**ZPI.271.51.2025 Załącznik nr 1**

###### **FORMULARZ OFERTY W TRYBIE PODSTAWOWYM BEZ NEGOCJACJI**

###### **DLA ZAMÓWIENIA:**

**„DOSTAWA SPRZĘTU SERWEROWEGO I OPROGRAMOWANIA W RAMACH PROJEKTU „CYBERBEZPIECZNY SAMORZĄD”**

Nr referencyjny nadany sprawie przez Zamawiającego: **ZPI.271.51.2025**

**1. ZAMAWIAJĄCY:**

**Gmina Zelów tel.: (0-44) 634 10 00,**

reprezentowana przez

**p. Kamila Świtałę – Burmistrza Zelowa**

**Adres Urzędu Miejskiego:**

**ul. Żeromskiego 23**

**97-425 Zelów**

**2. WYKONAWCA:**

Pełna nazwa wykonawcy: .........................................................................................................................

...................................................................................................................................................................

Adres (kod, miejscowość, ulica): ...............................................................................................................

NIP: ...........................................................

Regon: ........................................................

Tel/fax, ……………………………………………………

e-mail: ........................................................

Adres skrzynki ePUAP: …………………………………………………………………………………………………………………………

Osoba upoważniona do kontaktu z zamawiającym: ………………………...........................

1. Ja (my) niżej podpisany(i) oświadczam(y), że:
   1. zapoznałem (zapoznaliśmy) się z treścią SWZ dla niniejszego zamówienia i nie wnoszę do niej uwag,
   2. gwarantuję (gwarantujemy) wykonanie całości niniejszego zamówienia zgodnie z treścią: SWZ, wyjaśnieniami do SWZ oraz jej modyfikacji,
   3. celem porównania ofert Wykonawca złoży ofertę cenową wedle poniższego wzoru:
2. **Serwer nadmiarowy – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |  |
| **Obudowa** | * Obudowa Rack o wysokości max 1U * Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serweraw tym adres IP karty zarządzającej * Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| **Procesor** | * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| **RAM** | * 8x 32GB DDR5 RDIMM 5600MT/s, |  |
| **Dyski twarde** | * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1. |  |
| **Gniazda PCI** | * Trzy sloty PCIe LP |  |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  |
| **Wbudowane porty** | * 4 porty USB w tym:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * 2 port VGA z czego jeden z przodu obudowy * Możliwość rozbudowy o port RS232 |  |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| **Zasilacze** | * Redundantne, Hot-Plug min. 700W klasy Titanium |  |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |  |
| **System operacyjny/dodatkowe oprogramowanie** | * Windows Server 2025 Standard – licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie 6 maszyn wirtualnych |  |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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 * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 V3 * 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. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń. |  |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej   + 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, SNMP, IPMI2.0, VLAN tagging, SSH   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer   + integracja z Active Directory   + możliwość obsługi przez ośmiu administratorów jednocześnie   + Wsparcie dla automatycznej rejestracji DNS   + wsparcie dla LLDP   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej   + możliwość podłączenia lokalnego poprzez złącze RS-232.   + możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.   + Monitorowanie zużycia dysków SSD   + możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,   + Automatyczne zgłaszanie alertów do centrum serwisowego producenta   + Automatyczne update firmware dla wszystkich komponentów serwera   + Możliwość przywrócenia poprzednich wersji firmware   + Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON   + Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych   + Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.   + Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera   + Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.   Możliwość rozszerzenia funkcjonalności karty o:   * + możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch   + kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania   + Automatyczne odświeżanie certyfikatów SSL   + możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej   + możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień   + możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera   + możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer   + możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe   + monitorowanie przepływu powietrza na bieżąco (w CFM) |  |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji 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   + 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     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + 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,   + 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   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + 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.   + 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) * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |  |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, oraz ISO-14001 **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Serwer musi posiadać deklaracja CE. **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu w formie dokumentacji technicznej lub oświadczenia producenta serwera.** * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu może być w szczególności wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej EPEAT Silver. Zamawiający, zgodnie z art. 104 ustawy Prawo zamówień publicznych, dopuszcza również inne odpowiednie środki dowodowe, w szczególności równoważne oznakowania środowiskowe lub dokumenty (certyfikaty, raporty, oświadczenia producenta) potwierdzające spełnienie wymagań równoważnych - **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025. |  |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * 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 z zakresu wdrażanej technologii na okres min. 36 miesięcy. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |  |

**Wymagania w zakresie instalacji i wdrożenia serwera nadmiarowego:**

Zamawiający wymaga:

1. Instalacji serwera we wskazanej serwerowni i szafie rack.
2. Podłączenia serwera do wskazanych segmentów sieci LAN, w tym zapewnienie komunikacji z klastrem serwerów wirtualizacyjnych oraz komunikacji iSCSI.
3. Instalacji systemu operacyjnego na posiadanych przez Zamawiającego serwerach oraz skonfigurowanie funkcji wysokiej dostępności.
4. Dołączenia serwera do wskazanego przez Zamawiającego klastra wirtualizacyjnego.
5. Wykonania migracji maszyn wirtualnych uruchomionych na klastrze wirtualizacyjnym na wskazane serwery, potwierdzenie poprawności pracy.
6. **Serwer backupu (serwer izolowanych kopii zapasowych) – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |  |
| **Obudowa** | * Obudowa Rack o wysokości 2U * 12 wnęk na dyski 3.5” * Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serweraw tym adres IP karty zarządzającej * Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| **Procesor** | * Zainstalowany jeden procesor min. 12-rdzeniowy, min. 2.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 216 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| **RAM** | * 2x 16GB DDR5 RDIMM 5600MT/s, |  |
| **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający   + Min. 8GB nieulotnej pamięci cache,   + Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.   + Wsparcie dla dysków samoszyfrujących |  |
| **Dyski twarde** | * Zainstalowane:   + 7x dysk SAS o pojemności min. 16TB, Hot-Plug * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |  |
| **Gniazda PCI** | * Cztery sloty PCIe |  |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  |
| **Wbudowane porty** | * 4 porty USB w tym min:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * 2 port VGA z czego jeden z przodu obudwy * Możliwość rozbudowy o port RS232 |  |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |  |
| **Wentylatory** | * Redundantne, Hot-Plug |  |
| **Zasilacze** | * Redundantne, Hot-Plug min. 700W klasy Titanium |  |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |  |
| **System operacyjny/dodatkowe oprogramowanie** | * Windows Server 2025 Standard w ilości niezbędnej do poprawnego zalicencjonowania wszystkich rdzeni procesorów oferowanego serwera |  |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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 * 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. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń. |  |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej   + 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 SNMP; IPMI2.0, VLAN tagging, SSH   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer   + integracja z Active Directory   + możliwość obsługi przez ośmiu administratorów jednocześnie   + Wsparcie dla automatycznej rejestracji DNS   + wsparcie dla LLDP   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej   + możliwość podłączenia lokalnego poprzez złącze RS-232.   + możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.   + Monitorowanie zużycia dysków SSD   + możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,   + Automatyczne zgłaszanie alertów do centrum serwisowego producenta   + Automatyczne update firmware dla wszystkich komponentów serwera   + Możliwość przywrócenia poprzednich wersji firmware   + Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON   + Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych   + Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.   + Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera   + Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.   Możliwość rozszerzenia funkcjonalności karty o:   * + możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch   + kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania   + Automatyczne odświeżanie certyfikatów SSL   + możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej   + możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień   + możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera   + możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer   + możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe   + monitorowanie przepływu powietrza na bieżąco (w CFM) |  |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| **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:   + 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   + 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     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + 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,   + 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   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + 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.   + 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) * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |  |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001 **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Serwer musi posiadać deklaracja CE. **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu w formie dokumentacji technicznej lub oświadczenie producenta serwera.** * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu może być w szczególności wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej EPEAT Silver. Zamawiający, zgodnie z art. 104 ustawy Prawo zamówień publicznych, dopuszcza również inne odpowiednie środki dowodowe, w szczególności równoważne oznakowania środowiskowe lub dokumenty (certyfikaty, raporty, oświadczenia producenta) potwierdzające spełnienie wymagań równoważnych - **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025. |  |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * 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 z zakresu wdrażanej technologii na okres min. 36 miesięcy. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie Zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty w formie oświadczenia producenta serwera. |  |

**Wymagania w zakresie instalacji i wdrożenia serwera wraz z systemem do składowania kopii zapasowych:**

Zamawiający wymaga:

1. Instalacji sprzętu we wskazanej serwerowni i szafie rack.
2. Instalacji i konfiguracji – dostarczonego wraz odpowiednimi urządzeniami – systemu operacyjnego Microsoft Windows Server na serwerze, podłączenie serwera do wskazanego przez Zamawiającego segmentu sieci.
3. Instalacja oprogramowania do wykonywania kopii zapasowych na odpowiednim serwerze.
4. Skonfigurowania dostarczonego serwera jako serwera kopii zapasowych, w tym zdefiniowanie zadań i harmonogramów kopii zapasowych oraz wykonanie testowego odtwarzania danych dla wskazanych przez Zamawiającego zasobów (serwery fizyczne, wirtualne – w ilości zgodnej z wymaganym licencjonowaniem).

**3. Serwer kopii zapasowych maszyn wirtualnych – 1 szt.**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |  |
| **Obudowa** | * Obudowa Rack o wysokości max 1U * Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serweraw tym adres IP karty zarządzającej * Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. |  |
| **Płyta główna** | * Płyta główna z możliwością zainstalowania do dwóch procesorów. * Obsługa procesorów 32 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. * Płyta główna powinna obsługiwać do 1TB pamięci RAM. |  |
| **Chipset** | * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |  |
| **Procesor** | * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |  |
| **RAM** | * 8x 32GB DDR5 RDIMM 5600MT/s, |  |
| **Dyski twarde** | * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1. |  |
| **Gniazda PCI** | * Trzy sloty PCIe LP |  |
| **Interfejsy sieciowe/FC/SAS** | * Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |  |
| **Wbudowane porty** | * 4 porty USB w tym:   + 1 port USB 3.0 z tyłu obudowy,   + 1 port micro USB z przodu obudowy * 2 port VGA z czego jeden z przodu obudowy * Możliwość rozbudowy o port RS232 |  |
| **Video** | * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| **Zasilacze** | * Redundantne, Hot-Plug min. 700W klasy Titanium |  |
| **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |  |
| **System operacyjny/dodatkowe oprogramowanie** | * Windows Server 2025 Standard – licencja dobrana tak, aby pry oferowanych procesorach umożliwić uruchomienie 6 maszyn wirtualnych |  |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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 * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 V3 * 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. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń. |  |
| **Karta Zarządzania** | * Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   + zdalny dostęp do graficznego interfejsu Web karty zarządzającej   + 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, SNMP, IPMI2.0, VLAN tagging, SSH   + możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.   + możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer   + integracja z Active Directory   + możliwość obsługi przez ośmiu administratorów jednocześnie   + Wsparcie dla automatycznej rejestracji DNS   + wsparcie dla LLDP   + wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej   + możliwość podłączenia lokalnego poprzez złącze RS-232.   + możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy.   + Monitorowanie zużycia dysków SSD   + możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi,   + Automatyczne zgłaszanie alertów do centrum serwisowego producenta   + Automatyczne update firmware dla wszystkich komponentów serwera   + Możliwość przywrócenia poprzednich wersji firmware   + Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON   + Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych   + Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.   + Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera   + Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne  - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.   Możliwość rozszerzenia funkcjonalności karty o:   * + możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch   + kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania   + Automatyczne odświeżanie certyfikatów SSL   + możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej   + możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień   + możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera   + możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer   + możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe   + monitorowanie przepływu powietrza na bieżąco (w CFM) |  |
| **Oprogramowanie do zarządzania** | * Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:   + Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych   + integracja z Active Directory   + Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta   + Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish   + Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram   + Szczegółowy opis wykrytych systemów oraz ich komponentów   + Możliwość eksportu raportu do CSV, HTML, XLS, PDF   + Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.   + Grupowanie urządzeń w oparciu o kryteria użytkownika   + Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji   + Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach   + Szybki podgląd stanu środowiska   + Podsumowanie stanu dla każdego urządzenia   + Szczegółowy status urządzenia/elementu/komponentu   + Generowanie alertów przy zmianie stanu urządzenia.   + Filtry raportów umożliwiające podgląd najważniejszych zdarzeń   + Integracja z service desk producenta dostarczonej platformy sprzętowej   + Możliwość przejęcia zdalnego pulpitu   + Możliwość podmontowania wirtualnego napędu   + Kreator umożliwiający dostosowanie akcji dla wybranych alertów   + Możliwość importu plików MIB   + Przesyłanie alertów „as-is” do innych konsol firm trzecich   + Możliwość definiowania ról administratorów   + Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów   + Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)   + Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta   + Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów   + Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.   + Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.   + Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile   + Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.   + Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.   + Zdalne uruchamianie diagnostyki serwera.   + Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.   + Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. |  |
| **Oprogramowanie do monitorowania** | Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji 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   + 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     - Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. * Aktualizacja firmware   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania   + możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania * Raporty   + 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,   + 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   + Generowanie raportów do plików CSV i PDF * Cyberbezpieczeństwo   + 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.   + 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) * Wirtualny asystent   + Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; * Możliwość rozszerzenia funkcjonalności   + Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. * Inne   + Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android |  |
| **Certyfikaty** | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Serwer musi posiadać deklaracja CE. **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu w formie dokumentacji technicznej lub oświadczenia producenta serwera.** * Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu może być w szczególności wydruk ze strony internetowej [www.epeat.net](http://www.epeat.net) potwierdzający spełnienie normy co najmniej EPEAT Silver. Zamawiający, zgodnie z art. 104 ustawy Prawo zamówień publicznych, dopuszcza również inne odpowiednie środki dowodowe, w szczególności równoważne oznakowania środowiskowe lub dokumenty (certyfikaty, raporty, oświadczenia producenta) potwierdzające spełnienie wymagań równoważnych - **Wykonawca złoży wraz z ofertą dokument potwierdzający spełnianie wymogu.** * Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022, Microsoft Windows Server 2025. |  |
| **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim. * 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 z zakresu wdrażanej technologii na okres min. 36 miesięcy. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki. * Naprawa ma się odbyć w siedzibie Zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. * Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. * Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   + Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.   + Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.   + Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.   + Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.   + Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. * Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |  |

**Wymagania w zakresie instalacji i wdrożenia serwera kopii zapasowych maszyn wirtualnych :**

Zamawiający wymaga:

1. Instalacji serwera we wskazanej serwerowni i szafie rack.
2. Podłączenia serwera do wskazanych segmentów sieci LAN, w tym zapewnienie komunikacji z klastrem serwerów wirtualizacyjnych oraz komunikacji iSCSI.
3. Instalacji systemu operacyjnego na posiadanych przez Zamawiającego serwerach oraz skonfigurowanie funkcji wysokiej dostępności.

**4. Macierz dyskowa – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Element konfiguracji/cecha/funkcjonalność** | **Wymagania minimalne** |  |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 12 dysków 3.5” |  |
| Przestrzeń dyskowa | Zainstalowane:  6x dysk SSD SAS o pojemności min. 1.92TB, Hot-Plug 6x dysk SAS o pojemności min. 16TB, Hot-Plug |  |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 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.  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 5 lat. |  |
| 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 rozwiązaniem. |  |
| Interfejsy | Macierz musi posiadać, co najmniej 8 portów 10Gb 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 (wymagana obsługa standardu T10 SCSI UNMAP).  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.  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.  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). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające spełnienie powyższych zaleceń. |  |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym  producenta. Wykonawca wraz z ofertą przedstawi oświadczenie producenta oferowanej macierzy, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.  Wymagane są wraz z ofertą dokumenty: Deklaracja zgodności CE oraz poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. |  |
| Warunki gwarancji | Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 36 miesięcy.  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.  Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.  Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:   * Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. * Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. * Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. * Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. * Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.   Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |  |

**Zamawiający wymaga:**

1. Instalacji sprzętu we wskazanej serwerowni i szafie rack.
2. Skonfigurowania wydzielonego segmentu sieci (VLAN) na potrzeby komunikacji iSCSI
3. Podłączenia macierzy dyskowej do wskazanego segmentu sieci iSCSI.
4. Skonfigurowania woluminów dyskowych i przypisanie ich do serwerów klastra wirtualizacyjnego Hyper-V.
5. Rekonfiguracji zależnych urządzeń/systemów.
6. Migracji danych na woluminy dyskowe nowej macierzy

**5. Urządzenie archiwizacyjne taśmowe jednonapędowe – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Minimalne wymagania** |  |
| **Obudowa i pojemność** | Wysokość maksymalnie 1U do instalacji w szafie Rack.  Co najmniej 8 slotów przeznaczonych na zestaw taśm. |  |
| **Połączenie** | Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów. |  |
| **Napęd** | Wyposażony w co najmniej 1 sztukę napędu SAS LTO 8.  W komplecie:   * kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m * 10 x taśma LTO8 * 1x taśma czyszcząca |  |
| **Gwarancja** | * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres min. 36 miesięcy. * Naprawa ma się odbyć w siedzibie Zamawiającego, chyba, że Zamawiający dla danej naprawy zgodzi się na inną formę. |  |

**6. Serwer plików NAS – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Opis minimalnych wymagań technicznych** |  |
| Typ | Sieciowy serwer plików NAS |  |
| Obudowa | Rack |  |
| Procesor | 4-rdzeniowy 64-bitowt procesor o taktowaniu min. 1.7 GHz |  |
| Pamięć RAM | 4 GB UDIMM DDR4 z możliwością rozszerzenia do 16GB RAM |  |
| Wewnętrzna pamięć masowa | 8 dysków 3,5-calowe SATA 6 Gb/s, 3 Gb/s  Zamawiający wymaga dostarczenia zestawu z 4 dyskami o pojemności 4 TB każdy |  |
| Kompatybilność dysków | 3,5-calowe wnęki: 3,5-calowe dyski twarde SATA 2,5-calowe dyski twarde SATA 2,5-calowe dyski SSD SATA |  |
| Interfejsy sieciowe | Min. 2 x 2,5 Gigabit Ethernet (2,5G/1G/100M/10M), 2 x 10GbE SFP+ |  |
| Złącza dodatkowe | Min. 2 porty typu A USB 3.2, |  |
| Gniazdo M.2 | Opcjonalne, poprzez kartę PCIe |  |
| Szyfrowanie | AES 256bit |  |
| Zasilacz | 250 W PSU, 100–240 V |  |
| Gwarancja | Minimum 36 miesięcy gwarancji |  |
| Dokumentacja użytkownika | Zamawiający wymaga dokumentacji w języku polskim lub angielskim, w formie elektronicznej. |  |

**Zamawiający wymaga:**

Skonfigurowania dostarczonego serwera jako serwera kopii zapasowych, w tym zdefiniowanie zadań i harmonogramów kopii zapasowych oraz wykonanie testowego odtwarzania danych dla wskazanych przez Zamawiającego zasobów (serwery fizyczne, wirtualne).

1. **Oprogramowanie do tworzenia kopii zapasowych**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Opis minimalnych wymagań technicznych** |  |
| Wymagania ogólne | Dostarczone oprogramowanie musi umożliwiać wykonywanie kopii zapasowych z minimum 20 maszyn wirtualnych pracujących w środowisku wirtualizacyjnym (składającym się z trzech serwerów wirtualizacyjnych) lub 20 serwerów fizycznych, każdy z własną instancją systemu operacyjnego.  • Dostarczone oprogramowanie musi być objęte wsparciem technicznym producenta przez okres 12 miesięcy.  • Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5.  • Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.  • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. |  |
| **Wymagania funkcjonalne** | * Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej   • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków  • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji  • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.  • Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.  • Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.  • Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.  • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania  • Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time)  • Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu  • Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API  • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji  • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji  • Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania  • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.  • Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej  • Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora)  • Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)  • Oprogramowanie musi posiadać integracje z systemami typu SIEM  • Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. |  |
| **Wymagania RPO** | * Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej   • Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.  • Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru  • Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.  • Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.  • Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).  • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)  • Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.  • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.  • Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.  • Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.  • Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.  • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik  • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)  • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |  |
| **Wymagania RTO** | * Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.   • Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)  • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami  • Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre  • Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.  • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków  • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.  • Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików  • Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.  • Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell  • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM  • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.  • Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.  • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.  • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.  • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.  • Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.  • Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.  • Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji  • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN  • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle  • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI  • Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2  • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |  |
| **Ograniczenie ryzyka** | * Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)   • Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.  • Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem  • Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.  • Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware  • Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania  • Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków  • Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |  |
| **Środowiska fizyczne** | * Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego   • Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych  • Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE  • Rozwiązanie musi wspierać system operacyjny macOS  • Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix  • Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą)  • Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster  • Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów  • Rozwiązanie musi wspierać backup podłączonych dysków USB  • Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym  • Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury)  • Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone  • Rozwiązanie musi wspierać kontrolę pasma sieciowego  • Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych  • Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN  • Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft  • Rozwiązanie musi wspierać technologię BitLocker  • Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania  • Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych  • Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych  • Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.  • Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform  • Rozwiązanie musi wspierać szyfrowanie  • Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne  • Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego  • Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej  • Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |  |
| **Monitoring** | * System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich   • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie  • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.  • System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter  • System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn  • System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel  • System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk  • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora  • System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów  • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)  • System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna  • System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego  • System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta  • System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.  • System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.  • System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware  • System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4 |  |
| **Raportowanie** | * System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie   • System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.  • System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.  • System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V  • System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF  • System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc  • System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach  • System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów  • System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych  • System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych  • System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury  • System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta  • System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.  • System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.  • System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware  • System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)  • System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |  |

**Wymagania w zakresie instalacji i wdrożenia oprogramowania do wykonywania kopii zapasowych**

* Instalacji oprogramowania do wykonywania kopii zapasowych na serwerze.
* Skonfigurowania wskazanego serwera jako serwera kopii zapasowych, w tym zdefiniowanie zadań i harmonogramów kopii zapasowych oraz wykonanie testowego odtwarzania danych dla wskazanych przez Zamawiającego zasobów (serwery fizyczne, wirtualne – w ilości zgodnej z wymaganym licencjonowaniem).

1. **Przełączniki zarządzalne TYP 1 – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Opis minimalnych wymagań technicznych** |  |
| Typ | * Ilość portów: 8 portów SFP+ oraz 8 portów 10GBaseT niezależne * Chłodzenie od przedu do tyłu obudowy * Tablica MAC min. 16K * Tablica ARP/NDP min. 888 * Bufor 16Mb * MTBF min. 264 miesiące * Wydajność min. 238 Mp/s * Przepustowość min. 320 Gb/s * Port USB * Port miniUSB * Port zarządzania Out-of-band; * Web GUI * HTTPs * CLI * Telnet * SSH * SNMP * MIB RSPAN * Radius * TACACS+ * DiffServ * Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram * IPv4/IPv6 Multicast filtering * IGMPv3 MLDv2 Snooping * ASM & SSM * IGMPv1,v2 Querier * Auto-VoIP * Auto-iSCSI * Policy-based routing (PBR) * LLDP-MED * Spanning Tree * Green Ethernet * STP * MTP * RSTP * PV(R)STP * BPDU/STRG Root Guard * EEE (802.3az) * GVRP/GMRP * Q in Q, * Private VLAN * DOT1X * MAB * Captive Portal * DHCP Snooping * Dynamic ARP * Inspection * IP Source Guard * CPU min 800 Mhz * Min 1GB RAM * Min 256MB Flash * Min ilość obsługiwanych VLAN 4K * DHCP Server min 2K rezerwacji * sFlow * Minimalna ilość przełączników w stosie: 8 * Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s * Możliwość łączenia w stos za pomocą interfejsów 10Gb/s * Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh * Non-stop forwarding (NSF) * Distributed Link Aggregation (LAGs across the stack) * Ilość interfejsów IP 128 * Double VLAN Tagging (QoQ) * Yes * PIM-DM (Multicast Routing - dense mode) * PIM-DM (IPv6) * PIM-SM (Multicast Routing - sparse mode) * PIM-SM (IPv6) * RIPv1 * RIPv2 * OSPFv2 * RFC 2328 * RFC 1583 * OSPFv3 * OSPFv2 min. sąsiadów 400 * OSPFv3 min. sąsiadów 400 * OSPFv3 min. sąsiadów na interfejs 100 * UDLD * LLPF * DHCPv6 Snooping * wysyłanie alertów na email * MMRP * Ilość ACL min. 100 * Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu |  |

Minimalne wymagania sprzętowe:

**Gwarancja**

Wymaga się aby urządzenie było objęte gwarancją producenta przez min. 36 miesięcy, realizowaną w systemie door-to-door przez serwis. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

**Wymagania Zamawiającego w zakresie wdrożenia zarządzalnych przełączników sieciowych TYP 1:**

1. Instalacja dostarczonych przełączników w wskazanych przez Zamawiającego punktach dystrybucji okablowania.
2. Konfiguracja funkcjonalności warstwy II: VLAN, Spanning Tree, agregacji łączy.
3. Konfiguracja zarządzania (SSH, HTTPS, SNMP).
4. Konfiguracja logowania zdarzeń.
5. **Przełączniki zarządzalne TYP 2 – 45 sztuk**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Opis minimalnych wymagań technicznych** |  |
| Typ przełącznika: zarządzalny | * Typ i liczba portów - 8x 10/100/1000 RJ45, 2x Gigabit copper/SFP combo * Bez wentylatorów (fanless) * Zasilanie przez zewnętrzny zasilacz AC 230V * Obudowa 1U, desktop |  |
| Pozostałe parametry techniczne: | Zarządzenie energią:  · Obsługa standardu Energy Efficient Ethernet (IEEE 802.3az)  · Możliwość wyłączenia diod LED w celu oszczędzania energii  · Parametry wydajnościowe:  · Przepustowość przełącznika (Switching capacity): 20 Gbps  · Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3:  14.88 Mpps  · Pamięć DRAM – 1GB  · Pamięć Flash – 512MB  · Obsługa 4000 VLAN  · 16000 adresów MAC  · Wire-speed IPv4 routing – 990 tras statycznych, 128 interfejsów IP  · Obsługa ramek jumbo – do 9000 bajtów  · 2000 IGMP group  · 8 połączeń zagregowanych typu „port channel” per grupa, obsługa 8 grup  · Ilość wpisów w listach kontroli dostępu Security ACL – 1000  · Obsługa protokołu SNTP  · Obsługa IGMPv1/2/3 i MLDv1/2 Snooping  · Obsługa routingu dynamicznego z wykorzystaniem protokołu RIPv2  · Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:  · IEEE 802.1w Rapid Spanning Tree  · IEEE 802.1s Multi-Instance Spanning Tree - obsługa 8 instancji  · Per-VLAN Rapid Spanning Tree (PVRST+) - obsługa 126 instancji  · Obsługa protokołu LLDP i LLDP-MED  · Obsługa translacji sieci VLAN 1:1 (mapowanie 1 do 1 z translacją identyfikatora sieci klienckiej VLAN (C-VLAN) na interfejsie brzegowym na identyfikator sieci VLAN używanej w sieci operatora (S-VLAN))  · Obsługa Q-in-Q oraz Selective Q-in-Q  · Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad (LACP)  · Realizacja funkcji UDLD w celu wykrywania jednokierunkowych połączeń spowodowanych uszkodzeniami linków  · Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego  · Możliwość uruchomienia funkcji serwera DHCP wraz z obsługą wielu puli adresowych i zakresów adresowych  · Obsługa opcji DHCP: opcje 12, 59, 60, 66, 67, 82, 125, 129 oraz 150  · Realizacja funkcji DHCP Relay wraz z obsługą funkcji DHCP opcja 82  · Możliwość konfiguracji interfejsów Layer 3 dla:  · Portów fizycznych przełącznika  · Interfejsów zagregowanych przy pomocy Link Aggregation (LAG)  · Interfejsów VLAN  · Interfejsów loopback  · Obsługa UDP Relay (User Datagram Protocol Relay)   * Obsługa funkcjonalności umożliwiającej powiadomienie przez przełącznik, z wykorzystaniem notyfikacji SYSLOG lub SNMP, nadrzędnego systemu monitorowania o wykryciu zaniku zasilania. Funkcjonalność umożliwia wysłanie komunikatu o zaniku zasilania przed całkowitą utratą zasilania przez urządzenie.   · Mechanizmy związane z bezpieczeństwem sieci:  · Trzy poziomy dostępu administracyjnego poprzez konsolę (3 poziomy uprawnień)  · Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN  · Obsługa różnych trybów uwierzytelniania 802.1x na porcie:  · Tryb pojedynczego hosta, w którym tylko jeden host może być podłączony do portu;  · Tryb wielu hostów, w którym port jest uwierzytelniony wówczas gdyż podłączony jest do niego co najmniej jeden uwierzytelniony klient;  · Tryb wielu sesji, w którym status uwierzytelnienia nie jest przypisany do portu a wyłącznie do każdego z klientów podłączonych do portu;  · Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X  · Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC  · Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X  · Realizacja funkcji Change of Authorization (CoA) realizującej dynamiczną zmianę uwierzytelnienia dla sesji użytkownika podłączonego do danego portu  · Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard  · Obsługa funkcji IPv6 RA Guard, ND Inspection, DHCPv6 Guard  · Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+  · Obsługa Private VLAN z możliwością definicji portów promiscuous, isolated i community  · Obsługa list kontroli dostępu (ACL) – możliwość filtracji ruchu w oparciu adresy MAC (source/destination), VLAN ID, adresy IPv4 lub IPv6, TCP/UDP source/destination port, 802.1p priorty, TCP flag. Obsługa czasowych list ACL  · Obsługa mechanizmów zapewaniających bezpieczną pracę urządzenia w tym ochronę procesów: Executable Space Protection [X-Space], Address Space Layout Randomization [ASLR], Built-In Object Size Checking [BOSC]  · Bezpieczny proces bootowania urządzenia  · Suplikant 802.1X - przełącznik można skonfigurować tak, aby działał jako suplikant do innego przełącznika  · Mechanizmy związane z zapewnieniem jakości usług w sieci:  · Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi  · Implementacja algorytmu Weighted Round-Robin (WRR) dla obsługi kolejek  · Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)  · Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP  · Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi  · Kontrola sztormów dla ruchu broadcast/multicast/unicast  · Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP  · Optymalizacja ruchu iSCSI - mechanizm nadawania priorytetu ruchowi iSCSI w stosunku do innych typów ruchu  · Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN i RSPAN  · Obsługa funkcji port mirroring polegającej na kopiowaniu ruchu z danego portu i przesłanie go do innego portu. Obsługa do 8 portów źródłowych kopiujących swój ruch do jednego portu docelowego (monitorującego)  · Obsługa funkcji VLAN mirroring polegającej na kopiowaniu ruchu z danej sieci VLAN i przesłanie go do innego portu. Obsługa do 8 źródłowych sieci VLAN kopiujących swój ruch do jednego portu docelowego (monitorującego)  · Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)  · Obsługa protokołu sFlow  · Obsługa standardów:  · IEEE 802.3 10BASE-T Ethernet,  · IEEE 802.3u 100BASE-TX Fast Ethernet,  · IEEE 802.3ab 1000BASE-T Gigabit Ethernet,  · IEEE 802.3ad Link Aggregation Control Protocol,  · IEEE 802.3z Gigabit Ethernet,  · IEEE 802.3ae 10 Gbps Ethernet over fiber for LAN,  · IEEE 802.3an 10GBASE-T 10 Gbps Ethernet over copper twisted pair cable,  · IEEE 802.3x Flow Control,  · IEEE 802.1D (STP, GARP, and GVRP),  · IEEE 802.1Q/p VLAN,  · IEEE 802.1w Rapid STP,  · IEEE 802.1s Multiple STP,  · IEEE 802.1X Port Access Authentication,  · IEEE 802.3af,  · IEEE 802.3at,  · IEEE 802.1AB Link Layer Discovery Protocol,  · IEEE 802.3az Energy Efficient Ethernet,  · RFC 768,RFC 783,RFC 791,RFC 792,RFC 793,RFC 813,RFC 826,RFC 879,RFC 896,RFC 854,RFC 855,RFC 856,RFC 858,RFC 894,RFC 919,RFC 920,RFC 922,RFC 950,RFC 951, RFC 1042,RFC 1071,RFC 1123,RFC 1141,RFC 1155,RFC 1157, RFC 1213,RFC 1215,RFC 1286,RFC 1350,RFC 1442,RFC1451,RFC1493,RFC 1533,RFC 1541,RFC 1542,RFC 1573, RFC 1624,RFC 1643, RFC 1700, RFC 1757, RFC 1867, RFC 1907, RFC 2011, RFC 2012, RFC 2013, RFC 2030, RFC 2131, RFC 2132, RFC 2233, RFC 2576, RFC 2616,RFC 2618, RFC 2665, RFC 2666, RFC 2674, RFC 2737, RFC 2819, RFC 2863, RFC 3164, RFC 3176, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 4330  · Zarządzanie:  · Port konsoli – USB typu C i RJ45  · Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu uaktualnienia oprogramowania urządzenia  · Obsługa protokołów SNMPv3, SSHv2, https, syslog, SCP  · Aplikacja mobilna umożliwiająca łatwe zarządzania urządzeniami  · Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki  · Tekstowy plik konfiguracyjny – z możliwością edycji z pomocą edytora tekstu  · Praca w szerokim zakresie temperatur: -5oC – +50oC  · Możliwość przechowywania w szerokim zakresie temperatur: -25oC – +70oC  · Głębokość urządzenia nie przekracza 35cm |  |
| Gwarancja | Wymaga się aby urządzenie było objęte gwarancją producenta przez min. 36 miesięcy, realizowaną w systemie door-to-door przez serwis. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |  |

**Wymagania Zamawiającego w zakresie wdrożenia zarządzalnych przełączników sieciowych TYP 2:**

1. Konfiguracja funkcjonalności warstwy II: VLAN, Spanning Tree, agregacji łączy.
2. Konfiguracja zarządzania (SSH, HTTPS, SNMP).
3. Konfiguracja logowania zdarzeń.
4. **Zakup subskrypcji dla urządzenia klasy UTM z zapewnieniem funkcjonalności DLP – 2 sztuki**

Zamawiający posiada 2 szt. urządzenia Fortigate FG60F. W ramach niniejszej pozycji Zamawiający oczekuje dostawy przedłużenia subskrypcji, (która wygasła w dniu 15.12.2022) na okres do 30.06.2026 r., lub dostawy równoważnego systemu bezpieczeństwa, **spełniającego poniższe wymagania:**

|  |  |  |
| --- | --- | --- |
| Podać producenta, model i Part Number |  | Parametr oferowany  Tak/Nie |
| Parametr | Opis minimalnych wymagań technicznych |  |
| Wymagania Ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |  |
| Redundancja, monitoring i wykrywanie awarii | * W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * Monitoring stanu realizowanych połączeń VPN. |  |
| Interfejsy, Dysk, Zasilanie: | * System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. * System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. * W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. * System musi być wyposażony w zasilanie AC. |  |
| Parametry wydajnościowe: | * W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. * Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. * Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps. * Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. * Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps. * Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps. * Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 750 Mbps. |  |
| Funkcje Systemu Bezpieczeństwa: | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. * Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. * Zarządzanie pasmem (QoS, Traffic shaping). * Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). * Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. * Analiza ruchu szyfrowanego protokołem SSL. |  |
| Polityki, Firewall | * Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. * System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP. * W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. * Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. * Amazon Web Services (AWS). * Microsoft Azure * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware vCenter (ESXi). |  |
| Połączenia VPN | System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:   * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.   System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:   * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| Zarządzanie pasmem | * System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. * Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. * System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| Ochrona przed malware | * Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). * System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. * System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). * System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. * System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| Ochrona przed atakami | * Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. * System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. * Baza sygnatur ataków powinna zawierać minimum 19000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. * System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. * Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. * Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| Kontrola aplikacji | * Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. * Baza Kontroli Aplikacji powinna zawierać minimum 6000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. * Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. * Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| Kontrola WWW | * Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 260 milionów adresów URL pogrupowanych w kategorie tematyczne. * W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. * Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. * Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. * Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. * Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. * W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| Uwierzytelnianie użytkowników w ramach sesji | * System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:   + Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.   + Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.   + Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. * Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. * Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| Zarządzanie | * Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. * Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. * Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. * System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. * System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. * Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. * Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| Logowanie | * Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. * W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. * Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. * Musi istnieć możliwość logowania do serwera SYSLOG. |  |
| Funkcjonalności: | W ramach postępowania powinien zostać dostarczony system obejmujący następujące funkcjonalności:   * Kontrola Aplikacji, * IPS, * Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), * Analiza typu Sandbox, * Antyspam, * Web Filtering, * bazy reputacyjne adresów IP/domen. * baza wzorców danych używanych do wykrywania wycieków informacji – oprogramowanie klasy DLP |  |
| Gwarancja oraz wsparcie | Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne. |  |
| Funkcjonalność DLP | Dopuszcza się aby funkcje systemu DLP były zrealizowane w postaci komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  W takim przypadku zamawiający wymaga spełnienie poniższych wymagań:  - monitorowanie protokołów internetowych, poczty elektronicznej i komunikatorów  - przeszukiwanie zawartości na podstawie ciągów tekstowych, wzorców, wyrażeń regularnych etc.  - skanowanie ruchu w celu poszukiwania wskazanych (poufnych) informacji  - możliwość zablokowania ruchu, przekazania do zaufanego miejsca docelowego lub zarchiwizowania wraz z jednoczesnym przekazaniem powiadomienia administratorowi  - możliwość blokowania wrażliwych informacji wchodzących lub wychodzących z sieci.  - możliwość archiwizacji całości lub części ruchu przechodzącego przez urządzenia brzegowe ( w tym strony internetowe, wiadomości e-mail, pliki w całości) |  |

1. **Zasilacz awaryjny – 1 sztuka**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Wymagania minimalne** |  |
| Technologia | online, VFI-SS-111, |  |
| Moc wyjściowa | 3kVA/3kW; PF=1 |  |
| Obudowa | Rack/Tower  Zestaw do montażu w szafie rack na wyposażeniu |  |
| Napięcie wejściowe | 110 ÷ 300 V AC ± 2 % |  |
| Napięcie znamionowe (wartość skuteczna) | 230V AC |  |
| Prąd znamionowy (wejście) | 15,6A |  |
| Częstotliwość napięcia wejściowego (zakres oraz tolerancja) | 45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz |  |
| Częstotliwość znamionowa napięcia wejściowego | 50Hz / 60Hz |  |
| Zniekształcenia prądu wejściowego THDi | < 5% |  |
| Zakres napięcia wyjściowego | 200/208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD (domyślnie 230V AC) |  |
| Zniekształcenia napięcia wyjściowego THDu | < 1% dla Pmax (liniowe)  < 5% (nieliniowe wg PN EN 62040-3) |  |
| Gniazda wyjściowe | 4x IEC320 C13 (10A) sterowalne + 4x IEC320 C13 (10A) + 1x IEC320 C19 (16A) |  |
| Akumulatory wewnętrzne UPS | Minimum 6szt akumulatorów 12V9Ah |  |
| Moduły bateryjne | Opcja – możliwość podpięcia do 4szt modułów (każdy z minimum 12szt akumulatorów 12V9Ah) |  |
| Czas podtrzymania UPS dla obciążenia 3kW/2kW/1,5kW | 3 / 6 / 9 min |  |
| Czas podtrzymania UPS + MODUŁY (odpowiednia ilość) dla obciążenia 1,0 kW/3kW  Moduły w wymaganej ilości dołączone do zestawu. | 120 min/30 min |  |
| Przeciążalność | 105-125% - 5min / 125-150% - 30s / >150% - 500ms |  |
| EPO | Wymagane – standard NC |  |
| Sygnalizacja | akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące usterkę, pracę bateryjną, pracę w trybie online, obejście bypass |  |
| Język oprogramowania | polski i angielski do wyboru z poziomu interfejsu użytkownika |  |
| Konfiguracja minimalnego poziomu naładowania baterii po powrocie zasilania sieciowego (po rozładowaniu baterii przed ponownym samoczynnym załączeniem zasilania na wyjściu) | Wymagane, konfigurowalne z poziomu oprogramowania (przez USB) |  |
| Wymagane certyfikaty | CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument potwierdzający do oferty) |  |
| Komunikacja z urządzeniem | RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; SNMP – karta w zestawie |  |
| Wymiary UPS i MODUŁY (rack) (wys x szer x gł) | Nie więcej niż 89 x 439 x 610 mm |  |
| Oprogramowanie do monitorowania pracy zasilacza UPS | 1. Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux. 2. Możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów:   Powyższe wymagania potwierdzone oświadczeniem producenta oprogramowania dołączonym do oferty. |  |
| Oprogramowanie - funkcjonalność | możliwość nadawania unikalnych nazw dla kilku tych samych modeli UPS’ów w oprogramowaniu |  |
| Oprogramowanie - funkcjonalność | Konfiguracja minimalnego poziomu naładowania baterii. UPS po rozładowaniu baterii przed samoczynnym załączeniem zasilania wyjść (po powrocie zasilania sieciowego) będzie musiał naładować baterie do tego poziomu. Parametr ten ma zastosowanie w przypadku, gdy załączenie zasilania wyjść może nastąpić tylko wtedy, gdy UPS zgromadzi niezbędny zapasa energii na wypadek kolejnego zaniku. |  |
| Oprogramowanie - funkcjonalność | Uruchom poprzez Bypass - Aktywacja tej funkcji powoduje, że UPS zawsze przed załączeniem zasilania wyjść na kilka sekund załączy zasilanie poprzez Bypass i po chwili przełączy się w zasilanie wyjść poprzez falownik (normalny tryb pracy). Funkcja ta umożliwia załączenie urządzeń o zwiększonym prądzie rozruchowym bez przeciążania falownika UPS. |  |
| Serwis producenta | wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty |  |
| Gwarancja | Minimum 24 miesiące elektronika, 24 miesiące akumulatory, serwis door to door, czas naprawy 5 dni roboczych |  |
| Dokumentacja | Instrukcja w języku polskim |  |

1. **Wdrożenie Oprogramowania do monitorowania dostępu do infrastruktury informatycznej urzędu (NAC)**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Wymagania minimalne** |  |
| **Podstawowa funkcjonalność systemu NAC:** | 1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych. 2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor) 3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek. 4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji. 5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji. 6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych. 7. System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania. 8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego. 9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia. 10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:     * VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x     * Maszyny fizyczne - serwery wspierane przez producenta. 11. System musi posiadać funkcjonalność serwerów:     * serwera RADIUS dla infrastruktury sieciowej,     * serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,     * serwera SYSLOG,     * serwera TACACS+,     * serwera Monitoringu,     * serwera DHCP,     * serwera polityk uwierzytelniania i kontroli dostępu 802.1X,     * serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego. 12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP. 13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC. 14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC. 15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now. 16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email. 17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci. 18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania. 19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników. 20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie. 21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status). 22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania. 23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim). 24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci. 25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP. 26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia. 27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP. 28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP. 29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu. 30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej. 31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP. 32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci. 33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3. 34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+. 35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych. 36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD). 37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn. 38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS. 39. System musi posiadać funkcję personalizacji strony gościnnej. 40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon. 41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor. 42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS. 43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory. 44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory. 45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu. 46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru. 47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim). 48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP. 49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni. 50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań. 51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP. 52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego. 53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny. 54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176. 55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych. 56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF. 57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc). 58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA. 59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:     * Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności     * Czy włączony jest firewall     * Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur     * Czy jest włączone szyfrowanie dysku systemowego     * Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory     * Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora     * Czy w systemie są uruchomione procesy wskazane przez administratora     * Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności     * Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:       + Wartości klucza rejestru       + Typu wartości: Number, String, Version 60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal. 61. System musi współpracować z serwerem tokenów. 62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:     * Microsoft Windows     * Mac OS     * iOS     * Android 63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci). 64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory. |  |
| **Mechanizmy uwierzytelniania** | 1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS. 2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:    * MAC,    * PAP/ASCII,    * CHAP,    * SNMP,    * 802.1X. 3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp. 4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości. 5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych. 6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant). 7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:    * Tożsamość/Urządzenie końcowe,    * Grupa tożsamości/urządzeń końcowych,    * Parametry urządzeń końcowych, min: system operacyjny, wersja,    * Atrybuty Active Directory,    * Jednostka organizacyjna tożsamości/urządzeń końcowych,    * Urządzenia sieciowe sieci przewodowej, bezprzewodowej,    * Grupy urządzeń sieciowych,    * Porty urządzeń sieciowych,    * Grupy portów urządzeń sieciowych,    * Jednostka organizacyjna portów,    * Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),    * Data, czas ważności polityki,    * Wewnętrzny Captive Portal,    * Metoda autoryzacji. 8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks. 9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC. 10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI. 11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli. 12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV. 13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV. 14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach. 15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal. 16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC. 17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC. 18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www. 19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników. 20. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP. |  |
| **Obsługa serwerów certyfikatów CA** | 1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA. 2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:    * możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.    * możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.    * Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).    * usługę OCSP (Online Certificate Status Protocol). |  |
| **Obsługa serwerów DHCP** | 1. System musi posiadać funkcję zintegrowanego serwera DHCP. 2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP. 3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:    * Uruchamianie usługi dla wybranych podsieci,    * Przypisanie ustalonego adresu IP dla adresu MAC.    * Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,    * Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,    * Możliwość określania braku dostępu dla wybranych adresów MAC,    * Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,    * Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,    * Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,    * Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,    * Dokonywanie zmian bez konieczności wyłączania usług. |  |
| **Obsługa serwerów TACACS+** | System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:   1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów. 2. System musi umożliwiać tworzenia haseł administratorom. 3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów 4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych. 5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu. 6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory. 7. System musi wspierać logowanie administratorów za pomocą tokenów OTP. 8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji. |  |
| **Raportowanie i monitoring** | System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:   1. Monitoring autoryzacji. 2. Monitoring dla zdarzeń systemowych. 3. Monitoring dla zdarzeń DHCP. 4. Monitoring dla tożsamości. 5. Monitoring dla urządzeń końcowych. 6. Monitoring dla urządzeń sieciowych. 7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email. 8. Raport ze zdarzeń logowania z informacją o nadam adresie IP. 9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług. 10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci. 11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym. 12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie. 13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku. 14. System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych. 15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja. 16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi. 17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS. 18. Raport zdarzeń Microsoft Active Directory, minimum:     * Logowania, wylogowania z system w tym błędne logowania     * Logowania do sieci 802.1X |  |
| **Alarmy** | 1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:    * wiadomości e-mail,    * Syslog,    * notyfikacji systemowych. 2. Alarmy mogą być generowane w sytuacjach, min:    * Ilości obsługiwanych transakcji RADIUS,    * Opóźnienie obsługi transkacji RADIUS,    * Statusu krytycznego modułów. 3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:    * badanie łączności IP za pomocą ping, traceroute,    * tcpdump protokołów RADIUS, TACACS+,    * wyszukiwanie zdarzeń RADIUS z uwzględnieniem:      + nazwy użytkownika,      + adresu MAC,      + statusu uwierzytelnienia (udana lub nieudana),      + powodu, jeżeli uwierzytelnienie nieudane,      + zakresu czasowego, co do dnia, godziny i minuty,    * wykonanie zdalnego polecenia na urządzeniu sieciowym. |  |
| **Wymagania dotyczące wdrożenia i harmonogram ramowy:** | * Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta. * Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA). * Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.). * Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list). * Integracja dostarczanych urządzeń sieciowych wzorcowych po jednym z każdej serii (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach. * Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy. * Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy. * Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 4 osób po 6h dziennie. * Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia. |  |
| **Szkolenia/warsztaty:** | * Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC * Warsztaty zostaną przeprowadzone dla maksymalnie 4 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC * Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC * Warsztaty odbędą się w formie zdalnej. * Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej. * Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym |  |
| **Licencja wsparcia technicznego producenta oprogramowania:** | Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 36 miesięczną licencję na wsparcie  producenta oprogramowania. Licencja ta powinna obejmować minimum:   * Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC * Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia. * Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów. * Dostęp do dokumentacji i instrukcji na stronie internetowej. * Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania. |  |

1. **Oprogramowanie SIEM**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Wymagania minimalne** |  |
| **Wymagania ogólne** | 1. Przedmiotem postępowania jest dostarczenie systemu **zarządzanie informacjami i zdarzeniami w zakresie bezpieczeństwa** systemu informatycznego, służącego do monitorowania i analizy danych z różnych źródeł w celu wykrywania zagrożeń i reagowania na incydenty. 2. **System w postaci aplikacji oparty powinien być na licencji Open Source oraz nie może generować kosztów licencyjnych po stronie Zamawiającego.** 3. Podstawowe funkcjonalności: 4. Analiza ustawień konfiguracji systemów i aplikacji, skan środowiska i alerty bezpieczeństwa. 5. Funkcja Monitorowania Integralności Plików (FIM). Zgodne z wymogami regulacji zgodności, takich jak PCI DSS, NIST. 6. Wbudowany zestaw reguł: Ocena Konfiguracji Bezpieczeństwa (SCA), Rootcheck  i Monitorowanie Integralności Plików (FIM). 7. Analiza logów z systemu operacyjnego i aplikacji na podstawie zdefiniowanych reguł  i przechowywane. 8. Przechowywanie, indeksacja i przeszukiwanie logów. Reguły detekcji zagrożeń powiązane z framework’iem MITRE ATT&CK. 9. Zbieranie informacji o zainstalowanym oprogramowania i jego aktualizacja bazami CVE (Common Vulnerabilities and Exposures). 10. Blokada dostępu sieciowego dla urządzeń pochodzących ze źródła zagrożenia. Udzielanie odpowiedzi na komendy i zapytania systemowe, identyfikacja wskaźników naruszeń bezpieczeństwa (IOC) i incydentów. 11. Generowanie raportów oraz interaktywnych pulpitów nawigacyjnych dla standardów takich jak PCI DSS, NIST, TSC i HIPAA. 12. Kontrola hostów i kontenerów Docker, monitoring silnika Docker oraz natywna integracja z silnikiem Docker. 13. Inwentaryzacja i monitorowanie urządzeń końcowych. 14. Współpraca z platformami cloud’owymi. 15. Monitoring i ochrona obciążeń zarówno w środowiskach chmurowych, jak i lokalnych. Możliwa integracja z platformami typu, m.in.: AWS, Microsoft Azure, GCP, Microsoft 365 czy GitHub. 16. Centralne zarządzanie logami. 17. Analiza danych dotyczących zdarzeń bezpieczeństwa w celu efektywnej identyfikacji anomalii lub wskaźników zagrożenia. 18. Identyfikacja potencjalnych luk w zabezpieczeniach oraz przyznawanie im określonych priorytetów. 19. Skan systemów IT i porównanie analizowanych danych do wzorcowych zaleceń Center for Internet Security (CIS). 20. Powiadomienia i alerty w czasie rzeczywistym w przypadku wykrycia incydentów bezpieczeństwa. Analiza zdarzeń z różnych źródeł, integracja danych z systemów wywiadu o zagrożeniach. 21. Tworzenie raportów w aspekcie analizy incydentów bezpieczeństwa. |  |

**Zamawiający wymaga:**

1. Wdrożenia najnowszej, dostępnej wersji systemu.
2. Wdrożenia/implementacji oferowanego sytemu w środowisku Zamawiającego.
3. Przygotowanie procedur awaryjnych.
4. **Oprogramowanie do zbierania i analizowania dzienników zdarzeń**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Wymagania minimalne** |  |
| Wymagania Ogólne | W ramach postępowania wymagane jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. System ten ma służyć do centralnego gromadzenia logów, zaawansowanego wyszukiwania i filtrowania oraz tworzenia systemu alarmów. |  |
| System w postaci aplikacji oparty powinna być na licencji Open Source oraz nie może generować kosztów licencyjnych po stronie Zamawiającego. | Minimalne rozwiązania systemowe:   * + centralne gromadzenie logów,   + eliminacja silosów danych poprzez analizę w jednym miejscu   + indeksowanie i analizowanie danych generowanych przez różne aplikacje – od wewnętrznych systemów operacyjnych po aplikacje webowe,   + możliwość wizualizacji danych w czasie rzeczywistym za pomocą interaktywnych pulpitów nawigacyjnych,   + automatyczne powiadamianie (system alarmów) pozwalający na informowanie o nietypowych zdarzeniach, takich jak potencjalne incydenty bezpieczeństwa,   + wbudowane funkcje analityczne wspierające identyfikację wzorców i trendów,   + modułowej architektura w celu dostosowania do potrzeb Zamawiającego, możliwość integracji z innymi narzędziami i usługami,   + zdolność do przechowywania logów w skondensowany, przeszukiwalny sposób,   + identyfikacja problemów i błędów,   + funkcjonalność elasticsearch w celu wyszukiwania i segmentacji logów,   + możliwość tworzenia powiadomień i alertów z pozycji administratora systemu. |  |
| Wymagania zamawiającego w zakresie wdrożenia oprogramowania do zbierania i analizowania dziennika zdarzeń: | * Instalacja oprogramowania. * Konfiguracja logowania zdarzeń. * Skonfigurowanie we współpracy z Zamawiającym pięciu typów raportów służących do oceny stopnia wykorzystania oraz ochrony styku z Internetem. |  |

**15. Urządzenie typu Router z funkcjonalnością klasy UTM – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Wymagania minimalne** |  |
| Procesor | 4-rdzeniowy 1.7 GHz |  |
| Pamięć systemowa | 4 GB DDR4 |  |
| Pamięć wbudowana | 16 GB eMMC  Zintegrowany dysk 128 GB SSD |  |
| Przepustowość IDS/IPS | 3.5 Gb/s (mierzona w iPerf3) |  |
| Maks. pobór mocy (nie licząć wyjścia PoE) | 50W |  |
| Sposób zasilania | 1x Uniwersalne wejście AC,  100-240VAC, 4.4A Maks, 50/60 Hz 1x USP-RPS wejście DC, 52VDC, 3.94A |  |
| Zasilanie | AC/DC, wewnętrzne, 240W |  |
| Obsługiwany zakres napięcia | 100 do 240VAC |  |
| Interfejs zarządzania | Ethernet   Bluetooth |  |
| Interfejs sieciowy | 1x port WAN: 2.5 Gigabit Ethernet RJ45 8x portów LAN: 10/100/1000 Mb/s RJ45 |  |
| Interfejs SFP+ | 1x WAN: 10G SFP+ 1x LAN: 10G SFP+ |  |
| PoE | 2x porty PoE+ IEEE 802.3at (pair A 1, 2+; 3, 6-) 6x portów PoE IEEE 802.3af (pair A 1, 2+; 3, 6-) |  |
| Maks. PoE na port 802.3af | 15.4W |  |
| Maks. PoE na port 802.3at | 30W |  |
| Zakres napięcia dla PoE 802.3af | 44 do 57V |  |
| Zakres napięcia dla PoE  802.3at | 50 do 57V |  |
| Zabezpieczenie ESD/EMP | Powietrze: ± 15 kV, kontakt: ± 8 kV |  |
| Wyświetlacz LCM | 1x dotykowy ekran 1.3" Animacja rozruchu: trwa rozruch Ikona aktualizacji oprogramowania: aktualizacja oprogramowania |  |
| Przyciski | Reset |  |
| Temp. pracy | -10 do 40° C (14 to 104° F) |  |
| Wilgotność pracy | 5 - 95% niekondensująca |  |
| Waga | Max. 4.95 kg (10.91 lb) |  |
| Uchwyt | stal SGCC, uszy do montażu w szafie rack |  |
| Gwarancja | Minimum 12 mies. |  |

**16. Punkt dostępowy Wi-Fi – 6 sztuk**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Wymagania minimalne** |  |
| Interfejs sieciowy | 1x GbE RJ45 port |  |
| Interfejs zarządzania | Ethernet |  |
| Sposób zasilania | PoE |  |
| Obsługiwany zakres napięcia | 44–57V DC |  |
| Maksymalny pobór mocy | 9W |  |
| Max. TX power 2.4 GHz 5 GHz | 23 dBm 23 dBm |  |
| MIMO 2.4 GHz 5 GHz | 2 x 2  2 x 2 |  |
| Współczynnik przepustowości 2.4 GHz 5 GHz | 573.5 Mbps 2402 Mbps |  |
| Zysk anteny 2.4 GHz 5 GHz | 3dBi 5.4 dBi |  |
| Przycisk | Factory reset |  |
| Dopuszczalna temperatura pracy | -30 to 60° C (-22 to 140° F) |  |
| Dopuszczalna wilgotność | 5 to 95% noncondensing |  |
| Certyfikacje | CE, FCC, IC |  |
| **Oprogramowanie** |  |  |
| Standardy Wi-Fi | 802.11a/b/g  WiFi 4/WiFi 5/WiFi 6 |  |
| Bezpieczeństwo sieci bezprzewodowej | WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3) |  |
| BSSID | 8 per radio |  |
| VLAN | 802.1Q |  |
| Izolacja ruchu gości | TAK |  |
| liczba klientów równocześnie | 300+ |  |
| Aplikacja do zarządzania | TAK |  |
| Gwarancja | Minimum 12 mies. |  |

**17. Zasilacz awaryjny do serwera – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **PARAMETRY \ TYP** | **Wymagania minimalne** |  |
| Moc wyjściowa (pozorna / czynna) | minimum 3000 VA |  |
| minimum 2250 W |  |
| **DANE OGÓLNE I ŚRODOWISKOWE** |  |  |
| Topologia | VI (line interactive) |  |
| Typ obudowy | Rack / Tower |  |
| Chłodzenie | Wymuszone, wewnętrzne wentylatory |  |
| **WEJŚCIE** |  |  |
| Napięcie znamionowe (wartość skuteczna) | 230 V AC |  |
| Zakres napięcia wejściowego (wartości skuteczne) i tolerancja | 178 ÷ 281 V AC ± 2 % |  |
| Częstotliwość znamionowa napięcia wejściowego | 50 Hz |  |
| Zakres częstotliwości i tolerancja | 45 ÷ 55 Hz ± 1 Hz |  |
| Progi przełączania: sieć – UPS | 178 ÷ 281 V AC ± 2 % |  |
| **WYJŚCIE** |  |  |
| Napięcie znamionowe (wartość skuteczna) | 230 V AC |  |
| Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa | 195 ÷ 253 V AC ± 2 % |  |
| Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa | 230 V AC ± 5 % |  |
| Automatyczna regulacja napięcia (AVR) | ± 10 % |  |
| Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej) | Sinusoidalny / Tak jak na wejściu |  |
| Częstotliwość znamionowa napięcia wyjściowego | 50 Hz |  |
| Filtracja napięcia wyjściowego | Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy |  |
| Progi przełączania: UPS – sieć | 183 ÷ 276 V AC ± 2 % |  |
| Czas przełączenia na pracę rezerwową | < 3 ms |  |
| Czas powrotu na pracę sieciową | 0 ms |  |
| Przeciążalność | > 105% - 15 s (wyłączenie UPS) |  |
| **AKUMULATORY I CZASY PODTRZYMANIA** |  |  |
| Akumulatory wewnętrzne | minimum 12 V / 9 Ah VRLA |  |
| Czas podtrzymania z baterii wewnętrznych dla obciążenia 2250W | minimum 3 min |  |
| Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza). | do 4 h |  |
| **PARAMETRY MECHANICZNE** |  |  |
| Wymiary – TOWER (wys. X szer. X gł.) | nie większe niż 440 x 132 x 460 mm (zasilacz) |  |
| Masa zasilacza | nie większa niż 28 kg |  |
| **ZABEZPIECZENIA** |  |  |
| Zabezpieczenie wejściowe | Przeciwzwarciowe – Bezpiecznik automatyczny |  |
| 16 A / 250 V AC |  |
| Przeciwprzepięciowe |  |
| Zabezpieczenie wyjściowe | Elektroniczne – przeciwzwarciowe i przeciążeniowe |  |
| Zabezpieczenia wejścia DC (akumulatory wewnętrzne) | Zabezpieczenie nadprądowe |  |
| Zabezpieczenia DC (zewnętrzny moduł bateryjny) | Zabezpieczenie nadprądowe |  |
| **WYPOSAŻENIE I FUNKCJE DODATKOWE** |  |  |
| Przyłącza wyjściowe (liczba i typ gniazd) | minimum 8 gniazd z podtrzymaniem bateryjnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym) |  |
| Sygnalizacja | Akustyczno – optyczna; graficzny wyświetlacz LCD w języku polskim |  |
| Interfejsy komunikacyjne | USB HID, SNMP/HTTP |  |
| Oprogramowanie monitorująco-zarządzające | 1. Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych - możliwość zamykania systemu na min. 75 stanowiskach komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux. 2. Możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów   Powyższe wymagania potwierdzone oświadczeniem producenta oprogramowania na etapie składania oferty. |  |
| możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP) |  |
| możliwość zdalnego wyłączenia zarządzalnej sekcji gniazd |  |
| możliwość edycji nazw urządzeń na liście monitorowanych UPSów |  |
| wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów. |  |
| wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer |  |
| Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego | wymagane |  |
| Możliwość aktualizacji oprogramowania firmware przez użytkownika | wymagane |  |
| **GWARANCJA / SERWIS** |  |  |
| Gwarancja | 24 miesięcy na elektronikę i 24 miesiące na akumulatory; |  |
| Serwis | autoryzowany serwis producenta zlokalizowany w Polsce. |  |
| serwis realizowany w systemie door to door |  |
| naprawa w maksymalnie 5 dni roboczych |  |
| **DODATKOWE OŚWIADCZENIA/DOKUMENTY** |  |  |
|  | ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania – dołączone do oferty |  |
|  | deklaracja CE producenta sprzętu – dołączone do oferty |  |

**18. Serwer plików NAS z integralnym osprzętem – 2 sztuki**

|  |  |  |
| --- | --- | --- |
| **Podać producenta, model i Part Number** |  | **Parametr oferowany**  **Tak/Nie** |
| **Parametr** | **Opis minimalnych wymagań technicznych** |  |
| Typ | Sieciowy serwer plików NAS |  |
| Obudowa | Tower |  |
| Procesor | 4-rdzeniowy o taktowaniu zwiększanym do 2,6 GHz |  |
| Pamięć RAM | 8 GB RAM z możliwością rozszerzenia do 16 GB |  |
| Wewnętrzna pamięć masowa | 4 dyski 3,5-calowe SATA 6 Gb/s  Dyski muszą znajdować się na liście kompatybilnych urządzeń publikowanej przez producenta serwera NAS. |  |
| Kompatybilność dysków | Dyski twarde SATA 3,5-calowe Dyski SSD SATA 2,5-calowe |  |
| Zestaw | Do każdego serwera należy dołączyć kompatybilne 4 dyski HDD 3,5” SATA o pojemności 12 TB każdy |  |
| Interfejsy sieciowe | Min. 2 x 2,5 Gigabit Ethernet (2,5G/1G/100M/10M) |  |
| Złącza dodatkowe | Min. 2 porty typu A USB 3.2, 2x HDMI 1.4 |  |
| Gniazdo M.2 | 2 x M.2 2280 PCIe Gen 3 x2 |  |
| Szyfrowanie | AES-NI |  |
| Zasilacz | 90W, 100–240 V |  |
| Gwarancja | Minimum 36 mies. |  |

Zamawiający wymaga:

Skonfigurowania dostarczonego serwera jako serwera kopii zapasowych, w tym zdefiniowanie zadań i harmonogramów kopii zapasowych oraz wykonanie testowego odtwarzania danych dla wskazanych przez Zamawiającego zasobów (serwery fizyczne, wirtualne).

1. **Wymagania ogólne w zakresie** **instalacji, wdrożenia oraz konfiguracji sprzętu   
   i oprogramowania:**

Zamawiający wymaga:

1. Zaktualizowania oprogramowania/sterowników/firmware dla wszystkich wdrażanych rozwiązań do najnowszej dostępnej w dniu wdrożenia i stabilnej wersji (wymaganie to dotyczy również infrastruktury zależnej, współpracującej z wdrażanymi rozwiązaniami).
2. Realizacji prac wdrożeniowych przez osoby posiadające certyfikaty producentów wdrażanych rozwiązań.
3. Realizacji prac wdrożeniowych, które będą skutkowały niedostępnością środowiska IT Zamawiającego, w godzinach 18:00 – 7:00 w dni od poniedziałku do piątku lub w sobotę i niedzielę przez cała dobę i planowane w uzgodnieniu z Zamawiającym z minimum trzydniowym wyprzedzeniem.
4. Opracowania dokumentacji powykonawczej wdrożenia, obejmującej całość wykonanych prac oraz zmiany wprowadzone w infrastrukturze zależnej.
5. Wykonawca w ramach wdrożenia zapewni szkolenie administratorom systemu z podstawowej obsługi i konfiguracji wdrożonych rozwiązań.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **L.P.** | **Przedmiot zamówienia** | **Ilość** | **Cena jednostkowa netto** | **Wartość netto**  *(cena jednostkowa x ilość)* |
| *1* | *2* | *3* | *4* | *5* |
| 1. | **Serwer nadmiarowy** | 1 | ,      zł | ,      zł |
| 2. | **Serwer backupu (serwer izolowanych kopii zapasowych)** | 1 | ,      zł | ,      zł |
| 3. | **Serwer kopii zapasowych maszyn wirtualnych** | 1 | ,      zł | ,      zł |
| 4. | **Macierz dyskowa** | 1 | ,      zł | ,      zł |
| 5. | **Urządzenie archiwizacyjne taśmowe jednonapędowe** | 1 | ,      zł | ,      zł |
| 6. | **Serwer plików NAS** | 1 | ,      zł | ,      zł |
| 7. | **Oprogramowanie do tworzenia kopii zapasowych** | 1 | ,      zł | ,      zł |
| 8. | **Przełączniki zarządzalne TYP 1** | 2 | ,      zł | ,      zł |
| 9. | **Przełączniki zarządzalne TYP 2** | 45 | ,      zł | ,      zł |
| 10. | **Zakup subskrypcji dla urządzenia klasy UTM z zapewnieniem funkcjonalności DLP** | 2 | ,      zł | ,      zł |
| 11. | **Zasilacz awaryjny** | 1 | ,      zł | ,      zł |
| 12. | **Wdrożenie Oprogramowania do monitorowania dostępu do infrastruktury informatycznej urzędu (NAC)** | 1 | ,      zł | ,      zł |
| 13. | **Oprogramowanie SIEM** | 1 | ,      zł | ,      zł |
| 14. | **Oprogramowanie do zbierania i analizowania dzienników zdarzeń** | 1 | ,      zł | ,      zł |
| 15. | **Urządzenie typu Router z funkcjonalnością klasy UTM** | 2 | ,      zł | ,      zł |
| 16. | **Punkt dostępowy Wi-Fi** | 6 | ,      zł | ,      zł |
| 17. | **Zasilacz awaryjny do serwera** | 2 | ,      zł | ,      zł |
| 18. | **Serwer plików NAS z integralnym osprzętem** | 2 | ,      zł | ,      zł |
| **Cena ogółem netto** | | | | ,      zł |
| Wartość VAT (23%): | | | | ,      zł |
| **Cena ogółem brutto**  *(wartość netto + wartość vat)*: | | | | ,      zł |

UWAGA: Podane w tabeli wymagania należy traktować jako minimalne. Dopuszcza się składa­nie ofert na urządzenia lepsze, a przynajmniej równoważne pod każdym względem. Wykonawca powinien określić w opisie przedmiotu zamówienia – producenta urządzenia oraz nazwę oferowanego produktu i ewentualne inne cechy konieczne do jego jednoznacznego zidentyfikowania oraz wykazać, że oferowane przez niego urządzenia spełniają wymagania określone przez Zamawiającego.

1. **Kryterium gwarancja:**
2. udzielam gwarancji na okres **36 miesięcy** od dnia odbioru bez zastrzeżeń przedmiotu umowy przez Zamawiającego (0 punktów) \*
3. udzielam gwarancji na okres **48 miesięcy** od dnia odbioru bez zastrzeżeń przedmiotu umowy przez Zamawiającego (20 punktów) \*
4. udzielam gwarancji na okres **60 miesięcy** od dnia odbioru bez zastrzeżeń przedmiotu umowy przez Zamawiającego (40 punktów) \*

W przypadku niezaznaczenia żadnej z możliwości w kryterium „okres gwarancji” Zamawiający przyzna 0 punktów.

1. Oferowany termin wykonania niniejszego zamówienia zgodnie z zapisami w SWZ – **60 dni od dnia podpisania umowy.**
2. Niniejsza oferta jest ważna przez 30dni.
3. Cena oferty obejmuje wszystkie koszty niezbędne do wykonania przedmiotu zamówienia oraz podatki obowiązujące na terenie Polski, w tym podatek VAT i została wyliczona w oparciu o opis podany SWZ.
4. Akceptuję(emy) warunki płatności zgodnie z zapisami Projektowanych postanowień umowy.
5. Akceptuję(emy) bez zastrzeżeń Projektowane postanowienia umowy przedstawione w Załączniku do SWZ.
6. W przypadku uznania mojej (naszej) oferty za najkorzystniejszą, umowę zobowiązuję(emy) się zawrzeć w miejscu i terminie jakie zostaną wskazane przez Zamawiającego.
7. Składam(y) niniejszą ofertę [***we własnym imieniu] / [jako Wykonawcy wspólnie ubiegający się o udzielenie zamówienia] \****
8. Nie uczestniczę(ymy) jako Wykonawca w jakiejkolwiek innej ofercie złożonej w celu udzielenia niniejszego zamówienia.
9. Oświadczam, że jestem **(odpowiednio podkreślić, jeśli dotyczy):**
10. Mikro przedsiębiorcą
11. Małym przedsiębiorcą
12. Średnim przedsiębiorcą
13. Prowadzę jednoosobową działalność
14. Osobą fizyczną nieprowadzącą działalności
15. Wykonawcą z innych państw Unii Europejskiej,
16. Wykonawcą z państw niebędących członkami Unii Europejskiej
17. Wadium w kwocie: **8.500,00** **zł** (słownie: osiem tysięcy pięćset złotych 00/100) zostało uiszczone w formie ...........................................................................................................................................

Zwrotu wadium wniesionego w pieniądzu proszę dokonać na rachunek bankowy\* **(\*jeśli dotyczy)**:

....................................................................................…………………………………………………………………………..

1. Wskazane poniżej informacje zawarte w ofercie **stanowią / nie stanowią**\* tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i w związku z niniejszym nie mogą być one udostępniane, w szczególności innym uczestnikom postępowania:

…………………………………………………………………………………………………..………………………………………………….

1. Część dostaw **zamierzam/nie zamierzam\* zlecić** podwykonawcy …………………………………………………………………………………………………………………………..………………………….

(wskazać nazwę podwykonawcy oraz zakres dostaw, jeżeli jest znany)

1. Oświadczenie dotyczące polegania na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 118 ust. 1 ustawy Prawo zamówień publicznych:

□ **Nie zamierzam(-y)** polegać na zdolnościach lub sytuacji innych podmiotów\*

□ **Zamierzam(-y)** polegać na zdolnościach lub sytuacji innych podmiotów\*:

Wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu: ……………………………………..  
………………………………………………………………………………………………………………………………………………………..

1. **Oświadczamy**, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

\*niepotrzebne skreślić

1. **Podpis(y): Ofertę składa się pod rygorem nieważności w formie elektronicznej lub   
   w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.**

**…………….………………………… ……………………………………..**

Miejscowość i data Podpis(y) osoby(osób) upoważnionej(ych)

do podpisania niniejszej oferty w imieniu   
 Wykonawcy(ów)