

Załącznik nr 4 do SWZ

**OPIS PRZEDMIOTU ZAMÓWIENIA  
(OPZ)**

**„Dostawa sprzętu komputerowego wraz z wdrożeniem”**

Bydgoszcz, październik 2024 r.

## OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa poniższego sprzętu komputerowego wraz z wdrożeniem:

1. Urządzenie klasy UTM - 3 szt.
2. Serwer - typ 1 – 3 szt.
3. Serwer - typ 2 - 1 szt.
4. Urządzenie archiwizacji danych - typ 1 – 3 szt.
5. Urządzenie archiwizacji danych - typ 2 – 1 szt.
6. Zasilacz awaryjny - 3 szt.
7. Przełącznik sieciowy - 3 szt.

Szczegółowe wymagania dotyczące poszczególnych urządzeń oraz warunków wdrożenia będących przedmiotem postępowania określone zostały w dalszej części niniejszego Opisu Przedmiotu Zamówienia.

### 1. INFORMACJE OGÓLNE

1. Wykonawca jest zobowiązany dostarczyć przedmiot zamówienia bezpośrednio do siedziby Zamawiającego.
2. Wykonawca zobowiązany będzie zrealizować dostawy objęte przedmiotem zamówienia z należytą starannością, zgodnie z obowiązującymi przepisami prawa, standardami oraz postanowieniami umowy, z uwzględnieniem wymogów bhp.
3. Wykonawca zabezpieczy we własnym zakresie i na własny koszt, wszystkie materiały niezbędne do prawidłowej realizacji przedmiotu zamówienia.
4. Dostarczony przez Wykonawcę sprzęt musi być fabrycznie nowy. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
5. Wszystkie urządzenia, na dzień składania oferty przez Wykonawcę, nie mogą być przeznaczone przez producenta tego sprzętu do wycofania z produkcji lub sprzedaży w okresie minimum 6 miesięcy od dnia składania ofert.
6. Wszystkie oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001 lub równoważną tj. równoważne inne zaświadczenie niezależnego podmiotu zajmującego się poświadczaniem zgodności działań producentów z normami jakościowymi.
7. Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
8. Urządzenia muszą być dostarczone do lokalizacji wskazanych w niniejszym OPZ w oryginalnych opakowaniach fabrycznych, bez śladów ich otwierania.
9. Oferowane urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej, a gwarancja musi pochodzić od producenta i być świadczona przez producenta na terenie Polski lub partnera z autoryzacją serwisową.

10. Dla wszystkich dostarczanych urządzeń Wykonawca dostarczy odpowiednią ilość, o odpowiednich parametrach: kabli zasilających, kabli Ethernet, kabli DAC, kabli AOC, kabli optycznych oraz innych akcesoriów, niezbędnych do przeprowadzenia prawidłowej instalacji urządzeń.
11. Wkładki, kable DAC, kable AOC, kable Splitter muszą być na liście kompatybilności oferowanych urządzeń (jeśli dotyczy i są elementem dostawy).
12. Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V  $\pm$  10%, 50 Hz, jedno lub trzy fazowo i być wyposażone w przewody zasilające.
13. Wszystkie oferowane urządzenia muszą działać pod kontrolą oprogramowania, które jest publiczną wersją, udostępnianą na rynku przez producenta oferowanych urządzeń. Zamawiający nie dopuszcza stosowania oprogramowania dedykowanego, stworzonego na potrzeby niniejszego zamówienia, dla zaoferowanych urządzeń.
14. Wszystkie oferowane urządzenia muszą być publicznie dostępne. Zamawiający nie dopuszcza stosowania urządzeń dedykowanych, stworzonych na potrzeby niniejszego zamówienia.
15. Infrastruktura sprzętowa stanowiąca przedmiot Zamówienia musi być fabrycznie nowa (tj. nieregenerowana, nienaprawiana, niefabrykowana, nieużywana we wcześniejszych wdrożeniach), kompletna (w szczególności ze wszystkimi podzespołami, częściami, materiałami niezbędnymi do uruchomienia i użytkowania).

## 2. SPECYFIKACJA DOSTAWY SPRZĘTU

### 2.1. Urządzenie klasy UTM

Komponent	Minimalne wymagania dla sprzętu
Wymagania Ogólne	<p>Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.</p> <p>System musi wspierać IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> <li>• Firewall</li> <li>• Ochrony w warstwie aplikacji</li> <li>• Protokołów routingu dynamicznego.</li> </ul>

<p><b>Interfejsy, Dysk, Zasilanie</b></p>	<ul style="list-style-type: none"> <li>• System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.</li> <li>• System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.</li> <li>• W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 64 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.</li> <li>• System musi być wyposażony w zasilanie AC.</li> <li>• System musi być wyposażony w wewnętrzny dysk 128GB SSD.</li> </ul>
<p><b>Redundancja, monitoring i wykrywanie awarii</b></p>	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.</p>
<p><b>Wydajność</b></p>	<ul style="list-style-type: none"> <li>• W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę</li> <li>• Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.</li> <li>• Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.</li> <li>• Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.</li> <li>• Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.</li> <li>• Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.</li> </ul>
<p><b>Bezpieczeństwo</b></p>	<ul style="list-style-type: none"> <li>• Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</li> <li>• Kontrola Aplikacji.</li> <li>• Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.</li> <li>• Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.</li> <li>• Ochrona przed atakami - Intrusion Prevention System.</li> <li>• Kontrola stron WWW.</li> <li>• Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.</li> <li>• Zarządzanie pasmem (QoS, Traffic shaping).</li> <li>• Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).</li> </ul>

	<ul style="list-style-type: none"> <li>Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</li> <li>Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.</li> <li>Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system</li> </ul>
<b>Serwisy i licencje</b>	Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 36 miesięcy.
<b>Gwarancja</b>	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

## 2.2. SERWER – TYP I

<b>Komponent</b>	<b>Minimalne wymagania dla sprzętu</b>
<b>Obudowa</b>	Obudowa typu wieża
<b>Płyta główna</b>	Płyta główna dedykowana do pracy w serwerach, wykonująca 64-bitowe instrukcje AMD64 lub EM64T.
<b>Procesor</b>	<p>Zainstalowany jeden procesor min. 8-rdzeniowy, min. 2.8GHz z częstotliwości nominalnej, klasy x86, osiągający minimalne wyniki testów w konfiguracji jednoprocessorowej:</p> <p>SPECrate2017_int_base wynik min. 85 pkt</p> <p>SPECrate2017_int_peak wynik min. 90 pkt</p> <p>SPECrate2017_fp_base wynik min. 100 pkt</p> <p>SPECrate2017_fp_peak wynik min. 100 pkt</p> <p>Maksymalny TDP dla procesora 80W.</p> <p>Wynik testu musi być opublikowany na stronie <a href="https://www.spec.org/cpu2017/results/">https://www.spec.org/cpu2017/results/</a> w dniu złożenia oferty. Wykonawca załączy do oferty wydruk ww. strony ze wskazaniem wiersza odpowiadającego właściwemu wynikowi testów. - <b>dokument wymagany jako przedmiotowy środek dowodowy.</b></p>

<b>RAM</b>	64GB. Płyta główna powinna obsługiwać min. 128GB pamięci RAM.
<b>Gniazda PCI</b>	Minimum 1 slot PCIe x16 generacji 4
<b>Interfejsy sieciowe/</b>	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb Ethernet w standardzie SFP+
<b>Dyski twarde</b>	Zainstalowane 2 dyski M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.  Zainstalowane 2 dyski o pojemności 8TB SATA Hot-Plug (możliwa konfiguracja RAID 0,1,10)  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.
<b>Wbudowane porty</b>	8 x USB z czego nie mniej niż 4x USB 3.2, 1xVGA.
<b>Video</b>	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
<b>Zasilacze</b>	Redundantne, Hot-Plug min. 700W każdy.
<b>Bezpieczeństwo</b>	Zintegrowany z płytą główną moduł TPM 2.0  Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
<b>Karta Zarządzania</b>	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: <ul style="list-style-type: none"> <li>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>• szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>• wsparcie dla IPv6;</li> <li>• wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>• integracja z Active Directory;</li> <li>• wsparcie dla dynamic DNS;</li> </ul>

	<ul style="list-style-type: none"> <li>wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li> </ul>
<b>Certyfikaty</b>	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.</p> <p>Serwer musi posiadać deklarację CE.</p>
<b>System operacyjny</b>	<p>Microsoft Windows Server 2022 Standard lub równoważny – ilość licencji musi odpowiadać konfiguracji sprzętowej oraz umożliwiać 15 użytkownikom korzystanie z funkcjonalności kontrolera domeny.</p>
<b>Warunki gwarancji</b>	<ol style="list-style-type: none"> <li>Minimum 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</li> <li>Wymagane dołączenie do umowy oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta;</li> <li>Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</li> <li>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.</li> <li>Możliwość rozszerzenia gwarancji przez producenta do 5 lat</li> <li>Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.</li> <li>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do umowy oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</li> </ol>
<b>Dokumentacja użytkownika</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

### 2.3. SERWER – TYP II

Parametr	Charakterystyka (wymagania minimalne parametrów technicznych)
----------	---

<b>Obudowa</b>	<p>Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.</p> <p>Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.</p>
<b>Płyta główna</b>	<p>Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.</p>
<b>Chipset</b>	<p>Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych.</p>
<b>Procesor</b>	<p>Zainstalowane 2 procesory minimum 16-rdzeniowe, min. 2.0GHz częstotliwości nominalnej, osiągające minimalne wyniki testów w konfiguracji dwuprocessorowej:</p> <p>SPECrate2017_int_base wynik min. 265pkt  SPECrate2017_int_peak wynik min. 270pkt  SPECrate2017_fp_base wynik min. 370 pkt  SPECrate2017_fp_peak wynik min. 380 pkt</p> <p>Maksymalny TDP dla procesora 150W</p> <p>Wynik testu musi być opublikowany na stronie <a href="https://www.spec.org/cpu2017/results/">https://www.spec.org/cpu2017/results/</a> w dniu złożenia oferty. Wykonawca załączy do oferty wydruk ww. strony ze wskazaniem wiersza odpowiadającego właściwemu wynikowi testów. - <b>dokument wymagany jako przedmiotowy środek dowodowy.</b></p>
<b>RAM</b>	<p>Minimum 256GB w układzie 8x32GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.</p>
<b>Gniazda PCI</b>	<p>Minimum 3 sloty PCIe Gen 4 w tym jeden x16</p>
<b>Interfejsy sieciowe/FC/SAS</b>	<p>Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)</p> <p>Wbudowane min. 2 interfejsy sieciowe 10Gb/25Gb w standardzie SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)</p> <p>Czteroportowa karta 12GB HBA SAS umożliwiająca podłączenie macierzy</p>
<b>Dyski twarde</b>	<p>Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.</p> <p>Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnek na dyski twarde.</p>



<b>System operacyjny/dodatkowe oprogramowanie</b>	Zainstalowany Windows Server 2022 Standard lub równoważny
<b>Wbudowane porty</b>	4x USB w tym min 2x USB 3.0 i jeden port wewnątrz obudowy, 2x VGA z czego jeden na panelu przednim.
<b>Video</b>	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
<b>Zasilacze</b>	Redundantne, Hot-Plug min. 700W każdy.
<b>Bezpieczeństwo</b>	<p>Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej.</p> <p>Możliwość wyłączenia w BIOS funkcji przycisku zasilania.</p> <p>BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła</p> <p>Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</p> <p>Moduł TPM 2.0</p> <p>Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera</p> <p>Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</p>
<b>Diagnostyka</b>	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
<b>Karta Zarządzania</b>	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:</p> <ul style="list-style-type: none"> <li>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>• szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>• możliwość podmontowania zdalnych wirtualnych napędów;</li> <li>• wirtualną konsolę z dostępem do myszy, klawiatury;</li> <li>• wsparcie dla IPv6;</li> <li>• wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> </ul>

- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
- integracja z Active Directory;
- możliwość obsługi przez dwóch administratorów jednocześnie;
- wsparcie dla dynamic DNS;
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
- możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
- możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

OPROGRAMOWANIE ZARZĄDZAJĄCE: umożliwiające zarządzanie poprzez sieć, spełniającego minimalne wymagania:

- wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
- możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
- wsparcie dla protokołów – WMI, SNMP, IPMI, WSMAN, Linux SSH;
- możliwość oskryptowywania procesu wykrywania urządzeń;
- możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
- szczegółowy opis wykrytych systemów oraz ich komponentów;
- możliwość eksportu raportu do CSV, HTML, XLS;
- grupowanie urządzeń w oparciu o kryteria użytkownika;
- automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
- szybki podgląd stanu środowiska;
- podsumowanie stanu dla każdego urządzenia;
- szczegółowy status urządzenia/elementu/komponentu;
- generowanie alertów przy zmianie stanu urządzenia;
- filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
- integracja z service desk producenta dostarczonej platformy sprzętowej;
- możliwość przejęcia zdalnego pulpitu;
- możliwość podmontowania wirtualnego napędu;
- kreator umożliwiający dostosowanie akcji dla wybranych alertów;

	<ul style="list-style-type: none"> <li>• możliwość importu plików MIB;</li> <li>• przesyłanie alertów „as-is” do innych konsol firm trzecich;</li> <li>• aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);</li> <li>• możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;</li> <li>• możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;</li> <li>• moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.</li> </ul>
<b>Certyfikaty</b>	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.</p> <p>Serwer musi posiadać deklarację CE.</p>
<b>Warunki gwarancji</b>	<ol style="list-style-type: none"> <li>1. Minimum 36 miesięcy gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</li> <li>2. Wymagane dołączenie do umowy oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</li> <li>3. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.</li> <li>4. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.</li> <li>5. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikro kodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.</li> <li>6. Możliwość rozszerzenia gwarancji przez producenta do 5 lat</li> <li>7. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.</li> <li>8. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do umowy oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</li> </ol>

<b>Dokumentacja użytkownika</b>	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
---------------------------------	--

#### 2.4. URZĄDZENIE ARCHIWIZACJI DANYCH – TYP I

<b>Komponent</b>	<b>Minimalne wymagania dla sprzętu</b>
<b>Obudowa</b>	Czterokieszeniowa pamięć masowa typu desktop
<b>Procesor</b>	Zainstalowany jeden procesor min. 4-wątkowy, min. 2.0 GHz z częstotliwości nominalnej / 2.7GHz w trybie turbo
<b>Pamięć RAM</b>	16GB z możliwością rozszerzania do 32GB
<b>Ilość obsługiwanych dysków</b>	4 dyski 2,5 lub 3,5"
<b>Ilość zainstalowanych dysków</b>	4 dyski znajdujące się na liście kompatybilności producenta macierzy o min. pojemności 8TB
<b>Interfejsy sieciowe</b>	2 x Gigabit (10/100/1000) 1 x 10GbE Wsparcie dla Link Aggregation, Jumbo Frame oraz WOL.
<b>Porty</b>	2 x USB 3.0 Gen
<b>Wskaźniki LED</b>	Status, LAN, HDD
<b>Obsługa RAID</b>	JBOD, 0,1,5,6,10
<b>Szyfrowanie</b>	Możliwość szyfrowania wybranych udziałów sieciowych, kluczem AES-256bitów
<b>Licencja na Kamery IP</b>	W zestawie licencja na dwie kamery z możliwością rozszerzenia do 50. Funkcja CMS.
<b>Protokoły</b>	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, WebDAV, CalDAV, SFTP,
<b>Usługi</b>	Wsparcie dla High Availability Serwer VPN Serwer pocztowy dla kilku domen Stacja monitoringu Windows ACL Integracja z Windows ADS

	<p>Firewall z kontrolą ruchu</p> <p>Serwer WWW</p> <p>Serwer plików</p> <p>Manager plików przez WWW</p> <p>Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie</p> <p>Antywirus</p> <p>Klient VPN</p> <p>Usługa DDNS</p> <p>Oprogramowanie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji Vmware, Hyper-V</p>
<b>Zarządzanie dyskami</b>	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,
<b>System plików</b>	Dyski wewnętrzne Btrfs, EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT4, EXT3, HFS+, exFAT
<b>Liczba wolumenów</b>	Do 64
<b>Liczba iSCSI Targetów</b>	Do 128
<b>Liczba iSCSI LUN</b>	Do 256
<b>Liczba kont użytkowników</b>	2048
<b>Liczba grup</b>	256
<b>Liczba udziałów</b>	512
<b>Ilość jednoczesnych połączeń</b>	1000 dla CIFS, FTP, AFP
<b>Zasilanie</b>	Zasilanie min. 100W
<b>Gwarancja i serwis</b>	min. 36 miesięcy gwarancji realizowanej w trybie NBD przez producenta lub Autoryzowanego Partnera Serwisowego producenta; dyski objęte wsparciem pozostawienia dysku w przypadku wystąpienia awarii.

## 2.5. URZĄDZENIE ARCHIWIZACJI DANYCH – TYP II

<b>Komponent</b>	<p><b>Minimalne wymagania dla sprzętu</b></p> <p>Nazwę producenta wraz z zaproponowanym modelem należy podać w formularzu cenowym przy pozycji 2.1</p>

<b>Procesor</b>	4 rdzeniowy / 8 wątkowy procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4600 pkt.
<b>Obudowa</b>	RACK max 3U w zestawie szyny do montażu w szafie RACK
<b>Pamięć RAM</b>	16GB z możliwością rozszerzania do 32GB
<b>Ilość obsługiwanych dysków</b>	16 dysków 3,5" / 2,5"
<b>Ilość zainstalowanych dysków</b>	min. 12 dysków w formacie 3,5" znajdujących się na liście kompatybilności producenta macierzy NAS o min. pojemności 8 TB
<b>Interfejsy sieciowe</b>	4 x Gigabit (10/100/1000) 2 x 10 GbE SFP+ obsadzona wkładkami SR 300m Wsparcie dla Link Aggregation, Jumbo Frame oraz WOL.
<b>Porty</b>	2 x USB 3.2 Gen 1, 1x port rozszerzenia dla dodatkowej półki dyskowej
<b>Gniazda PCIe</b>	1x Gen3 x8 slots (x4 link)
<b>Wskaźniki LED</b>	Status, LAN, HDD
<b>Obsługa RAID</b>	Basic, JBOD, SHR, 0,1,5,6,10 + Hot Spare 1,5,6,10
<b>Funkcje RAID</b>	Możliwość zwiększania pojemności i migracja między poziomami RAID online
<b>Szyfrowanie</b>	Możliwość szyfrowania wybranych udziałów sieciowych, kluczem AES-256bitów
<b>Licencja na Kamery IP</b>	W zestawie licencja na dwie kamery z możliwością rozszerzenia do 50. Funkcja CMS.
<b>Protokoły</b>	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, WebDAV, CalDAV, SFTP,
<b>Usługi</b>	Wsparcie dla High Availability Serwer VPN Serwer pocztowy dla kilku domen Stacja monitoringu Windows ACL Integracja z Windows ADS Firewall z kontrolą ruchu Serwer WWW Serwer plików Manager plików przez WWW Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie Antyvirus

	Klient VPN Usługa DDNS Oprogramownie do backup stacji roboczych, serwerów fizycznych i środowiska wirtualizacji Vmware, Hyper-V oraz środowiska Microsoft Office 365
<b>Zarządzanie dyskami</b>	SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,
<b>Język GUI</b>	Polski
<b>System plików</b>	Dyski wewnętrzne Btrfs, EXT4. Dyski zewnętrzne Btrfs, FAT, NTFS, EXT4, EXT3, HFS+, exFAT
<b>Liczba wolumenów</b>	Do 64
<b>Liczba iSCSI Targetów</b>	Do 128
<b>Liczba iSCSI LUN</b>	Do 256
<b>Liczba kont użytkowników</b>	2048
<b>Liczba grup</b>	256
<b>Liczba udziałów</b>	512
<b>Ilość jednoczesnych połączeń</b>	2000 dla CIFS, FTP, AFP
<b>Zasilanie</b>	Zasilanie redundantne min. 550W
<b>Gwarancja i serwis</b>	min. 36 miesięcy gwarancji realizowanej w trybie NBD przez producenta lub Autoryzowanego Partnera Serwisowego producenta; dyski objęte wsparciem pozostawienia dysku w przypadku wystąpienia awarii.

## 2.6. ZASILACZ AWARYJNY

Komponent	Minimalne wymagania dla sprzętu
<b>Wymagania techniczne</b>	<ul style="list-style-type: none"> <li>• Moc znamionowa jednostki nie mniej niż 1kW/ 1kVA</li> <li>• Montaż Tower</li> <li>• Technologia Podwójnej konwersji (online)</li> <li>• Zniekształcenia napięcia wyjściowego poniżej 2%</li> <li>• Temperatura eksploatacji 0 - 40 °C</li> <li>• Wilgotność względna podczas pracy 0 - 95 %</li> <li>• Wysokość n.p.m. podczas pracy 0-3000 m</li> <li>• Hałas słyszalny w odległości 1 m od powierzchni urządzenia 50 dBA</li> </ul>

	<ul style="list-style-type: none"> <li>• Rozpraszanie ciepła w trybie online 317,00 BTU/h</li> <li>• Sprawność: Praca on-line <math>\geq 93,5\%</math> przy pełnym obciążeniu</li> <li>• Klasa ochrony IP 20</li> <li>• Klasa energetyczna sprzętu przeciwprzepięciowego 340J</li> </ul>
<b>Parametry wejściowe</b>	<ul style="list-style-type: none"> <li>• Nominalne napięcie wejściowe 230V</li> <li>• Częstotliwość wejściowa 40–70 Hz (wykrywanie automatyczne)</li> <li>• Typ gniazda wejściowego: British BS1363A, IEC-320 C20, Schuko CEE 7/EU1-16P</li> <li>• Zmienny zakres napięcia wejściowego w trybie podstawowym 100 – 275V 40% obciążenia, 176-275V</li> <li>• Inne napięcia wejściowe 220, 240</li> </ul>
<b>Parametry wyjściowe</b>	<p>Napięcie wyjściowe 230VAC</p> <ul style="list-style-type: none"> <li>• Zniekształcenia napięcia wyjściowego <math>\leq 2\%</math></li> <li>• Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 50/60Hz <math>\pm 3</math> Hz</li> <li>• Inne napięcia wyjściowe 220, 240</li> <li>• Współczynnik szczytu 3: 1</li> <li>• Typ przebiegu sinusoida</li> <li>• Złącza/gniazda wyjściowe (6) IEC 320 C13</li> <li>• Układ obejściowy (bypass) wewnętrzny tor obejściowy (automatyczny lub ręczny)</li> </ul>
<b>Akumulator i czas podtrzymania</b>	<ul style="list-style-type: none"> <li>• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu szczelny</li> <li>• Czas autonomii: 8 minut 27 sekund dla pełnego obciążenia 21 minut 8 sekund dla połowy obciążenia</li> <li>• Typowy czas ładowania 3 godziny</li> <li>• Oczekiwana żywotność akumulatora (lata) 3 – 5</li> <li>• Rozszerzalny czas podtrzymania za pomocą dodatkowych modułów</li> <li>• Baterie wymieniane na gorąco</li> <li>• Opcje przedłużonego podtrzymania zasilania: do 10 zewnętrznych modułów bateryjnych</li> </ul>
<b>Komunikacja i zarządzanie</b>	<ul style="list-style-type: none"> <li>• Gniazdo do montażu karty WEB/SNMP - Smart Slot x1</li> <li>• W zestawie przewodowy czujnik temperatury</li> <li>• Porty komunikacyjne: RJ-45, Smart-Slot, USB</li> </ul>



	<ul style="list-style-type: none"> <li>• Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD</li> <li>• Alarm dźwiękowy: Alarmy dźwiękowe i wizualne według priorytetu ważności zdarzenia</li> <li>• Awaryjny wyłącznik zasilania (EPO) <span style="float: right;">Tak</span></li> </ul>
<b>Gwarancja fabryczna Producenta</b>	min. 36 miesięcy gwarancji naprawy lub wymiany (bez akumulatora) i 24 miesiące na akumulator

## 2.7. PRZEŁĄCZNIK SIECIOWY

Komponent	Minimalne wymagania dla sprzętu
<b>Parametry fizyczne platformy</b>	Nazwę producenta wraz z zaproponowanym modelem należy podać w formularzu cenowym przy pozycji 2.7 Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V.
<b>Interfejsy sieciowe wymagania minimalne</b>	- Wymaganiem jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: 48 porty GE RJ-45 i 4 porty 10 GE SFP+.
<b>Zarządzanie</b>	<ol style="list-style-type: none"> <li>1. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</li> <li>2. Wsparcie dla SNMP w wersjach 1-3</li> <li>3. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</li> <li>4. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</li> <li>5. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.</li> <li>6. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</li> <li>7. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</li> <li>8. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</li> <li>9. Automatycznie wykonywane rewizje konfiguracji.</li> </ol>
<b>Parametry wydajnościowe</b>	<ol style="list-style-type: none"> <li>1. Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps.</li> <li>2. Tablica adresów MAC o pojemności co najmniej 32k wpisów.</li> </ol>

	<ol style="list-style-type: none"><li>Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.</li></ol>
<b>Wymagane funkcje</b>	<ol style="list-style-type: none"><li>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.</li><li>Obsługa Jumbo Frames.</li><li>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).</li><li>Agregacja portów zgodna ze standardem 802.3ad.</li><li>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.</li><li>Port-mirroring.</li><li>Uwierzytelnianie 802.1x na poziomie portu.</li><li>Uwierzytelnianie 802.1x w oparciu o adres MAC.</li><li>W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).</li><li>W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.</li><li>W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.</li></ol>
<b>Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC</b>	<ol style="list-style-type: none"><li>Przełącznik musi wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:<ol style="list-style-type: none"><li>centralne zarządzanie konfiguracją urządzenia</li><li>aktualizacja oprogramowania realizowana z systemu centralnego zarządzania</li><li>centralne zarządzanie sieciami vlan.</li><li>blokowanie ruchu pomiędzy klientami w ramach jednego vlan'u</li><li>rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.</li><li>przenoszenie zidentyfikowanych urządzeń do właściwych stref. w przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.</li><li>integrację z systemem kontroli dostępu. urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.</li></ol></li></ol>

	<ul style="list-style-type: none"> <li>h. automatyczna detekcja i rekomendacje konfiguracji.</li> <li>i. przesyłanie logów na zewnętrzny serwer syslog.</li> <li>j. funkcja uruchomienia captive portalu w celu identyfikacji użytkowników.</li> <li>k. obsługa białych i czarnych list adresów mac.</li> <li>l. wykrywanie aplikacji komunikujących się w sieci.</li> </ul> <p>2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.</p>
<b>Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa</b>	<ul style="list-style-type: none"> <li>1. Przełącznik musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.</li> <li>2. Przełącznik musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.</li> </ul>
<b>Okablowanie</b>	<p>Dla każdego przełącznika należy dostarczyć:</p> <ul style="list-style-type: none"> <li>15 x patchcord kat. 5e RJ45 0.25m – zielony</li> <li>15 x patchcord kat. 5e RJ45 0.5m – zielony</li> <li>4 x patchcord światłowodowy LC-UPC/ LC-UPC – 2m</li> <li>4 x patchcord kat. 5e RJ45 2m – czerwony</li> <li>4 x wkładka kompatybilna SR 10Gbit</li> </ul>
<b>Gwarancja oraz wsparcie</b>	<p>Przełącznik musi być objęty serwisem gwarancyjnym producenta polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości, przez okres zgodny ze złożoną ofertą, lecz nie krótszy niż 36 miesięcy. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania.</p>

### 3. WYMAGANIA ODNOŚNIE WDROŻENIA SPRZĘTU

#### 3.1. WARUNKI WSTĘPNE

1. Wykonawca przygotowuje i omówi koncepcję instalacji i konfiguracji z administratorem sieci Zamawiającego.
2. Wykonawca będzie uzgadniał z Zamawiającym harmonogramy dostawy i montażu.
3. Wykonawca zamontuje urządzenia będące przedmiotem dostawy w każdej z lokalizacji Zamawiającego uwzględniając wszelkie aspekty związane z montażem tego typu urządzeń przewidzianych przez producenta dostarczanych rozwiązań.
4. Prace, które będą powodować przerwy w segmentach sieci w dostępności do usług dla pracowników urzędu winny być wykonywane poza godzinami pracy urzędu. Możliwe jest również wykonywanie prac w dni wolne od pracy w urzędzie po wcześniejszym uzgodnieniu z Zamawiającym.
5. Na zakończenie prac Wykonawca przekaze Zamawiającemu dokumentację uwzględniającą co najmniej:

- a. Schemat topologii sieci
- b. Schemat ideowy każdej z ośmiu szaf dystrybucyjnych oraz czterech szaf w serwerowni głównej uwzględniający zamontowany sprzęt
- c. Adresację wdrożonych urządzeń uwzględniającą IP / VLAN ID
- d. Schemat połączeń sieciowych
- e. Karty katalogowe urządzeń.

### **3.2. WDROŻENIE SPRZĘTU W SIEDZIBIE ZDW BYDGOSZCZ**

#### **3.2.1.WDROŻENIE SERWERA – TYP II**

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego lokalizacji.
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych.
3. Upgrade oprogramowania układowego.
4. Konfiguracja klastra pracy awaryjnej poprzez dodanie dostarczonego serwera jako kolejny węzeł w klastrze.
5. Weryfikacja poprawności działania klastra.

#### **3.2.2.WDROŻENIE URZĄDZENIA ARCHIWIZACJI DANYCH – TYP II**

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego lokalizacji.
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych
3. Upgrade oprogramowania układowego.
4. Konfiguracja przestrzeni dyskowej, migawek
5. Konfiguracja polityk backupu dla danych klastra pracy awaryjnej.
6. Wykonanie backupu testowego.
7. Weryfikacja poprawności działania polityk backupu.

#### **3.2.3.LOKALIZACJA WDROŻENIA**

1. Zarząd Dróg Wojewódzkich w Bydgoszczy, ul. Dworcowa 80, 85-010 Bydgoszcz,

### **3.3. WDROŻENIE SPRZĘTU W TRZECH JEDNOSTKACH RDW**

#### **3.3.1.WDROŻENIE URZĄDZENIA UTM**

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego lokalizacji.
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych.
3. Upgrade oprogramowania układowego.
4. Konfiguracja adresacji dla sieci WAN i LAN.
5. Konfiguracja VLAN (maksymalnie 4 podsieci).
6. Konfiguracja polityk ochronnych UTP.
7. Konfiguracja VPN IP SEC – połączenie z ZDW Bydgoszcz.

### 3.3.2. WDROŻENIE SERWERA – TYP I

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego lokalizacji.
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych.
3. Upgrade oprogramowania układowego.
4. Konfiguracja przestrzeni dyskowej.
5. Uruchomienie co najmniej dwóch maszyn wirtualnych: AD oraz FS.
6. Konfiguracja środowiska ActiveDirectory – serwer będzie pełnił rolę kontrolera domeny w trybie ReadOnly dla głównego kontrolera ZDW Bydgoszcz.
7. Konfiguracja zasobów FS dla użytkowników lokalnych.
8. Testowa konfiguracja komputera lokalnego do pracy z AD, weryfikacja uprawnień i dostępów do FS.

### 3.3.3. WDROŻENIE URZĄDZENIA ARCHIWIZACJI DANYCH – TYP I

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego lokalizacji.
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych.
3. Upgrade oprogramowania układowego.
4. Konfiguracja przestrzeni dyskowej, migawek.
5. Konfiguracja polityk backupu dla danych serwera – typ I.
6. Wykonanie backupu testowego.
7. Weryfikacja poprawności działania polityk backupu.

### 3.3.4. WDROŻENIE ZASILACZA AWARYJNEGO

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego lokalizacji.

2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych.
3. Upgrade oprogramowania układowego.
4. Konfiguracja oprogramowania do zarządzania zasilaczem, w tym powiadomień.
5. Konfiguracja poszczególnych portów zasilania z opisem urządzeń, które zasilają.

### 3.3.5. WDROŻENIE PRZEŁĄCZNIKA SIECIOWEGO

Wdrożenie obejmuje wykonanie między innymi czynności:

1. Rozpakowanie i montaż urządzenia we wskazanej przez Zamawiającego lokalizacji.
2. Uruchomienie i konfiguracja urządzenia z zaadresowaniem interfejsów sieciowych.
3. Upgrade oprogramowania układowego.
4. Przeniesienie konfiguracji z aktualnie używanych przełączników.
5. Podłączenie wskazanych portów patchpaneli do switcha i konfiguracja VLAN'ów
6. Podłączenie urządzenia do centralnej konsoli zarządzania urządzeniami sieciowymi w urządzeniu UTM.

### 3.3.6. LOKALIZACJE WDROŻENIA

1. Rejon Dróg Wojewódzkich w Wąbrzeźnie, ul. 1 Maja 61, 87-200 Wąbrzeźno
2. Rejon Dróg Wojewódzkich we Włocławku, ul. Chopina 1, 87-800 Włocławek
3. Rejon Dróg Wojewódzkich w Żołędowie, ul. Pałacowa 15, 86-031 Osielsko

## Warunki równoważności dla Windows Server 2022 Standard

Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta.

SSO musi posiadać następujące, wbudowane cechy:

- a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,
- b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,
- c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,
- d) 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,

- e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
- f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
- g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,
- h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),
- i) wbudowane wsparcie instalacji i pracy na wolumenach, które:
- pozwalają na zmianę rozmiaru w czasie pracy systemu,
  - umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
  - umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
  - umożliwiają zdefiniowanie list kontroli dostępu (ACL),
- j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
- k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2
- l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
- m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
- n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,
- o) graficzny interfejs użytkownika,
- p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
- q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
- s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
- t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
- u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
- podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
  - usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
    - podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

- ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
  - odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
- zdalna dystrybucja oprogramowania na stacje robocze,
- praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
- centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
  - dystrybucję certyfikatów poprzez http,
  - konsolidację CA dla wielu lasów domeny,
  - automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,
- szyfrowanie plików i folderów,
- szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
- możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,
- serwis udostępniania stron WWW,
- wsparcie dla protokołu IP w wersji 6 (IPv6),
- wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
  - dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
  - obsługi ramek typu jumbo frames dla maszyn wirtualnych,
  - obsługi 4-KB sektorów dysków,
  - nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
  - możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
  - możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),
- v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,
- w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),
- x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,
- y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,
- z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.