Załącznik Nr 2
do zapytania nr CS.271.1.2025.MCZ z dnia 09.10.2025 r.
opis przedmiotu zamówienia (OPZ) – szczegółowa specyfikacja techniczna

I. Zakup serwera – 1 szt.

Element konfiguracji	Wymagania minimalne
W ofercie należy wpisać: producent, model	Producent ……. Model ……
Obudowa	Maksymalnie 1U RACK 19 cali wraz z szynami montażowymi i ramieniem kablowym umożliwiającym wysunięcie, do celów serwisowych, serwera z szafy bez konieczności odłączania kabli zasilających i sygnałowych (kable LAN SAN) Serwer wyposażony w zdejmowanym panelem przedni z zamkiem. Serwer wyposażony w czujnik otwarcia obudowy współpracującego z BIOS/UEFI. Serwer wyposażony w moduł TPM 2.0.
Procesor	Procesor 16-rdzeniowy, x86 - 64 bity, o taktowaniu min. 3.0GHz, - lub równoważny procesor 16-rdzeniowy, osiągający w testach SPECrate2017_int_base powyżej 173 punktów wraz z oferowanym serwerem. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna wspierająca zastosowanie procesorów od 16 do 128 rdzeniowych, mocy do min. 400W i taktowaniu CPU do min. 4.1GHz.
Liczba procesorów	Min. 1 procesor, płyta główna min. jednoprocesorowa
Pamięć operacyjna	128GB RDIMM DDR5 min. 4800 MT/s w modułach o pojemności min. 32GB każdy. Płyta główna z minimum 12 slotami na pamięć i umożliwiająca instalację minimum 3TB. Obsługa zabezpieczeń: Advanced ECC.
Sloty rozszerzeń	Serwer musi być wyposażony w: - 2 aktywne gniazda PCI-Express generacji 5, każde gniazdo x16 Serwer musi mieć dodatkowo dedykowane dwa sloty OCP: - na kontroler dyskowy lub - na kartę sieciową niezajmującą slotów PCI-Express.
Dysk twardy	Zatoki dyskowe gotowe do zainstalowania min.10 dysków 2.5” typu Hot Swap, NVME/SAS12G/SATA/SSD. Zainstalowane: - 3 x dysk 1,92TB SSD RI (Read Intensive) 2.5” typu hot swap
Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 8GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 16 napędów dyskowych NVMe/SAS12G oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
Interfejsy sieciowe	Minimum 4 porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń” wyposażone w chipset BCM5719 wraz z patchcordami - 2m Karta, minimum 2 porty Ethernet 10/25GbE SFP28 wyposażona w chipset BCM57414. wraz z kablami DAC - 2m Karta, minimum 4 porty Ethernet 100/1000 Mb/s RJ-45 wyposażona w chipset BCM5719. wraz z patchcordami - 2m
Karta graficzna	Zintegrowana karta graficzna

Porty	5 x USB 3.2 Gen1 (w tym min. 2 porty wewnętrzny) 1x VGA z tyłu serwera 1x DisplayPort z przodu serwera. Możliwość rozbudowy/rekonfiguracji o: - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45 oraz bez konieczności instalowania kart w slotach PCI-Express
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 1000W.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Karta/moduł zarządzający	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne) dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub przez współdzielony port zintegrowanej karty sieciowej serwera dostęp do karty możliwy z poziomu przeglądarki webowej (GUI) z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) wbudowane narzędzia diagnostyczne zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego obsługa mechanizmu remote support - automatyczne połączenie z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) obsługa zdalnego serwera logowania (remote syslog) wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i wirtualnych folderów mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy) monitorowanie zasilania oraz zużycia energii przez serwer w czasie z możliwością graficznej prezentacji konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) zdalna aktualizacja oprogramowania (firmware) zarządzanie grupami serwerów, w tym: tworzenie i konfiguracja grup serwerów sterowanie zasilaniem (wł/wył) ograniczenie poboru mocy dla grupy (power caping) aktualizacja oprogramowania (firmware) wspólne wirtualne media dla grupy możliwość równoczesnej obsługi przez min. 2 administratorów autentykacja dwuskładnikowa (Kerberos)

	wsparcie dla Microsoft Active Directory obsługa TLS i SSH wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
System Operacyjny	Serwer MS Windows Server 2025 Standard, wersja polskojęzyczna z nieujawnianym wcześniej, nieaktywowanym kluczem licencyjnym, pochodzący z oficjalnej sieci dystrybucji producenta wraz z licencjami dostępowymi CAL dla 20 użytkowników lub równoważny. Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym lub umożliwiać zainstalowanie 2 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać dobrana tak aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze. System operacyjny – fabrycznie nowy, nieużywany, nie pochodzący z recyklingu, z licencją na czas nieoznaczony, nie naruszający praw osób trzecich. System operacyjny wraz ze wszystkimi wymaganymi sterownikami podzespołów ma być zainstalowany lub preinstalowany na oferowanym urządzeniu komputerowym. Zabrania się instalowania lub preinstalowania systemu operacyjnego w jakimkolwiek środowisku wirtualnym. Zamawiający nie dopuszcza zaoferowania systemu operacyjnego, programów i planów licencyjnych opartych o rozwiązania chmurowe oraz rozwiązań wymagających wnoszenia przez Zamawiającego jakichkolwiek dodatkowych opłat związanych z użytkowaniem zakupionego systemu operacyjnego. Zamawiający wymaga, aby wszystkie elementy systemu operacyjnego oraz jego licencja pochodziły od tego samego producenta. Warunki równoważności: 1. System operacyjny musi być przeznaczony do zastosowań serwerowych w środowiskach fizycznych lub o minimalnej wirtualizacji. 2. System operacyjny musi być najnowszą wersją rodziny systemów operacyjnych danego producenta. 3. Licencja na system operacyjny musi uwzględniać prawo do bezpłatnej instalacji udostępnianych przez producenta poprawek krytycznych i opcjonalnych do zakupionej wersji oprogramowania. 4. Licencja na system operacyjny musi umożliwiać uruchomienie kontrolera domeny. 5. Licencja na system operacyjny musi być licencją stałą, bez ograniczeń czasowych. 6. Licencja na system operacyjny musi uprawniać do uruchamiania systemu operacyjnego w środowisku fizycznym i min. 2 środowisku wirtualnym za pomocą wbudowanego mechanizmu wirtualizacji, bez konieczności zakupu dodatkowych licencji. 7. Zaimplementowanie w systemie operacyjnym środowiska wirtualizacyjnego musi umożliwiać dodawanie i usuwanie pamięci wirtualnej oraz wirtualnych kart sieciowych podczas pracy maszyny wirtualnej. 8. System operacyjny musi posiadać graficzny interfejs użytkownika. 9. System operacyjny musi być w pełni kompatybilny z usługą Active Directory w zakresie: a) zarządzania użytkownikami, b) zarządzania certyfikatami dla użytkowników wraz ze wsparciem możliwości logowania do domeny kartą mikroprocesorową,

	c) możliwości przydzielania praw dostępu do zasobów sieciowych, d) instalacji zdalnej oprogramowania z pakietów msi, e) definiowania polityk bezpieczeństwa dla użytkowników, grup oraz stacji roboczych z systemami MS Windows: 10. 11. 10. System operacyjny musi wspierać pracę domenową wraz z automatyczną synchronizacją dla dodatkowych serwerów. 11. System operacyjny musi wspierać zarządzanie przez dostępne narzędzia administracji serwera dla systemu Windows 10 (RSAT) oraz Windows Admin Centre. 12. System operacyjny musi posiadać obsługę zdalnego pulpitu poprzez protokół RDP. 13. System operacyjny musi umożliwiać ustawianie relacji zaufania pomiędzy domenami. 14. Wszystkie narzędzia i usługi systemu operacyjnego powinny być rozwiązaniem jednego producenta. 15. System operacyjny musi posiadać obsługę pamięci USB jako monitora klastra. 16. System operacyjny musi pozwalać na stopniowe uaktualnienia systemu operacyjnego klastra. 17. System operacyjny musi posiadać obsługę deduplikacji na potrzeby systemu plików ReFS. 18. System operacyjny musi posiadać obsługę optymalizacji transportu w tle pod kątem opóźnień. 19. System operacyjny musi posiadać wbudowaną zaporę internetową (firewall) dla ochrony połączeń internetowych; zapora musi być zintegrowana z systemem konsoli do zarządzania ustawieniami zapory i regułami ipv4 i v6; 20. System operacyjny musi posiadać możliwość uruchomienia serwera DNS z możliwością integracji z kontrolerem domeny; 21. System operacyjny musi posiadać możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 22. System operacyjny musi posiadać domyślną obsługę PowerShell 5.1; 23. System operacyjny musi posiadać obsługę certyfikatów w Active Directory. 24. Wszystkie wymienione powyżej parametry, role, funkcje, itp. systemu operacyjnego objęte musza być dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).
Wsparcie techniczne	3-letnia gwarancja producenta w miejscu instalacji. Zgłoszenia przyjmowane w trybie 24x7. Czas reakcji w ciągu następnego dnia roboczego od zgłoszenia. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera. W razie awarii dyski twarde pozostają u Zamawiającego.

Wymagania na oprogramowanie zarządzające serwerem

Parametr	**Opis**
Interfejs i dostęp do systemu zarządzania	System zarządzania w oparciu o jednolite oprogramowanie, czyli z jednego panelu o jednym adresie IP. Dostęp do oprogramowania zarządzającego poprzez: - interfejs graficzny wykonany w technologii HTML5; - REST API (np. PowerShell). Oprogramowanie zarządzające musi być w formie gotowej wirtualnej maszyny, tzw. virtual appliance. Oprogramowanie musi być wspierane na co najmniej takich wirtualizatorach: - VMware vSphere ESXi 6.5U2;

	- Microsoft Hyper-V Server 2016; - RHEL KVM 7.x.
Podstawowe funkcje zarządzania	Oprogramowanie musi w sposób graficzny wizualizować stan poszczególnych elementów infrastruktury (stan normalnej pracy, ostrzeżenia, awarie). Musi istnieć możliwość modyfikacji panelu głównego aplikacji poprzez zmianę kategorii systemów, dla których prezentowany jest „stan zdrowia”/status. Na przykład musi istnieć możliwość zawężenia prezentacji stanu zdrowia do serwerów o konkretnym modelu. Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera. Przedstawienie graficznej reprezentacji serwerowni, w formie trójwymiarowej, z prezentacją temperatury panującej w szafie rack i w poszczególnych serwerach. Rysunek musi prezentować też serwery i ich położenie w szafach rack. Wizualizacja wykorzystania procesorów (CPU), poboru energii przez serwer i temperatury w czasie rzeczywistym w formie wykresów. Bezagentowe zarządzanie i monitorowanie stanu urządzeń. Pojedynczy interfejs zapewniający widoki, podsumowanie szczegółowych informacji o sprzęcie i oprogramowania układowego. Zebrane dane udostępniane poprzez interfejs REST API oraz interfejs graficzny użytkownika; Zarządzanie uprawnieniami użytkowników poprzez definiowanie ról użytkowników i przypisywanie im dostępu do poszczególnych urządzeń.
Liczba jednoczesnych sesji zarządzania	W danym momencie musi być niezależny, równoległy dostęp do konsol graficznych wszystkich serwerów.
Zdalna identyfikacja	Zdalna identyfikacja fizycznego serwera za pomocą sygnalizatora optycznego
Dodatkowe cechy oprogramowania do zarządzania	Konfiguracja środowiska serwerów w oparciu o logiczne profile serwerowe obejmujące konfigurację serwera w zakresie: - oprogramowania układowego i sterowników z funkcją automatycznej aktualizacji firmware i sterowników w serwerze; - konfiguracji dysków lokalnych zainstalowanych w serwerze – konfiguracja RAID lub JBOD; - ustawienia bootowania (m.in. ustawienie Secure Boot); - konfiguracja BIOS – ustawienie poziomu zabezpieczenia pamięci RAM, włączenie/wyłączenie obsługi wirtualizacji w procesorach Intel, ustawienie technologii Turbo Boost, ustawienie trybu poboru energii (tryb oszczędzania lub maksymalna wydajność, itp.), ustawienie zachowania się serwera w razie krytycznej awarii chłodzenia (wyłączenie lub kontynuowanie pracy); - konfiguracja użytkowników i ich poświadczeń dla wbudowanego interfejsu zarządzania serwerem. Wymagana integracja z narzędziami VMware vCenter Server, VMware LogInsight oraz Microsoft SystemCenter przez specjalną wtyczkę (np. dodatkowe zakładki) w tych aplikacjach, rozszerzającą możliwości zarządzania o warstwę sprzętową. Wbudowane raporty dotyczące użycia zasobów jak również zarejestrowanych zdarzeń z możliwością eksportu do plików w formacie xls, lub csv lub pdf. Oprogramowanie zarządzające musi posiadać wbudowany system tworzenia kopii zapasowych. Kopia musi być automatycznie zapisywana na udostępnionym zasobie sieciowym po protokole SCP lub SFTP. Musi

	istnieć możliwość utworzenia harmonogramu automatycznego tworzenia kopii zapasowych. Oprogramowanie zarządzające musi mieć możliwość obsługi co najmniej 700 serwerów w swoim interfejsie.
Bezpieczeństwo	Oprogramowanie zarządzające musi integrować się z Active Directory oraz obsługiwać dwupoziomowe uwierzytelnianie (Two-factor authentication).
Automatyczne otwieranie zgłoszeń	Oprogramowanie zarządzające musi posiadać funkcjonalność automatycznego wysyłania zgłoszeń do serwisu producenta, gdy dojdzie do awarii serwera lub jego komponentu.
Licencje	Licencje na powyższą funkcjonalność na wszystkie oferowane serwery i macierze dyskowe.
Wsparcie techniczne dla aplikacji zarządzającej	Wymagane co najmniej 3 letnie wsparcie techniczne świadczone w trybie 24x7, upoważniające poza zgłaszaniem awarii i problemów z oprogramowaniem również do pobierania przez okres 3 lat aktualizacji dla tego oprogramowania. Wsparcie techniczne musi obejmować wszystkie oferowane aplikacje.

Zakres wdrożenia serwera

1. Przygotowanie infrastruktury:

- Zweryfikowanie dostępności miejsca w szafie rack oraz zapewnienie odpowiednich warunków zasilania.
- Zapewnienie dostępu do odpowiednich przełączników sieciowych oraz przygotowanie przewodów sieciowych i zasilających.

Montaż serwera:

- Rozpakowanie serwera, weryfikacja kompletności zestawu.
- Zamontowanie serwera w szafie rack przy użyciu dostarczonych szyn montażowych
- Instalacja dysków twardych (SSD) w dedykowanych slotach.

Podłączenie i uruchomienie:

- Podłączenie zasilania redundantnego do serwera.
- Podłączenie kabli sieciowych (1Gb i 25Gb Ethernet) do portów serwera i przełączników sieciowych.
- Uruchomienie serwera i monitorowanie wskaźników LED w celu sprawdzenia poprawności działania komponentów (wentylatory, zasilacze, dyski).
- Testowanie połączeń fizycznych między serwerem a przełącznikami sieciowymi.
- Konfiguracja zintegrowany systemu zdalnego zarządzania serwerami (konfiguracja adresacji, ustawienie powiadomień)

Testy działania:

- Sprawdzenie poprawności zasilania redundantnego przez odłączenie jednego źródła zasilania.
- Testowanie temperatury pracy urządzenia w zamkniętej szafie rack.
- Przeprowadzenie diagnostyki urządzenia w celu sprawdzenia stanu komponentów (dyski, interfejsy sieciowe, pamięć RAM).

Organizacja i zabezpieczenie:

- Optymalizacja układu kabli, ich estetyczne rozmieszczenie i zabezpieczenie w szafie rack.
- Zabezpieczenie fizycznego dostępu do urządzenia (np. mechanizm blokady obudowy).

2. Konfiguracja sieciowa

Skonfigurowanie sieci w serwerze:

- Przypisanie adresów IP, konfiguracja DNS i integracja serwera z istniejącą siecią.

Testy sieciowe:

- Weryfikacja przepustowości połączeń sieciowych i stabilności przesyłu danych.

3. Konfiguracja oprogramowania

1) **Dostawa i wdrożenie platformy wirtualizacji z centralnym zarządzaniem**

WYMAGANIA FUNKCJONALNE

Platforma wirtualizacji (Hypervisor)

- Typ hypervisor: Type 1 (bare metal)
- Wsparcie dla parawirtualizacji: TAK
- Wsparcie dla pełnej wirtualizacji: TAK
- Wsparcie dla wirtualizacji sprzętowej: Intel VT-x, AMD-V
- Maksymalna liczba procesorów wirtualnych na maszynę: min. 64 vCPU
- Maksymalna ilość pamięci RAM na maszynę: min. 1TB
- Wsparcie dla live migration: TAK
- Wsparcie dla high availability: TAK
- Wsparcie dla storage pools: TAK (lokalne, NFS, iSCSI, FC)

Obsługiwane systemy operacyjne gości

- Windows: Windows Server 2016/2019/2022, Windows 10/11
- Linux: Debian, Ubuntu, CentOS, RHEL, SUSE
- Unix: FreeBSD, OpenBSD
- Inne: zgodność z standardami wirtualizacji

Funkcje zaawansowane

- Snapshots: tworzenie, zarządzanie i przywracanie migawek
- Templates: tworzenie i zarządzanie szablonami maszyn
- Backup: natywne wsparcie dla kopii zapasowych
- Monitoring: monitorowanie zasobów w czasie rzeczywistym
- Networking: wsparcie dla VLAN, bonding, Open vSwitch
- GPU passthrough: wsparcie dla GPU

SYSTEM CENTRALNEGO ZARZĄDZANIA

Wymagania podstawowe

- Interfejs: webowy (HTML5)
- Aplikacja desktop
- Protokół dostępu: HTTPS z certyfikatami SSL/TLS
- Autentykacja: lokalna, LDAP, Active Directory
- Wielojęzyczność: minimum język angielski i polski
- Responsywność: interfejs dostosowany do urządzeń mobilnych

Funkcjonalności zarządzania

- Zarządzanie hostami: dodawanie, usuwanie, monitoring
- Zarządzanie maszynami wirtualnymi: tworzenie, konfiguracja, uruchamianie, zatrzymywanie
- Zarządzanie storage: konfiguracja storage repositories
- Zarządzanie siecią: konfiguracja sieci wirtualnych
- Zarządzanie użytkownikami: role i uprawnienia
- Dashboard: przegląd stanu infrastruktury
- Alerty: powiadomienia o zdarzeniach systemu

Funkcje operacyjne

- Backup & Restore: planowanie i wykonywanie kopii zapasowych
- Live Migration: migracja maszyn bez przestojów
- Load Balancing: równoważenie obciążenia między hostami
- Disaster Recovery: funkcje odzyskiwania po awarii
- Reporting: raporty wykorzystania zasobów
- Portal: portal dla użytkowników końcowych

WYMAGANIA DOTYCZĄCE KOMPATYBILNOŚCI

Protokoły i standardy

- API: RESTful API dla integracji z systemami trzecimi
- Protokoły storage: NFS v3/v4, iSCSI, FC, CIFS/SMB

- Protokoły sieciowe: VLAN (802.1Q), Link Aggregation (802.3ad)
- Formaty eksportu: OVF, OVA
- Protokoły zarządzania: SNMP v2/v3

Integracje

- Monitoring: możliwość integracji z systemami monitoringu (Nagios, Zabbix)
- Backup: kompatybilność z rozwiązaniami backup firm trzecich
- Directory Services: LDAP, Active Directory
- Cloud: możliwość integracji z chmurami publicznymi

WYMAGANIA DOTYCZĄCE WDROŻENIA

Wykonawca zobowiązany jest do realizacji wszystkich etapów wdrożenia systemu, obejmujących:

- opracowanie szczegółowego planu wdrożenia,
- instalację i konfigurację systemu,
- migrację istniejących maszyn i danych,
- konfiguracja backupu maszyn wirtualnych
- konfiguracja powiadomień oraz raportów
- przeprowadzenie kompleksowych testów funkcjonalności,
- szkolenie użytkowników,

bezpośrednio na miejscu u Zamawiającego. Wszelkie prace wdrożeniowe, w tym instalacja, konfiguracja, migracja, testy oraz szkolenia muszą być realizowane w siedzibie Zamawiającego, z udziałem jego przedstawicieli i z uwzględnieniem specyfiki środowiska produkcyjnego.

Dodatkowo, Wykonawca zobowiązany jest do takiego prowadzenia prac, aby nie zakłócać bieżącej działalności Zamawiającego, a wszelkie przerwy wynikające z wdrożenia muszą być uzgadniane z Zamawiającym

2) Dostawa instalacja i konfiguracja systemu operacyjnego

Instalacja systemu operacyjnego

Instalacja Microsoft Windows Server 2025 Standard (w wersji pełnej – Desktop Experience).

Konfiguracja podstawowa serwera:

- Ustawienie statycznego adresu IP,
- Nazwa hosta,
- Synchronizacja czasu z zewnętrznym źródłem NTP,
- Instalacja aktualizacji systemowych,
- Konfiguracja zapory systemowej.

Instalacja i konfiguracja Active Directory

- Instalacja ról:
- Active Directory Domain Services,
- DNS Server,
- Group Policy Management.

Utworzenie nowej domeny lokalnej

Konfiguracja struktury jednostek organizacyjnych (OU):

- Użytkownicy,
- Komputery,
- Administratorzy,
- Serwery,
- Goście itp.

Konfiguracja polityk grupowych (GPO)

- Przygotowanie i wdrożenie podstawowych polityk zabezpieczeń, m.in.:
- Polityka haseł: min. 12 znaków, złożoność, wygaśnięcie co 90 dni,
- Polityka blokady konta: blokada po 5 błędnych logowaniach, 15 minut przerwy,
- Wyłączenie autologowania,

- Wyłączenie funkcji autorun i automatycznego montowania nośników,
- Wymuszenie aktualizacji systemu Windows,
- Włączenie rejestrowania zdarzeń zabezpieczeń (audytów),
- Ograniczenia dostępu do Panelu sterowania i ustawień systemowych (dla użytkowników nieuprzywilejowanych).
- Polityki wymuszającej szyfrowanie wszystkich dysków twardych na komputerach podłączonych do domeny z wykorzystaniem mechanizmu BitLocker

Testy i odbiór

- Weryfikacja działania domeny:
- Logowanie użytkownika do domeny z maszyny klienckiej,
- Zastosowanie polityk GPO,
- Replikacja usług AD i DNS (jeśli dotyczy),
- Odbiór środowiska na podstawie protokołu.

3) Instalacja i konfiguracja oprogramowania antywirusowego posiadanego przez zamawiającego na zainstalowanym systemie operacyjnym

Instalacja i konfiguracja najnowszej dostępnej wersji **ESET PROTECT (on-premises)**:

- ESET PROTECT Server,
- ESET Web Console (konsola zarządzająca przez przeglądarkę),
- ESET Management Agent,

Integracja i konfiguracja

- Połączenie konsoli z domeną Active Directory (jeśli występuje):
  - Synchronizacja użytkowników i jednostek organizacyjnych (OU),
  - Automatyczne wykrywanie stacji końcowych,
  - Wstępna klasyfikacja urządzeń wg grup dynamicznych i statycznych.
- Konfiguracja dostępu administratorów i operatorów:
  - Utworzenie kont użytkowników konsoli,
  - Nadanie odpowiednich uprawnień (role, zakresy działania).

Wdrożenie polityk bezpieczeństwa

- Utworzenie zestawu polityk dla:
  - **Stacji roboczych** – ochrona w czasie rzeczywistym, kontrola nośników, PUA, zapora, aktualizacje sygnatur,
  - **Serwerów** – minimalna ingerencja w wydajność, ochrona przed ransomware, harmonogramy skanowania.
- Zdefiniowanie harmonogramów skanowania oraz automatycznych działań w przypadku wykrycia zagrożenia.

Testy i odbiór
Weryfikacja poprawności działania systemu:

- Widoczność stacji i serwerów w konsoli,
- Przypisane polityki i ich egzekwowanie,
- Komunikacja między agentami a serwerem,
- Wysyłka powiadomień e-mail, generowanie raportów.

4) Instalacja i konfiguracja oprogramowania typu SIEM (Wazuh)

Przedmiotem zamówienia jest świadczenie usługi polegającej na:

- przygotowaniu i skonfigurowaniu maszyny wirtualnej z systemem Debian 12
- instalacji oraz wstępnej Wazuh w najnowszej stabilnej wersji
- integracji funkcjonalności systemu Wazuh z agentami oraz wdrożenia monitorowania bezpieczeństwa sieci i serwerów.

Wymagane funkcjonalności do konfiguracji w systemie Wazuh

Wykonawca zobowiązany jest do zainstalowania oraz pełnej konfiguracji poniższych funkcjonalności w ramach wdrażanego systemu Wazuh:

1. Zbieranie logów (Log Data Collection)
   Konfiguracja zbierania logów z systemów Linux i Windows (przykładowych agentów),
   Obsługa logów systemowych (syslog, journalctl, eventlog)
   Możliwość przyjmowania zdalnych logów (np. z UTM lub serwerów po UDP/TCP).
2. Wykrywanie integralności plików (File Integrity Monitoring - FIM)
   Monitorowanie zmian w krytycznych plikach systemowych i konfiguracyjnych,
   Konfiguracja monitorowania ścieżek,
   Wysyłanie alertów przy zmianach zawartości lub uprawnień.
3. Wykrywanie rootkitów (Rootkit Detection)
   Włączenie mechanizmów do wykrywania rootkitów na systemach Linux,
   Skonfigurowanie cyklicznych skanów.
4. Wykrywanie anomalii i nadużyć (Security Configuration Assessment - SCA)
   Włączenie modułów analizy polityk bezpieczeństwa (np. CIS Benchmarks),
   Konfiguracja co najmniej jednego szablonu SCA na system Linux i Windows.
5. Monitorowanie systemowe (Syscheck / Auditd / Syscollector)
   Zbieranie informacji o procesach, usługach, pakietach i aktualizacjach,
   Aktywacja i konfiguracja Auditd (na Debianie),
   Konfiguracja harmonogramu skanów i ich widoczność w dashboardzie.
6. Alertowanie
   Konfiguracja wysyłki powiadomień (e-mail / webhook) na wskazany adres,
   Próg alertów oparty o poziomy zagrożeń (np. poziom 7+),
   Możliwość filtrowania alertów po hostach / modułach.
7. Użytkownicy i dashboard
   Utworzenie konta administratora i kont użytkowników zgodnie z wytycznymi Zamawiającego,
   Konfiguracja certyfikatu SSL (Let’s Encrypt lub self-signed),
   Ograniczenie dostępu do interfejsu tylko dla wskazanych IP,
   Widoczność aktywnych agentów oraz alertów w interfejsie Wazuh Dashboard.
8. Konfiguracja agentów
   Instalacja i konfiguracja agenta na systemie Linux i Windows
   Konfiguracja automatycznej rejestracji agentów (rejestracja przez managera),
   Możliwość ręcznego dodawania agentów przez administratora.

Wymagania bezpieczeństwa

Wykonawca zobowiązany jest do:

- Ograniczenia dostępu do portów systemu tylko do wskazanych adresów IP (firewall lokalny lub inny wskazany mechanizm).
- Przekazania wszelkich danych dostępowych (hasła, certyfikaty, klucze) w sposób zaszyfrowany (np. za pomocą archiwum zabezpieczonego hasłem lub systemu szyfrowania plików).

Wykonawca zobowiązany jest do przekazania dokumentacji zawierającej:

- Szczegóły dotyczące zainstalowanych komponentów,
- Instrukcja dodawania kolejnych agentów,
- Hasła dostępowe (zabezpieczone),
- Lokalizacja plików konfiguracyjnych i logów,

Warunki dodatkowe

- Wykonawca musi posiadać doświadczenie w instalacji ww systemów (co najmniej jedno udokumentowane wdrożenie),
- Miejsce realizacji – siedziba zamawiającego

5) Instalacja i konfiguracja oprogramowania do inwentaryzacji (OcsInventory+GLPI)

Przedmiotem zamówienia jest świadczenie usługi polegającej na:
- Przygotowaniu i skonfigurowaniu maszyny wirtualnej z systemem Debian 12 (minimalna instalacja),
- Instalacji oraz konfiguracji oprogramowania OCS Inventory NG Server wraz z bazą danych,
- Instalacji oraz konfiguracji systemu GLPI,
- Integracji GLPI z OCS Inventory NG i wstępna konfiguracja systemu do ewidencji sprzętu IT i zarządzania zasobami.

Wykonawca zobowiązany jest do wdrożenia i skonfigurowania poniższych funkcjonalności:
1. Automatyczna inwentaryzacja sprzętu
   - Zbieranie informacji o sprzęcie (CPU, RAM, dyski, BIOS, urządzenia peryferyjne),
   - Zbieranie informacji o zainstalowanym oprogramowaniu,
   - Przesyłanie danych z agentów OCS z systemów Windows i Linux,
   - Automatyczne przypisywanie urządzeń do lokalizacji / użytkowników.
2. Integracja OCS z GLPI
   - Ustawienie importu zasobów z OCS do GLPI,
   - Synchronizacja danych o sprzęcie i oprogramowaniu,
   - Automatyczne tworzenie pozycji w bazie danych GLPI z danych OCS.
3. Zarządzanie zasobami w GLPI
   - Rejestracja i edycja zasobów: komputery, monitory, drukarki, sieć, oprogramowanie,
   - Przypisywanie zasobów do użytkowników, działów, lokalizacji,
   - Tworzenie relacji między zasobami (np. komputer – użytkownik – licencja – miejsce).
4. Obsługa zgłoszeń (Helpdesk)
   - Włączenie systemu zgłoszeń (ticketing) w GLPI,
   - Możliwość zgłaszania awarii przez formularz webowy,
   - Powiadomienia e-mail o nowych zgłoszeniach i zmianach statusu,
   - Możliwość przydzielania zgłoszeń do techników.
5. Zarządzanie użytkownikami i dostępem
   - Utworzenie kont administratora i użytkowników zgodnie z zaleceniami Zamawiającego,
   - Konfiguracja uprawnień zgodnie z rolami,
   - Możliwość logowania przez LDAP
6. Raportowanie i przeszukiwanie danych
   - Tworzenie prostych raportów o stanie zasobów,
   - Przeglądanie historii zmian i logów inwentaryzacyjnych,
   - Eksport danych do CSV / PDF.
7. Agent OCS Inventory
   - instalacja agenta OCS na systemach Windows Linux,
   - Skonfigurowanie harmonogramu przesyłania danych do serwera OCS.

Wykonawca zobowiązany jest do przekazania dokumentacji zawierającej:
- Opis instalacji OCS i GLPI,
- Lista zainstalowanych komponentów,
- Dane dostępowe,
- Instrukcja dodawania nowych agentów OCS i użytkowników GLPI,
- Lokalizacja plików konfiguracyjnych.

Warunki dodatkowe
- Wykonawca musi posiadać doświadczenie w instalacji ww. systemów (co najmniej jedno udokumentowane wdrożenie),
- Miejsce realizacji – siedziba zamawiającego

6) **Instalacja i konfiguracja oprogramowania do monitorowania sieci (Zabbix)**

Przedmiotem zamówienia jest świadczenie usługi polegającej na:

- Przygotowaniu i skonfigurowaniu maszyny wirtualnej z systemem Debian 12 (minimalna instalacja),
- Instalacji oraz konfiguracji oprogramowania Zabbix w wersji LTS lub najnowszej stabilnej,
- Konfiguracji monitorowania infrastruktury IT Zamawiającego z wykorzystaniem wybranych funkcji systemu Zabbix.

Wykonawca zobowiązany jest do zainstalowania oraz pełnej konfiguracji poniższych funkcjonalności w ramach wdrażanego systemu Zabbix:

1. Monitorowanie systemów operacyjnych (Zabbix Agent)
   - Instalacja i konfiguracja Zabbix Agent na wybranych systemach Linux/Windows,
   - Zbieranie danych o:
     - Obciążeniu CPU, RAM, dysku,
     - Działających procesach i usługach,
     - Dostępności portów i usług sieciowych.
2. Monitorowanie SNMP
   - Konfiguracja SNMPv2/v3 dla urządzeń sieciowych (przełączniki, routery, UPS),
   - Wczytanie plików MIB i szablonów dla min. 1 urządzenia SNMP,
   - Monitorowanie statusów portów, użycia pasma, błędów transmisji.
3. Monitoring logów i plików (log file monitoring)
   - Konfiguracja monitoringu wskazanych plików logów,
   - Wykrywanie słów kluczowych (alertów) i generowanie powiadomień.
4. Alertowanie i eskalacje
   - Konfiguracja powiadomień e-mail lub webhook,
   - Ustalenie progów alarmowych,
   - Eskalacja alertów w zależności od poziomu zagrożenia i czasu braku reakcji,
   - Przykładowy test alertowania.
5. Dashboard i wizualizacja danych
   - Konfiguracja dashboardów systemowych dla serwerów i urządzeń,
   - Tworzenie wykresów (triggers, items, graphs),
   - Widoczność statusów urządzeń i zdarzeń.
6. Automatyczne wykrywanie hostów (auto-discovery)
   - Konfiguracja reguł wykrywania hostów w sieci lokalnej,
   - Automatyczne przypisywanie szablonów,
   - Możliwość klasyfikacji hostów według typów.
7. Szablony monitoringu
   - Użycie gotowych i/lub własnych szablonów Zabbix,
   - Modyfikacja szablonów do potrzeb Zamawiającego,
   - Możliwość przypisania szablonów per grupa urządzeń.

Wykonawca zobowiązany jest do przekazania dokumentacji zawierającej:

- Szczegóły dotyczące zainstalowanych komponentów,
- Instrukcja dodawania kolejnych hostów i agentów,
- Hasła dostępowe (zabezpieczone),
- Lokalizacja plików konfiguracyjnych i logów,

Warunki dodatkowe

- Wykonawca musi posiadać doświadczenie w instalacji ww systemów (co najmniej jedno udokumentowane wdrożenie),
- Miejsce realizacji – siedziba zamawiającego

7) **Instalacja i konfiguracja oprogramowania do gromadzenia logów (Grafana Loki)**

Przedmiotem zamówienia jest świadczenie usługi polegającej na:

- Przygotowaniu i skonfigurowaniu maszyny wirtualnej z systemem Debian 12 (minimalna instalacja),
- Instalacji oraz konfiguracji systemu monitorowania Grafana wraz z modułem do zbierania i analizy logów Grafana Loki,
- Skonfigurowaniu źródeł danych, integracji z systemami logowania oraz wizualizacji danych z wykorzystaniem dashboardów.

Wykonawca zobowiązany jest do skonfigurowania poniższych funkcji:

1. Centralizacja logów
   - Zbieranie logów z systemów Linux, Windows,
   - Obsługa niestandardowych plików logów (logi aplikacji),
   - Rejestrowanie zmian konfiguracyjnych i systemowych.
2. Wizualizacja i analiza danych
   - Tworzenie dashboardów logów z możliwością filtrowania po czasie, poziomie błędów i słowach kluczowych,
   - Grupowanie logów po hostach, usługach lub źródłach,
   - Wyszukiwanie pełnotekstowe w logach (LogQL).
3. Alertowanie
   - Ustawienie powiadomień dla określonych zdarzeń (słowo kluczowe, poziom logu ERROR),
   - Wysyłanie alertów na e-mail, webhook, MS Teams, Slack lub inne (na podstawie ustaleń),
   - Definiowanie warunków powiadomień.
4. Zarządzanie użytkownikami i dostępem
   - Utworzenie ról użytkowników (admin, read-only itp.),
   - Zabezpieczenie interfejsu logowania (HTTPS, IP filtering),
   - Możliwość rozbudowy o zewnętrzne mechanizmy SSO/LDAP.
5. Monitorowanie i wydajność
   - Monitoring samego działania instancji Grafana i Loki,
   - Dashboardy systemowe (obciążenie CPU, zużycie RAM, dysku),
   - Alerty dotyczące niedostępności serwisów.

Wykonawca zobowiązany jest do przekazania dokumentacji zawierającej:

- Szczegóły dotyczące zainstalowanych komponentów,
- Instrukcja tworzenia nowych dashboardów i źródeł danych,
- Hasła dostępowe (zabezpieczone),
- Lokalizacja plików konfiguracyjnych i logów,

Warunki dodatkowe

- Wykonawca musi posiadać doświadczenie w instalacji ww. systemów (co najmniej jedno udokumentowane wdrożenie),
- Miejsce realizacji – siedziba zamawiającego

II. Zakup urządzenia NAS – 1szt.

W ofercie należy wpisać: producent, model	Producent ……. Model ……
Obudowa	Rack 2U o wymiarach, 88,6 × 482,14 × 346,43 mm (wys. x szer. x gł.)
Procesor	Zainstalowany jeden procesor, min. 2.0GHz, klasy x86 osiągnięcie w teście PASSMARK CPU Benchmarks wynik nie gorszy niż 4 000 punktów w teście PassMark Average CPU Mark - Multithread Rating

	<u>Do oferty należy dołączyć wydruk ze strony potwierdzający osiągnięty wynik dla oferowanych procesorów. Dopuszcza się wydruk w języku angielskim.</u>
RAM	8 GB SO-DIMM DDR4 (1 x 8 GB), możliwość rozszerzenia pamięci do 16GB (2x8GB)
Ilość obsługiwanych dysków	8 dysków 3,5-calowych SATA 6 Gb/s, 3 Gb/s
Interfejsy sieciowe	2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) wraz z patchcordami - 2m 1 port 10 Gigabit sieci Ethernet (RJ-45) (możliwość uzyskania poprzez dołożenie karty rozszerzeń tego samego producenta). wraz z patchcordem CAT7 - 2m
Porty	2x USB 2.0, 2x USB 3.2 Gen 2, 1x HDMI 1.4b, 1x PCIe Gen 3 x2
Wskaźniki LED	HDD 1–8, stan, LAN, rozszerzenie, zasilanie
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare,6,6+Spare,10 i 10+Spare, RAID50, RAID60. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
Obsługiwane systemy operacyjne	Apple Mac OS 10.10 i nowsze Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 i nowsze IBM AIX 7, Solaris 10 i nowsze Microsoft Windows 10, 11 Microsoft Windows Server 2016, 2019, 2022, 2025
Stacja monitoringu	Obsługa do 24 kamer IP (8 licencji domyślnie).
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Obsługa paczek QPKG, Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Virtualization Station
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Język GUI	Polski
Gwarancja i serwis	36 miesięcy, producenta
Waga	10,71 kg (brutto), 9,21kg (netto)
Pobór mocy	Uśpienie: 31.742 W Praca: 55.83 W
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń (CIFS)	1500
Max liczba migawek	1024
Zasilanie	Redundantne 300 W (x2), 100–240 V
Wentylatory	3 x 60mm, 12VDC
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.
Dyski twarde	4 dyski 3,5-cala HDD, SATA 6Gb/s, 512 cache, 7200RPM, o pojemności co najmniej 10TB każdy, znajdujących się na liście kompatybilności producenta, gwarancja 60 miesięcy, o współczynniku MTBF równym 2,000,000 godzin. Prędkość transferu wewnętrznego powinna wynosić

	do min. 267 MB/s. Gęstość powierzchniowa min. 1020Gbits na cal kwadratowy. Średnie opóźnienie na poziomie 4.16ms. Zużycie mocy w trybie spoczynku: max. 9.2W, w trybie pracy: max. 8.4W. Dysk klasy enterprise, objęty 60 miesięczną gwarancją producenta.
Elementy montażowe	Komplet wysuwanych szyn umożliwiających montaż w szafie rack

Zakres wdrożenia serwera NAS

1. Przygotowanie infrastruktury:

- Zweryfikowanie dostępności miejsca w szafie rack oraz zapewnienie odpowiednich warunków zasilania.
- Zapewnienie dostępu do odpowiednich przełączników sieciowych oraz przygotowanie przewodów sieciowych i zasilających.

Montaż serwera NAS:

- Rozpakowanie serwera NAS, weryfikacja kompletności zestawu.
- Zamontowanie serwera NAS w szafie rack przy użyciu dostarczonych szyn montażowych
- Instalacja dysków twardych w dedykowanych slotach.

Podłączenie i uruchomienie:

- Podłączenie zasilania redundantnego do serwera NAS.
- Szyfrowanie przestrzeni dyskowej NAS
- Podłączenie kabli sieciowych (1Gb i 10Gb Ethernet) do portów serwera NAS i przełączników sieciowych.

Testy działania:

- Sprawdzenie poprawności zasilania redundantnego przez odłączenie jednego źródła zasilania.
- Testowanie temperatury pracy urządzenia w zamkniętej szafie rack.
- Przeprowadzenie diagnostyki urządzenia w celu sprawdzenia stanu komponentów (dyski, interfejsy sieciowe, pamięć RAM).

Organizacja i zabezpieczenie:

- Optymalizacja układu kabli, ich estetyczne rozmieszczenie i zabezpieczenie w szafie rack.
- Zabezpieczenie fizycznego dostępu do urządzenia (np. mechanizm blokady obudowy).

2. Konfiguracja sieciowa

Skonfigurowanie sieci w serwerze NAS:

- Przypisanie adresów IP, konfiguracja DNS i integracja serwera z istniejącą siecią.

Testy sieciowe:

- Weryfikacja przepustowości połączeń sieciowych i stabilności przesyłu danych.

III. Zakup zarządzalnych urządzeń sieciowych z obsługą VLAN – Switch – 1szt.

W ofercie należy wpisać: producent, model	Producent ……. Model ……
Obudowa	• Przełącznik w obudowie typu RACK o wysokości max. 1U wraz z zestawem montażowym
Rodzaj urządzenia	• Zarządzalny przełącznik L3
Porty i gniazda	• - min. 48 porty RJ45 1G • - min. 2 porty RJ45 o przepustowości 10G • - min. 4 porty SFP+ o przepustowości 10G • Gniazdo zasilania AC
Obsługa zarządzania	• Web, CLI, Telnet, SNMP, Cloud, aplikacja mobilna
Wydajność	• Przepustowość przełączania: min 210 Gbps

	• Szybkość przesyłania danych: min 150 Mpps • Bufor pakietów: 2 MB • Tablica adresów MAC: 32 000 • Ramka Jumbo: 9 KB • Tablica przekierowań L3: do 1000 wpisów IPv4, do 512 wpisów IPv6 • Tabela routingu: 64 wpisy • Routing VLAN: Tak • Interfejsy IP: 32
Bezpieczeństwo	• Warstwa 3 Filtrowanie IP • Warstwa 4 Filtrowanie gniazd TCP/UDP • Statyczne przekierowanie MAC • Wiele serwerów TACACS+ • Przypisywanie 802.1x VLAN i 802.1p przez RADIUS • Uwierzytelnianie logowania przez RADIUS • Uwierzytelnianie logowania przez TACACS+ • Rachunkowość TACACS+ • Rachunkowość RADIUS • Autoryzacja w RADIUS • Uwierzytelnianie złożone • Autoryzacja przez TACACS+ • SSL • Zamrożenie MAC • Ochrona źródła IP (IPv4*/IPv6) • DHCP snooping • Ochrona serwera DHCP • Inspekcja ARP • Zamrożenie ARP • Skanowanie anty-ARP • Statyczne wiązanie IP-MAC-Port • Filtrowanie bezpieczeństwa oparte na polityce • Ochrona procesora • Włączanie/wyłączanie pułapek związanych z interfejsem (przez port) • Uwierzytelnianie oparte na MAC dla VLAN • Przezroczystość BPDU • Przekazywanie WoL/WoL
Routing	• Trasa statyczna • Przenoszenie portów IP • Przekazywanie DHCP
Kontrola ruchu	• VLAN oparty na portach • Izolacja VLAN • VLAN oparty na protokole • VLAN oparty na podsieci IP • VLAN oparty na MAC • Prywatna VLAN • Niezależne uczenie się VLAN (IVL) • Translacja VLAN • Trunking VLAN • Mapowanie VLAN • IEEE 802.1AD Układanie VLAN w stos (QinQ) • Filtrowanie wejścia VLAN • GVRP

	• L2PT
Centralne zarządzanie	• System zarządzania siecią musi być oparty o chmurę (SaaS), umożliwiający centralne zarządzanie urządzeniami sieciowymi w wielu lokalizacjach z poziomu jednej platformy webowej. • Wymagane jest wsparcie dla urządzeń: punkty dostępowe Wi-Fi, przełączniki sieciowe oraz bramy zabezpieczające (firewalle), zarządzane przez chmurę. • Możliwość zarządzania wieloma lokalizacjami i użytkownikami z jednego panelu. • Przypisywanie uprawnień administracyjnych na podstawie ról (role-based access control). • Monitorowanie i raportowanie w czasie rzeczywistym oraz dostęp do historii zdarzeń. • Powiadomienia o zmianach konfiguracji i zdarzeniach sieciowych w czasie rzeczywistym. • Audyt logowań i zmian konfiguracji. • Automatyczne aktualizacje firmware i funkcji przez chmurę. • Możliwość klonowania konfiguracji i szybkiego wdrażania nowych lokalizacji. • Szyfrowana komunikacja między urządzeniami a chmurą (TLS/SSL). • Możliwość tworzenia bezkontaktowych tuneli VPN pomiędzy lokalizacjami. • Obsługa uwierzytelniania 802.1X, RADIUS, MAC, captive portal. • Konfiguracja i monitoring punktów dostępowych Wi-Fi (minimum standard 802.11ac Wave 2, obsługa WPA3, VLAN, SSID). • Zarządzanie przełącznikami warstwy 2 • Wsparcie dla aplikacji mobilnej (Android/iOS) umożliwiającej rejestrację i monitoring urządzeń.
Warunki gwarancji	• Zamawiający wymaga gwarancji Producenta na okres 5 lat.

Zakres wdrożenia switcha

1. Przygotowanie infrastruktury:

- Demontaż dwóch aktualnie zainstalowanych switchy z szafy, rack montaż nowych urządzeń na ich miejsce oraz zapewnienie odpowiednich i stabilnych warunków zasilania.
- Zapewnienie dostępu do odpowiednich przełączników sieciowych oraz przygotowanie przewodów sieciowych i zasilających.

Montaż switch:

- Rozpakowanie switcha, weryfikacja kompletności zestawu.
- Zamontowanie switcha w szafie rack przy użyciu dostarczonych szyn montażowych

Podłączenie i uruchomienie:

- Podłączenie zasilania do switcha.
- Podłączenie kabli sieciowych (1Gb i 25Gb Ethernet)
- Testowanie połączeń fizycznych między serwerem a przełącznikami sieciowymi.
- Konfiguracja UTM Fortigate wraz ze switchem (konfiguracja adresacji, ustawienie powiadomień, konfiguracja segmentacji sieci (WI-FI, serwery, administracja, goście)

Testy działania:

- Testowanie temperatury pracy urządzenia w zamkniętej szafie rack.
- Przeprowadzenie diagnostyki urządzenia.

Organizacja i zabezpieczenie:

- Optymalizacja układu kabli, ich estetyczne rozmieszczenie i zabezpieczenie w szafie rack.

IV. Zakup systemów UPS do serwerowni – 1 szt.

W ofercie należy wpisać: producent, model	Producent ……. Model ……
Minimalne wymagania techniczne dla jednostki UPS	Moc wyjściowa pozorna [VA]: 3000 Moc wyjściowa czynna [W]: 2700 Topologia: line-interactive Typ obudowy: Rack 2U Temperatura pracy [°C]: 0 do 40°C Stopień ochrony IP 20 Masa zasilacza [kg]: 31 Wymiary (wys. x szer. x gł.) [mm]: 86 (2U) x 438 x 608
Parametry wejściowe	Znamionowe napięcie wejściowe [V]: 230 Zakres napięcia wejściowego [V]: 161 - 276 +/-4% Znamionowy prąd wejściowy [A]: 15 Częstotliwość znamionowa napięcia wejściowego [Hz]: 50/60 Zakres częstotliwości wejściowej [Hz] i tolerancja [Hz]: 45 ÷ 55 / 55 ÷ 65 ± 0.1 Typ gniazda wejściowego: C20 Współczynnik mocy PF: > 0,9 Zabezpieczenie wejściowe: przeciwprzepięciowe
Parametry wyjściowe	Znamionowe napięcie wyjściowe [V]: 230 Zakres napięcia wyjściowego [V] - 184 – 243 +/-4% Znamionowy prąd wyjściowy [A]: 13,6 Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej): Sinusoidalny / Tak jak na wejściu Częstotliwość znamionowa napięcia wyjściowego [Hz]: 50/60 Zakres częstotliwości - praca sieciowa [Hz]: Synchronicznie z siecią Zakres częstotliwości - praca rezerwowa [Hz]: 50 / 60 +/-0,1 Zakres regulacji napięcia AVR: -30% - +20% Czas przełączenia na pracę rezerwową [ms]: <6 Czas powrotu na pracę sieciową [ms]: 0 Przeciążalność [%]: <110 – wyłączenie UPS po 3 minutach / 110 – 150 – wyłączenie UPS po 200 ms Zabezpieczenie wyjściowe: Elektroniczne – przeciwzwarciowe i przeciążeniowe Przyłącza wyjściowe (liczba i typ gniazd): 4 x IEC 320 C13 (10 A) - sterowalne, 4 x IEC 320 C13 (10 A) niesterowalne, 1x IEC 320 C19 (16A) sterowalne
Akumulatory i czas podtrzymania	Akumulatory wewnętrzne: 12 V / 9 Ah VRLA Liczba akumulatorów wewnętrznych: 1 x 6 Dopuszczalna całkowita pojemność akumulatorów wewnętrznych [Ah]: 9 Zewnętrzne moduły bateryjne: TAK Maksymalna liczba modułów bateryjnych: 10 Napięcie nominalne obwodu DC [V]: 72 Maksymalny prąd ładowania [A]: 1,5 Czas podtrzymania z baterii wewnętrznych (100 % / 80 % / 50 % Pmax) [min]: 4 / 5 / 9 Maksymalny czas ładowania baterii wewnętrznych UPS - po 80 % wyładowaniu baterii [h]: ≤ 7 h Zabezpieczenia wejścia DC (akumulatory wewnętrzne) [A / V DC]: Zabezpieczenie nadprądowe

Komunikacja i zarządzanie	Interfejsy komunikacyjne: karta styków bezpotencjałowych AS 400 – (opcja), RS232, zamontowana karta sieciowa SNMP/http Oprogramowanie monitorująco-zarządzające Sygnalizacja: Akustyczno – optyczna, graficzny wyświetlacz LCD EPO: Jest (NC)
Certyfikaty, zgodności oraz gwarancja	CE, PN-EN 62040-1:2009, PN-EN 62040-2:2008 Okres gwarancji na urządzenie: 24 miesiące Okres gwarancji na akumulatory: 24 miesiące

Zakres wdrożenia UPS-a

1. Przygotowanie infrastruktury:

- Demontaż aktualnie zainstalowanego UPS-a z szafy rack, montaż nowego urządzenia na jego miejsce oraz zapewnienie odpowiednich, stabilnych i bezpiecznych warunków zasilania.
- przygotowanie przewodów sieciowych i zasilających.

Montaż switch:

- Rozpakowanie UPS-a, weryfikacja kompletności zestawu.
- Zamontowanie UPS-a w szafie rack przy użyciu dostarczonych szyn montażowych

Podłączenie i uruchomienie:

- Podłączenie zasilania do UPS-a.
- Podłączenie kabla sieciowego
- Testowanie połączeń fizycznych między UPS-em a przełącznikami sieciowymi.
- Konfiguracja czujników pomiaru warunków środowiskowych

Testy działania:

- Testowanie temperatury pracy urządzenia w zamkniętej szafie rack.
- Przeprowadzenie diagnostyki urządzenia.

Organizacja i zabezpieczenie:

- Optymalizacja układu kabli, ich estetyczne rozmieszczenie i zabezpieczenie w szafie rack.

V. Urządzenie centralnie zarządzane stanowiące punktu dostępu bezprzewodowego do sieci – 3 szt.

W ofercie należy wpisać: producent, model	Producent ……. Model ……
Standard	• Wi-Fi 6E (802.11a/b/g/n/ac/ax)
Obsługiwane protokoły	• IEEE 802.3af • IEEE 802.3at
Obsługiwane częstotliwości	• 2.4 GHz • 5 GHz • 6 GHz
Prędkość transmisji	• 2.4 GHz – 575 Mbps • 5 GHz – 4800 Mbps • 6 GHz– 4800 Mbps
Porty i gniazda	• 1 x LAN 10/100/1000 Mb/s • 1 x LAN 10/100/1000/2500 Mb/s
Szyfrowanie	• WEP • WPA • WPA2 • WPA3

Typ anteny	• 4x4 • 2x2 MIMO
Zysk anten	• 2.4 GHz: Peak Gain 3dBi • 5 GHz: Peak Gain 5dBi • 6 GHz: Peak Gain 6dBi
Funkcje WLAN	• Sterowanie pasmem • Mesh • DCS • Load balancing
Uwierzytelnianie	• IEEE 802.1X • RADIUS authentication
Centralne zarządzanie	• System zarządzania siecią musi być oparty o chmurę (SaaS), umożliwiający centralne zarządzanie urządzeniami sieciowymi w wielu lokalizacjach z poziomu jednej platformy webowej. • Wymagane jest wsparcie dla urządzeń: punkty dostępowe Wi-Fi, przełączniki sieciowe oraz bramy zabezpieczające (firewalle), zarządzane przez chmurę. • Możliwość zarządzania wieloma lokalizacjami i użytkownikami z jednego panelu. • Przypisywanie uprawnień administracyjnych na podstawie ról (role-based access control). • Monitorowanie i raportowanie w czasie rzeczywistym oraz dostęp do historii zdarzeń. • Powiadomienia o zmianach konfiguracji i zdarzeniach sieciowych w czasie rzeczywistym. • Audyt logowań i zmian konfiguracji. • Automatyczne aktualizacje firmware i funkcji przez chmurę. • Możliwość klonowania konfiguracji i szybkiego wdrażania nowych lokalizacji. • Szyfrowana komunikacja między urządzeniami a chmurą (TLS/SSL). • Możliwość tworzenia bezkontaktowych tuneli VPN pomiędzy lokalizacjami. • Obsługa uwierzytelniania 802.1X, RADIUS, MAC, captive portal. • Konfiguracja i monitoring punktów dostępowych Wi-Fi (minimum standard 802.11ac Wave 2, obsługa WPA3, VLAN, SSID). • Zarządzanie przełącznikami warstwy 2 • Wsparcie dla aplikacji mobilnej (Android/iOS) umożliwiającej rejestrację i monitoring urządzeń.
Zasilanie	• Switch smart (dostęp poprzez przeglądarkę www) • Architektura sieci - gigabit Ethernet • Złącza RJ-45 10/100/1000 Mbps - 5 szt. • Power over Ethernet (PoE) • PoE - 802.3af (PSE) do 15.4 W • Liczba portów PoE/PoE+ - 4 portów • Przepustowość 10 Gb/s • Materiał obudowy – Metal • Dodatkowe informacje - Automatyczne krosowanie portów (Auto MDI-MDIX) - Automatyczne rozpoznawanie kabla krosowego (MDI/MDIX) - QoS - VLAN

Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta na okres 5 lat.

Zakres wdrożenia AP

Montaż AP:
- Rozpakowanie AP, weryfikacja kompletności zestawu.
- Zamontowanie AP w miejscu wskazanym przez zamawiającego

Podłączenie i uruchomienie:
- Podłączenie zasilania do AP
- Podłączenie kabla sieciowego
- Konfiguracji sieci WI-FI dla pracowników i oddzielnej izolowanej sieci dla gości

Testy działania:
- Testowanie prędkości sieci Wi-FI
- Przeprowadzenie diagnostyki urządzenia.

VI. Urządzenie centralnie zarządzane stanowiące punktu dostępu bezprzewodowego do sieci – 3 szt.

W ofercie należy wpisać: producent, model	Producent ……. Model ……
Obudowa	• Przełącznik w obudowie metalowej typu desktop
Rodzaj urządzenia	• Zarządzalny przełącznik L2
Porty i gniazda	• - min. 5 porty RJ45 1G
Obsługa zarządzania	• Przeglądarka www
Obsługiwane standardy	• IEEE 802.3 u • IEEE 802.3 x • IEEE 802.3 z • IEEE 802.3 ab • IEEE 802.3 az • IEEE 802.1 p • IEEE 802.1 Q
Rozmiar tablicy MAC	• 2k
Ramka Jumbo	• 9,000 B
Dodatkowe informacje	• Automatyczne rozpoznawanie kabla krosowego (MDI/MDIX) • Detekcja pętli • Link Aggregation • QoS • VLAN
Maksymalny pobór mocy	• 3 W
Warunki gwarancji	• Zamawiający wymaga zapewnienia gwarancji Producenta na okres 5 lat.