Szczegółowy Opis Przedmiotu Zamówienia

„Cyberbezpieczna Gmina Będzino”

Jednostka: Gminny Zakład Komunalny w Będzinie

1. Zakup serwera głównego dla Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**Serwer fizyczny wraz z systemem operacyjnym, wsparciem i aktualizacjami producenta**
Ilość:	1 sztuka
Okres gwarancji producenta:	Min. 60 m-cy
Parametry	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max. 1U, umożliwiającą instalację min. 8 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
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	Zainstalowany jeden procesor min. szesnasto-rdzeniowy klasy x86 do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 28 456 punktów w teście CPU Mark z dnia 17.06.2025 dostępnym na stronie internetowej:

	https://www.cpubenchmark.net/cpu_list.php (wyniki dołączone do zapytania)
RAM	Min. 128GB DDR5 RDIMM 5600MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Sloty PCIe	Trzy sloty PCIe LP.
Interfejsy sieciowe/FC/SAS	Wbudowane dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT Dwa interfejsy sieciowe 25Gb Ethernet w standardzie SFP28.
Dyski twarde	Zainstalowane 8 x 1,92GB SSD SATA.
Kontroler RAID	Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60, non-RAID (JBOD).
Wbudowane porty	min. port USB 2.0 oraz port USB 3.0, port VGA,
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Min. dwa zasilacze Hot-Plug maksymalnie 1100W Titanium.
Bezpieczeństwo	Zatrzask 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 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. Możliwość integracji z RSA SecurID

	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.
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 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. Karta powinna umożliwiać rozszerzenie funkcjonalności o: • możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych • 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
Oprogramowanie do zarządzania	Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniające poniższe wymagania: • Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia

	• Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

	• Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.
Normy Środowiskowe	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 rozporządzenia nr 1272/2008WE. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność

	sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera
Warunki gwarancji	Zamawiający wymaga min. 60 miesięcy gwarancji producenta 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 wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. 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 sie 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

	Zamawiający wymaga żeby w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostał u Zamawiającego. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Pozycja	
Przedmiot zamówienia:	**Licencja na serwerowy system operacyjny**
Ilość:	2 sztuki
Parametry	
Opis licencji	Licencja na serwerowy system operacyjny która zapewni poniżej opisane funkcjonalności dla serwera posiadającego 16 rdzeni procesora. Zamawiający wymaga dostarczenia licencji imiennej (na organizację), umożliwiającej przeniesienie w ramach programu licencji zbiorczych. Forma licencjonowania powinna zapewniać dostęp do platformy pozwalającej zarządzać posiadanymi licencjami, pobierać pakiety instalacyjne, uzyskiwać klucze licencyjne. Nie dopuszcza się licencjonowania typu OEM (przypisanego do maszyny fizycznej).
Minimalne parametry	• Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i 2 wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

	• Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. • Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. • Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. • Możliwość migracji maszyn wirtualnych z możliwością kompresji danych, bez zatrzymywania ich pracy, między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. • Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. • Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. • Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. • Wbudowane wsparcie instalacji i pracy na wolumenach, które: 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). • Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. • Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. • Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET • Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. • Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. • Graficzny interfejs użytkownika. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, • Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). • Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. • Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. • Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: Podstawowe usługi sieciowe: DHCP oraz DNS

	wspierający DNSSEC, Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, Ustanawianie praw dostępu do określonych zasobów dla użytkowników nie dołączonych do domeny, Zdalna dystrybucja oprogramowania na stacje robocze, Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: -dystrybucję certyfikatów poprzez http, -konsolidację CA dla wielu lasów domeny, -konsolidację CA dla wielu lasów domeny, szyfrowanie plików i folderów, Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, Serwis udostępniania stron WWW, Wsparcie dla protokołu IP w wersji 6 (IPv6), Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają

	zapewnić wsparcie dla: -Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, - Obsługi ramek typu jumbo frames dla maszyn wirtualnych, - Obsługi 4-KB sektorów dysków, - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, • Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, • Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) • Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. • Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). • Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. • Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. • Sterowniki i dokumentacja od producenta sprzętu • Oprogramowanie musi być dostarczone w najnowszej wersji

Pozycja	
Przedmiot zamówienia:	**Licencje dostępowe do serwerowego systemu operacyjnego**
Ilość:	15 sztuk
Parametry	
Opis	Licencja dostępowa na użytkownika dedykowana do zamawianego serwerowego systemu operacyjnego. Forma licencjonowania powinna zapewniać dostęp do platformy pozwalającej zarządzać posiadanymi licencjami, pobierać pakiety instalacyjne, uzyskiwać klucze licencyjne.

2. Zakup serwera do zarządzania kopiami bezpieczeństwa dla Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**Serwer zarządzania kopiami**
Ilość:	1 sztuka
Okres gwarancji producenta:	36 m-cy
Parametry	
Obudowa	• tower
Płyta główna	• Płyta główna z możliwością zainstalowania jednego procesora. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • na płycie głównej powinny znajdować się minimum 2 sloty przeznaczonych do instalacji pamięci
Procesor	• Zainstalowany jeden procesor 10-rdzeniowy klasy x86, min. 1,9GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 31 265 na dzień 17.06.2025 w teście

	PassMark dostępnym na stronie internetowej: https://www.cpubenchmark.net/
Pamięć RAM	• 16GB DDR5 4400 MT/s
Dysk twardy	• 512GB SSD • 10TB HDD, dedykowany do pracy ciągłej (Zamawiający dopuszcza możliwość montażu dysku producenta innego niż producent komputera)
Interfejs sieciowy	• 1x 1GE RJ45
Porty	• 1x USB 3.2 Gen1 Type-C • 5x USB 3.2 Gen1 Type-A • 4x USB 2.0 • 1x Audio • 3x DP
Zasilanie	• 260W PSU
Warunki gwarancji	• 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 wykonawcy (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. 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, dostawę 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. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

3. Zakup serwera NAS na potrzeby kopii zapasowych Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**Serwer NAS na potrzeby kopii zapasowych jednostek.**
Ilość:	1 sztuka
Okres gwarancji producenta:	36 m-cy
Parametry	
Typ	Sieciowy serwer plików NAS
Procesor	Procesor czterordzeniowy 64-bitowy o taktowaniu nie niższym niż 3.3GHz

Obudowa	RACK 19" 2U – wraz z kompletem szyn umożliwiającym zamontowanie w szafie RACK
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	• Minimum 8GB DDR4 ECC - RAM tego samego producenta, co serwer NAS, 1 x 8GB. Pamięć RAM zgodna z listą kompatybilności producenta oferowanego serwera. Możliwość rozszerzenia RAM do 32GB.
Liczba zatok na dyski twarde	12
Obsługiwane dyski twarde	3.5" SATA HDD / 2.5" SATA SSD – Hot Plug Zamawiający wymaga dostarczenia 5 dysków 3.5” SATA HDD o pojemności 8 TB każdy o parametrach nie gorszych niż: Prędkość obrotowa: 7200 RPM MTTF: 2 500 000 Obciążenie roczne: 550 TB Gwarancja producenta dysku: 5 lat Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera. Dyski zgodne z listą kompatybilności producenta oferowanego serwera. Oraz Minimum 2 dysków 2.5” SATA SSD o pojemności 1.92 TB każdy o parametrach nie gorszych niż: Odczyt losowy: 98.000 IOPS Zapisane terabajty (TBW): > 3.500 TB Gwarancja producenta dysku: 5 lat Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego serwera. Możliwość analizy okresu eksploatacji dysku w oparciu o rzeczywiste obciążenie z poziomu oferowanego serwera. Dyski zgodne z listą kompatybilności producenta oferowanego serwera.

Możliwość podłączenia modułu rozszerzającego	Tak
Minimalna ilość dysków z opcjonalnymi modułami rozszerzającymi, nie mniej niż:	○ 24
Porty na karty rozszerzeń	Minimum 1 x Gen3 x8 slot (x4 link)
Porty LAN	Wbudowane min. 2 x 1GbE RJ-45, 1 x 10GbE RJ-45
Porty USB 3.2	Minimum 2
Gniazdo rozszerzenia	Minimum 1

4. Zakup zarządzalnego UPS-a do serwera Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**Zasilacz awaryjny UPS**
Ilość:	1 sztuka
Okres gwarancji producenta:	36 m-cy
Parametry	
Obudowa	Uniwersalna tower/rack max. 2U
Moc, napięcia, gniazda, ochrony, dodatkowe dane	Moc pozorna: 3000 VA Moc rzeczywista: 3000 W Współczynnik mocy: 1 Topologia (klasyfikacja IEC 62040-3): line-interactive Liczba, typ gniazd wyjściowych: 8 x C13, 2 x C19 Typ gniazda wejściowego: Gniazdo C20 Czas podtrzymania dla 100% obciążenia: 3 minuty Napięcie znamionowe: 230 V Tolerancja napięcia prostownika: 160 - 294 V (regulowana do 150 - 294 V) Częstotliwość znamionowa: 50/60 Hz autodetekcja Tolerancja częstotliwości: 47 - 70 Hz (system 50 Hz); 56,5 - 70 Hz (system 60 Hz); 40 Hz w trybie niskiej czułości Napięcie znamionowe wyjściowe: 230 V (domyślnie) /

	200/208/220/240 V Częstotliwość wyjściowa: 50/60 Hz Baterie wymieniane przez użytkownika "na gorąco": Tak Ochrona przed przeładowaniem: Tak Ochrona przed głębokim rozładowaniem: Tak Okresowy automatyczny test baterii: Tak Zimny start: Tak Max. wymiary UPS (szer. x gł. x wys. w mm): 438 x 603 x 85,5 Poziom hałasu w odl. 1m: < 45 dBA
System zarządzania pracą baterii	System nieciągłego ładowania baterii. Do oferty dołączyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
Interfejs komunikacyjny	USB, RS232 DB-9 żeński (HID), miniport wyłącznik awaryjny RPO, miniport wyłącznik ON/OFF, listwa zaciskowa dla przekaźnika wyjściowego
Panel sterowania z wyświetlaczem LCD	Panel LCD obrotowy (do ułatwienia odczytów przy obu wariantach montażu UPS'a) ze wskazaniami chwilowego poziomu obciążenia i poziomu naładowania baterii, z możliwością sterowania poszczególnymi segmentami odbiorów oraz pomiarem sprawności i zużycia energii przez odbiory (w kWh)
Przyciski sterujące i wskaźniki diodowe LED	Poziomy rząd przycisków sterowania; Poziomy rząd wskaźników stanu: trybu normalnego (zielony), trybu bateryjnego (żółty), usterki (czerwony); Pasek LED sygnalizujący stan; sygnalizator akustyczny (awaria, serwis, niski stan naładowania baterii, przeciążenie); przycisk Escape (anulowanie); przyciski funkcyjne (przewijanie w górę i w dół); przycisk Enter (potwierdzający)
Wyposażenie	UPS 3 kVA, instrukcja obsługi, instrukcja bezpieczeństwa; przewód zasilający; kabel RS232; kabel USB; karta SNMP; uchwyty kablowe; podstawki do montażu pionowego (wieża); 2 przewody IEC 10 A; zestaw szyn montażowych do szafy 19" Karta SNMP "cyberbezpieczeństwo (certyfikaty UL 2900-2-2 /IEC62443 /HTTPS/MQTT/NDIS/LDAP/NVD//SSH/PKI, pakiet szyfrów TLS 1.2 z minimum SHA256)"; certyfikaty CA i PKl; prędkość gigabitowa (half-duplex, full-duplex); różne poziomy

	nadawania dostępu do konta administratora lub użytkownika
Dołączone oprogramowanie	Do bezpiecznego zamykania systemów operacyjnych przy wyczerpaniu baterii (minimum: Windows: 10, 2000, XP, 2003, Vista, Server 2008, 7; Linux: Red Hat, Fedora Core, SuSE; UNIX: AIX, HP-UX, SCO, SGI Irix, Mac OS, Sun Solaris; Novell NetWare do v 6.5). Oprogramowanie musi mieć możliwość wyboru polskiej wersji językowej.
Zgodność z normami UE	Deklaracja zgodności producenta
Dodatkowe cetyfikaty	ISO9001 producenta urządzenia

5. Zakup 5 UPS-ów na stanowiska pracy dla Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**Zasilacz awaryjny UPS**
Ilość:	5 sztuk
Okres gwarancji producenta:	24 m-ce
Parametry	
Moc pozorna	700 VA
Moc rzeczywista	360 W
Technologia	Line-Interactive
Gniazda wyjściowe z podtrzymaniem bateryjnym	typu E (2P+Z), minimum 2szt
Przewód zasilający	Przymocowany na stałe do zasilacza UPS
Port komunikacyjny	USB umieszczony na przednim panelu zasilacza UPS
Wskaźnik stanu UPS	Dioda LED
Parametry wejściowe	
Prąd znamionowy	5A

Napięcie znamionowe	220-240 V; 50/60 Hz
Zakres napięcia wejściowego	140-300 V; 45-65 Hz
Parametry wyjściowe	
Znamionowe napięcie wyjściowe	220/230/240 V
Regulacja napięcia w trybie bateryjnym	+/-20%
Sprawność w trybie normalnym	>95%
Sprawność w trybie bateryjnym	>60%
Regulacja częstotliwości w trybie normalnym	zgodnie z siecią zasilającą
Regulacja częstotliwości w trybie bateryjnym	+/-1 Hz
Częstotliwość w trybie normalnym	zgodnie z siecią zasilającą
Częstotliwość w trybie bateryjnym	50/60 Hz
Przeciążalność	[110%,120%] 5 min; >120% 1 s
Zdolność zwarciowa w trybie bateryjnym	5A
Wytrzymywany czas przepływu prądu zwarciowego	50 ms
Czas przełączania	10 ms dla przejścia z trybu normalnego do trybu bateryjnego
Bateria	
Specyfikacja	12 V DC – 1 x 12 V, 7 Ah
Typ	Valve Regulated Lead-Acid (VRLA) szczelne, bezobsługowe, z minimalną żywotnością 3-5 lat w temperaturze 25°C
Monitoring	Zaawansowany monitoring z wczesnym wykrywaniem awarii oraz powiadamianiem.

Zimny start	Tak
Parametry środowiskowe i bezpieczeństwo	
Normy	IEC/EN 62040-1 Safety
	IEC/EN 62040-2 Electromagnetic Compatibility EMC
	IEC/EN 62040-3 Performance
EMC (emisyjność)	CISPR32 Class A
	IEC/EN 61000-3-2 Flickers
	IEC/EN 61000-3-3 Harmonics
EMC (odporność)	IEC 61000-4-2, (ESD): 4 kV Contact Discharge / 8 kV Air Discharge
	IEC 61000-4-3, (Radiated field): 10 V/m
	IEC 61000-4-4, (EFT): 4 kV
	IEC 61000-4-5, (Surges): 1 kV Differentiel Mode / 2 kV Common Mode
	IEC 61000-4-6, (Electromagnetic field): 10 V
	IEC 61000-4-8, (Conducted magnetic field): 30 A/m
Oznaczenia	CE, EAC, Cm, Ukr, UKCA,
Stopień ochrony	IP20
Układ sieci	UPS można podłączyć do układów zasilania TN, TT, IT, ten sam system jest dostarczany do obciążenia.
Klasa ochronności	Klasa I
Temperatura pracy	0°C do 40°C (32°F do 104°F)
Temperatura przechowywania	0°C do 40 °C (32°F do 104 °F) z baterią
	-25°C do 55 °C (-13°F do 131 °F) bez baterii
Wilgotność względna	Przechowywanie: 0-93% bez kondensacji
	Praca: 0-85% bez kondensacji
Wysokość n.p.m. podczas pracy	2000 m

Wysokość n.p.m. podczas transportu	Do 10000 m (32,808 ft) nad poziomem morza
Poziom hałasu	<25 dBA
Gwarancja	24 iesiące

6. Zakup 1 switcha zarządzalnego wraz z 1-letnim wsparciem dla Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**Switch z licencjami na 1 rok**
Ilość:	1 sztuka
Okres gwarancji producenta:	24 m-ce
Parametry	
Przełącznik sieciowy	W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.
Parametry fizyczne platformy	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V.
Interfejsy sieciowe - wymagania minimalne	1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a. 48 porty GE RJ-45. b. 4 porty 10 GE SFP+.
Zarządzanie	• Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). • Wsparcie dla SNMP w wersjach 1-3 • Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne

	konfigurowanie oraz zarządzanie przełącznikami. • Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. • Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. • Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). • Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. • Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. • Automatycznie wykonywane rewizje konfiguracji.
Wymagane funkcje	• Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
Dodatkowe funkcje	1. Przełączniki muszą wspierać tryb pracy, w którym są

urządzenia przy integracji z systemem centralnego zarządzania / NAC	zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN. • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na zewnętrzny serwer syslog. • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. • Obsługa białych i czarnych list adresów MAC. • Wykrywanie aplikacji komunikujących się w sieci. 2. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego

	zarządzania lub NAC.
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	• System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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.

7. Zakup UTM z licencją na 1 rok dla Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**UTM wraz ze wsparciem oraz licencją na 1 rok**
Ilość:	1 sztuka
Okres gwarancji producenta:	24 m-ce
Parametry	
Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być 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. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

	System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: • 10 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System jest wyposażony w zasilanie AC.
Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware.

	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. Rozwiązanie posiada 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 uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: a. Translację jeden do jeden oraz jeden do wielu. b. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje 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 umożliwia 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 integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. a. Amazon Web Services (AWS). b. Microsoft Azure. c. Cisco ACI.Google Cloud Platform (GCP). d. OpenStack. e. VMware NSX. f. Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: a. Wsparcie dla IKE v1 oraz v2. b. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). c. Obsługa protokołu Diffie-Hellman grup 19, 20. d. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. e. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. f. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. g. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. h. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. i. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. j. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. k. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. l. Mechanizm „Split tunneling” dla połączeń Client-to-Site.

	2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: a. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. b. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. 3. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia 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 RIPng), 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 umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
	1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

	2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje 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 współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia 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 opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 6. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 4. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 5. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 6. System daje 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 korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

	2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość 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 ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall umożliwia 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 daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 3. System umożliwia 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 jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia 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.
Logowanie	1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu,

	aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres 24 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.

8. Zakup oprogramowania antywirusowego wraz z konsolą na 1 rok dla Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**Oprogramowanie antywirusowe z usługą chmurową**
Ilość:	10 sztuk
Parametry	
Administracja zdalna w chmurze	1.Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego. 2.Rozwiązanie musi umożliwiać dostęp do konsoli centralnego

	zarządzania z poziomu interfejsu WWW. 3.Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL. 4.Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji. 5.Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy. 6.Rozwiązanie musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM. 7.Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej. 8.Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak. 9.Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta. 10.Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów. 11.Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera. 12.Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
Ochrona stacji roboczych	1.Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11). 2.Rozwiązanie musi wspierać architekturę ARM64. 3.Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4.Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet. 5.Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 6.Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 7.Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych

	katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. 8.Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych. 9.Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku. 10.Rozwiązanie musi integrować się z Intel Threat Detection Technology. 11.Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 12.Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS. 13.Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 14.Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych. 15.Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia. 16.Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: •tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, •tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, •tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, •tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, •tryb inteligentny, w którym rozwiązanie będzie powiadamiało

	wyłącznie o szczególnie podejrzanych zdarzeniach. 17.Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 18.Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa. 19.Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji. 20.Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 21.Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 22.Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook. 23.Zapora osobista rozwiązania musi pracować w jednym z czterech trybów: •tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, •tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie, •tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora, •tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 24.Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki. 25.Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 26.Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 27.Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych. 28.Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 29.Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

	30.W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
Ochrona serwera	1.Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux. 2.Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami. 3.Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 4.Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS. 5.Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 6.Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji. 7.Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów. 8.Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. Dodatkowe wymagania dla ochrony serwerów Windows: 9.Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive. 10.Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS). 11.Rozwiązanie musi wspierać skanowanie magazynu Hyper-V. 12.Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 13.Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.

	14.Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. 15.Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 16.Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP. 17.Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu. Dodatkowe wymagania dla ochrony serwerów Linux: 18.Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej. 19.Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web. 20.Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon. 21.Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
Ochrona urządzeń mobilnych opartych o system Android	1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie. 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne. 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki). 4. Rozwiązanie musi posiadać możliwość skonfigurowania zaufanej karty SIM. 5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi: a. usunięcie zawartości urządzenia, b. przywrócenie urządzenie do ustawień fabrycznych, c. zablokowania urządzenia, d. uruchomienie sygnału dźwiękowego, e. lokalizację GPS. 6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji. 7. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o: a. nazwę aplikacji,

	b. nazwę pakietu, c. kategorię sklepu Google Play, d. uprawnienia aplikacji, e. pochodzenie aplikacji z nieznanego źródła.

Wdrożenie systemu antywirusowego	Instalacja potrzebnych maszyn wirtualnych, systemów operacyjnych i odpowiednie przygotowanie serwera do systemu antywirusowego. Wdrożenie polis GPO umożliwiających dystrybucję spreparowanego agenta w sieci zamawiającego. Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencje), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego. Aktualizacja do najnowszej wersji oprogramowania. Dwuletnie nieodpłatne wsparcie ze trony pracowników Wykonawcy w wyżej wymienionym zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego. Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z: • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych. Prace zostaną zakończone protokołem.

9. Usługa wdrożenia zakupionych sprzętów przez specjalistów IT - kompleksowe zainstalowanie oraz konfiguracja sprzętu dla Gminnego Zakładu Komunalnego w Będzinie

Pozycja	
Przedmiot zamówienia:	**Usługa wdrożenia oraz dostosowania serwera, urządzeń sieciowych i oprogramowania zgodnie z wymogami KRI**
Ilość:	1 sztuka
Parametry	
Wdrożenie urządzenia UTM oraz integracja z środowiskiem IT.	Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencje), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego. Aktualizacja do aktualnych wersji oprogramowania. Wydzielenie podsieci VLAN w tym sieci bezprzewodowych zgodnie z wskazaniami Zamawiającego. Zabezpieczenie ruchu we wszystkich podsieciach zgodnie z wymaganiami Zamawiającego. Integracja z Istniejącym środowiskiem IT. Wdrożenie VPN – konfiguracja, integracja z GPO i zabezpieczenie Tuneli VPN. Wdrożenie wydzielonej, galwanicznej sieci zarządzającej systemami IT. Wdrożenie wykonywane na miejscu. Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego. Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z: • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany

	informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych. Prace zostaną zakończone protokołem.
Wdrożenie Serwera wraz z kontrolerem zdalnego zarządzania	Fizyczny montaż serwera w siedzibie Zmawiającego. Podłączanie do sieci elektrycznej w tym urządzeń dystrybucji zasilania. Konfiguracja z systemami dystrybucji zasilania Zamawiającego. Montaż serwera z prowadnicami musi zostać wykonany w sposób umożliwiający wysunięcie w czasie pracy. Wszystkie elementy instalacyjne w tym kable sieciowe, kable elektryczne, adaptery zasilania, itp. zapewnia Wykonawca w cenie usługi. Wdrożenie zintegrowanego modułu zdalnego zarządzania serwerem. Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencję), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego. Aktualizacja do najnowszej wersji oprogramowania. Zapewnienie konfiguracji wszystkich parametrów w tym macierzy dyskowych zgodnie z wymogami prawa i wytycznymi Zamawiającego. Podłączenie do podsieci zgodnie w wymaganiami Zamawiającego. Integracja z istniejącym środowiskiem IT. Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego. Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z: • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych.

	Prace zostaną zakończone protokołem.
Wdrożenie Hypevisor	Fizyczna i techniczna Instalacja oprogramowania w siedzibie Zamawiającego wraz z pełną konfiguracją opisaną powyżej. Migracja starego środowiska na nowy Hypervisor. Migracja musi odbyć się z rozbiciem na poszczególne serwery wirtualne zgodnie ze wskazaniami Zamawiającego. Proces przejścia ze starego serwera na nowy serwer trzeba wykonać poza godzinami pracy instytucji, w celu zachowania ciągłości pracy Zamawiającego. Wdrożenie wydzielonej, galwanicznej sieci wirtualnej zarządzającej systemami IT, do wykonywania kopii serwera wirtualnego. Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego. Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z: • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych. Prace zostaną zakończone protokołem.
Wdrożenie systemu kopii bezpieczeństwa	Wdrożenie kompletnego systemu kopii bezpieczeństwa w jednostce na nowo zakupionym urządzeniu NAS. Konfiguracja przesyłania kopii do zewnętrznej lokalizacji. Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na

	miejscu. Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego. Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z: • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych. Prace zostaną zakończone protokołem.
Wdrożenie usługi katalogowej Active Directory	Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z: • Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych. Instalacja maszyn wirtualnych, systemów operacyjnych i przygotowanie serwerów. Migracja istniejącego środowiska IT Zamawiającego. W przypadku braku możliwości migracji istniejących rozwiązań, wdrożenie od podstaw nowej domeny wraz z przeniesieniem zasobów. Wdrożenie polis GPO dostosowujących środowisko do wyżej wymienionych wymogów prawa i Zamawiającego - takich jak polisy synchronizacji czasu, dokumentów, haseł, blokowania, dostępu do zasobów, etc. Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencje), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego. Aktualizacja do najnowszych wersji oprogramowania. Wdrożenie usługi File Server, utworzenie, przeniesienie, przypisanie uprawnień i zabezpieczenie zasobów zgodnie z zaleceniami Zamawiającego. (np. dyski wspólne z podziałem uprawnień).

	Wdrożenie usługi Print Server, wraz z konfiguracją i zabezpieczeniami. Wdrożenie i zabezpieczenie usługi DNS. Przygotowanie maszyn wirtualnych, podłączenie do domeny oraz ich zabezpieczenie. Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych, Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail i numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego. Udzielenie zdalnego wsparcia dla pracowników IT Zamawiającego, nie będącego następstwem błędów i awarii w liczbie 30 godzin. Prace zostaną zakończone protokołem.
Wdrożenie systemu antywirusowego	Instalacja potrzebnych maszyn wirtualnych, systemów operacyjnych i odpowiednie przygotowanie serwera do systemu antywirusowego. Wdrożenie polis GPO umożliwiających dystrybucję spreparowanego agenta w sieci zamawiającego. Aktywacja i rejestracja wszystkich komponentów (urządzenia i licencje), przypisanie licencji do adresu e-mail wskazanego przez Zamawiającego. Aktualizacja do najnowszej wersji oprogramowania. Dwuletnie nieodpłatne wsparcie ze strony pracowników Wykonawcy w wyżej wymienionym zakresie. Przez 24 miesiące od wykonania usługi wdrożenia, w przypadku wystąpienia błędów wdrożeniowych – Wykonawca wykona naprawę zdalnie w czasie do 5 godzin, jeżeli nie będzie możliwości wykonania naprawy zdalnie, pracownik Wykonawcy dojedzie w czasie do 24 godzin do siedziby Zamawiającego, gdzie dokona naprawy na miejscu. Wykonawca udostępni adres e-mail oraz numer telefonu. Czas jest liczony od wysłania wiadomości e-mail przez Zamawiającego. Usługa musi zawierać wymagane konfiguracje i zostać wykonana zgodnie z:

	• Polską Normą PN-ISO/IEC 27002, • Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które określa minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także minimalne wymagania dla systemów teleinformatycznych. Prace zostaną zakończone protokołem.
Szkolenia	• Szkolenie dla działu IT – moduł zdalnego zarządzania serwerem • Szkolenie dla działu IT – zarządzanie oprogramowaniem do tworzenia kopii zapasowej Wszystkie szkolenia wykonane w siedzibie zamawiającego. Szkolenia należy wykonać z uwzględnieniem konfiguracji zastosowanych w systemach IT Zamawiającego. Osoby prowadzące szkolenia muszą posiadać udokumentowaną wiedzę. Szkolenia zakończone protokołem. Wykonawca zapewni nieodpłatne wsparcie w wyżej wymienionym zakresie przez okres 24 miesięcy od zakończenia szkolenia w liczbie 30 godzin. Wsparcie zostanie udzielone w terminie 48 godzin od chwili zgłoszenia. Wykonawca udostępni do kontaktu adres e-mail i numer telefonu. Czas jest liczony od wysłania e-mail przez Zamawiającego. Prace zostaną zakończone protokołem.