyskowej Wykonawca udzieli gwarancji na okres wskazany w Ofercie nie krótszy niż 36 miesięcy.
      3.1.6. Dla pozostałych urządzeń okres udzielonej gwarancji powinien odpowiadać okresowi gwarancji udzielanej dla danego urządzenia przez Producenta z uwzględnieniem wymaganego przez Zamawiającego minimalnego okresu gwarancji nie krótszego niż 24 miesiące, chyba, że w specyfikacji niniejszych wymagań dla danego urządzenia wymagany jest – dłuższy okres gwarancji.
      3.1.7. W przypadku kiedy okres gwarancji Producenta dla oferowanego urządzenia jest dłuższy niż wymagany przez Zamawiającego, wówczas Wykonawca powinien zapewniać udzielenie gwarancji na okres oferowany przez Producenta, co obejmuje w szczególności przypadki gwarancji dożywotniej tj. do czasu użytkowania danego urządzenia przez Zamawiającego.

3.1.8. W przypadku kiedy okres gwarancji Producenta jest krótszy od wymaganego w specyfikacji przez Zamawiającego, wówczas Wykonawca powinien zapewniać udzielenie gwarancji na okres wymagany przez Zamawiającego przez wykupienie dodatkowego okresu gwarancji u Producenta lub zapewnienie świadczenia gwarancji we własnym zakresie za pomocą dostępnych środków technicznych oraz zasobów własnych.

3.2. Część II zamówienia „Dostawa dla Gminnego Ośrodka Pomocy Społecznej w Lubinie" obejmuje:

3.2.1. Dostawę: serwera NAS – 1 sztuka, przełączników sieciowych – 3 sztuki, serwera sprzętowego - 1 sztuka, oprogramowania systemowego – licencji systemu operacyjnego, UTM – 1 sztuka, UPS – 1 sztuka;

3.2.2. Przekazanie dokumentacji technicznej producenta sprzętu komputerowego oraz oprogramowania będącego przedmiotem zamówienia;

3.2.3. Przeprowadzenie czynności montażu, instalacji, testów diagnostycznych oraz konfiguracji dostarczonego sprzętu komputerowego celem dokonania odbioru ilościowego oraz potwierdzenia poprawności technicznej przedmiotu dostawy, iż nie posiada ono wady fizycznej;

3.2.4. Udzielenie gwarancji dla przedmiotu dostawy, co obejmuje udzielenie gwarancji Producenta dla dostarczanego sprzętu komputerowego na warunkach Producenta zgodnie z wymaganiami niniejszej specyfikacji (Opisu Przedmiotu Zamówienia skrót OPZ) oraz zapewnienie asysty technicznej dla dostarczanego oprogramowania.

3.2.5. Dla kluczowej infrastruktury technicznej tj. serwera sprzętowego Wykonawca udzieli gwarancji w terminie wskazanym w Ofercie na okres nie krótszy niż 36 miesięcy.

3.2.6. Dla pozostałych urządzeń okres udzielonej gwarancji powinien odpowiadać okresowi gwarancji udzielanej dla danego urządzenia przez Producenta z uwzględnieniem wymaganego przez Zamawiającego minimalnego okresu gwarancji nie krótszego niż 24 miesiące, chyba, że w specyfikacji niniejszych wymagań dla danego urządzenia wymagany jest – dłuższy okres gwarancji.

3.2.7. W przypadku kiedy okres gwarancji Producenta jest dłuższy niż wymagany przez Zamawiającego, wówczas Wykonawca powinien zapewniać udzielenie gwarancji na okres oferowany przez Producenta, co obejmuje w szczególności przypadki gwarancji dożywotniej tj. do czasu użytkowania danego urządzenia przez Zamawiającego.

3.2.8. W przypadku kiedy okres gwarancji Producenta dla danego urządzenia jest krótszy od wymaganego w specyfikacji przez Zamawiającego, wówczas Wykonawca powinien zapewniać udzielenie gwarancji na okres wymagany przez Zamawiającego przez wykupienie dodatkowego okresu gwarancji u Producenta lub zapewnienie świadczenia usług gwarancji we własnym zakresie za pomocą dostępnych środków technicznych oraz zasobów własnych.

4. Miejsce dostawy i realizacji zamówienia to odpowiednio siedziba:

4.1. Dla części I zamówienia - Urząd Gminy Lubin (UG) ul. Księcia Ludwika I 3, 59-300 Lubin

4.2. Dla części II zamówienia - Gminny Ośrodek Pomocy Społecznej (GOPS) ul. Księcia Ludwika I 3, 59-300 Lubin

5. **Termin wykonania zamówienia dla każdej z części - nie później niż 60 dni od daty zawarcia umowy z Wykonawcą.**

6. Szczegółowe wymagania oraz parametry techniczne przedmiotu dostawy dla każdej z części przedmiotu zamówienia określono w dalszej części niniejszego dokumentu.

7. W realizacji każdej części zamówienia Wykonawca jest zobowiązany w Ofercie uwzględnić koszt dostawy tj. koszty transportu, cła, podatków, ubezpieczenia, gwarancji oraz inne koszty operacyjne, a także zależnie od zakresu niniejszych wymagań, koszty montażu, instalacji i konfiguracji dostarczonych produktów: sprzętu komputerowego i oprogramowania oraz inne niezbędne usługi wskazane w niniejszej specyfikacji.

   7.1. Powyższe odnosi się także do wszelkich kosztów naprawy sprzętu komputerowego, w tym naprawy lub wymiany jego części w ramach serwisu gwarancyjnego, co obejmuje także koszty dojazdu, transportu, demontażu i montażu naprawionego lub wymienianego sprzętu.

8. Z uwagi na realizację zamówienia w ramach Grantu „Cyberbezpieczny Samorząd" jest zobowiązany do:

   8.1. Prowadzenia wspólnej z Zamawiającym polityki informacyjnej, której podstawą dla Zamawiającego są wytyczne w zakresie promocji i polityki informacyjnej, jakie nakłada na Zamawiającego, jako Grantobiorcę Instytucja Pośrednicząca, co dotyczy głównie właściwego oznakowania prowadzonej korespondencji, pism, dokumentów zgodnie z obowiązującymi w tym zakresie wytycznymi (https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad - materiały reklamowe / logotypy).

1.2.1 Ogólne wymagania dot. przedmiotu dostawy dla obu części zamówienia

1. Sprzęt musi być fabrycznie nowy i pochodzić z oficjalnego kanału sprzedaży, musi być nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż w II półroczu 2024 roku, dostarczony w oryginalnym opakowaniu, które musi być nienaruszone i posiadać zabezpieczenie zastosowane przez Producenta danego urządzenia. Nie dopuszcza się użycia sprzętu odnawianego, demonstracyjnego lub powystawowego lub poleasingowego, co odnosi się również do oprogramowania.

   1.1. Na etapie realizacji dostawy na pisemne żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające pochodzenie dostarczanego urządzenia z oficjalnego kanału dystrybucyjnego danego Producenta. Niespełnienie przedmiotowego wymagania we wskazanym przez Zamawiającego terminie stanowić będzie o niezgodności realizacji przedmiotu zamówienia z wymaganiami przedmiotowego zamówienia zawartymi w Opisie Przedmiotu Zamówienia oraz SWZ.

   1.2. Dla dostawy sprzętu w liczbie sztuk większej niż jedno urządzenie, Wykonawca musi zapewnić dostawę jednorodnego sprzętu tj. od tego samego producenta oraz o tym samym numerze katalogowym.

2. Sprzęt musi być wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie.

3. Elementy, z których zbudowany jest sprzęt muszą być produktami producenta tego sprzętu lub być przez niego certyfikowane oraz muszą być objęte gwarancją producenta w zakresie wymaganym w niniejszej specyfikacji.

4. Dostarczone oprogramowanie musi pochodzić z oficjalnego kanału dystrybucyjnego Producenta, oprogramowania oraz musi być nowe, nieużywane, nieaktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej, stabilnej wersji oraz nie może być obciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) muszą być wolne od wad fizycznych i prawnych.

4.1. W przypadku oprogramowana technicznego stanowiącego integralną części oferowanych urządzeń przyjmuje się, że zapewnienie legalności oprogramowania z oficjalnego kanału dystrybucyjnego jest w gestii zobowiązań oraz udzielonych gwarancji ze strony Producenta danego urządzenia.

5. Zamawiający zastrzega możliwość przeprowadzenia weryfikacji oryginalności dostarczonego sprzętu i oprogramowania u Producenta w przypadku wystąpienia wątpliwości co do jego legalności.

6. Wykonawca jest zobowiązany dołączyć do oferty przedmiotowe środki dowodowe wskazane odpowiednio w specyfikacji technicznej w zakresie wymagań dla danego urządzenia.

7. Każde dostarczane urządzenie musi spełniać wymagania w zakresie:

   7.1. deklaracji zgodności Producenta danego urządzenia z obowiązującymi wymaganiami w całej UE i musi posiadać oznakowanie CE,

   7.2. ograniczenia stosowania niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (RoHS) obowiązujące w Unii Europejskiej (UE) uregulowane przez przepisy Dyrektywy RoHS[1] II oraz III,

   7.3. regulacje związane z postępowaniem z zużytym sprzętem elektrycznym i elektronicznym wprowadzone przez Dyrektywę WEEE[2] (2012/19/UE) obejmującą przepisy dotyczące zbiórki, przetwarzania, recyklingu oraz odzysku odpadów, których celem jest ograniczenie ich negatywnego wpływu na środowisko.

8. Stosowne oświadczenia we wskazanym powyżej zakresie wymagań, a także o dostarczeniu produktów z oficjalnego kanału dystrybucyjnego danego Producenta, Wykonawca złoży w formularzu oferty.

9. Wykonawca jest zobowiązany dostarczyć sprzęt komputerowy z niezbędnym osprzętem do instalacji, w tym w szczególności ze wskazanym w specyfikacji.

10. Miejsce realizacji przedmiotu zamówienia odpowiednio dla danej części zamówienia wskaże Zamawiający.

11. Wszystkie prace montażowe, instalacyjne muszą być przeprowadzone w uzgodnieniu z Zamawiającym w godzinach pracy danej jednostki organizacyjnej wskazanej dla realizacji danej części przedmiotu zamówienia. Godziny pracy UG oraz GOPS dostępne są odpowiednio na stronach internetowych:

    11.1. UG - https://bip.ug.lubin.pl/5905

[1] tj. Dyrektywy 2011/65/UE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2011 r. w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym, Dyrektywa delegowana Komisji (UE) 2015/863 z dnia 31 marca 2015 r. zmieniająca załącznik II do dyrektywy Parlamentu Europejskiego i Rady 2011/65/UE w odniesieniu do wykazu substancji objętych ograniczeniem, Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/2102 z dnia 15 listopada 2017 r. zmieniająca dyrektywę 2011/65/UE w sprawie ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym

[2] WEEE (ang: Waste Electrical and Electronic Equipment)

11.2. GOPS - http://bip.gops.lubin.pl/

12. Czynności instalacji obejmują również przeprowadzenie testów diagnostyki dostarczonych produktów celem potwierdzenia poprawności technicznej przedmiotu dostawy, iż nie posiada ono wad fizycznych.

13. Wykonawca jest zobowiązany do dostarczenia dokumentacji technicznej danego produktu lub wskazania jej źródła zgodnie ze specyfikacją produktu, określoną przez producenta produktu lub przez jego dystrybutora.

14. Dla zainstalowanego, skonfigurowanego sprzętu Wykonawca przeprowadzi w siedzibie Zamawiającego (w lokalizacji wskazanej odpowiednio dla danej części zamówienia) niezbędny instruktaż techniczny dot. użytkowania danego produktu dla personelu technicznego Zamawiającego.

15. Oprogramowanie będące przedmiotem dostawy, instalacji i konfiguracji, Wykonawca jest zobowiązany instalować zgodnie z zaleceniami producenta z uwzględnieniem tzw. modyfikacji („łatek") na podstawie publikowanej przez danego producenta listy aktualizacji lub listy aktualizacji wskazanej przez CERT www.cert.pl (co w szczególności dotyczy "łatek" obejmujących aktualizacje mechanizmów zabezpieczeń dla danego Oprogramowania - ang. security patch).

    15.1. Każde odstępstwo od ww. reguły będące wynikiem praktycznych doświadczeń Wykonawcy, wiążące się z zapewnieniem według Wykonawcy większej stabilności działania przedmiotowego oprogramowania, powinno być uzasadnione i uzgodnione z Zamawiającym oraz powinno zostać zawarte w ramach podpisanego protokołu z instalacji lub protokołu odbioru.

16. Dla każdego Oprogramowania będącego przedmiotem dostawy Wykonawca jest zobowiązany udzielić lub przekazać stosowne licencje uprawniające Zamawiającego do korzystania z dostarczonego przez Wykonawcę Oprogramowania. Warunki dot. udzielania lub przekazania licencji, sublicencji określa projekt umowy.

17. Podstawą odbioru przedmiotu zamówienia, w tym każdego produktu jest przeprowadzenie odbioru ilościowego oraz jakościowego zgodnie z niniejszą specyfikacją.

18. Podczas prowadzenia przez Zamawiającego czynności odbioru Wykonawca jest zobowiązany do ścisłego współdziałania z Zamawiającym celem skutecznego doprowadzenia do odbioru, w tym zobowiązany jest do udzielania niezbędnych wyjaśnień i / lub wypełnienia niezrealizowanych zobowiązań, wynikających ze zgłoszonych przez Zamawiającego uwag i zastrzeżeń.

19. Wykonawca jest zobowiązany udzielić Zamawiającemu gwarancji zgodnie z wymaganiami SWZ oraz zgodnie ze złożoną przez Wykonawcę Ofertą.

20. Świadczenia gwarancyjne oraz serwisowe muszą być realizowane w języku polskim.

21. Świadczenia gwarancyjne oraz serwisowe muszą spełniać ogólne warunki niniejszej specyfikacji oraz szczegółowe wymagania, jakie w tym zakresie zostały określone w treści wymagań dla poszczególnych urządzeń.

22. Świadczenia gwarancyjne muszą być realizowane w miejscu dostawy. Poza tym, dla:

    22.1. Kluczowej infrastruktury technicznej (serwery, macierz) oferowanej przez Wykonawcę, Producent oferowanych urządzeń powinien posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego lub innego parametru / kodu identyfikującego dane urządzenie, możliwe będzie zweryfikowanie, co najmniej takiej informacji, jak: czas i poziom oferowanego serwisu gwarancyjnego producenta, datę

zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego typu urządzenia.

22.2. Pozostałej grupy urządzeń Wykonawca powinien zapewnić, aby Producent lub jego certyfikowany partnera / dystrybutor umożliwił dostęp do serwisu informacyjnego lub infolinii lub kontaktu poprzez email celem zweryfikowania przez Zamawiającego, co najmniej takiej informacji, jak: czas i poziom oferowanego serwisu gwarancyjnego producenta, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego typu urządzenia.

23. Realizacja świadczeń gwarancyjnych i serwisowych dla sprzętu komputerowego musi być prowadzona zgodnie z gwarancją Producenta, której warunki, co do sposobu realizacji oraz terminów muszą być zawarte w treści Oferty i powinny być potwierdzone przez dołączone do Oferty dokumenty zgodnie z wymaganiami, jakie określono w formularzu technicznym oferty.

23.1. Bez względu na warunki gwarancji i świadczonych usług serwisowych Producenta:

23.1.1. Zamawiający musi mieć zapewnioną możliwości zgłoszenia usterki / wady urządzenia (co obejmuje także błędy w działaniu oprogramowania technicznego stanowiącego integralną cześć oferowanego produktu) na formularzu zgłoszenia poprzez serwis „Helpdesk" Producenta, Dystrybutora lub Wykonawcy (lub rozwiązanie równoważne) z zapewnieniem potwierdzenia przyjęcia zgłoszenia przez podmiot świadczący zobowiązania z tytułu gwarancji. Dopuszcza się możliwość zgłoszenia poprzez email lub telefonicznie, przy czym tak dokonane zgłoszenie uważane będzie za doręczone skutecznie, i będzie wywoływać takie same skutki, jak wezwanie poprzez serwis „Help-Desk" lub inne rozwiązanie równoważne – lub wezwanie skierowane na piśmie.

23.1.2. Zamawiający wymaga wymiany sprzętu komputerowego na wolny od wad w przypadku kiedy w okresie 14 dni od daty zgłoszenia wady Wykonawca lub działający w jego imieniu gwarant nie zdołał doprowadzić urządzenia do stanu gotowości oraz prawidłowego działania zgodnie z dokumentacją i przeznaczeniem danego urządzenia. Wymieniane, nowe urządzenie musi posiadać, co najmniej takie same, nie gorsze niż cechy oraz parametry funkcjonalne wymienianego urządzenia.

24. Dla każdego oferowanego urządzenia (zgodnie z wymaganiami, jakie określono w formularzu technicznym oferty) Wykonawca jest zobowiązany dołączyć dokument, z którego będą wynikały oraz zostaną potwierdzone wszystkie wymagania / parametry oferowanego urządzenia wskazane w niniejszym Opisie Przedmiotu Zamówienia.

24.1. W przypadku kiedy zakres treści karty katalogowej danego urządzenia nie pokrywa całości wymagań OPZ np. z uwagi na konieczność rozszerzenia przedmiotu dostawy dla danego urządzenia o dodatkowe elementy / części / rozszerzenia, wówczas tego rodzaju informacje potwierdzające przedmiot dostawy należy wprowadzić do formularza technicznego. Zamawiający dopuszcza w tym miejscu również podanie informacji o unikalnym numerze identyfikacyjnym oferowanego przez Wykonawcę urządzenia, które będzie przedmiotem dostawy. Do wskazanego numeru należy jeszcze podać adres strony internetowej Producenta, na której wprowadzeniu numeru indentyfikacyjnego będzie możliwe zweryfikowanie wymagań oferowanego produktu.

25. Na wniosek Wykonawcy Zamawiający może zapewnić zdalny dostęp do Infrastruktury Technicznej Zamawiającego (odpowiednio dla UG lub GOPS) celem realizacji przedmiotu zamówienia pod następującymi warunkami:

25.1. dostęp dla Wykonawcy możliwy będzie wyłącznie po podpisaniu przez Wykonawcę oświadczenia o zapewnieniu stosowania zasad określonych w obowiązującej w organizacji Zamawiającego polityce bezpieczeństwa, przy uwzględnieniu, iż:

25.1.1. zdalny dostęp do Infrastruktury Technicznej poprzez łącze VPN posiadać będą wyłącznie wskazane imiennie osoby podane na wykazie: /imię/nazwisko/e-mail/tel/firma – o ile jest to podwykonawca;

25.1.2. dostęp będzie realizowany na żądanie lub w trybie określonym przez harmonogram ustalonych „okien czasowych”;

25.1.3. dostęp do zasobów będzie realizowany poprzez VPN poprzez konta imienne aktywowane w oparciu o harmonogram;

25.1.4. naruszenie przez Wykonawcę ustalonych powyżej zasad skutkować będzie zablokowaniem dostępu zdalnego.

2 CZĘŚĆ I ZAMÓWIENIA – DOSTAWA DLA URZĘDU GMINY W LUBINIE

2.1 Wymagania szczegółowe dot. realizacji Części I zamówienia

1. Zakres prac Wykonawcy obejmuje w szczególności:

   1.1. dostawę i montaż kompletnego sprzętu wraz z niezbędnym oprogramowaniem i osprzętem umożliwiającym uruchomienie danego urządzenia,

   1.2. uruchomienie każdego dostarczanego urządzenia celem przeprowadzenia (wewnętrznych) testów diagnostycznych zgodnie ze specyfikacją techniczną urządzenia,

   1.3. przekazanie dokumentacji technicznej dla każdego urządzenia lub wskazanie,

   1.4. dostarczenie i przekazanie licencji oprogramowania systemowego – systemu operacyjnego,

   1.5. udzielenie gwarancji dla każdego dostarczonego, zamontowanego urządzenia.

2.2 Serwer sprzętowy - 1 sztuka

Cecha, parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Obudowa wyposażona w diody LED lub panel LCD umieszczony na froncie obudowy umożliwiający wyświetlenie informacji o stanie serwera: procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 56 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 8TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	• Zainstalowane dwa procesory 12 rdzeniowe klasy x86, min. 2.4GHz, dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 240 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. • Ograniczenie dot. liczby rdzeni (12 rdzeni / na procesor) wynika z ograniczeń aktualnie użytkowanej licencji wirtualizatora WMvare. • Wymaganie dotyczące architektury fizycznej procesora x86 jest krytyczne i niezbędne dla zastosowania dostarczanego serwera do pracy w układzie klastra serwerów dla środowiska systemowego Zamawiającego opartego o system MS Windows Server 2019 Standard oraz wirtualizator VMvare.

Cecha, parametr	Charakterystyka (wymagania minimalne)
	• Rekomendowane jest, aby zainstalowany procesor posiadał maksymalnie zgodne parametry w stosunku do konfiguracji aktualnie działającej opartej o: procesor Intel Xeon Silver 4214 (2,2GHz, 12 rdzeni/24 wątki, 9,6GT/s, 16,5MB pamięci podręcznej, Turbo, HT, 85W), pamięć DDR4-2400
RAM	• Minimum 512GB DDR5 RDIMM 5600MT/s
Gniazda PCI	• Min. 8 slotów PCIe w tym minimum 4 sloty Gen5
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 4 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • Dwie, dwuportowe karty sieciowe 10Gb Ethernet w standardzie BaseT
Dyski twarde	• Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.

Porty	• 4 porty USB w tym min:
	  ○ 1 port USB 3.0,
	  ○ 1 port micro USB,
	• 2 porty VGA z czego jeden z przodu obudowy

Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	• Redundantne, Hot-Plug
Zasilacze	• Redundantne, Hot-Plug min. 700W klasy Titanium • 2 kable zasilające z wyczką C13-C14, min 1.8m
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

Cecha, parametr	Charakterystyka (wymagania minimalne)
	○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ 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	• Niezależne od zainstalowanego na serwerze systemu operacyjnego oprogramowanie posiadające dedykowany port Gigabit Ethernet RJ-45 i umożliwiające: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie;

Cecha, parametr	Charakterystyka (wymagania minimalne)
	○ wsparcie dla automatycznej rejestracji DNS ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ 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

Cecha, parametr	Charakterystyka (wymagania minimalne)
	○ 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. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną i wdrożoną przez Zamawiającego, jako środowisko systemowe platformą wirtualizacyjną VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych

Cecha, parametr	Charakterystyka (wymagania minimalne)
	○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów

Cecha, parametr	Charakterystyka (wymagania minimalne)
	▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia o Urządzenie Producenta dostarczane w ramach postępowania o Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego)

Cecha, parametr	Charakterystyka (wymagania minimalne)
	• Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
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	• Zamawiający wymaga zapewnienia gwarancji Producenta zgodnie z Ofertą Wykonawcy na okres nie krótszy niż 36 miesięcy od daty odbioru. • Zamawiający wymaga możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Czas reakcji – najpóźniej następny dzień roboczy po przekazaniu zgłoszenia serwisowego, co oznacza, iż czynności naprawy następują w tym terminie. • W przypadku awarii nośników danych, uszkodzony nośnik pozostaje u Zamawiającego i nie podlega wymianie na nowy będący przedmiotem świadczenia gwarancyjnego – serwisowego. • Serwis urządzenia musi być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Podmiot serwisujący urządzenie musi posiadać wdrożony system zarządzania jakością oparty na normie ISO 9001:2015 lub równoważnej oraz wdrożony w organizacji System Zarządzania Bezpieczeństwem Informacji (SZBI) oparty na normie ISO-27001 lub równoważnej, a także musi posiadać autoryzacje Producenta urządzenia na świadczenie usług serwisowych / gwarancyjnych. • Zamawiający wymaga, aby dostarczony serwer znajdował się na listach typu End-of-Life / End-of-Support i posiadał możliwość odpłatnego przedłużenia gwarancji i wsparcia producenta na okres minimum 7 lat liczony od momentu odbioru przedmiotu umowy.
Wymagania specyficzne, w tym dot. kryterium środowiskowego	• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla, co najmniej systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. • Urządzenie powinno być wyprodukowane przez Producenta, u którego wdrożono system zarządzania jakością oparty o normę ISO 9001:2015 lub równoważną, w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych (producent posiada certyfikat ISO 9001:2015 lub równoważny). • Urządzenie powinno być wyprodukowane przez Producenta, u którego wdrożono normę ISO 14001 lub równoważną, w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych (producent posiada certyfikat ISO 14001 lub równoważny). • Urządzenie powinno być wyprodukowane przez Producenta, u którego wdrożono normę ISO 50001 lub równoważną, w zakresie co najmniej produkcji

Cecha, parametr	Charakterystyka (wymagania minimalne)
	lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych (producent posiada certyfikat ISO 50001 lub równoważny). • Oczekuje się, aby urządzenie spełniało kryteria klasyfikacji EPAET określone dla tego typu urządzenia i posiadało przyznany certyfikat klasyfikacji: brown, silver lub gold www.epeat.net
Certyfikaty, dokumenty	Do oferty należy dołączyć wymagane, następujące dokumenty potwierdzające wymagania wobec oferowanego urządzenia oraz powiązanych z nim usług / rozwiązań: • Oświadczenie Producenta potwierdzające, że serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Dokumenty potwierdzający, iż Podmiot / Podmioty serwisujące urządzenie posiada / posiadają: o wdrożony system zarządzania jakości zgodnie z normą ISO 9001:2015 lub równoważną w zakresie co, najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych, obejmujący także zakres zadań związanych z obsługą serwisową urządzeń lub systemów lub rozwiązań informatycznych, o wdrożony system zarządzania bezpieczeństwem informacji zgodnie z normą ISO-27001 lub równoważą, obejmujący swoim zakresem usługi serwisowe, • Dokument potwierdzający, iż Podmiot serwisujący urządzenie posiada autoryzację Producenta na świadczenie usług serwisowych dla oferowanego urządzenia (nie dotyczy, o ile serwis urządzenia będzie realizowany bezpośrednio przez Producenta) • Wydruk ze strony internetowej z datą nie wcześniejszą niż 7 dni przed składaniem ofert ze wskazaniem wiersza odpowiadającego właściwemu wynikowi testów, który potwierdzi wymagania w zakresie wydajności procesora umożliwiające osiągnięcie wyniku min. 240 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. • Oświadczenie Producenta serwera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych przez Wykonawcę albo ogłoszenia upadłości lub likwidacji Wykonawcy, przejmie na siebie wszelkie zobowiązania związane z serwisem na zasadach określonych w Umowie, gdzie dokumenty potwierdzające tenże stan rzeczy należy przedłożyć w dniu dostawy sprzętu. • W przypadku kiedy urządzenie spełnia kryteria w ramach klasyfikacji EPAET, Wykonawca powinien dołączyć do Oferty wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy w przyznanej dla tego urządzenia klasyfikacji: brown, silver lub gold. Załączany do oferty wydruk musi być podpisany przez osobę reprezentującą Wykonawcę.

Cecha, parametr	Charakterystyka (wymagania minimalne)
	• Każdy dokument, certyfikat lub wydruk przedkładany przez Wykonawcę oraz składany razem z Ofertą celem potwierdzenia spełnienia wymagań musi być podpisany przez osobę reprezentującą Wykonawcę.

2.3 Macierz dyskowa – sztuk 1

Cecha, parametr	Charakterystyka (wymagania minimalne)
Typ obudowy	• Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5”.
Przestrzeń dyskowa	• Zainstalowane: ○ 22x dyski SAS 10K o pojemności min. 2.4TB, Hot-Plug ○ 2x dyski SSD 10K o pojemności min. 1.92TB, Hot-Plug
Możliwość rozbudowy	• Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Obsługa dysków	• Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
Sposób zabezpieczenia danych	• Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). • Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. • Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). • Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	• Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	• Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.

Cecha, parametr	Charakterystyka (wymagania minimalne)
	• Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. • Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum jednego roku.
Rozbudowa pamięci cache	• Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z oferowanym rozwiązaniem.
Interfejsy	• Macierz musi posiadać, co najmniej 8 portów 10GbE iSCSI BaseT (4 porty na kontroler),
Zarządzanie	• Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	• Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. • Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. • Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	• Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. • Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych. • Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	• Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. • Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. • Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	• Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.

Cecha, parametr	Charakterystyka (wymagania minimalne)
	• Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	• Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. • Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	• Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Zdalna replikacja danych	• Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. • Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
Podłączanie zewnętrznych systemów operacyjnych	• Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). • Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. • Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. • Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	• Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. • Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.

Cecha, parametr	Charakterystyka (wymagania minimalne)
	• Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. • Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.
Dodatkowe wymagania	• Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. • Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	• Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta zgodnie z Ofertą Wykonawcy na okres nie krótszy niż 36 miesięcy od daty odbioru. • Zamawiający wymaga możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Czas reakcji – najpóźniej następny dzień roboczy po przekazaniu zgłoszenia serwisowego, co oznacza, iż czynności naprawy następują w tym terminie. • W przypadku awarii nośników danych, uszkodzony nośnik pozostaje u Zamawiającego i nie podlega wymianie na nowy będący przedmiotem świadczenia gwarancyjnego – serwisowego. • Serwis urządzenia musi być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Podmiot serwisujący urządzenie musi posiadać wdrożony system zarządzania jakością oparty na normie ISO 9001:2015 lub równoważnej oraz wdrożony w organizacji System Zarządzania Bezpieczeństwem Informacji (SZBI) oparty na normie ISO-27001 lub równoważnej, a także musi posiadać autoryzacje Producenta urządzenia na świadczenie usług serwisowych / gwarancyjnych. • Zamawiający wymaga, aby dostarczony serwer znajdował się na listach typu End-of-Life / End-of-Support i posiadał możliwość odpłatnego przedłużenia gwarancji i wsparcia producenta na okres minimum 7 lat liczony od momentu odbioru przedmiotu umowy.
Wymagania dot. jakości oraz specyficzne dot. kryterium środowiskowego	• Urządzenie powinno być wyprodukowane przez Producenta, u którego wdrożono system zarządzania jakością oparty o normę ISO 9001:2015 lub równoważną, w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych (producent posiada certyfikat ISO 9001:2015 lub równoważny). • Urządzenie powinno być wyprodukowane przez Producenta, u którego wdrożono normę ISO 14001 lub równoważną, w zakresie co najmniej produkcji

Cecha, parametr	Charakterystyka (wymagania minimalne)
	lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych (producent posiada certyfikat ISO 14001 lub równoważny).
Certyfikaty, dokumenty	Do oferty należy dołączyć wymagane, następujące dokumenty potwierdzające wymagania wobec oferowanego urządzenia oraz powiązanych z nim usług / rozwiązań: • Oświadczenie Producenta potwierdzające, że serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Dokumenty potwierdzający, iż Podmiot / Podmioty serwisujące urządzenie posiada / posiadają: o wdrożony system zarządzania jakości zgodnie z normą ISO 9001:2015 lub równoważną w zakresie co, najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych, obejmujący także zakres zadań związanych z obsługą serwisową urządzeń lub systemów lub rozwiązań informatycznych, o wdrożony system zarządzania bezpieczeństwem informacji zgodnie z normą ISO-27001 lub równoważą, obejmujący swoim zakresem usługi serwisowe, • Dokument potwierdzający, iż Podmiot serwisujący urządzenie posiada autoryzację Producenta na świadczenie usług serwisowych dla oferowanego urządzenia (nie dotyczy, o ile serwis urządzenia będzie realizowany bezpośrednio przez Producenta) • Oświadczenie Producenta serwera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych przez Wykonawcę albo ogłoszenia upadłości lub likwidacji Wykonawcy, przejmie na siebie wszelkie zobowiązania związane z serwisem na zasadach określonych w Umowie, gdzie dokumenty potwierdzające tenże stan rzeczy należy przedłożyć w dniu dostawy sprzętu. Każdy dokument, certyfikat lub wydruk przedkładany przez Wykonawcę oraz składany razem z Ofertą celem potwierdzenia spełnienia wymagań musi być podpisany przez osobę reprezentującą Wykonawcę.

2.4 Przełączniki sieciowe klasy A – 3 sztuki

Cecha, parametr	Charakterystyka (wymagania minimalne)
Typ obudowy	• Przystosowana do montażu w szafie rack, wys. 1U
Porty i interfejsy	• 48 portów 10/100/1000 Mbps (RJ-45) • 4 porty 1/10 GbE SFP+ • Port zarządzania (RS-232C lub micro USB)

Cecha, parametr	Charakterystyka (wymagania minimalne)
Wydajność i przepustowość	• Zdolność przełączania: 176 Gbps • Przepustowość: do 112 Mpps
Funkcje sieciowe	• Obsługa routingu: RIP, OSPF (Access), statyczne trasy IP • Obsługa VLAN i priorytetów QoS • Możliwość tworzenia stosu do 8 urządzeń (Virtual Switching Framework) • Mechanizmy zabezpieczeń: 802.1X, ACL, RADIUS/TACACS+, SSL, MAC Address Lockout • Wbudowana obsługa PoE+ (do 740W)
Bezpieczeństwo	• Zarządzanie przez CLI, Web GUI, SNMP • Wsparcie dla Zero-Touch Provisioning (ZTP) • Możliwość monitorowania przez sFlow i RMON
Gwarancja	• Okres gwarancji 36 miesięcy lub gwarancja dożywotnia

2.5 Przełączniki sieciowe klasy B – 2 sztuki

Cecha, parametr	Charakterystyka (wymagania minimalne)
Typ obudowy	• Przystosowana do montażu w szafie rack, wys. 1U
Porty i interfejsy	• 20 portów 10GBase-T RJ-45 • 4 porty combo 10GBase-T / 10G SFP+ • 1 port konsoli RJ-45 • 1 port konsoli USB-C • 1 dodatkowy port USB • 1 port RJ-45
Wydajność i przepustowość	• Zdolność przełączania: 480 Gbps • Przepustowość: 357.12 Mpps
Funkcje sieciowe	• Obsługa VLAN (4093 ID) i Private VLAN, MVR • Obsługa routingu: RIP-2, CIDR, policy-based routing (PBR) • Obsługa agregacji łączy (8 grup) • Mechanizmy zabezpieczeń: 802.1X, ACL, RADIUS/TACACS+, DHCP snooping, IP Source Guard • QoS: DSCP, WRR, DiffServ, priorytety ruchu • Ochrona DoS, ARP spoofing oraz zapobieganie pętlom w sieciach • Obsługa PoE • Zapobieganie atakom typu DoS, WRR, ToS
Zarządzanie i monitorowanie	• Zarządzanie przez CLI, Web GUI, SNMP • Wsparcie dla Zero-Touch Provisioning (ZTP) • Możliwość monitorowania przez sFlow i RMON

Cecha, parametr	Charakterystyka (wymagania minimalne)
Gwarancja	• Okres gwarancji 36 miesięcy lub gwarancja dożywotnia

2.6 Oprogramowanie systemowe – licencje systemu operacyjnego

1. Licencje na serwerowy system operacyjny dla dostarczanego serwera sprzętowego muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Udzielone licencje muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym oraz dla dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.
2. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy - wymagania:
   2.1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
   2.2. 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.
   2.3. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
   2.4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
   2.5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
   2.6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
   2.7. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
   2.8. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
   2.9. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
   2.10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
   2.11. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
   2.12. Graficzny interfejs użytkownika.
   2.13. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
   2.14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

2.15. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

2.16. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

2.17. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).

2.18. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

2.19. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.

2.20. 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.

2.21. Zdalna dystrybucja oprogramowania na stacje robocze.

2.22. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.

2.23. PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

2.23.1. dystrybucję certyfikatów poprzez http,

2.23.2. konsolidację CA dla wielu lasów domeny,

2.24. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.

2.25. Szyfrowanie plików i folderów.

2.26. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

2.27. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

2.28. Serwis udostępniania stron WWW.

2.29. Wsparcie dla protokołu IP w wersji 6 (IPv6).

2.30. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

2.31. 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.

2.32. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

2.33. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

2.34. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

2.35. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF

3. Dla oferowanego produktu musi być dostępny na rynku usług IT zorganizowany system certyfikowanych szkoleń oraz muszą być dostępne materiały edukacyjne w języku polskim.

4. Z uwagi na przeznaczenie nabywanego przez Zamawiającego serwera sprzętowego (Rozdz. 2.1 Serwer sprzętowy) do obsługi klastra maszyn wirtualnych dostarczone oprogramowanie (w zakresie liczby licencji) musi zapewnić m.in:

   4.1. środowisko uruchomieniowe (w ramach klastra) dla aktualnej infrastruktury aplikacyjnej Zamawiającego, co oznacza, iż liczba licencji systemu operacyjnego dla dostarczonego serwera fizycznego musi być adekwatna i odpowiednio dobrana do parametrów technicznych serwera tj. liczby procesorów, liczby rdzeni (łącznie 24 rdzenie), warunków udzielania licencji przez Producenta przedmiotowego oprogramowania oraz powinna, zapewnić jednocześnie prawidłową technicznie (i prawnie) pracę minimum 18 maszyn wirtualnych w tak utworzonym środowisku systemowym, co technicznie przekłada się na konieczność zapewnienia łącznej obsługi 216 rdzeni oraz obsługę 120 użytkowników, w ramach tzw. licencji dostępowej (o ile takie wymagania nakładają warunki licencyjne producenta oprogramowania).

5. Oprogramowanie musi być dostarczone w najwyższej wersji dostępnej w ofercie Producenta oprogramowania.

3 CZEŚĆ II ZAMÓWIENIA – DOSTAWA DLA GMINNEGO OŚRODKA POMOCY SPOŁECZNEJ W LUBINIE

3.1 Wymagania szczegółowe dot. realizacji Części II zamówienia

1. Zakres prac Wykonawcy obejmuje w szczególności:

   1.1. dostawę kompletnego sprzętu, z niezbędnym oprogramowaniem oraz niezbędnymi przewodami,

   1.2. uruchomienie oraz wstępną konfiguracja serwera NAS (zainicjowanie dysków twardych, wgranie najnowszego oprogramowania, konfiguracja kart sieciowych zgodnie z wymogami Zamawiającego, aktywacja oprogramowania do archiwizacji komputerów), instalację i wstępną konfigurację oprogramowania do archiwizacji VM oraz serwera Hyper-V.

   1.3. uruchomienie oraz instalacja najnowszego firmware dla przełączników sieciowych

   1.4. konfiguracja sieci VLAN wskazanych przez Zamawiającego na przełącznikach sieciowych

   1.5. uruchomienie podłączenie oraz konfiguracja karty SNMP w UPS.

   1.6. instalację i wstępną konfigurację oprogramowania do archiwizacji danych.

   1.7. uruchomienie systemu UTM przez:

      1.7.1. przeniesienie konfiguracji z urządzenia Stormshield SN 300 do dostarczonego urządzenia,

      1.7.2. aktualizacja firmware UTM do najnowszej wersji,

      1.7.3. analizę aktualnej konfiguracji mechanizmów bezpieczeństwa oraz konfiguracji firewall-a oraz wprowadzenie zmian mających na celu zwiększenie poziomu bezpieczeństwa cyfrowego, w tym uzgodnienie z Zamawiającym polityki bezpieczeństwa ruchu sieciowego uwzględniającej wyniki przeprowadzonej analizy,

      1.7.4. wprowadzenie do konfiguracji urządzenia UTM m.in. zmian umożliwiających izolację serwerów od sieci produkcyjnej oraz identyfikacja usług (portów) niezbędnych do zachowania komunikacji ze stacjami roboczymi użytkowników (bez konieczności zmiany adresacji IP),

      1.7.5. odseparowanie serwerów aplikacyjnych od sieci Internet oraz identyfikację, a także przepuszczenie połączeń niezbędnych do poprawnej pracy tych serwerów,

      1.7.6. przygotowanie opisu konfiguracji oraz przekazanie go Zamawiającemu w wersji papierowej oraz elektronicznej (edytowalnej),

   1.8. opracowanie dokumentacji powykonawczej zawierającą m.in. opis konfiguracji urządzeń, wykaz przekazanych licencji. Dodatkowo do dokumentacji należy dołączyć, o ile zajdzie taka konieczność, rejestru dostępu w czasie prac Wykonawcy do miejsc ograniczonego dostępu,

   1.9. udzielenie gwarancji dla każdego dostarczonego, zamontowanego urządzenia.

2. Wykonawca zagwarantuje, że zadania określone w zakresie konfiguracji, uruchomienia systemu UTM wykonywa osoba wskazane w ofercie wchodząca w skład Personelu Wykonawcy posiadająca niezbędne umiejętności w tym aktualne poświadczenie / certyfikat kompetencji zgodnie z wymaganiami SWZ.

3. W przypadku konieczności prowadzenia prac w strefach chronionych w OPS Wykonawca jest zobowiązany prowadzić dziennik pracy, w którym zostaną odnotowane poszczególne działania oraz terminy ich realizacji wraz ze wskazaniem osób, które wykonywały w tym okresie przedmiotowe prace. Wydruk poświadczony podpisem Przedstawiciela Wykonawcy powinien być dołączony przez Wykonawcę do zgłoszenia gotowości do Odbioru Końcowego (zgodnie z warunki umowy).

3.2 Serwer NAS wraz z oprogramowaniem – 1 sztuka

Cecha, parametr	Charakterystyka (wymagania minimalne)
Typ urządzenia	Serwer NAS
Obudowa	Rack 1U
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na sierpień 2022 co najmniej 4 580 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 8 GB pamięci ECC z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA.
Dyski twarde	Sprzęt powinien być wyposażony w 4 dyski o pojemności min. 8 TB 3,5” HDD o prędkości obrotowej 5400 rpm i interfejsem SATA 6 Gb/s
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1 • 1 port eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: • 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 2.0	Min. 1x 4-liniowe gniazdo x8 gen. 3
Wentylator obudowy	Min. 3 wentylatory (40 × 40 × 20 mm)
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalny liczba wewnętrznych wolumenów: 64 • Minimalny liczba obiektów iSCSI Target: 128 • Minimalny liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji
Wirtualizacja	Obsługa VMware vSphere with VAAI, Microsoft Hyper-V®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP

Cecha, parametr	Charakterystyka (wymagania minimalne)
Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane przeglądarki	Google Chrome®, Firefox®, Microsoft Edge®, Safari® 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach
Oprogramowanie	• Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu muszą mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agent na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wpierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Montaż	• Montaż urządzenia należy przeprowadzać przy użyciu dodatkowych, przesuwnych szyn rack
Gwarancja	• Okres gwarancji 36 miesięcy, w tym jeden (1) rok na dodatkowe akcesoria montażowe w postaci przesuwnych szyn rack

3.3 Przełącznik sieciowy – 3 sztuki

Cecha, parametr	Charakterystyka (wymagania minimalne)
Porty przełącznika	minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 100/1000Base-X SFP
Port konsolowy	RJ45 (RS-232)
Szybkość przełączania	minimum 56Gb/s
Przepustowość	minimum 41Mp/s (dla pakietów 64Kb)
Bufor pakietów	minimum 1,5MB
Ramki Jumbo	minimum 12k
Tablica adresów MAC	minimum 16k
Tablica ACL	minimum 512
Tablica VLAN	minimum 4094
Taktowanie procesora	minimum 700MHz
Pamięć RAM	minimum 256MB
Zasilanie	zabudowany zasilacz 230V AC
VLAN	• Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
DHCP	• IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82,Option 37/38, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server
Spanning tree	• IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding,
Agregacja łączy	• IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group
Bezpieczeństwo	• Storm Control based on bytes, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting Radius, TACACS+
Multicast	• IGMP v1/v2/v3 snooping, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
Lista kontroli dostępu	• IP ACL, MAC ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, VLAN ACL
Diagnostyka	• VCT, DDM, Ping, Trace Route, RSPAN, Dying GASP, sFlow
Zarządzanie	• TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMPv1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, , SNTP/NTP (IPv4/IPv6), Multiple Configuration Files, Port Mirror, CPU Mirror, ULDP (like UDLD), LLDP/LLDP MED., auto provisioning
Oprogramowanie oraz wsparcie techniczne	• oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
Dodatkowe wymagania	• Przeniesienie konfiguracji z istniejących przełączników.
Gwarancja	• Okres gwarancji 24 miesiące.

3.4 UTM – 1 sztuka

Cecha, parametr	Charakterystyka (wymagania minimalne)
Obsługa sieci	• Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich, jak np. DHCP.
Zapora korporacyjna (firewall)	• Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. • Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. • Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). • Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. • Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. • Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. • Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. • Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. • Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. • Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). • System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe
Intrusion prevention system (IPS)	• System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. • Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. • Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. • Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.

	• Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. • Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. • Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. • Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. • Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV). • Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (traffic shapping)	• Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. • Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP. • Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). • Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	• Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania). • Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem. • Skaner antywirusowy ma pochodzić od europejskiego producenta. • Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. • Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	• Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). • Ochrona antyspam ma działać w oparciu o: białe/czarne listy, DNS RBL, Skaner heurystyczny. • W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.

	• Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

Wirtualne sieci prywatne (VPN)	• Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
	• Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
	  ○ PPTP VPN,
	  ○ IPSec VPN,
	  ○ SSL VPN.
	  ○ SSL VPN ma działać co najmniej w trybach tunelu i portalu.
	• Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
	• Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
	• Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
	• Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
	• Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

Filtr dostępu do stron www	• Urządzenie ma posiadać wbudowany filtr URL.
	• Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
	• Administrator ma mieć możliwość dodawania własnych kategorii URL.
	• Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
	  ○ blokowanie dostępu do adresu URL,
	  ○ zezwolenie na dostęp do adresu URL,
	  ○ blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
	• Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
	• Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
	• Filtr URL musi uwzględniać komunikację po protokole HTTPS.
	• Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
	• Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
	• Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.

Uwierzytelnianie	• Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
	  ○ lokalną bazę użytkowników (wewnętrzny LDAP),
	  ○ zewnętrzną bazę użytkowników (zewnętrzny LDAP),

	○ usługę katalogową Microsoft Active Directory. • Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. • Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: ○ SSL, ○ Radius, ○ Kerberos. • Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. • Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. • Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. • Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). • Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). • Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneliSSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Administracja łączami do internetu (ISP)	• Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). • Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: ○ równoważenie względem adresu źródłowego, ○ równoważenie względem połączenia. • Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. • Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover). • Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza. • W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). • Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	• Urządzenie ma umożliwiać statyczne trasowanie pakietów. • Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. • Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).

	• Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

Administracja urządzeniem	• Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
	• Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
	• Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
	• Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
	• Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
	• Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
	• Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
	• Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
	• Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
	• Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
	• Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
	• Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
	• System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
	• Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
	• Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
	• Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
	• Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
	  ○ manualnego eksportu do pliku w dowolnym momencie czasu,
	  ○ automatycznego eksportu do serwerów producenta lub na dedykowany serwer
	  ○ zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu

	• Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. • Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. • Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	• Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. • System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. • System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. • System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. • System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. • System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. • Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. • Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. • Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	• Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej. • Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). • Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. • Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). • Urządzenie ma posiadać usługę DNS Proxy. • Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. • Urządzenie musi mieć zaimplementowane Open API • Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. • Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP. • Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie

	wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
Gwarancja i serwis	• Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. • W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. • Urządzenie ma posiadać na czas 24 miesięcy w ramach serwisu aktualizacje do FW+IPS, VPN, filtr URL, AV, AS, Obsługa kart SD.
Parametry sprzętowe	• Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. • Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. • Liczba portów Ethernet 2,5Gbps – min. 8. • Liczba portów światłowodowych 1Gbps – min. 1. • Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. • Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps. • Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps. • Przepustowość filtrowania Antywirusowego – minimum 500Mbps. • Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps. • Maksymalna liczba tuneli VPN IPSec – minimum 100. • Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50. • Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50. • Obsługa interfejsów 802.11q (VLAN) – minimum 128 • Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę. • Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. • Urządzenie nie ma limitu na liczbę użytkowników. • Liczba reguł filtrowania – minimum 8 192. • Liczba tras statycznego routingu – minimum 512. • Liczba tras dynamicznego routingu – minimum 10 000. • Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. • Urządzenie musi być wyposażone w moduł TPM

3.5 Serwer sprzętowy – 1 sztuka

Cecha, parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa typu Tower z możliwością instalacji do 8 dysków twardych 2,5”. • Obudowa musi mieć możliwość wyposażenia w kartę umożliwiającą zdalny dostęp i zarządzenie przez sieć Internet.

Cecha, parametr	Charakterystyka (wymagania minimalne)
Płyta główna	• Płyta główna z możliwością instalacji dwóch fizycznych procesorów, • Płyta główna posiadająca minimum 16 slotów na pamięć RAM RDIMM • Płyta główna z możliwością zainstalowania do minimum 1TB pamięci RAM, • Płyta główna zaprojektowana przez producenta serwera i oznaczona trwale jego znakiem firmowym.
Procesor	• Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 279 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
Pamięć RAM	• 128GB RDIMM 5600MT/s
Kontroler RAID	• Sprzętowy kontroler dyskowy, posiadający o Min. 8GB nieulotnej pamięci cache, o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. o Wsparcie dla dysków samoszyfrujących
Dyski twarde	• Zainstalowane: o 5x dysk SAS 10K o pojemności min. 1.2TB, Hot-Plug o Możliwość zainstalowania dwóch dysków M.2 NVMe o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet BaseT
Wbudowane porty	• Minimum 4 portów USB z czego min. 1 w technologii 3.0 • 1x VGA • Możliwość rozbudowy o port RS-232
Video	• Zintegrowana karta graficzna, umożliwiająca wyświetlanie obrazu w rozdzielczości minimum 1920x1200 pikseli
Zasilanie	• redundantne zasilacze o mocy minimum 1100W klasy Titanium • 2 kable zasilające z wyczką C13-C14, min 1.8m
System operacyjny	• Dostarczony razem z serwerem system musi spełniać wymagania, jakie określono w Rodz. 3.5.1. • Zamawiający dopuszcza możliwość dostawy urządzenia razem z licencją OEM dla oferowanego systemu operacyjnego.
Diagnostyka i Bezpieczeństwo	• Zintegrowany z płytą główną moduł TPM 2.0 V3 • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

Cecha, parametr	Charakterystyka (wymagania minimalne)
	• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem • Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: o zdalny dostęp do graficznego interfejsu Web karty zarządzającej; o zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); o szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; o możliwość podmontowania zdalnych wirtualnych napędów; o wirtualną konsolę z dostępem do myszy, klawiatury; o wsparcie dla IPv6; o wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; o integracja z Active Directory; o możliwość obsługi przez dwóch administratorów jednocześnie; o wsparcie dla dynamic DNS; o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. o możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera o możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: o Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej o Przesyłanie danych telemetrycznych w czasie rzeczywistym o Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze o Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram

Cecha, parametr	Charakterystyka (wymagania minimalne)
	○ 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.

Cecha, parametr	Charakterystyka (wymagania minimalne)
Oprogramowanie do monitorowania	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z posiadaną platformą wirtualizacji VMware. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring: o ilość podłączonych oraz rozłączonych systemów o stan podłączonych urządzeń o informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów o Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia o informacje o statusie gwarancji dla poszczególnych urządzeń o informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń o informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. o Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych o Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. o Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. o Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. o Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. o Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. o Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów.

Cecha, parametr	Charakterystyka (wymagania minimalne)
	▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów o Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System

Cecha, parametr	Charakterystyka (wymagania minimalne)
	musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
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	• Zamawiający wymaga zapewnienia gwarancji Producenta zgodnie z Ofertą Wykonawcy na okres nie krótszy niż 36 miesięcy od daty odbioru. • Zamawiający wymaga możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet. • Czas reakcji – najpóźniej następny dzień roboczy po przekazaniu zgłoszenia serwisowego, co oznacza, iż czynności naprawy następują w tym terminie. • W przypadku awarii nośników danych, uszkodzony nośnik pozostaje u Zamawiającego i nie podlega wymianie na nowy będący przedmiotem świadczenia gwarancyjnego – serwisowego. • Serwis urządzenia musi być realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. • Podmiot serwisujący urządzenie musi posiadać wdrożony system zarządzania jakością oparty na normie ISO 9001:2015 lub równoważnej oraz wdrożony w organizacji System Zarządzania Bezpieczeństwem Informacji (SZBI) oparty na normie ISO-27001 lub równoważnej, a także musi posiadać autoryzacje Producenta urządzenia na świadczenie usług serwisowych / gwarancyjnych. • Zamawiający wymaga, aby dostarczony serwer znajdował się na listach typu End-of-Life / End-of-Support i posiadał możliwość odpłatnego przedłużenia gwarancji i wsparcia producenta na okres minimum 7 lat liczony od momentu odbioru przedmiotu umowy.

Cecha, parametr	Charakterystyka (wymagania minimalne)
Wymagania specyficzne, w tym dot. kryterium środowiskowego	• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla co najmniej systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022. • Urządzenie powinno być wyprodukowane przez Producenta, u którego wdrożono system zarządzania jakością oparty o normę ISO 9001:2015 lub równoważną, w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych (producent posiada certyfikat ISO 9001:2015 lub równoważny). • Urządzenie powinno być wyprodukowane przez Producenta, u którego wdrożono normę ISO 14001 lub równoważną, w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych (producent posiada certyfikat ISO 14001 lub równoważny). • Urządzenie powinno być wyprodukowane przez Producenta, u którego wdrożono normę ISO 50001 lub równoważną, w zakresie co najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych (producent posiada certyfikat ISO 50001 lub równoważny). • Oczekuje się, aby urządzenie spełniało kryteria klasyfikacji EPAET określone dla tego typu urządzenia i posiadało przyznany certyfikat klasyfikacji: brown, silver lub gold www.epeat.net

Certyfikaty, dokumenty	Do oferty należy dołączyć wymagane, następujące dokumenty potwierdzające wymagania wobec oferowanego urządzenia oraz powiązanych z nim usług / rozwiązań:
	
	• Oświadczenie Producenta potwierdzające, że serwis urządzenia będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
	• Dokumenty potwierdzający, iż Podmiot / Podmioty serwisujące urządzenie posiada / posiadają:
	  ○ wdrożony system zarządzania jakości zgodnie z normą ISO 9001:2015 lub równoważną w zakresie co, najmniej produkcji lub projektowania lub rozwoju - urządzeń lub systemów lub rozwiązań informatycznych, obejmujący także zakres zadań związanych z obsługą serwisową urządzeń lub systemów lub rozwiązań informatycznych,
	  ○ wdrożony system zarządzania bezpieczeństwem informacji zgodnie z normą ISO-27001 lub równoważą, obejmujący swoim zakresem usługi serwisowe,
	
	• Dokument potwierdzający, iż Podmiot serwisujący urządzenie posiada autoryzację Producenta na świadczenie usług serwisowych dla oferowanego urządzenia (nie dotyczy, o ile serwis urządzenia będzie realizowany bezpośrednio przez Producenta)
	• Oświadczenie Producenta serwera, że w przypadku niewywiązywania się z obowiązków gwarancyjnych przez Wykonawcę albo ogłoszenia upadłości lub likwidacji Wykonawcy, przejmie na siebie wszelkie zobowiązania związane z serwisem na zasadach określonych w Umowie, gdzie dokumenty potwierdzające tenże stan rzeczy należy przedłożyć w dniu dostawy sprzętu.

Cecha, parametr	Charakterystyka (wymagania minimalne)
	• Wydruk ze strony internetowej z datą nie wcześniejszą niż 7 dni przed składaniem ofert ze wskazaniem wiersza odpowiadającego właściwemu wynikowi testów, który potwierdzi wymagania w zakresie wydajności procesora umożliwiające osiągnięcie wyniku min. 279 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej • W przypadku kiedy oferowane urządzenie spełnia kryteria w ramach klasyfikacji EPAET, Wykonawca powinien dołączyć do Oferty wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy w przyznanej dla tego urządzenia klasyfikacji: brown, silver lub gold. Załączany do oferty wydruk musi być podpisany przez osobę reprezentującą Wykonawcę. Każdy dokument, certyfikat lub wydruk przedkładany przez Wykonawcę oraz składany razem z Ofertą celem potwierdzenia spełnienia wymagań musi być podpisany przez osobę reprezentującą Wykonawcę.

3.5.1 Oprogramowanie systemowe – licencje systemu operacyjnego

1. Licencje na serwerowy system operacyjny dla dostarczanego serwera sprzętowego muszą być przypisane do każdego rdzenia procesora fizycznego na serwerze. Udzielone licencje muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym oraz dla dwóch wirtualnych środowisk serwerowego systemu operacyjnego niezależnie od liczby rdzeni w serwerze fizycznym.
2. Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy - wymagania:
   2.1. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
   2.2. 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.
   2.3. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
   2.4. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
   2.5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
   2.6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
   2.7. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

2.8. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

2.9. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.

2.10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

2.11. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

2.12. Graficzny interfejs użytkownika.

2.13. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.

2.14. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

2.15. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

2.16. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

2.17. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).

2.18. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

2.19. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.

2.20. 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.

2.21. Zdalna dystrybucja oprogramowania na stacje robocze.

2.22. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.

2.23. PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

2.23.1. dystrybucję certyfikatów poprzez http,

2.23.2. konsolidację CA dla wielu lasów domeny,

2.24. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.

2.25. Szyfrowanie plików i folderów.

2.26. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

2.27. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

2.28. Serwis udostępniania stron WWW.

2.29. Wsparcie dla protokołu IP w wersji 6 (IPv6).

2.30. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

2.31. 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.

2.32. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

2.33. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

2.34. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

2.35. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF

3. Dla oferowanego produktu musi być dostępny na rynku usług IT zorganizowany system certyfikowanych szkoleń oraz muszą być dostępne materiały edukacyjne w języku polskim.

4. Liczba licencji oferowanego systemu musi być tak dobrana, aby:

4.1. przy oferowanych w serwerze procesorach umożliwić uruchomienie 4 maszyn wirtualnych,

4.2. zapewnić (o ile ogólne warunki licencji Producenta taki wymóg nakładają) - licencje dostępowe dla użytkowników w liczbie 30 sztuk.

5. Oprogramowanie musi być dostarczone w najwyższej wersji dostępnej w ofercie Producenta oprogramowania.

3.6 UPS – 1 sztuka

Cecha, parametr	Charakterystyka (wymagania minimalne)
Parametry wejściowe	• Napięcie: 230 V (1-fazowe), tolerancja 166 - 288V AC bez zmniejszenia mocy. • Częstotliwość: 50/60 Hz, tolerancja 40-70 Hz • Ochrona przeciwudarowa: 624J
Parametry wyjściowe	• Napięcie (czysty przebieg sinusoidalny): 230V • Częstotliwość: 50 Hz (lub 60Hz) • Współczynnik mocy 1 • Przeciążalność: 151% - 200% przez 2 s, 125% - 150% przez 50 s, 105% - 125% przez 60 s. • Sprawność w trybie liniowym 93%, eco 98%
Bateria	• Hermetyczne, bezobsługowe akumulatory typu VRLA AGM muszą zapewnić czas podtrzymania minimum 11 minut dla obciążenia 700W. • Czas ładowania do 90% pojemności 3h

Cecha, parametr	Charakterystyka (wymagania minimalne)
Zasilacz UPS musi być zgodny z Normami	• Parametry i topologia: IEC/EN 62040-3 (VFI-SS-111) • Bezpieczeństwo: IEC62040-1:2008 version, GS mark; CE: UL1778 5th Edition and CSA 22.2 No 107.1 • Kompatybilność elektromagnetyczna EN 62040-2:2006; EN 61000-3-3:2013; EN 61000-3-3:2013 • ESD: EN 61000-4-5; ANSI C62.41 Kategoria B • Podatność na wyemitowane zakłócenia: CISPR22 Class A (RFI)/ FCC Part 15 (Class A) • Stopień ochrony: IP20
Zasilacz UPS musi spełniać parametry środowiskowe, co najmniej takie jak	• Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie temperatur od 15 °C do 25 °C) • Wilgotność: do 95 % bez kondensacji • Głośność: <46 db w trybie normalnym z odległości 1m • Wymiary zasilacza UPS nie mogą być większe niż: szer. x głęb. x wys. (mm) 400 x 430 x 85 Waga: 16,5kg • Sterowanie zdalne, komunikacja • Zasilacz UPS musi być wyposażony w slot na kartę SNMP, wbudowany port EPO oraz gniazda USB, terminal do uziemienia. • Kolorowy ciekłokrystaliczny wyświetlacz graficzny
UPS wyposażony w kartę zarządzającą	• Zapewnia dostęp internetowy do zainstalowanych urządzeń za pośrednictwem popularnych przeglądarek internetowych Microsoft Internet Explorer, Mozilla Firefox, Google Chrome i Safari. • Zapewnia powiadomienia alarmowe za pośrednictwem poczty e-mail i wiadomości tekstowych. • Obsługuje monitorowanie środowiska za pomocą czujników Liebert SN do pomiaru temperatury, wilgotności, wykrywania wycieków, drzwi i złącz styków. • Obsługuje protokoły stron trzecich dla aplikacji do zarządzania budynkiem i siecią dla statusu i alarmów za pośrednictwem SNMP i Modbus TCP. • Obsługuje szybki transfer plików do zarządzanych urządzeń w celu aktualizacji oprogramowania układowego i konfiguracji przez klienta. • Opcje obsługi uwierzytelniania SNMP v3 (brak, MD5 lub SHA), obsługa prywatności (brak, DES lub AES) i pułapki SNMP.
Gwarancja	Okres gwarancji 24 miesiące