

OPIS PRZEDMIOTU ZAMÓWIENIA**„Cyberbezpieczny Samorząd dla Gminy Włocławek” – dostawy**

- 1. Serwer z oprogramowaniem serwerowym (z wbudowanymi mechanizmami wirtualizacji) – 2 sztuki.**

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami serwera **Dell PowerEdge R360**.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none">Obudowa Rack o wysokości max 1U z możliwością instalacji 8 dysków 2.5"Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Płyta główna	<ul style="list-style-type: none">Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci
Chipset	<ul style="list-style-type: none">Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	<ul style="list-style-type: none">Jeden procesor 8-rdzeniowy, min. 2.8GHz, umożliwiający osiągnięcie wyniku min. 89.8 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocessorowej.
Pamięć RAM	<ul style="list-style-type: none">2x32GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 4800MT/s.
Karta graficzna	<ul style="list-style-type: none">Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wbudowane porty	<ul style="list-style-type: none">min. 4 porty USB w tym 1 port USB 3.0 z tyłu obudowy,1 port VGA na tylnym panelu,1 port RS232

Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 1x dysk SATA o pojemności min. 2TB, Hot-Plug. 2 x dysk M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
Zasilacze	<ul style="list-style-type: none"> Redundantne, o mocy maks. 700W klasy Titanium - 2 sztuki.
Bezpieczeństwo	<ul style="list-style-type: none"> Zatrask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0 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. Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych
Karta Zarządzania	<ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none"> zdalny dostęp do graficznego interfejsu Web karty zarządzającej; zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; możliwość podmontowania zdalnych wirtualnych napędów; wirtualną konsolę z dostępem do myszy, klawiatury; wsparcie dla IPv6; wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

	<ul style="list-style-type: none"> możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; integracja z Active Directory; możliwość obsługi przez dwóch administratorów jednocześnie; wsparcie dla dynamic DNS; wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej Przesyłanie danych telemetrycznych w czasie rzeczywistym Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> 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

	<ul style="list-style-type: none"> o Integracja z service desk producenta dostarczonej platformy sprzętowej o Możliwość przejęcia zdalnego pulpitu o Możliwość podmontowania wirtualnego napędu o Kreator umożliwiający dostosowanie akcji dla wybranych alertów o Możliwość importu plików MIB o Przesyłanie alertów „as-is” do innych konsol firm trzecich o Możliwość definiowania ról administratorów o Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów o Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) o Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta o Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów o 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. o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. o Wdrażanie serwerów, rozwiązań modułowych oraz przełączników sieciowych w oparciu o profile o Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. o Zdalne uruchamianie diagnostyki serwera. o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na

	<p>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.</p> <ul style="list-style-type: none"> • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022 oraz Microsoft Windows Server 2025.
Dokumentacja użytkownika	<ul style="list-style-type: none"> • Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Gwarancja	<ul style="list-style-type: none"> • Zamawiający wymaga zapewnienia gwarancji producenta z zakresu wdrażanej technologii na okres 60 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. • Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. 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 otrzymania zgłoszenia / 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 wsparciem 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.

- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.

Licencja na oprogramowanie serwerowe – 2 sztuki.

Wymagane minimalne parametry

Oprogramowanie Windows Server 2025 Standard (licencja wieczysta na 16 rdzeni procesora, wersja OEM) lub równoważne.

Opis równoważności dla systemu Windows Server 2025 Standard:

1. System operacyjny musi być przeznaczony do zastosowań serwerowych w Środowiskach fizycznych lub o minimalnej wirtualizacji.
2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta.
3. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
4. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2026.
5. Licencja na system operacyjny musi być bez ograniczeń czasowych.
6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowiskach wirtualnych za pomocą wbudowanych mechanizmów wirtualizacji, bez konieczności zakupu dodatkowych licencji.
7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej.
8. System operacyjny musi posiadać graficzny interfejs użytkownika.
9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie:
 - a. zarządzania użytkownikami,
 - b. zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,
 - c. możliwości przydzielania praw dostępu do zasobów sieciowych,
 - d. instalacji zdalnej oprogramowania z pakietów msi,
 - e. definiowanie polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 11.
10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów.
11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 11 (RSAT) oraz Windows Admin Center.
12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP.
13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami.
14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta.
15. System operacyjny musi posiadać obsługę pamięci USB jako monitora kłaster

16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra
17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS.
18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień.
19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zaporę musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ip v4 i v6;
20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny;
21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;
22. System operacyjny musi posiadać obsługę PowerShell,
23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory
24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte muszą być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

2. Serwer z oprogramowaniem serwerowym (z wbudowanymi mechanizmami wirtualizacji) – 2 sztuki.

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami serwera **Dell PowerEdge R760xs**.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Szyny montażowe muszą być kompatybilne z szafą serwerową Zamawiającego TRITON 42U 600x900mm Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. Obudowa z możliwością wyposażenia 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	<ul style="list-style-type: none"> • 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 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	<ul style="list-style-type: none"> • Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	<ul style="list-style-type: none"> • Zainstalowany jeden procesor min. 16-rdzeniowy klasy x86, min. 2.0GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 265 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej
RAM	<ul style="list-style-type: none"> • Minimum 256GB DDR5 RDIMM 4800MT/s,
Funkcjonalność pamięci RAM	<ul style="list-style-type: none"> • Demand Scrubbing, • Patrol Scrubbing, • Permanent Fault Detection (PFD)
Gniazda PCI	<ul style="list-style-type: none"> • Min. dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> • Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Dyski twarde	<ul style="list-style-type: none"> • Zainstalowane dwa dyski M.2 NVME o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. • Zainstalowane dwa dyski 8TB HDD NLSAS (12Gb/s, 7.2k obr/min, Hot-Plug 3.5")
Wbudowane porty	<ul style="list-style-type: none"> • 4x USB, w tym min. 1 porty USB 3.0 • 2x port VGA (jeden na panelu przednim) • Możliwość rozbudowy o Serial Port
Video	<ul style="list-style-type: none"> • Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	<ul style="list-style-type: none"> • Redundantne, Hot-Plug
Zasilacze	<ul style="list-style-type: none"> • Redundantne, Hot-Plug min. 1100W klasy Titanium - 2 sztuki
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrzaszk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera

	<ul style="list-style-type: none"> • 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. • Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	<ul style="list-style-type: none"> • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą: <ul style="list-style-type: none"> ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: <ul style="list-style-type: none"> ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • 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



	<p>sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.</p> <ul style="list-style-type: none">o Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.o Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profileo Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.o Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.o Zdalne uruchamianie diagnostyki serwera.o Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.o Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	<ul style="list-style-type: none">• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001• Serwer musi posiadać deklaracja CE.• Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.• 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.• Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022 oraz Microsoft Windows Server 2025.
Dokumentacja użytkownika	<ul style="list-style-type: none">• Zamawiający wymaga dokumentacji w języku polskim lub angielskim.• Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Gwarancja	<ul style="list-style-type: none">• Zamawiający wymaga zapewnienia gwarancji producenta z zakresu wdrażanej technologii na okres 60 miesięcy.

- Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.
- Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych)
- Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania.
- Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.
- Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.
- Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. 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 otrzymania zgłoszenia / 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 wsparciem 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

	<p>problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.</p> <ul style="list-style-type: none"> • 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. • Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.
--	--

Licencja na oprogramowanie serwerowe – 2 sztuki

Wymagane minimalne parametry

Oprogramowanie Microsoft Windows Server 2025 Datacenter 16-core lub oprogramowanie równoważne.

Licencje nie mogą posiadać ograniczeń czasowych, muszą pochodzić z oficjalnego kanału dystrybucji i nie mogą być dedykowane tylko do jednego producenta sprzętu serwerowego.

Warunki równoważności:

W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2025 Datacenter, Zamawiający wymaga dostarczenia licencji dla 2 serwerów oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:

1. Współpraca z procesorami o architekturze x86 – 64bit.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Pojedyncza licencja musi obsługiwać serwer fizyczny wyposażony w 16 rdzeni.
5. Praca w roli klienta domeny Microsoft Active Directory.

6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.
7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).
9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
11. Możliwość uruchomienia roli serwera stron WWW.
12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiające wirtualizowanie zasobów sprzętowych serwera.
13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.
14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
 - a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
 - b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
 - c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
 - d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość
19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET
21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
22. Możliwość wykorzystania standardu http/2.
23. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
26. Mechanizmy logowania w oparciu o: a) login i hasło,
 - a. karty z certyfikatami (smartcard),
 - b. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).
27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:

- a. określonych grup użytkowników,
 - b. zastosowanej klasyfikacji danych,
 - c. centralnych polityk dostępu w sieci,
 - d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
- a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.
 - b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
 - podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 - ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
 - bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS
 - c. zdalna dystrybucja oprogramowania na stacje robocze,
 - d. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,
 - e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
 - Dystrybucję certyfikatów poprzez http,
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
 - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
 - f. szyfrowanie plików i folderów,
 - g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
 - h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,
 - i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
 - j. serwis udostępniania stron WWW,
 - k. wsparcie dla protokołu IP w wersji 6 (IPv6),



- l. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- m. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),
- n. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- o. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
- p. mechanizmy wirtualizacji mające wsparcie dla:
 - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
 - obsługi ramek typu jumbo frames dla maszyn wirtualnych.
 - obsługi 4-KB sektorów dysków,
 - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
 - możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
- q. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
- r. wsparcie dla rozwiązań Kubernetes.
- s. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
- t. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
- u. mechanizmy deduplikacji i kompresji na wolumenach.
- v. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
- w. mechanizm konfiguracji połączenia VPN do platformy Azure.
- x. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
- y. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
- z. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard).

3. Serwer do wykonywania kopii zapasowych – 1 sztuka.

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami urządzenia **Dell PowerVault TL1000**.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa i pojemność	Wysokość maksymalnie 1U do instalacji w szafie Rack. Szyny montażowe muszą być kompatybilne z szafą serwerową Zamawiającego TRITON 42U 600x900mm Co najmniej 9 slotów przeznaczonych na zestaw taśm.
Połączenie	Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów.
Interfejsy sieciowe/FC/SAS	Dodatkowa karta SAS (4x mini SAS-HD, 12Gb/s, SAS, PCIe)
Napęd	Wyposażony w co najmniej 1 sztukę napędu SAS LTO8. W komplecie: <ul style="list-style-type: none"> kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m 10x taśma LTO8 WORM Oznaczenia dla taśm LTO8, numery: 1-200 Oznaczenia dla taśm LTO8 WORM, numery: 1-200 Taśma czyszcząca
Gwarancja	60 miesięcy gwarancji producenta. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.

	<p>Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.</p> <p>Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</p> <p>Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.</p> <p>Zamawiający wymaga możliwości sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.</p> <p>Zamawiający wymaga możliwości automatycznej diagnostyki i zdalnego otwierania zgłoszeń serwisowych. .</p> <p>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.</p>
--	--

4. Serwer NAS – 2 sztuki.

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami urządzenia **Synology DS423+**.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Tower
Procesor	Czterordzeniowy procesor o taktowaniu min. 2.0 GHz (maksymalnie 2,7 GHz z przyspieszeniem) osiągający wartość „CPU Mark” w teście PassMark co najmniej 2900 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 2 GB pamięci non-ECC SODIMM z możliwością rozszerzenia do min. 6 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap Wbudowane 2 gniazda M.2 obsługujące dyski NVMe. Dyski NVMe mogą posłużyć do utworzenia pamięć podręcznej bądź przestrzeni dyskowej

	Typy obsługiwanych dysków: 3.5" SATA HDD, 2.5" SATA SSD, M.2 2280 NVMe SSD
Porty zewnętrzne	Minimum: • 2 porty USB 3.2.1
Porty sieciowe	Minimum: • 2 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Wentylator obudowy	Min. 2 wentylatory
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: • Wewnętrzny: Btrfs, ext4 • Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	• Maksymalny rozmiar pojedynczego wolumenu: 108 TB • Minimalna liczba wewnętrznych wolumenów: 64 • Minimalna liczba obiektów iSCSI Target: 128 • Minimalna liczba jednostek iSCSI LUN: 256 • Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Minimum JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Funkcja udostępniania plików	• Minimalna liczba kont użytkowników: 2048 • Minimalna liczba grup użytkowników: 256 • Minimalna liczba folderów współdzielonych: 512 • Minimalna liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 500 • Minimalna liczba jednoczesnych połączeń protokołu SMB/AFP/FTP (z rozbudową pamięci RAM): 1500
Uprawnienia	Uprawnienia aplikacji listy kontroli dostępu systemu Windows (ACL)
Wirtualizacja	Obsługa VMware vSphere®, Citrix®, OpenStack®
Usługa katalogowa	Integracja z usługami Windows® AD Logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowanie folderu współdzielonego, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)

Obsługiwane systemy klienckie	Windows 11
Obsługiwane przeglądarki	Najnowsze wersje Chrome®, Firefox®, Edge®, Internet Explorer®, Safari®
Zasilanie	Wymogiem jest dostarczenie sprzętu wyposażonego w zasilacz maks. 90 W
Oprogramowanie	<ul style="list-style-type: none"> • Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych • Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów • Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. • Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera • pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Gwarancja	36 miesięcy gwarancji producenta

5. Dyski twarde – 10 sztuk.

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami dysków **WD Red Pro 8TB**.

Parametr	Charakterystyka (wymagania minimalne)
Pojemność	min. 8000 GB
Typ	HDD (magnetyczny)
Format	Format 3,5 cala
Interfejs	Serial ATA III
Pamięć cache	min. 256 MB
Prędkość obrotowa	7200 obr/min
Gwarancja	60 miesięcy gwarancji producenta

6. UPS (biurkowy) – 40 sztuki.

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami urządzenia **Eaton 5E 700 USB FR G2 5E700UF**.

Parametr	Charakterystyka (wymagania minimalne)
Moc pozorna	700 VA
Moc rzeczywista	360 W
Topologia (klasyfikacja IEC 62040-3)	Line-interactive
Liczba, typ gniazd wyjściowych	Min. 2 x FR
Typ gniazda wejściowego	1 x FR
Czas podtrzymania przy 50% obciążenia	Min. 6 minut
Tolerancja napięcia wejściowego	140-300V
Napięcie znamionowe wyjściowe	230 V

Zakres zmian napięcia wyjściowego (praca z baterii)	+/- 20%
Częstotliwość znamionowa wyjściowa	50/60 Hz
Zakres zmian częstotliwości wyjściowej (praca z baterii)	+/- 1 Hz
Układ automatycznej regulacji napięcia (AVR)	Tak
Kształt napięcia	modyfikowana sinusoida
Zimny start	Tak
Ochrona przed głębokim rozładowaniem	Tak
Interfejs komunikacyjny	<ul style="list-style-type: none"> • USB
Baterie wewnętrzne o pojemności	1x 7Ah/12V
Czas ładowania baterii do poziomu 90%	6 godz. do 90% pojemności użytkowej
Sygnały akustyczne	<ul style="list-style-type: none"> • Tryb bateryjny • Niski stan naładowania baterii • Przeciążenie • Wymiana baterii • Awaria
Sygnalizacja wizualna	dioda LED
Poziom hałasu	< 40 dBA dla pracy normalnej
Temperatura pracy	0 do 40 stopni C.
Znaki bezpieczeństwa	CE, TUV, raport CB
Bezpieczeństwo	IEC/EN 62040-1
Kompatybilność EMC	IEC/EN 62040-2
Gwarancja	24 miesiące gwarancji producenta

7. UPS (do serwerowni) – 4 sztuki.

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami urządzenia **Eaton 5SC2200IRT**.

Parametr	Charakterystyka (wymagania minimalne)
Moc pozorna	Min. 2200 VA
Moc rzeczywista	Min. 1980 W
Topologia (klasyfikacja IEC 62040-3)	Line-interactive z AVR
Współczynnik mocy	0,9
Czas przełączenia na baterię	<4 ms
Liczba, typ gniazd wyjściowych	8 x IEC C13 oraz 1 x IEC C19 16A
Typ gniazda wejściowego	IEC C20 16A
Czas podtrzymania dla 100% obciążenia dla pf=0,9	Min. 2 min
Czas podtrzymania przy 50% obciążenia dla pf=0,9	Min. 7 min
Napięcie znamionowe	200/208/220/230/240/250 V
Tolerancja napięci prostownika	184V - 276V
Częstotliwość znamionowa	50/60 Hz autodetekcja
Tolerancja częstotliwości	45– 55 Hz (sieć 50 Hz) 55 - 65 (sieć 60Hz)
Kształt napięcia	Sinusoidalny
Napięcie znamionowe wyjściowe	220/230/240 V do wyboru przez użytkownika
Zakres zmian napięcia	+6/-10% napięcia nominalnego
Częstotliwość wyjściowa	50/60 Hz
Współczynnik szczytu	3:1
Baterie wymieniane przez użytkownika "na gorąco"	Tak

Ochrona przed przetładowaniem	Tak (ograniczenie prądu ładowarki, wyłączenie ładowarki / alarm)
Ochrona przed głębokim rozładowaniem	Tak
Okresowy automatyczny test baterii	Tak
System zarządzania pracą baterii	System nieciągłego ładowania baterii.
Możliwość uruchomienia bez napięcia w sieci	Tak
Baterie wewnętrzne o pojemności nie mniejszej niż	9Ah 12V, minimum 4 szt.
Czas ładowania baterii do poziomu 90%	< 3 godz. do 90% pojemności użytkowej
Interfejs komunikacyjny	• USB
	• RS232 DB-9 żeński (HID)
	• port ROO oraz RPO
Panel sterowania z wyświetlaczem LCD	• Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPSa).
Sygnały akustyczne	• Awaria
	• Niski stan naładowania baterii
	• Przeciążenie
	• Serwis
Typ obudowy	Uniwersalna Tower/Rack 2U
Wposażenie standardowe	UPS, instrukcja obsługi(CD), instrukcja bezpieczeństwa
	1 x kabel szeregowy RS-232,
	1 x kabel komunikacyjny USB
	2 x kable wyjściowe IEC 10A
	2 x uchwyty kablów
	1 x zestaw szyn montażowych 19'
	1x kabel wejściowy
Poziom hałasu w odl. 1m	do 45 dBA dla pracy normalnej
Znaki bezpieczeństwa	CE, IEC/EN 62040-1 (CB Report), IEC/EN 62040-2 class B

Gwarancja	24 miesiące gwarancji producenta
Możliwość montażu ręcznego bypassu serwisowego	Tak

8. Zarządzalne urządzenia sieciowe z obsługą VLAN – 3 sztuki.

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami urządzenia **Cisco CBS350-48FP-4X-EU**.

Parametr	Charakterystyka (wymagania minimalne)
CECHY ZARZĄDZANIA	
Typ przełącznika	Zarządzany
Przełącznik wielowarstwowy	L2/L3
Obsługa jakości serwisu (QoS)	Tak
Zarządzany w chmurze	Tak
Zarządzanie przez stronę www	Tak
Inspekcja ARP	Tak
Konfigurowanie ustawień lokalizacji (CLI)	Tak
Obsługa MIB	Tak
OCHRONA	
Funkcje DHCP	DHCP relay, DHCP server, DHCPv6 client
Lista kontrolna dostępu (ACL)	Tak
Zasady Listy Kontroli Dostępu (ACL)	1024
IGMP snooping	Tak
Ochrona hasłem	Tak
obsługuje SSH/SSL	Tak

Filtrowanie adresów MAC	Tak
Szyfrowanie / bezpieczeństwo	HTTPS, SSH, SSL/TLS
PORTY I INTERFEJSY	
Podstawowe przełączanie RJ-45 Liczba portów Ethernet	48
Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)
Ilość slotów Modułu SFP+	4
Liczba portów USB 2.0	1
SIEĆ	
Standardy komunikacyjne	IEEE 802.1D, IEEE 802.1w, IEEE 802.1s, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad
Obsługa 10G	Tak
Dublowanie portów	Tak
Protokół drzewa rozpinającego	Tak
Blokowanie head-of-line (HOL)	Tak
Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
Kontrola wzrostu natężenia ruchu	Tak
Automatyczne MDI/MDI-X	Tak
Podpora kontroli przepływu	Tak
Agregator połączenia	Tak
Obsługa sieci VLAN	Tak

Liczba VLANs	4094
PRZESYŁANIE DANYCH	
Wielkość tabeli adresów	16000 wejścia
Zgodny z Jumbo Frames	Tak
Rozszerzenie Jumbo Frames	9000
FUNKCJE MULTICAST	
Obsługa Multicast	Tak
PROTOKOŁY	
Protokoły zarządzające	SNMP
KONSTRUKCJA	
Możliwości montowania w stelażu	Tak
Przycisk reset	Tak
Diody LED	Tak
WYDAJNOŚĆ	
Procesor wbudowany	Tak
Taktowanie procesora	1.4 GHz
Pojemność pamięci wewnętrznej	1 GB DDR
Aktualizacje oprogramowania urządzenia	Tak
MOC	
Zasilacz dołączony	Tak
GWARANCJA	
Gwarancja	Dożywotnia producenta (min. do 60 miesięcy od wycofania z produkcji/sprzedaży przez producenta)

9. UTM – 2 sztuki.

Zamawiający informuje, że przygotowując opis przedmiotu zamówienia posiłkował się cechami urządzenia **FortiGate-40F**.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania	<p>Wymagania Ogólne</p> <p>System bezpieczeństwa musi realizować wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.</p> <p>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 muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>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.</p> <p>System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. <p>Redundancja, monitoring i wykrywanie awarii</p> <ol style="list-style-type: none"> 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – wymagana jest możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall powinna istnieć funkcja synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych. 3. Monitoring stanu realizowanych połączeń VPN.

4. Agregacja linków statyczna oraz w oparciu o protokół LACP. Ponadto system na umożliwiać tworzenie interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

- System realizujący funkcję Firewall powinien dysponować co najmniej 5 portami Gigabit Ethernet RJ-45.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
 3. System Firewall powinien pozwalać skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
 4. System ma być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporę ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall musi uwzględniać: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System powinien realizować translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
 - Translację jeden do jeden oraz jeden do wielu.
 - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu powinna istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
5. Polityka firewall umożliwiająca filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
7. Element systemu realizujący funkcję Firewall musi integrować się z rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPsec VPN. W zakresie tej funkcji musi zapewniać:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługę protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh.
 - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
 - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System 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 łącz W

W zakresie routingu rozwiązanie musi zapewniać obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System musi umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz W

2. SD-WAN musi wspierać zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System musi dawać możliwość określania pasma dla poszczególnych aplikacji.
3. System musi pozwalać zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy musi zapewniać skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System musi umożliwiać skanowanie archiwów, w tym co najmniej: Zip, RAR.
4. System musi umożliwiać blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. 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 licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System musi zapewniać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
6. Możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. Możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

3. Filtr WWW powinien dostarczać kategorii stron zabronionych prawem np.: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW powinien umożliwiać statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwalając definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW powinien umożliwiać wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System powinien pozwalać określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. 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.
2. System powinien dawać możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System powinien umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

	<ol style="list-style-type: none"> 3. Możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. 4. System powinien współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System powinien dawać możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. <p>Logowanie</p> <ol style="list-style-type: none"> 1. Elementy systemu bezpieczeństwa powinny realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall musi zapewniać przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto musi zapewniać możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System musi zapewniać możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów powinno być możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Serwisy i licencje	<p>W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla</p>



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

	systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
Gwarancja i wsparcie	Sprzęt musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.