Fundusze Europejskie
na Rozwój Cyfrowy

Nr sprawy: RGK.271.1.2026

Opis Przedmiotu Zamówienia

Dostawa sprzętu i oprogramowania teleinformatycznego w ramach projektu Zwiększenie cyberbezpieczeństwa w gminie Zawidz w ramach projektu „Cyberbezpieczny Samorząd”

Umowa o powierzenie grantu o numerze:
FERC.02.02-CS.01-001/23/2570/ FERC.02.02-CS.01-001/23/2024

Luty 2026

Spis treści

1. Zakres zamówienia

Przedmiotem zamówienia są następujące zadania:

1) Urządzenie UTM - 2 szt.
2) Przełączniki sieciowe - 3 szt.
3) Dostawa i instalacja serwera – 1 szt.
4) Serwer do backupu – 1 szt.
5) Rozwiązanie do zbierania i analizowania danych z urządzeń sieciowych – 1 szt.
6) System tworzenia i zarządzania kopiami zapasowymi – 1 szt.
7) System kontroli dostępu NAC – 1 szt.

2. Wymagania ogólne

1. Wszystkie dostarczane urządzenia muszą być fabrycznie nowe, nieużywane, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostawy.
2. Wykonawca zobowiązany jest do dostarczenia wszelkich niezbędnych kabli zasilających, połączeniowych i akcesoriów wymaganych do prawidłowego uruchomienia i pracy infrastruktury.
3. Dostarczone oprogramowanie i dokumentacja techniczna muszą być w języku polskim lub angielskim. Interfejs administracyjny systemów powinien umożliwiać zmianę języka na polski.
4. Wykonawca zapewni instruktaż administratorów w zakresie obsługi dostarczonego sprzętu i oprogramowania.
5. Wszystkie prace instalacyjne i wdrożeniowe muszą być zrealizowane w siedzibie Zamawiającego, w terminie wskazanym w OPZ.
6. Wykonawca zobowiązany jest do prowadzenia prac w sposób minimalizujący przerwy w dostępności systemów teleinformatycznych Zamawiającego

3. Urządzenie UTM - 2 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Wymagania ogólne	1. 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. 2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 3. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. 4. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. 5. 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 instalację oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest 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 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
Funkcje systemu bezpieczeństwa	1. W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 2. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 3. Kontrola Aplikacji. 4. Poufność transmisji danych - połączenia szyfrowane IPSec VPN. 5. Ochrona przed malware. 6. Ochrona przed atakami - Intrusion Prevention System. 7. Kontrola stron WWW. 8. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 9. Zarządzanie pasmem (QoS, Traffic shaping). 10. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 11. 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. 12. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 13. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.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: ● Translację jeden do jeden oraz jeden do wielu. ● 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: adresy 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.

	● Amazon Web Services (AWS). ● Microsoft Azure. ● Cisco ACI. ● Google Cloud Platform (GCP). ● OpenStack. ● VMware NSX. ● Kubernetes.
Połączenia VPN	1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: ● Wsparcie dla IKE v1 oraz v2. ● Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). ● Obsługa 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. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec 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). 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. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	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. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 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 usłudze chmurowej realizowanej na terenie Unii Europejskiej. 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. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia 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. 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. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).

	7. 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 wieloskładnikowego. 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 wieloskładnikowego 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. W ramach logowania element systemu pełniący 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.
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni.
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 do 15 maja 2026 r.
Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.
Opisy do wymagań ogólnych	1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.
Instalacja i wdrożenie	1. Wykonawca dostarczy urządzenia do siedziby Zamawiającego oraz przeprowadzi fizyczny montaż urządzeń w szafie rack, zgodnie z dokumentacją producenta i standardami inżynierskimi.

	2. Konfiguracja dwóch urządzeń UTM do pracy w klastrze w trybie wysokiej dostępności (High Availability). 3. Ustalenie głównych zasad routingu, filtrowania ruchu oraz współdzielenia obciążeń pomiędzy urządzeniami w klastrze. 4. Implementacja polityk kontroli dostępu (Firewall) w oparciu o adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje, kategorie URL, kraje. Polityki muszą być synchronizowane między urządzeniami w klastrze. 5. Przeprowadzenie testów weryfikujących poprawność działania urządzeń w klastrze oraz ich wydajności. 6. Testowanie mechanizmu przełączania w przypadku awarii jednego z urządzeń (failover). 7. Wykonawca zobowiązany jest do dokumentowania wykonanych prac. 8. Prace instalacyjne i wdrożeniowe muszą być zrealizowane w siedzibie Zamawiającego. Nie dopuszcza się pracy zdalnej. 9. Instruktaż stanowiskowy administratora IT Zamawiającego z wdrożonego rozwiązania i konfiguracji (minimum 8 godzin) w siedzibie Zamawiającego. 10. Oferent w zakresie przedmiotu zamówienia musi uwzględnić czas pracy inżyniera, na potrzeby uruchomienia urządzenia w siedzibie Zamawiającego. 11. Z uwagi na typ pracy urzędu, wykonywane prace nie mogą powodować problemów w dostępności do systemu komputerowego Zamawiającego.

4. Przełączniki sieciowe - 3 szt.

Parametry	Opis
Parametry fizyczne platformy	• Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V. • Maksymalny pobór mocy: 60 W. • Minimalny zakres temperatury pracy: 0–40°C.
Interfejsy sieciowe – wymagania minimalne	• 48 portów GE RJ-45 (nie dopuszcza się portów combo). • 4 porty 10 GE SFP+
Zarządzanie	• Zarządzanie przez CLI (w tym SSH) i GUI (HTTPS). • SNMP v1/v2c/v3. • Zarządzanie przez dedykowany kontroler/system zarządzania z funkcjami automatycznego wykrywania i centralnego zarządzania. • Aktualizacja oprogramowania przez TFTP/FTP i GUI. • Konfiguracja jako edytowalny plik tekstowy (offline). • Backup konfiguracji przez GUI i CLI (TFTP/FTP). • Definiowanie administratorów lokalnie i przez serwery Radius/TACACS+. • Definiowanie ról administratorów z określeniem uprawnień dostępu. • Automatyczne rewizje konfiguracji.
Parametry wydajnościowe	• Przepustowość min. 175 Gbps (wire-speed na wszystkich portach). • Min. 250 Mpps. • Tablica MAC: min. 32k wpisów. • Opóźnienie: poniżej 2 mikrosekund.
Wymagane funkcje	• Automatyczna negocjacja prędkości i duplexu. • Jumbo Frames. • Obsługa 802.1d/w/s (STP/RSTP/MSTP).

	• Agregacja portów (802.3ad). • Obsługa co najmniej 4,000 VLANów (802.1Q). • Routing statyczny. • Port-mirroring. • Uwierzytelnianie 802.1x na port i na adres MAC. • Guest VLAN i wsparcie dla urządzeń nieobsługujących 802.1x. • Dynamiczne VLAN w 802.1x. • Obsługa protokołu sFlow.
Dodatkowe funkcje przy integracji z centralnym zarządzaniem/NAC	• Wsparcie trybu port extender/leaf w architekturze spine-leaf. • Centralne zarządzanie konfiguracją, VLANami, aktualizacjami. • Blokowanie ruchu w ramach VLANu. • Rozpoznawanie i automatyczne przypisywanie stref urządzeniom. • Integracja z systemem dostępu – decyzje na podstawie nazwy hosta/użytkownika, typu urządzenia/OS. • Automatyczna detekcja i rekomendacje konfiguracji. • Przesyłanie logów na serwer syslog. • Captive Portal. • Obsługa białych/czarnych list MAC. • Wykrywanie aplikacji w sieci. • Redundantne połączenie z elementami zarządzającymi. • Wszystkie niezbędne licencje dla funkcjonalności integracji NAC.
Funkcje przy integracji z zarządzaniem / bezpieczeństwem	• Stateful Firewall pomiędzy VLAN. • Routing statyczny i dynamiczny (OSPF), Policy Based Routing.
Gwarancja	• 12 miesięcy gwarancji producenta: naprawa lub wymiana sprzętu w trybie 24 / 7.
Wymagania ogólne	• Dostawca powinien przedstawić dokument od importera potwierdzający spełnienie wymogów prawnych dla produktów podwójnego zastosowania (w tym certyfikat systemu zarządzania jakością dla kontroli eksportu, transferu, pośrednictwa i tranzytu). • Oferent musi przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora o posiadaniu autoryzacji na sprzedaż oferowanych rozwiązań.
Instalacja, logiczny podział sieci na sieci wirtualne	W ramach wdrożenia Wykonawca zobowiązany jest do: • Dostawy urządzeń do wskazanej lokalizacji, • Przeprowadzenia analizy sieci oraz zaprojektowania sieci VLAN oraz przedstawienie projektu sieci do zaakceptowania Zamawiającemu, • Montażu i przeprowadzenia podstawowej konfiguracji urządzeń: - ustawienie podstawowych parametrów pracy urządzeń, aktualizację firmware, podłączenie do sieci energetycznej i logicznej, itp. • Konfiguracja połączeń pomiędzy przełącznikami sieci LAN • Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych, aby odseparować różne typy ruchu, ale nie mniej niż: - VLAN Pracowniczy – 3 szt. - VLAN Serwer

	- VLAN Drukarki - VLAN Klienta / Gościa - VLAN telefonów VoIP - VLAN monitoringu wizyjnego • Sprawdzenia poprawności działania urządzeń po konfiguracji. • Weryfikacji komunikacji między VLAN-ami zgodnie z założeniami bezpieczeństwa. • Sporządzenia dokumentacji powykonawczej zawierającej konfigurację urządzeń, schemat sieci i przyjęte polityki bezpieczeństwa i przekazania dokumentacji Zamawiającemu. Oferent w zakresie przedmiotu zamówienia musi uwzględnić czas pracy inżyniera, na potrzeby uruchomienia urządzenia w siedzibie zamawiającego. Z uwagi na typ pracy urzędu, wykonywane prace nie mogą powodować problemów w dostępności do systemu komputerowego Zamawiającego. • Po zakończeniu prac, Wykonawca dokona instruktażu stanowiskowego dla Administratora IT obejmującego zapoznanie z wdrożoną konfiguracją. Instruktaż odbędzie się w siedzibie Zamawiającego i obejmie nie mniej niż 4 godzin.

5. Dostawa i instalacja serwera – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Obudowa	Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków SAS/SATA 2.5”. Możliwość rozbudowy o kolejne min. 8 wnęk na dyski SAS/SATA/NVMe 2.5”. Serwer musi mieć możliwość wyposażenia w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający: • wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS • wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy • przywracanie konta administratora • wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera • wyświetlanie w czasie rzeczywistym temperatury procesorów • konfigurowanie ustawień sieciowych modułu zarządzania. Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera w celach serwisowych. Przedni panel zamykany na klucz, chroniący dyski przed nieuprawnionym wyjęciem z serwera.

Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor 16-rdzeniowy o taktowaniu pojedynczego rdzenia min. 2.0GHz (base frequency) osiągający wynik wydajnościowy w teście PassMark – CPU Mark min. 49 000 pkt. dla konfiguracji dwuprocesorowej. Testy dla oferowanego modelu procesora muszą być opublikowane i ogólnie dostępne na stronie https://www.cpubenchmark.net/multi_cpu.html
Pamięć RAM	Minimum 128 GB RAM DDR5 RDIMM 5600MT/s. Płyta główna serwera powinna posiadać min. 32 sloty DIMM.
Zabezpieczenie pamięci	Memory mirroring, ECC, patrol scrubbing, SDDC, memory thermal throttling, ADDDC-SR.
Pamięć masowa	Zainstalowane minimum 4 dyski serwerowe SAS SSD 24Gb/s o pojemności min. 1.6 TB każdy. Zainstalowany sprzętowy kontroler RAID SAS/SATA wyposażony w min. 4GB Cache i podtrzymanie bateryjne, umożliwiający skonfigurowanie poziomów RAID 0, 1, 10, 5, 50, 6, 60.
Wbudowane porty	4 x USB z czego nie mniej niż 2 x USB 3.0. Port USB TYP-C lub microUSB na przednim panelu obudowy. 1 x VGA na tylnym panelu obudowy oraz 1 x VGA na tylnym panelu obudowy. Złącze USB TYP-C / microUSB na przednim panelu musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń, jak również nie mogą zajmować wymaganych wnęk dyskowych.
Interfejsy sieciowe	Zainstalowane i w pełni funkcjonalne interfejsy: • minimum 1 x RJ-45 Ethernet management port, • minimum 4 porty 1Gb/s Ethernet Base-T niezajmujące slotów PCI-E, • minimum 2 porty 10/25 Gb/s Ethernet obsługujące wkładki optyczne Multimode oraz Singlemode SFP+ 10Gb/s oraz SFP28 25Gb/s, • minimum 2 porty 10Gb/s Ethernet Base-T
Sloty PCI-E	Minimum 3 aktywne sloty PCI-E 4.0 x8 obsługujące karty FHHL. Możliwość rozbudowy / rekonfiguracji serwera w celu uzyskania min. 8 slotów PCIE.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wentylatory	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla oferowanej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).

Zasilanie	Minimum dwa identyczne zasilacze klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie więcej niż 1600W.
Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą serwera jako fabryczne rozwiązanie producenta. Moduł TPM 2.0
Zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca: • monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), • monitorowanie w czasie rzeczywistym poboru prądu przez serwer, • zbieranie logów błędów hardware, • przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, • montowanie wirtualnych napędów, • zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, • wysyłanie zawiadomień droga mailową i poprzez SNMP • wsparcia dla IPMI, SSH, Redfish • wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows, • nadawanie ról użytkownikom, • możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, • możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem z urządzeń mobilnych z systemem Android i iOS.
Dodatkowe oprogramowanie do zarządzania i monitorowania	Wraz z serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na: • włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów. • tworzenie szablonów instalacyjnych dla systemów operacyjnych. • tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów. • zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera. • aktualizacja sterowników i BIOS serwerów. • zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.

Kompatybilność	Producent serwerów musi posiadać certyfikat jakości według normy ISO 9001 na produkcję oferowanego asortymentu lub równoważny certyfikat jakości oraz certyfikat według normy ISO-14001 Systemu Zarządzania Środowiskowego lub równoważną normę zarządzania środowiskowego. Należy dołączyć do oferty dokumenty potwierdzające spełnianie wymogów w zakresie opisanym powyżej. Wykonawca zobowiązany jest do dostarczenia sprzętu posiadającego oznaczenie CE, potwierdzające zgodność z obowiązującymi dyrektywami Unii Europejskiej w zakresie bezpieczeństwa, zdrowia i ochrony środowiska. Wykonawca przedstawi oświadczenie producenta sprzętu potwierdzające, że oferowany sprzęt posiada oznakowanie CE oraz spełnia wymagania odpowiednich dyrektyw UE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Windows Server 2022, Windows Server 2025.
Gwarancja	Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP. • Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie 5x9 onsite z gwarantowanym czasem reakcji najpóźniej na następny dzień roboczy od momentu zgłoszenia usterki. • Nośniki danych (dyski) uległe uszkodzeniu pozostają na stałe własnością Zamawiającego- załączyć do oferty oświadczenie producenta. • Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. • Możliwość darmowego pobierania aktualizacji firmware i sterowników bezpośrednio ze strony producenta serwera po ustaniu wsparcia serwisowego przez okres co najmniej 7 lat. Przy braku takiej możliwości, dopuszcza się spełnienie tego wymogu poprzez zaoferowanie wsparcia serwisowego dla serwera na minimum 7 lat od momentu dostawy serwera do Zamawiającego. Wymaga się, aby gwarancja była realizowana z zachowaniem następujących warunków: • zapewnienie możliwości pobierania najnowszych wersji firmware, • dostęp do bazy wiedzy producenta dotyczącej dostarczanych urządzeń, • zapewnienie dostępu do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego, • możliwość otwierania zgłoszeń serwisowych w przypadku podejrzenia błędu w oprogramowaniu lub sprzęcie, • otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.

System operacyjny/System wirtualizacji	Licencja systemu Microsoft Windows Server 2025 lub równoważnego (kryteria równoważności: obsługa wirtualizacji typu hypervisor z możliwością uruchomienia 6 ilości maszyn wirtualnych, wsparcie dla klastrów wysokiej dostępności (failover

	clustering), obsługa Active Directory lub równoważnej usługi katalogowej, wsparcie dla protokołów sieciowych: TCP/IP, DNS, DHCP, iSCSI, możliwość zarządzania zdalnego poprzez interfejs webowy lub dedykowaną konsolę, wsparcie techniczne producenta przez minimum 10 lat od daty wydania) spełniającego poniższe wymagania: ● Dostarczone rozwiązanie powinno obsłużyć procesor 16-rdzeniowy. ● Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. ● 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. ● Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. ● 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. ● Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. ● Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 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. ● Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. ● Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. ● Możliwość migracji konfiguracji do systemu Microsoft Windows Server 2022/2016.
Dodatkowe licencje	Dostarczone rozwiązanie powinno obsłużyć dostarczony serwer z uwzględnieniem rdzeni procesora. W przypadku gdy licencjonowanie producenta oferowanego rozwiązania tego wymaga, należy dostarczyć 40 licencji dostępowych typu User CAL, które

	przypisane są do konkretnych użytkowników i umożliwiają każdemu z nich dostęp do systemu z dowolnego urządzenia. Licencje usługi RDS CAL serwera Windows Server 2025 - 4 sztuki.
Instalacja i wdrożenie	W ramach wdrożenia Wykonawca zobowiązany jest do: ● dostawy urządzenia do wskazanej lokalizacji, ● montażu i przeprowadzenia podstawowej konfiguracji urządzeń, ● ustawienia podstawowych parametrów pracy urządzenia, aktualizacji firmware, podłączenia do sieci energetycznej i logicznej, itp. ● instalacji i konfiguracji oprogramowania zarządzającego, ● instalacji i konfiguracji dostarczonych systemów wirtualizacji serwerów, ● migracji Active Directory na serwer, ● migracji systemu antywirusowego na serwer, ● opracowania dokumentacji powykonawczej wdrożonego rozwiązania. ● Oferent w zakresie przedmiotu zamówienia musi uwzględnić czas pracy inżyniera, na potrzeby uruchomienia urządzenia w siedzibie Zamawiającego. ● Prace instalacyjne i wdrożeniowe muszą być zrealizowane w siedzibie Zamawiającego. Nie dopuszcza się pracy zdalnej. ● Z uwagi na typ pracy urzędu, wykonywane prace nie mogą powodować problemów w dostępności do systemu komputerowego Zamawiającego. ● Instruktaż stanowiskowy administratora IT Zamawiającego z wdrożonego rozwiązania i konfiguracji (minimum 4 godzin) w siedzibie Zamawiającego.

6. Serwer do backupu – 1 szt.

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Obudowa	Obudowa Rack o wysokości maksymalnie 2U z możliwością instalacji min. 8 dysków SAS/SATA 2.5”. Możliwość rozbudowy o kolejne min. 8 wnęk na dyski SAS/SATA/NVMe 2.5”. Serwer musi mieć możliwość wyposażenia w panel diagnostyczny (LCD) umieszczony z przodu obudowy serwera, umożliwiający: ● wyświetlenie podstawowych informacji o serwerze, w tym numer seryjny oraz wersja oprogramowania zarządzającego i BIOS ● wyświetlanie stanu i logów, dla pamięci RAM, procesorów, pamięci masowej, wentylatorów, czujników temperatury i zasilaczy ● przywracanie konta administratora ● wyświetlanie w czasie rzeczywistym temperatury wlotu powietrza do serwera ● wyświetlanie w czasie rzeczywistym temperatury procesorów ● konfigurowanie ustawień sieciowych modułu zarządzania. Serwer wraz z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera w celach serwisowych. Przedni panel zamykany na klucz, chroniący dyski przed nieuprawnionym wyjęciem z serwera.

Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor 8-rdzeniowy o taktowaniu pojedynczego rdzenia min. 2.1GHz (base frequency). Procesor powinien posiadać wsparcie dla AVX-512.
Pamięć RAM	Minimum 64 GB RAM DDR5 RDIMM 5600MT/s. Płyta główna serwera powinna posiadać min. 32 sloty DIMM.
Zabezpieczenie pamięci	Memory mirroring, ECC, patrol scrubbing, SDDC, memory thermal throttling, ADDDC-SR.
Pamięć masowa	Zainstalowane minimum 2 dyski serwerowe SSD Mixed Use (DWPD nie mniejsze niż 3) o pojemności min. 960 GB każdy. Zainstalowany sprzętowy kontroler RAID SAS/SATA wyposażony w min. 4GB Cache i podtrzymanie bateryjne, umożliwiający skonfigurowanie poziomów RAID 0, 1, 10, 5, 50, 6, 60.
Wbudowane porty	4 x USB z czego nie mniej niż 2 x USB 3.0. Port USB TYP-C lub microUSB na przednim panelu obudowy. 1 x VGA na tylnym panelu obudowy oraz 1 x VGA na tylnym panelu obudowy. Złącze USB TYP-C / microUSB na przednim panelu musi umożliwiać dostęp do modułu zarządzania serwerem przez komputer PC z systemem Windows lub urządzenia mobilne z systemem Android lub iOS. Powyższe porty USB, USB-C oraz VGA nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek oraz kart rozszerzeń, jak również nie mogą zajmować wymaganych wnęk dyskowych.
Interfejsy sieciowe	Zainstalowane i w pełni funkcjonalne interfejsy: ● minimum 1 x RJ-45 Ethernet management port, ● minimum 4 porty 1Gb/s Ethernet Base-T niezajmujące slotów PCI-E, ● minimum 2 porty 10Gb/s Ethernet Base-T,
Sloty PCI-E	Minimum 3 aktywne sloty PCI-E 4.0 x8 obsługujące karty FHHL. Możliwość rozbudowy / rekonfiguracji serwera w celu uzyskania min. 8 slotów PCIE.
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200
Wentylatory	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo. Ilość zainstalowanych wentylatorów musi umożliwiać wydajne chłodzenie dla oferowanej konfiguracji serwera (CPU, RAM, PCI-E, dyski, zasilacze).
Zasilanie	Minimum dwa identyczne zasilacze klasy Titanium zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie więcej niż 1600W.
Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą serwera jako fabryczne rozwiązanie producenta. Moduł TPM 2.0

Zarządzanie	Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port 1 Gigabit Ethernet RJ-45 (1000Mbps) i umożliwiająca: • monitoring stanu serwera oraz pracy komponentów (temperatura kluczowych komponentów, prędkość obrotowa wentylatorów, itp.), • monitorowanie w czasie rzeczywistym poboru prądu przez serwer, • zbieranie logów błędów hardware, • przechwycenie wirtualnej konsoli wraz z dostępem do myszy i klawiatury, • montowanie wirtualnych napędów, • zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego, • wysyłanie zawiadomień droga mailową i poprzez SNMP • wsparcia dla IPMI, SSH, Redfish • wparcie dla funkcji screenshot BSOD (Blue Screen of Death) dla systemów Windows, • nadawanie ról użytkownikom, • możliwość wykonania aktualizacji oprogramowania do zarządzania serwerem, BIOS, • możliwość zainstalowania modułu Wi-Fi umożliwiającego połączenie z modułem zarządzania serwerem z urządzeń mobilnych z systemem Android i iOS.
Dodatkowe oprogramowanie do zarządzania i monitorowania	Wraz z serwerem dostarczone powinno być oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające zdalne zarządzanie wszystkimi dostarczonymi serwerami jako grupą serwerów (klastrem), posiadające interfejs graficzny dostępny z poziomu przeglądarek internetowych (HTML), pozwalające m.in. na: • włączenie, wyłączenie, restart, podgląd logów serwerów, sprawdzenie statusu sprzętu, przejęcie pełnej konsoli graficznej serwerów. • tworzenie szablonów instalacyjnych dla systemów operacyjnych. • tworzenie profili serwerów ze zdefiniowanymi parametrami BIOS, procesora/-ów, pamięci, kontrolera RAID które umożliwiają szybkie wdrożenie identycznej konfiguracji na grupie serwerów. • zdalne montowanie obrazów ISO pozwalające na uruchomienie z nich serwera. • aktualizacja sterowników i BIOS serwerów. • zbieranie statystyk zużycia energii dla wszystkich serwerów z możliwością graficznej prezentacji danych historycznych.
Kompatybilność	• Zamawiający oczekuje, że dostarczony sprzęt został wyprodukowany z zachowaniem najwyższych standardów jakości. Wykonawca przedstawi oświadczenie producenta sprzętu potwierdzające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001 lub równoważnymi. • Wykonawca zobowiązany jest do dostarczenia sprzętu posiadającego oznaczenie CE, potwierdzające zgodność z obowiązującymi dyrektywami Unii Europejskiej w zakresie bezpieczeństwa, zdrowia i ochrony środowiska. Wykonawca przedstawi oświadczenie producenta sprzętu

	potwierdzające, że oferowany sprzęt posiada oznakowanie CE oraz spełnia wymagania odpowiednich dyrektyw UE. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Windows Server 2022, Windows Server 2025.
Gwarancja	1. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta na terenie RP. 2. Urządzenie objęte minimum 36 miesięcznym okresem gwarancji w trybie 5x9 onsite z gwarantowanym czasem reakcji najpóźniej na następny dzień roboczy od momentu zgłoszenia usterki. 3. Nośniki danych (dyski) uległe uszkodzeniu pozostają na stałe własnością Zamawiającego- dołączyć do oferty oświadczenie producenta potwierdzające spełnienie powyższego zapisu. 4. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta. 5. Usługi gwarancyjne świadczone przez autoryzowanego partnera serwisowego producenta lub producenta sprzętu posiadającego certyfikat ISO co najmniej 9001 lub równoważny na świadczenie usług serwisowych. Dokument potwierdzający spełnienie w/w wymogu należy dołączyć do oferty. 6. Możliwość darmowego pobierania aktualizacji firmware i sterowników bezpośrednio ze strony producenta serwera po ustaniu wsparcia serwisowego przez okres 7 lat. Przy braku takiej możliwości, dopuszcza się spełnienie tego wymogu poprzez zaoferowanie wsparcia serwisowego dla serwera na minimum 7 lat od momentu dostawy serwera do Zamawiającego. 7. Wymaga się, aby gwarancja była realizowana z zachowaniem następujących warunków: • zapewnienie możliwości pobierania najnowszych wersji firmware, • dostęp do bazy wiedzy producenta dotyczącej dostarczanych urządzeń, • zapewnienie dostępu do centrum pomocy technicznej producenta lub autoryzowanego partnera serwisowego, • możliwość otwierania zgłoszeń serwisowych w przypadku podejrzenia błędu w oprogramowaniu lub sprzęcie, • otrzymywanie poprawek oraz aktualizacji wersji oprogramowania.
Instalacja i wdrożenie	W ramach wdrożenia Wykonawca zobowiązany jest do: • dostawy urządzenia do wskazanej lokalizacji, • montażu i przeprowadzenia podstawowej konfiguracji urządzeń, • ustawienia podstawowych parametrów pracy urządzenia, aktualizacji firmware, podłączenia do sieci energetycznej i logicznej, itp. • instalacji i konfiguracji oprogramowania zarządzającego,

	• instalacji i konfiguracji systemu operacyjnego, • opracowania dokumentacji powykonawczej wdrożonego rozwiązania. • Oferent w zakresie przedmiotu zamówienia musi uwzględnić czas pracy inżyniera, na potrzeby uruchomienia urządzenia w siedzibie Zamawiającego. • Prace instalacyjne i wdrożeniowe muszą być zrealizowane w siedzibie Zamawiającego. Nie dopuszcza się pracy zdalnej. • Z uwagi na typ pracy urzędu, wykonywane prace nie mogą powodować problemów w dostępności do systemu komputerowego Zamawiającego. Instruktaż stanowiskowy administratora IT Zamawiającego z wdrożonego rozwiązania i konfiguracji (minimum 8 godzin) w siedzibie Zamawiającego.
System operacyjny	Licencja systemu Microsoft Windows Server 2025 lub system równoważny, który spełnia wszystkie poniższe kryteria równoważności: - Pełna kompatybilność z oprogramowaniem do wykonywania i zarządzania kopiami zapasowymi oferowanym w ramach zamówienia, • Obsługa procesora 16 rdzeniowego, • Obsługa usługi katalogowej Active Directory lub równoważnej (w tym LDAPv3), • Wsparcie dla protokołów sieciowych: TCP/IP, DNS, DHCP, iSCSI, • Możliwość zdalnego zarządzania poprzez interfejs webowy lub dedykowaną konsolę administracyjną, • Wsparcie producenta systemu przez minimum 10 lat od daty jego wydania, • Obsługa (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM oraz procesorów bez przerywania pracy systemu, • Automatyczna weryfikacja podpisów cyfrowych sterowników, • Możliwość dynamicznego zmniejszania poboru mocy przez niewykorzystywane rdzenie CPU, • Mechanizm klasyfikowania i indeksowania plików na podstawie zawartości, • Wbudowana zapora sieciowa (firewall) z obsługą reguł konfigurowalnych przez administratora, • Lokalizacja interfejsu w języku polskim (menu, komunikaty, przeglądarka, pomoc) z możliwością zmiany języka na co najmniej jeden dodatkowy, • Wsparcie dla popularnych urządzeń peryferyjnych (drukarki, urządzenia sieciowe, USB, Plug&Play), • Możliwość zdalnej konfiguracji, administrowania i aktualizacji systemu, • Możliwość instalacji poprawek poprzez ich wdrożenie do obrazu instalacyjnego, • Mechanizmy zdalnej administracji i administracji przez skrypty (lokalnie i zdalnie), • Możliwość migracji konfiguracji do systemu Microsoft Windows Server 2022 lub 2016.

7. System kontroli dostępu NAC – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Ogólne cechy systemu	• System współpracujący z urządzeniami wielu producentów (multi vendor). • Obsługa minimum 100 urządzeń klienckich (w tym gości). • Licencje przypisane tylko do aktualnie podłączonych urządzeń, zwalniane po ich rozłączeniu. • Wbudowany serwer RADIUS oraz TACACS+ (rozbudowa możliwa poprzez dodatkową licencję – nie wymagana na etapie wdrożenia). • Obsługa RADIUS VSA co najmniej 100 producentów, w tym: Cisco Systems, Fortinet, Microsoft, Alcatel-Lucent Enterprise, Huawei Networks, Extreme Networks, PaloAlto Networks. • Możliwość przesyłania atrybutów VSA (rola użytkownika, VLAN) do kontrolera Wi-Fi bez dodatkowej konfiguracji kontrolera. • Możliwość odbierania od kontrolera Wi-Fi informacji o autoryzacji użytkownika (SSID, grupa AP, IP AP). • Wszystkie licencje permanentne (dożywotnie).
Baza użytkowników i integracje	• Wbudowana baza użytkowników. • Integracja z: Microsoft Active Directory, RADIUS, Kerberos, LDAP, ODBC, serwerami tokenów.
Metody profilowania	• Obsługa metod: DHCP, TCP, MAC OUI, SNMP, Cisco Device Sensor (z możliwością rozbudowy licencjami).
Protokoły i standardy	• Obsługa protokołów: RADIUS, RADIUS CoA, TACACS+, Web Authentication, SAML v2.0. • Obsługa metod uwierzytelniania: EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS), PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD), TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP), EAP-TLS, PAP, CHAP, MSCHAPv1/v2, EAP-MD5. • Wsparcie NAC, Microsoft NAP, Windows Machine Authentication, MAC Auth. • Obsługa audytu (role oparte na porcie, skanowanie podatności). • OCSP, SNMP (generic i private MIB). • Format logów: CEF, LEEF. • TLS 1.2.
Integracja z systemami monitorowania	• Integracja z systemami do monitorowania sieci w celu diagnozowania problemów z klientami (rozbudowa możliwa przez licencję dodatkową).
Platformy wirtualizacyjne	• Możliwość uruchomienia na: ESX 4.0, ESXi 4.1–6.0, Hyper-V 2012 R2, Windows 2012 R2 Enterprise.
Moduł dostępu gościnnego	• Obsługa gości w liczbie ≥ minimalnej liczby urządzeń klienckich. • Samodzielna rejestracja: e-mail, SMS, dostęp sponsorowany, logowanie przez media społecznościowe. • Integracja z systemami trzecimi poprzez API. • Automatyczne skalowanie portalu gościnnego na urządzenia mobilne. • Personalizacja strony logowania.

Moduł BYOD	• Konfiguracja urządzeń bez angażowania działu IT. • Wsparcie: MS Windows, MacOS X, iOS, Android, Chromebook, Ubuntu. • Samorejestracja i bezpieczna konfiguracja urządzenia do sieci. • Automatyczna konfiguracja dla sieci przewodowej i Wi-Fi. • Profilowanie urządzeń (rodzaj, producent, model). • Generowanie unikalnych certyfikatów dla urządzeń, wbudowane CA. • Konfiguracja urządzeń Wi-Fi w oparciu o 1–2 SSID.
Moduł kontroli końcówek klienckich	• Wsparcie systemów: Windows 7+, MacOS X 10.7+, Red Hat Enterprise Linux 4+, CentOS 4+, Fedora Core 5+, SUSE Linux 10.x+. • Kontrola stanu: antywirus, antyspyware, firewall. • Informacje online o statusie końcówek. • Obsługa agentów: Persistent Agent, Dissolvable Agent, NAP Agent.
Wsparcie i gwarancja	• System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. • Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
Potwierdzenia rynkowe	• Wymienienie w bieżącym raporcie Gartner Market Guide for NAC lub Gartner Peer Insights (min. 100 opinii, status „Customer's Choice").
Dokumentacja techniczna	• Publicznie dostępna dokumentacja wdrożeniowa i użytkowa opisująca oferowane funkcje (funkcje dostępne w momencie składania oferty).
Wymogi formalne oferty	• Pełny wykaz numerów katalogowych oferowanych produktów. • Możliwość przeprowadzenia testów funkcji w siedzibie zamawiającego (max. 2 tyg. od żądania). • Wszystkie urządzenia fabrycznie nowe, zarejestrowane na Zamawiającego bezpośrednio po opuszczeniu fabryki lub z deklaracją producenta o nowości.
Instalacja i wdrożenie	1. Weryfikacja infrastruktury, przygotowanie środowiska wirtualnego lub serwerowego, uzgodnienie parametrów konfiguracyjnych. 2. Dostarczenie i instalacja wszystkich modułów systemu. 3. Konfiguracja – utworzenie bazy użytkowników, integracja z AD, ustawienie polityk bezpieczeństwa, personalizacja portalu gościnnego, konfiguracja BYOD i certyfikatów. 4. Sprawdzenie zgodności działania systemu z wymaganiami OPZ, sporządzenie protokołu odbioru. 5. Instruktaż dla administratora IT z obsługi systemu, monitorowania, raportowania i konfiguracji w wymiarze 6 godzin w siedzibie Zamawiającego. 6. Dostarczenie dokumentacji wdrożeniowej, danych dostępowych i uruchomienie wsparcia producenta. 7. Oferent w zakresie przedmiotu zamówienia musi uwzględnić czas pracy inżyniera, na potrzeby uruchomienia urządzenia w siedzibie Zamawiającego. 8. Prace instalacyjne i wdrożeniowe muszą być zrealizowane w siedzibie Zamawiającego. Nie dopuszcza się pracy zdalnej.

	9. Z uwagi na typ pracy urzędu, wykonywane prace nie mogą powodować problemów w dostępności do systemu komputerowego Zamawiającego.

8. System tworzenia i zarządzania kopiami zapasowymi – 1 szt.

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Backup komputerów i serwerów	Backup 40 komputerów, 2 serwerów fizycznych, 12 serwerów wirtualnych
Architektura oprogramowania	Klient-serwer, protokół TCP/IP, centralny moduł sterowania kopiami zapasowymi
Kompatybilność serwera	Windows 11; Windows Server 2016, 2019, 2022, 2025; Linux, BSD, Mac OS X, QNAP, Synology
Kompatybilność klienta	Windows 2000, XP, Vista, 7, 8, 10, 11; Windows Server 2000, 2003, 2008, 2012, 2016, 2019, 2022, 2025; Linux, BSD, Mac OS X, QNAP, Synology
Typy archiwizacji	Pełna, przyrostowa, różnicowa, delta (fragmenty plików)
Archiwizacja plików otwartych	Backup otwartych i zablokowanych plików bez użycia Volume Shadow Copy Service (VSS)
Automatyczny backup	Backup podczas wyłączania komputera
Selekcja plików do backupu	Możliwość wyboru lub wykluczenia woluminów, katalogów, plików za pomocą symboli „*” i „?”
Backup systemu i programów Windows	Backup całego systemu oraz programów zainstalowanych (tylko Windows)
Backup baz danych i poczty	Online i offline
Kopie rotacyjne (wersjonowanie)	Obsługa wersjonowania kopii
Format archiwów	Otwarte formaty, ZIP 64-bit
Backup i odzyskiwanie maszyn wirtualnych	Microsoft Hyper-V, VMWare ESX/ESXi
Odzyskiwanie systemu	Bare metal restore – na czysty dysk bez ponownej instalacji
Odzyskiwanie plików	Bezpośrednie odzyskiwanie do oryginalnej lokalizacji
Odzyskiwanie z kopii delta i różnicowych	Tak jak z kopii pełnych
Bezpieczeństwo	Szyfrowanie archiwów i transferu
Kompresja	Kompresja po stronie stacji roboczej
Replikacja archiwów	Replikacja na drugi dysk, NAS, serwer FTP
Centralne zarządzanie	Sterowanie systemem z jednego miejsca
Transparentna archiwizacja	Backup działający w tle, niezauważalny dla użytkowników
Równoległa archiwizacja	Backup równoczesny wszystkich komputerów w sieci LAN/WAN
Alerty administracyjne	Wysyłanie alertów na e-mail
Uruchamianie zewnętrznych programów	Możliwość uruchamiania programów, skryptów, plików wsadowych na serwerze i klientach

Raportowanie	Raporty z przebiegu archiwizacji, statystyki, informacje o zaległych zadaniach
Automatyczna aktualizacja	Aktualizacja oprogramowania na komputerach zdalnych
Licencja	Bezterminowa, bez ograniczeń czasowych
Język interfejsu i wsparcia	Polski
Replikacja na nośniki optyczne i taśmowe	CD, DVD, Blu-Ray, HD-DVD, DDS, DLT, LTO, AIT (tylko Windows)
Instalacja klienta	Instalacja klienta przez GPO
Integracja SIEM	Współpraca z systemami SIEM (Security Information and Event Management)
Certyfikaty SSL	Możliwość stosowania własnych certyfikatów SSL
Instalacja i wdrożenie	1. Kompleksowa instalacja oprogramowania serwerowego i klienckiego, konfiguracja harmonogramów backupu, polityk bezpieczeństwa oraz testowe przywrócenie danych w celu weryfikacji działania systemu 2. Instruktaż dla administratora IT z obsługi systemu, monitorowania, raportowania i konfiguracji w wymiarze 4 godzin w siedzibie Zamawiającego. 3. Oferent w zakresie przedmiotu zamówienia musi uwzględnić czas pracy inżyniera, na potrzeby uruchomienia urządzenia w siedzibie Zamawiającego. 4. Prace instalacyjne i wdrożeniowe muszą być zrealizowane w siedzibie Zamawiającego. Nie dopuszcza się pracy zdalnej. 5. Z uwagi na typ pracy urzędu, wykonywane prace nie mogą powodować problemów w dostępności do systemu komputerowego Zamawiającego.

9. Rozwiązanie do zbierania i analizowania danych z urządzeń sieciowych – 1 szt.

Nazwa komponentu	**Wymagane minimalne parametry techniczne**
Wymagania ogólne	• Centralny system logowania, raportowania i korelacji zdarzeń umożliwiający centralizację logów sieciowych, systemowych i bezpieczeństwa. • Rozwiązanie komercyjne działające jako maszyna wirtualna lub platforma bazująca na systemie Linux w środowisku wirtualnym. • Możliwość uruchomienia na hypervisorach: VMware ESX/ESXi 5.0–6.7, Microsoft Hyper-V 2008 R2–2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS, Microsoft Azure, Google Cloud (GCP).
Interfejsy i zasoby	• Obsługa minimum 4 interfejsów sieciowych. • Obsługa przestrzeni dyskowej o pojemności minimum 3 TB.

Parametry wydajnościowe	• Możliwość przyjmowania minimum 5 GB logów dziennie. • Możliwość kolekcjonowania logów z minimum 1000 systemów/urządzeń.
Logowanie	• Podgląd logów w czasie rzeczywistym. • Przeglądanie logów historycznych z funkcją filtrowania. • Predefiniowane lub konfigurowalne raporty obejmujące co najmniej: najczęściej wykrywane ataki, najbardziej aktywnych użytkowników, najczęściej wykorzystywane aplikacje, najczęściej odwiedzane strony WWW, kraje docelowe połączeń, najczęściej wykorzystywane polityki Firewall, informacje o połączeniach IPSec. • Możliwość przesyłania kopii logów do innych systemów (z mechanizmem filtrowania). • Obsługa przyjmowania logów przez UDP/514 oraz TCP/514. • Cykliczny eksport logów do systemów zewnętrznych (SFTP lub zasób sieciowy).
Raportowanie	• Generowanie raportów w formatach minimum PDF oraz CSV. • Predefiniowane raporty z możliwością modyfikacji parametrów. • Możliwość definiowania własnych raportów. • Możliwość spolszczenia raportów. • Generowanie raportów cyklicznych lub na żądanie. • Automatyczne wysyłanie raportów na wskazane adresy e-mail.
Korelacja logów	• Korelacja zdarzeń z możliwością wyboru urządzeń objętych korelacją. • Powiadomienia o zdarzeniach przez e-mail oraz SNMP. • Tworzenie reguł korelacyjnych dla co najmniej kategorii: Malware, Aplikacje sieciowe, Email, IPS, Traffic, Zdarzenia systemowe (utrata VPN, utrata połączenia sieciowego).
Zarządzanie i administracja	• Zarządzanie lokalne przez HTTPS i SSH lub dedykowaną konsolę szyfrowaną. • Uwierzytelnianie administratorów: lokalna baza, RADIUS, LDAP, PKI. • Możliwość zdefiniowania minimum 4 administratorów z różnymi poziomami uprawnień.
Serwisy i licencje	• Licencja bezterminowa (brak blokady działania po wygaśnięciu wsparcia). • Minimum 12 miesięcy wsparcia producenta 24/7 obejmującego aktualizacje i pomoc techniczną.

Wymagania formalne	• W przypadku produktów podwójnego zastosowania – dokument importera potwierdzający zgodność z przepisami prawa. • Oświadczenie producenta lub autoryzowanego dystrybutora o autoryzacji oferenta do sprzedaży rozwiązania.

10.