**Załącznik nr 3 do SWZ. Szczegółowy opis przedmiotu zamówienia**

Dotyczy zamówienia publicznego pn. Dostawa sprzętu komputerowego z oprogramowaniem z usługami wdrożeniowymi i szkoleniowymi dla Gminy Ropczyce w ramach projektu „Cyfrowa Gmina” Nr postępowania PPZP.271.14.2022

# Część 1. Dostawa stacji roboczych, laptopów i oprogramowania

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Sprzęt i oprogramowanie musi pochodzić z oficjalnego kanału sprzedaży producenta na teren UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
7. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

|  |  |
| --- | --- |
| Przedmiot dostawy | Ilość |
| Stacje robocze (komputery stacjonarne z systemem operacyjnym) | 35 |
| Laptopy z systemem operacyjnym | 3 |
| Pakiety oprogramowania biurowego | 3 |

Kody CPV:

* + - * 30213000-5 Komputery osobiste
      * 30213100-6 Komputery przenośne
      * 48000000-8 Pakiety oprogramowania i systemy informatyczne
      * 48422000-2 Zestawy pakietów oprogramowania
      * 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
      * 48900000-7 Różne pakiety oprogramowania i systemy komputerowe

## Stacje robocze (komputery stacjonarne z systemem operacyjnym)

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Komputer stacjonarny odpowiedni dla użytkowania aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. | TAK / NIE |
| Wydajność | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach stacjonarnych, uzyskujący wynik co najmniej 8 500 punktów w teście PassMark - CPU Mark według wyników opublikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. | TAK / NIE  Procesor: …………………………………………………………….  (należy wpisać model procesora) |
| Pamięć RAM | Zainstalowane co najmniej 16 GB, możliwość rozbudowy do co najmniej 64 GB, co najmniej jeden wolny slot na moduły pamięci. | TAK / NIE |
| Pamięć masowa | Co najmniej 512 GB NVMe SSD M.2.  Obudowa musi umożliwiać montaż dodatkowego dysku 2.5” lub 3.5”. | TAK / NIE |
| Karta graficzna | Zintegrowana lub dedykowana karta graficzna. | TAK / NIE |
| Wyposażenie multimedialne | Karta dźwiękowa co najmniej dwukanałowa zintegrowana z płytą główną. Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie typu combo (wspólny port słuchawkowo – mikrofonowy), na tylnym panelu co najmniej port audio line-out. | TAK / NIE |
| Obudowa | Typu small form factor (suma wymiarów obudowy nieprzekraczająca 700 mm).  Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Otwory wentylacyjne usytuowane wyłącznie na przednim oraz tylnym panelu obudowy.  Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń bez konieczności użycia narzędzi. Obudowa w jednostce centralnej musi być otwierana bez konieczności użycia narzędzi (wyklucza się użycie standardowych wkrętów, śrub motylkowych) oraz powinna posiadać czujnik otwarcia obudowy współpracujący z oprogramowaniem zarządzająco – diagnostycznym.  Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej oraz kłódki (oczko w obudowie do założenia kłódki).  Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie i wpisanym na stałe w BIOS. | TAK / NIE |
| Zasilacz | Zasilacz o mocy nieprzekraczającej 250W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności co najmniej 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności co najmniej 80% przy obciążeniu zasilacza na poziomie 100%. | TAK / NIE |
| Bezpieczeństwo | Układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu musi prowadzić do uszkodzenia całej płyty głównej. | TAK / NIE |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego w oferowanym urządzeniu. | TAK / NIE |
| Diagnostyka | System diagnostyczny z interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. | TAK / NIE |
| Wirtualizacja | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty główej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji dla poszczególnych komponentów systemu). | TAK / NIE |
| System operacyjny | Zainstalowany system operacyjny w wersji odpowiedniej dla administracji samorządowej spełniający następujące wymagania (poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):  Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;  Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;  Internetowa aktualizacja zapewniona w języku polskim;  Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi);  Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;  Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;  Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;  Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;  Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;  Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;  Wbudowany system pomocy w języku polskim;  Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;  Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową);  Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  Graficzne środowisko instalacji i konfiguracji;  Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;  Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;  Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  Możliwość przywracania plików systemowych;  System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);  Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);  Klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  Do oferty należy załączyć potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). | TAK / NIE  System operacyjny: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję systemu) |
| Wymagania dodatkowe | Wbudowane porty – co najmniej:  2 szt. DisplayPort lub 2 szt. HDMI lub 1 szt. DisplayPort i 1 szt. HDMI (wymagane dostarczenie kabla umożliwiającego podłączenie monitora ze złączem DVI).  Co najmniej 6 portów USB, w tym co najmniej 4 porty USB 3.x typu A.  Co najmniej 2 porty USB spośród ww. muszą być umieszczone na przednim panelu obudowy.  Port audio typu combo (słuchawki/mikrofon) na przednim panelu obudowy.  Port audio-out na tylnym panelu obudowy.  Port RJ – 45.  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich ww. portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej.  Karta sieciowa 10/100/1000 zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika).  Klawiatura USB w układzie polski programisty.  Mysz USB z rolką (scroll).  Nagrywarka DVD +/-RW o prędkości co najmniej 8x.  Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu. | TAK / NIE |
| Ergonomia | Głośność komputera mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji obserwatora w trybie pracy dysku twardego nie może przekraczać 28 dB. Do oferty należy załączyć dokument potwierdzający spełnienie wymagania sporządzony przez laboratorium akredytowane przez Polskie Centrum Akredytacji lub jako dokument równoważny oświadczenie producenta zestawu komputerowego dotyczące głośności tej jednostki. | TAK / NIE |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta, obejmująca wszystkie komponenty komputera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). | TAK / NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego komputera:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Laptopy z systemem operacyjnym

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Komputer mobilny odpowiedni dla użytkowania aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej. | TAK / NIE |
| Ekran | Przekątna 15,6”, rozdzielczość co najmniej full HD (1920 x 1080), powłoka przeciwodblaskowa, jasność co najmniej 250 nitów, kontrast co najmniej 700:1. | TAK / NIE |
| Wydajność | Procesor wielordzeniowy, zaprojektowany do pracy w komputerach przenośnych, uzyskujący wynik co najmniej 6 000 punktów w teście PassMark - CPU Mark według wyników procesorów publikowanych na stronie <http://www.cpubenchmark.net/cpu_list.php> w okresie nie wcześniej niż 14 dni przed terminem składania ofert.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. | TAK / NIE  Procesor: …………………………………………………………….  (należy wpisać model procesora) |
| Pamięć RAM | Zainstalowane co najmniej 16 GB, możliwość rozbudowy do co najmniej 32 GB, co najmniej jeden wolny slot na moduły pamięci. | TAK / NIE |
| Pamięć masowa | Co najmniej 512GB NVMe SSD M.2. | TAK / NIE |
| Karta graficzna | Karta graficzna zintegrowana lub dedykowana. | TAK / NIE |
| Karta sieciowa | Zintegrowana, 10/100/1000 (RJ-45) dostępna bezpośrednio z obudowy bez konieczności używania dodatkowych adapterów. | TAK / NIE |
| Multimedia | Karta dźwiękowa zintegrowana z płytą główną, wbudowane dwa głośniki stereo.  Port audio typu combo (wspólne złącze obsługujące słuchawki i mikrofon).  Wbudowana kamera co najmniej 720p z mechaniczną przysłoną.  Czytnik kart czytający co najmniej karty micro SD. | TAK / NIE |
| Łączność bezprzewodowa | Wi-Fi generacji co najmniej 6  Bluetooth standardu co najmniej 5.1 | TAK / NIE |
| Bateria i zasilanie | Bateria co najmniej 45 Whr, umożliwiająca jej szybkie naładowanie do poziomu 80% w czasie 1 godziny i do poziomu 100% w czasie 2 godzin.  Zasilacz dedykowany przez producenta. | TAK / NIE |
| Waga | Nie więcej niż 2 kg z baterią. | TAK / NIE |
| Obudowa | Szkielet obudowy i zawiasy notebooka wzmacniane, dookoła matrycy uszczelnienie chroniące klawiaturę notebooka po zamknięciu przed kurzem i wilgocią. | TAK / NIE |
| BIOS | BIOS producenta oferowanego komputera zgodny ze specyfikacją UEFI, pełna obsługa za pomocą klawiatury i myszy lub urządzenia wskazującego zintegrowanego w oferowanym urządzeniu. | TAK / NIE |
| Diagnostyka | System diagnostyczny z interfejsem użytkownika dostępny z poziomu BIOS lub z poziomu menu boot, umożliwiający przetestowanie komponentów komputera. | TAK / NIE |
| Bezpieczeństwo | Zintegrowany z płytą główną dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Próba usunięcia układu musi powodować uszkodzenie płyty głównej. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Weryfikacja wygenerowanych przez komputer kluczy szyfrowania musi odbywać się w dedykowanym chipsecie na płycie głównej.  Czytnik linii papilarnych. | TAK / NIE |
| System operacyjny | Zainstalowany system operacyjny w wersji odpowiedniej dla administracji samorządowej spełniający następujące wymagania (poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji):  Bezpłatne aktualizacje w ramach wersji systemu operacyjnego przez Internet z możliwością wyboru instalowanych poprawek (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW;  Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu;  Internetowa aktualizacja zapewniona w języku polskim;  Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;  Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe;  Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi);  Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer;  Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta;  Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu;  Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników;  Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych;  Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych;  Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika;  Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi;  Wbudowany system pomocy w języku polskim;  Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);  Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji;  Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;  Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;  Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji;  Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;  Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach;  Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń;  Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji za logowanego użytkownika celem rozwiązania problemu z komputerem;  Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami (obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową);  Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację;  Graficzne środowisko instalacji i konfiguracji;  Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe;  Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe;  Oprogramowanie dla tworzenia kopii zapasowych (backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej;  Możliwość przywracania plików systemowych;  System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.);  Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu);  Klucz licencyjny zapisany trwale w BIOS, umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  Do oferty należy załączyć potwierdzenie kompatybilności komputera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). | TAK / NIE  System operacyjny: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję systemu) |
| Klawiatura | Klawiatura z wydzieloną częścią numeryczną, podświetlana.  Touchpad z dwoma przyciskami. | TAK / NIE |
| Porty i złącza | Wbudowane porty i złącza – co najmniej:  1 szt. HDMI,  1 szt. RJ-45,  3 szt. USB (w tym co najmniej 1 szt. USB 3.x i 1 szt. USB 3.x z zasilaniem),  1 szt. USB 3.x typu C z zasilaniem,  port zasilania (nie zajmujący portu USB typ C),  złącze linki zabezpieczającej. | TAK / NIE |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej pięcioletnia gwarancja producenta obejmująca wszystkie komponenty komputera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja komputera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). | TAK / NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Pakiety oprogramowania biurowego

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, nazwa oprogramowania: ………………………………………………………………… |
| Zawartość pakietu | Pakiet musi zawierać:   * edytor tekstów, * arkusz kalkulacyjny, * narzędzie do przygotowania i prowadzenia prezentacji, * narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami). | TAK / NIE |
| Wymagania ogólne dla pakietu | Wymagana pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim. Pakiet powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim.  Dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8 do 17 – cena połączenia nie większa niż cena połączenia lokalnego.  Wymagany publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu.  Możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).  Wymagane dostarczenie licencji bezterminowej, odpowiedniej dla jednostek samorządu terytorialnego. |  |
| Edytor teksu | Edytor tekstu musi umożliwiać:   * Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty. * Wstawianie oraz formatowanie tabel. * Wstawianie oraz formatowanie obiektów graficznych. * Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne). * Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków. * Automatyczne tworzenie spisów treści. * Formatowanie nagłówków i stopek stron. * Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie. * Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. * Określenie układu strony (pionowa/pozioma). * Wydruk dokumentów. * Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną. * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. * Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa. | TAK / NIE |
| Arkusz kalkulacyjny | Arkusz kalkulacyjny musi umożliwiać:   * Tworzenie raportów tabelarycznych. * Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych. * Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu. * Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice). * Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. * Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych. * Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych. * Wyszukiwanie i zamianę danych. * Wykonywanie analiz danych przy użyciu formatowania warunkowego. * Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie. * Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności. * Formatowanie czasu, daty i wartości finansowych z polskim formatem. * Zapis wielu arkuszy kalkulacyjnych w jednym pliku. * Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji. | TAK / NIE |
| Narzędzie do przygotowywania i prowadzenia prezentacji | Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:   * Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego. * Drukowanie w formacie umożliwiającym robienie notatek. * Zapisanie jako prezentacja tylko do odczytu. * Nagrywanie narracji i dołączanie jej do prezentacji. * Opatrywanie slajdów notatkami dla prezentera. * Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo. * Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego. * Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym. * Możliwość tworzenia animacji obiektów i całych slajdów. * Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera. | TAK / NIE |
| Narzędzie do zarządzania informacją prywatną | Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:   * Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego. * Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych. * Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców. * Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną. * Automatyczne grupowanie poczty o tym samym tytule. * Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy. * Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów. * Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie. * Zarządzanie kalendarzem. * Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników. * Przeglądanie kalendarza innych użytkowników. * Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach. * Zarządzanie listą zadań. * Zlecanie zadań innym użytkownikom. * Zarządzanie listą kontaktów. * Udostępnianie listy kontaktów innym użytkownikom. * Przeglądanie listy kontaktów innych użytkowników. * Możliwość przesyłania kontaktów innym użytkowników. | TAK / NIE |

# Część 2. Dostawa sprzętu serwerowego i sieciowego z oprogramowaniem i usługami wdrożeniowymi i szkoleniowymi

Ogólne warunki realizacji zamówienia

1. Przedmiot zamówienia obejmuje dostarczenie do siedziby Zamawiającego nw. elementów w ilościach wskazanych w zestawieniu rzeczowo - ilościowym poniżej.
2. Dostarczany sprzęt i oprogramowanie muszą być fabrycznie nowe, nieużywane, nieuszkodzone i nieobciążone prawami osób trzecich.
3. Sprzęt i oprogramowanie musi pochodzić z oficjalnego kanału sprzedaży producenta na teren UE.
4. Wykonawca zapewni takie opakowanie sprzętu jakie jest wymagane, żeby nie dopuścić do jego uszkodzenia lub pogorszenia jego jakości w trakcie transportu do miejsca dostawy.
5. Sprzęt będzie oznaczony zgodnie z obowiązującymi przepisami, a w szczególności znakami bezpieczeństwa.
6. Wykonawca wyda Zamawiającemu instrukcje obsługi sprzętu lub – jeśli są one udostępniane przez producenta w formie elektronicznej – przekaże adresy WWW, pod którymi można je pobrać.
7. Dla oprogramowania Wykonawca zobowiązany jest do udzielenia niewyłącznej licencji Zamawiającemu lub przeniesienia na Zamawiającego niewyłącznego uprawnienia licencyjnego zgodnego z zasadami licencjonowania określonymi przez producenta.

Zestawienie rzeczowo - ilościowe

|  |  |
| --- | --- |
| Przedmiot dostawy | Ilość |
| Przełączniki sieciowe typ A | 2 |
| Przełączniki sieciowe typ B | 4 |
| Access-pointy | 4 |
| Serwer typ A | 1 |
| Serwer typ B | 1 |
| Serwerowy zasilacz awaryjny | 1 |
| Szafa rack | 1 |
| Macierz dyskowa | 1 |
| Serwer typ C (backup) | 1 |
| Streamer | 1 |
| Oprogramowanie do tworzenia kopii zapasowych | 1 |
| Klaster urządzeń UTM | 1 |
| Usługi wdrożenia sprzętu oraz oprogramowania | 1 |
| Szkolenie dla administratora w zakresie obsługi zakupionego sprzętu | 1 |

Kody CPV:

* + - * 48820000-2 Serwery
      * 30233000-1 Urządzenia do przechowywania i odczytu danych
      * 31213300-5 Szafy kablowe
      * 32420000-3 Urządzenia sieciowe
      * 31682530-4 Awaryjne urządzenia energetyczne
      * 48000000-8 Pakiety oprogramowania i systemy informatyczne
      * 48422000-2 Zestawy pakietów oprogramowania
      * 48600000-4 Pakiety oprogramowania dla baz danych i operacyjne
      * 48900000-7 Różne pakiety oprogramowania i systemy komputerowe
      * 72263000-6 Usługi wdrażania oprogramowania
      * 80510000-2 Usługi szkolenia specjalistycznego

## Przełączniki sieciowe typ A

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Obudowa do montażu w szafie RACK 19” – 1U wraz z zestawem montażowym. | TAK/NIE |
| Porty | Co najmniej:  24 x 10 Gigabit Ethernet SFP+,  2 x 40 Gigabit Ethernet QSFP+, Porty QSFP+ powinny mieć możliwość rozszycia w celu konfiguracji 4x10GbE  1 x RJ45 console/management port (RS232),  1 x RJ45 management port,  1 x USB 2.0 type A,  Przełącznik musi umożliwiać zestawienie stosu portami/magistralami minimum Full Duplex 40GbE (do min 2 urządzeń). | TAK/NIE |
| Wydajność | Przepustowość przełącznika minimum 620Gb/s.  Wydajność przełączania minimum 460Mpps.  Obsługa minimum 32,000 adresów MAC.  Bufor pakietów minimum 1,5MB.  Taktowanie procesora: 1GHz.  Pamięć RAM 512MB. | TAK/NIE |
| Zasilanie | Zasilanie 230V AC | TAK/NIE |
| Funkcje i protokoły | Musi obsługiwać następujące protokoły drzewa rozpinającego:  • 802.1D – STP  • 802.1w – RSTP  • 802.1s – MSTP  Musi obsługiwać jeden z protokołów do tworzenia wirtualnych nadmiarowych bram sieciowych np. (VRRP lub HSRP).  Obsługa multicastów z wykorzystaniem protokołów:  • IGMP,  • IGMP Snooping,  • Multicast VLAN.  Możliwość monitorowania ruchu na porcie (Port Mirroring).  Możliwość agregacji połączeń z wykorzystaniem protokołu LACP – IEEE 802.3ad.  Musi obsługiwać następujące protokoły odnajdywania urządzeń w sieci:  • LLDP,  • LLDP-MED.  Musi obsługiwać następujące protokoły autoryzacji:  • TACACS+,  • RADIUS.  Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.  Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC. | TAK/NIE |
| Zarządzanie | Tekstowy interfejs zarządzania z podpowiedziami kontekstowymi.  Tekstowy plik konfiguracyjny możliwy do wyeksportowania, edytowania poza urządzeniem i ponownego zaimportowania do urządzenia.  Możliwość zarządzania urządzeniem z wykorzystaniem protokołów SSHv2 oraz TELNET.  Możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI),  Bezpośredni dostęp do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji.  Wysyłanie powiadomień o zdarzeniach z użyciem protokołów SNMPv1, SNMPv2c oraz SNMPv3,  Przesyłanie dzienników zdarzeń z wykorzystaniem protokołu SYSLOG.  Obsługujący synchronizację czasu systemowego z użyciem protokołów SNTP lub NTP.  Możliwość konfiguracji pracy w trybie klienta DNS. | TAK/NIE |
| Gwarancja | Gwarancja producenta co najmniej 3 lata. | TAK/NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Przełączniki sieciowe typ B

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Obudowa do montażu w szafie RACK 19” – 1U wraz z zestawem montażowym. | TAK/NIE |
| Porty | Co najmniej:  48 x 1 Gigabit Ethernet 1000BASE-T (RJ45), PoE+  4 x 10 Gigabit Ethernet SFP+,  1 x RJ45 console/management port (RS232),  1 x RJ45 management port,  1 x USB 2.0 type A,  Przełącznik musi umożliwiać zestawienie stosu portami/magistralami minimum, 10GbE Full Duplex 10GbE (do min 2 urządzeń). | TAK/NIE |
| Wydajność | Przepustowość przełącznika minimum 170Gb/s.  Wydajność przełączania minimum 130Mpps.  Obsługa minimum 16,000 adresów MAC.  Bufor pakietów minimum 1,5MB | TAK/NIE |
| Zasilanie | Zasilanie 230V AC | TAK/NIE |
| Funkcje i protokoły | Musi obsługiwać następujące protokoły drzewa rozpinającego:  • 802.1D – STP  • 802.1w – RSTP  • 802.1s – MSTP  Musi obsługiwać jeden z protokołów do tworzenia wirtualnych nadmiarowych bram sieciowych np. (VRRP lub HSRP).  Obsługa multicastów z wykorzystaniem protokołów:  • IGMP,  • IGMP Snooping.  Możliwość monitorowania ruchu na porcie (Port Mirroring).  Możliwość agregacji połączeń z wykorzystaniem protokołu LACP – IEEE 802.3ad.  Musi obsługiwać następujące protokoły odnajdywania urządzeń w sieci:  • LLDP,  • LLDP-MED.  Musi obsługiwać następujące protokoły autoryzacji:  • TACACS+,  • RADIUS,  Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.  Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC. | TAK/NIE |
| Zarządzanie | Tekstowy interfejs zarządzania z podpowiedziami kontekstowymi.  Tekstowy plik konfiguracyjny możliwy do wyeksportowania, edytowania poza urządzeniem i ponownego zaimportowania do urządzenia.  Możliwość zarządzania urządzeniem z wykorzystaniem protokołów SSHv2 oraz TELNET.  Możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI).  Bezpośredni dostęp do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji.  Wysyłanie powiadomień o zdarzeniach z użyciem protokołów SNMPv1, SNMPv2c oraz SNMPv3.  Przesyłanie dzienników zdarzeń z wykorzystaniem protokołu SYSLOG.  Obsługujący synchronizację czasu systemowego z użyciem protokołów SNTP lub NTP.  Możliwość konfiguracji pracy w trybie klienta DNS. | TAK/NIE |
| Gwarancja | Gwarancja producenta co najmniej 3 lata. | TAK/NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Access-pointy

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Obudowa przeznaczona do montażu na ścianie, suficie podwieszanym lub suficie trwałym.  Stopień ochrony urządzenia: IP41. | TAK/NIE |
| Porty | Co najmniej:  2 porty 10/100/1000Base-T,  1 port szeregowy konsoli (interfejs RJ-45),  1 port USB 2.0. | TAK/NIE |
| Anteny | Wbudowane anteny 2.4 GHz zysk minimum 4dBi,  wbudowane anteny 5GHz zysk minimum 5dBi,  moc nadawcza (moc wyjściowa na złączu antenowym): dla 2,4GHz minimum 23dBm, dla 5GHz minimum 23dBm,  regulacja mocy: z krokiem maksimum 1dBm,  ilość obsługiwanych strumieni przestrzennych: 2,  obsługa wirtualnych punktów dostępowych (BSSID): minimum 32 jednocześnie. | TAK/NIE |
| Tryby i częstotliwości pracy radia | IEEE 802.11a/n/ac : 5.150 GHz - 5.850 GHz  IEEE 802.11b/g/n/ax: 2.4 GHz - 2.483 GHz  IEEE 802.11ax: 5.150 GHz – 5.250 GHz 5.250 GHz - 5.350 GHz 5.725 GHz – 5.850 GHz | TAK/NIE |
| Technologie modulacji | IEEE 802.11b: BPSK,QPSK,CCK  IEEE 802.11a/g/n: BPSK, QPSK,16-QAM, 64-QAM  IEEE 802.11ac: BPSK, QPSK,16-QAM, 64-QAM, 256-QAM  IEEE 802.11ax: BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM | TAK/NIE |
| Wydajność | Sumaryczna prędkość przesyłania danych nie mniejsza niż 1,7 Gb/s  równoczesna praca na częstotliwościach 2.4 GHz oraz 5 GHz,  komunikacja bezprzewodowa 2x2:2 MIMO. | TAK/NIE |
| Integracja | Wymagana integracja z oferowanym urządzeniem UTM, które będzie pełnić rolę kontrolera sieci WiFi lub z dedykowanym kontrolerem WiFi (zależnie od rozwiązania przyjętego przez Wykonawcę). | TAK/NIE |
| Zasilanie | Power over Ethernet IEEE 802.3af/at oraz zewnętrzny zasilacz 230 V. | TAK/NIE |
| Funkcje i protokoły | * DCA (dynamiczne dostosowanie kanałów), * TPC (kontrola mocy nadawania), * wykrywanie martwych obszarów, * ukrywanie SSID, * RTS/CTS, * skanowanie środowiska radiowego, * limitowanie liczby użytkowników, * eliminacja terminali ze zbyt słabym sygnałem, * wymuszanie roamingu terminali o słabym sygnale, * inteligentna kontrola terminali w oparciu o równomierne rozłożenie czasu transmisji, * statyczny adres IP, * klient DHCP, * obsługa pakietów IPv6, * IGMP Snooping, * roaming pomiędzy AP, * roaming pomiędzy AC, * WDS, * kontrola dostępu do punktów dostępowych. | TAK/NIE |
| Funkcje bezpieczeństwa | * Szyfrowanie 64/128 WEP, TKIP, CCMP; * IEEE 802.11i; * WAPI, autentykacja po adresie MAC; * autentykacja LDAP; * autentykacja PEAP; * WIDS/WIPS; * ochrona widma w czasie rzeczywistym; * zabezpieczenie przed atakami typu DoS; * bezpieczeństwo przekierowywania: filtrowanie ramek, biała lista, statyczna czarna lista i dynamiczna czarna lista; * izolowanie stacji bezprzedowodych, SAVI, Izolacja użytkownika; * obsługa list kontroli dostępu; * kontrola dostępu do wolnych zasobów; * kontrola dostępu terminali bezprzewodowych; * Lista ACL; * bezprzerwowa praca urządzenia w przypadku utraty połączenia z kontrolerem; * możliwość automatycznego wyłączania usług w przypadku przekroczenia zakładanego czasu dostępności usługi. | TAK/NIE |
| Obsługa QoS | * IEEE 802.11e (WMM), * mapowanie różnych sieci VLAN oraz SSID do różnych polityk QoS, * mapowanie różnych strumieni danych (na podstawie różnych pól pakietów) do rożnych polityk QoS, * load balancing w oparciu o liczbę użytkowników/ilość ruchu/zakres częstotliwości, * limit przepustowości możliwy do zdefiniowania dla AP/SSID/terminali/strumieni danych, * tryb oszczędzania energii, * automatyczne odzyskiwanie komunikacji z AC, * inteligentne identyfikowanie terminali, * urządzenie musi umożliwiać początkową inicjalizację na paśmie 5GHz dla urządzeń odbiorczych pracujących w paśmie 2,4GHz oraz 5GHz. | TAK/NIE |
| Zarządzanie | * zarządzanie centralne poprzez kontroler sieci bezprzewodowej (AC), * lokalny log, * obsługa syslog, * funkcja AP Escape (w przypadku braku komunikacji z kontrolerem sieci WiFi, AP pracują jako niezależne urządzenia wciąż obsługując obecnych i nowych użytkowników), * sprzętowy watchdog. | TAK/NIE |
| Gwarancja | Gwarancja producenta co najmniej 3 lata. | TAK/NIE |

## Serwer typ A

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Typu rack o wysokości maksymalnie 1U w konfiguracji bezdyskowej, z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli . | TAK/NIE |
| Płyta główna | Płyta główna pozwalająca na zainstalowanie minimum dwóch procesorów, zaprojektowana przez producenta. Chipset dedykowany przez producenta procesora do pracy w systemach dwuprocesorowych. | TAK/NIE |
| Procesor | Zainstalowane dwa procesory minimum ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem uzyskujące w układzie dwuprocesorowym wynik co najmniej 145 punktów w teście SPECrate2017\_fp\_base dla oferowanego modelu serwera według wyników opublikowanych na stronie <http://spec.org>.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. | TAK/NIE  Procesor: …………………………………………………………….  (należy wpisać model procesora) |
| Pamięć RAM | Zainstalowane co najmniej 128 GB w modułach po co najmniej 16 GB każdy. Płyta główna w konfiguracji dwuprocesorowej musi obsługiwać do 4 TB pamięci RAM lub więcej.  Zabezpieczenia pamięci RAM - Memory Mirror. | TAK/NIE |
| Grafika | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1280x1024. | TAK/NIE |
| Sieć | Interfejsy sieciowe LAN:   * minimum 2 porty typu Ethernet 1Gbps RJ45 * minimum 2 porty typu Ethernet 10Gbps SFP+. | TAK/NIE |
| Przestrzeń dyskowa | Dedykowany fizyczny moduł pozwalający na konfigurację nadmiarowej przestrzeni dyskowej (min. RAID 1) zrealizowanej z wykorzystaniem min. dwóch nośników FLASH i/lub SSD o pojemności 240GB każdy, pozwalający na instalację i uruchamianie systemu operacyjnego serwera. | TAK/NIE |
| Porty | Wbudowane porty:   * minimum 2 porty USB 2.0 * minimum 1 port USB 3.0, * 1 port RJ45 dedykowany do zarządzania, * 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), * minimum 1 port RS232. | TAK/NIE |
| Diagnostyka, bezpieczeństwo | Znajdujący się na froncie obudowy panel LCD, umożliwiający wyświetlanie informacji o stanie: temperatury, pamięci RAM, dysków, slotów PCIe, wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą.  Zintegrowany z płytą główną moduł TPM 2.0.  Wsparcie dla trybu blokady, polegającego na zapobieganiu przed wprowadzaniem modyfikacji i aktualizacji ustawień konfiguracji oraz oprogramowania wewnętrznego serwera. | TAK/NIE |
| Wentylacja | Redundantne wentylatory. | TAK/NIE |
| Zasilanie | Dwa redundantne zasilacze Hot Plug o mocy co najmniej 800 Wat. | TAK/NIE |
| Zarządzanie | Karta zarządzania, niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność :   * + - komunikacja poprzez interfejs RJ45,   + - podstawowe zarzadzanie poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging,   + - wbudowana diagnostyka,   + - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń,   + - monitorowanie temperatury oraz zużycia energii w czasie rzeczywistym,   + - lokalna oraz zdalna konfiguracja serwera,   + - wsparcie dla IPv4 i IPv6,   + - możliwość zdalnego dostępu do konsoli graficznej, zainstalowanego systemu operacyjnego serwera. | TAK/NIE |
| Oprogramowanie – system wirtualizacji | Z serwerem należy dostarczyć pakiet oprogramowania przeznaczonego do wirtualizacji serwerów. Oprogramowanie do wirtualizacji serwerów będzie przeznaczone na cele utworzenia klastra wirtualizacyjnego składającego się z serwerów będących przedmiotem zamówienia.  Oprogramowanie musi posiadać następujące cechy i funkcjonalności:   1. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. 2. Musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 3. Powinien w możliwie największym stopniu być niezależny od producenta platformy sprzętowej. 4. Rozwiązanie musi wspierać oferowany z serwerem system operacyjny oraz następujące systemy operacyjne: Windows Server 2019, Windows Server 2022, Windows 10, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Solaris, Debian GNU/Linux, CentOS. 5. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. 6. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej. 7. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. 8. Powinien zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. 9. Musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. 10. System wirtualizacyjny oraz oprogramowanie zarządzające tymże systemem musi posiadać możliwość integracji z usługami katalogowymi – co najmniej Active Directory. 11. Rozwiązanie musi mieć możliwość przenoszenia uruchomionych maszyn wirtualnych pomiędzy serwerami fizycznymi (tzw. „migracja na gorąco”). Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. 12. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych pomiędzy fizycznymi zasobami dyskowymi. Mechanizm powinien umożliwiać realizację co najmniej 2 takich procesów przenoszenia jednocześnie. 13. Musi umożliwiać zapewnienie odpowiedniej redundancji i takiego mechanizmu (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego działające na nim wirtualne maszyny zostały automatycznie uruchomione na innych fizycznych serwerach klastra z zainstalowanym oferowanym oprogramowaniem wirtualizacyjnym. 14. Musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. 15. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. 16. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).   Wymagane dostarczenie licencji bez ograniczeń czasowych.  Wymagane zapewnienie wsparcia technicznego dla oprogramowania do wirtualizacji przez co najmniej 1 rok. Wsparcie techniczne musi umożliwiać zgłaszanie problemów w trybie 5dni/8h. Możliwość pobierania nowych wersji i poprawek w okresie wsparcia. | TAK / NIE  Oprogramowanie – system wirtualizacji: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję systemu) |
| System operacyjny | Z serwerem należy dostarczyć licencje na system operacyjny posiadający następujące cechy, funkcje i minimalne parametry:   * 1. Współpraca z procesorami o architekturze x86-64.   2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.   3. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu.   4. Zawarta możliwość uruchomienia roli kontrolera domeny Active Directory.   5. Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.   6. 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.   7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.   8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.   9. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.   10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.   11. Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.   12. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).   13. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.   14. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).   15. 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. * Zdalna dystrybucja oprogramowania na stacje robocze. * Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. * PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:   + Dystrybucję certyfikatów poprzez http,   + Konsolidację CA dla wielu lasów domeny,   + Automatyczne rejestrowania certyfikatów pomiędzy rożnymi lasami domen. * Szyfrowanie plików i folderów. * Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). * Serwis udostępniania stron WWW. * Wsparcie dla protokołu IP w wersji 6 (IPv6). * Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.   1. 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.   2. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).   3. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.   4. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.   Licencje na system operacyjny:   1. muszą obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 2. licencje dostarczane z serwerem typ A oraz z serwerem typ B muszą łącznie uprawniać do zainstalowania tego systemu na co najmniej sześciu serwerach wirtualnych, każdy z nich zainstalowany w klastrze wirtualizacyjnym składającym się z dwóch serwerów fizycznych – serwer typ A i serwer typ B będących przedmiotem zamówienia, 3. nie mogą posiadać ograniczeń czasowych, 4. muszą obejmować licencje dostępowe dla 100 użytkowników.   Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). | TAK / NIE  System operacyjny: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję systemu) |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej trzyletnia gwarancja producenta, obejmująca wszystkie komponenty serwera.  Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja serwera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). | TAK/NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Serwer typ B

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Typu rack o wysokości maksymalnie 1U w konfiguracji bezdyskowej, z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli . | TAK/NIE |
| Płyta główna | Płyta główna pozwalająca na zainstalowanie minimum dwóch procesorów, zaprojektowana przez producenta. Chipset dedykowany przez producenta procesora do pracy w systemach dwuprocesorowych. | TAK/NIE |
| Procesor | Zainstalowane dwa procesory minimum ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem uzyskujące w układzie dwuprocesorowym wynik co najmniej 145 punktów w teście SPECrate2017\_fp\_base dla oferowanego modelu serwera według wyników opublikowanych na stronie <http://spec.org>.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. | TAK/NIE  Procesor: …………………………………………………………….  (należy wpisać model procesora) |
| Pamięć RAM | Zainstalowane co najmniej 128 GB w modułach po co najmniej 16 GB każdy. Płyta główna w konfiguracji dwuprocesorowej musi obsługiwać do 4TB pamięci RAM lub więcej.  Zabezpieczenia pamięci RAM - Memory Mirror. | TAK/NIE |
| Grafika | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1280x1024. | TAK/NIE |
| Sieć | Interfejsy sieciowe LAN:   * minimum 2 porty typu Ethernet 1Gbps RJ45 * minimum 2 porty typu Ethernet 10Gbps SFP+. | TAK/NIE |
| Przestrzeń dyskowa | Dedykowany fizyczny moduł pozwalający na konfigurację nadmiarowej przestrzeni dyskowej (min. RAID 1) zrealizowanej z wykorzystaniem min. dwóch nośników FLASH i/lub SSD o pojemności 240GB każdy, pozwalający na instalację i uruchamianie systemu operacyjnego serwera. | TAK/NIE |
| Porty | Wbudowane porty:   * minimum 2 porty USB 2.0 * minimum 1 port USB 3.0, * 1 port RJ45 dedykowany do zarządzania, * 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), * minimum 1 port RS232. | TAK/NIE |
| Diagnostyka, bezpieczeństwo | Znajdujący się na froncie obudowy panel LCD, umożliwiający wyświetlanie informacji o stanie: temperatury, pamięci RAM, dysków, slotów PCIe, wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą.  Zintegrowany z płytą główną moduł TPM 2.0.  Wsparcie dla trybu blokady, polegającego na zapobieganiu przed wprowadzaniem modyfikacji i aktualizacji ustawień konfiguracji oraz oprogramowania wewnętrznego serwera. | TAK/NIE |
| Wentylacja | Redundantne wentylatory. | TAK/NIE |
| Zasilanie | Dwa redundantne zasilacze Hot Plug o mocy co najmniej 800 Wat. | TAK/NIE |
| Zarządzanie | Karta zarządzania, niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność :   * + - komunikacja poprzez interfejs RJ45,   + - podstawowe zarzadzanie poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging,   + - wbudowana diagnostyka,   + - dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń,   + - monitorowanie temperatury oraz zużycia energii w czasie rzeczywistym,   + - lokalna oraz zdalna konfiguracja serwera,   + - wsparcie dla IPv4 i IPv6,   + - możliwość zdalnego dostępu do konsoli graficznej, zainstalowanego systemu operacyjnego serwera. | TAK/NIE |
| Oprogramowanie bazodanowe | Z serwerem należy dostarczyć licencje na oprogramowanie bazodanowe.  Oprogramowanie bazodanowe (OSB) musi spełniać następujące wymagania poprzez wbudowane mechanizmy:   1. Możliwość wykorzystania OSB jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL. 2. Zintegrowane narzędzia graficzne do zarządzania systemem – OSB musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania. 3. Zarządzanie serwerem za pomocą skryptów - OSB musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem. 4. Dedykowana sesja administracyjna - OSB musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów. 5. Możliwość automatycznej aktualizacji systemu - OSB musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania). 6. OSB musi umożliwiać tworzenie klastrów niezawodnościowych. 7. Wysoka dostępność - OSB musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:  * bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam OSB), * niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe), * klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,  1. Kompresja kopii zapasowych - OSB musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Powinna to być cecha OSB niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych. 2. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych. 3. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory. 4. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - OSB musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność. 5. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - OSB musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:  * odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system), * wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur), * para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).  1. Zarządzanie pustymi wartościami w bazie danych - OSB musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci. 2. Definiowanie nowych typów danych - OSB musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Wykonawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji. 3. Wsparcie dla technologii XML - OSB musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:  * udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli, * udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD, * udostępniać język zapytań do struktur XML, * udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML), * udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.  1. Wsparcie dla danych przestrzennych - OSB musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:  * zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów, * oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, * testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp., * obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu OSB, * typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja - punkt, seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).  1. Możliwość tworzenia funkcji i procedur w innych językach programowania - OSB musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego OSB. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania. 2. Możliwość tworzenia rekursywnych zapytań do bazy danych - OSB musi udostępniać wbudowany mechanizm umożliwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny. 3. Obsługa błędów w kodzie zapytań - język zapytań i procedur w OSB musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania. 4. Raportowanie zależności między obiektami - OSB musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych. 5. Mechanizm zamrażania planów wykonania zapytań do bazy danych - OSB musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji OSB, wprowadzeniu zmian sprzętowych serwera. 6. System transformacji danych - OSB musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:  * mechanizm debuggowania tworzonego rozwiązania, * mechanizm stawiania „pułapek” (breakpoints), * mechanizm logowania do pliku wykonywanych przez transformację operacji, * możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu), * możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo), * mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli), * mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach), * mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego, * mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.  1. Wbudowany system analityczny - OSB musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina. 2. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail). 3. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki). 4. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych. 5. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta). 6. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli. 7. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - OSB musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu. 8. System raportowania - OSB musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:  * raporty parametryzowane, * cache raportów (generacja raportów bez dostępu do źródła danych), * cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów), * współdzielenie predefiniowanych zapytań do źródeł danych, * wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File), * możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport, * możliwość wizualizacji wskaźników KPI, * możliwość wizualizacji danych w postaci obiektów sparkline.  1. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services). 2. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF, PowerPoint. 3. OSB musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów. 4. OSB musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja). 5. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT. 6. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD. 7. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań. 8. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit). 9. OSB musi posiadać wbudowane mechanizmy do obsług danych grafowych (struktur złożonych z węzłów i krawędzi - reprezentujących relacje między węzłami). System musi mieć wbudowane funkcje (dostępne z poziomu kodu SQL) do analizy powiązań między węzłami grafu oraz wyszukiwania najkrótszej ścieżki w grafie. 10. OSB musi posiadać mechanizmy klasyfikacji informacji przechowywanych w bazie danych w celu łatwej identyfikacji obszarów (obiektów) w bazie danych, gdzie składowane są dane wrażliwe. Mechanizm ten powinien umożliwiać przypisanie kolumnom w tabeli m.in. takich atrybutów jak: typ przechowywanych informacji oraz poziom wrażliwości danych. Dodatkowo OSB powinien udostępniać zestaw predefiniowanych raportów prezentujących m.in. listę sklasyfikowanych tabel i kolumn oraz liczbę tabel zawierających dane wrażliwe.   Wymagane dostarczenie licencji bez ograniczeń czasowych na co najmniej 4 rdzenie procesora. | TAK / NIE  Oprogramowanie bazodanowe: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję oprogramowania) |
| System operacyjny | Z serwerem należy dostarczyć licencje na system operacyjny taki sam jak dla serwera typ A.  Licencje na system operacyjny:   1. muszą obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 2. licencje dostarczane z serwerem typ A oraz z serwerem typ B muszą łącznie uprawniać do zainstalowania tego systemu na co najmniej sześciu serwerach wirtualnych, każdy z nich zainstalowany w klastrze wirtualizacyjnym składającym się z dwóch serwerów fizycznych – serwer typ A i serwer typ B będących przedmiotem zamówienia, 3. licencje nie mogą posiadać ograniczeń czasowych.   Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). | TAK / NIE  System operacyjny: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję systemu) |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej trzyletnia gwarancja producenta, obejmująca wszystkie komponenty serwera.  Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja serwera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). | TAK/NIE |
|  | Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Serwerowy zasilacz awaryjny

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ urządzenia | Serwerowy zasilacz awaryjny jednofazowy | TAK/NIE |
| Typ obudowy | Obudowa do montażu w szafie RACK 19” – 2U wraz z zestawem montażowym. | TAK/NIE |
| Moc urządzenia | Co najmniej 2700W (3300 VA) | TAK/NIE |
| Gniazda | Gniazdo zasilania (wejścia):  IEC320-C20  Gniazda wyjściowe:  - co najmniej 8x IEC320-C13  - co najmniej 1x IEC320-C19 | TAK/NIE |
| Czas podtrzymania | Minimalny czas podtrzymania bateryjnego dla 75% mocy nominalnej: 20 minut.  Zamawiający dopuszcza użycie dodatkowej baterii w obudowie do montażu w szafie RACK 19” o wysokości 2U. | TAK/NIE |
| Sygnalizacja | Wskaźnik graficzny wyświetlający stan urządzenia, informujący minimum o:  - trybie pracy (normalny/z użyciem baterii)  - parametrach zasilania na wejściu  - stanie naładowania baterii  - poziomie obciążenia  - wystąpieniu alarmu/awarii | TAK/NIE |
| Komunikacja | Urządzenie musi być wyposażone w port komunikacyjny RJ-45 umożliwiający:  - działanie z prędkością co najmniej 10/100 Mbps  - Obsługę adresacji IPv4 oraz IPv6  - obsługę protokołów:  • HTTP/HTTPS  • DHCP  • SNMP (v1,v2c,v3)  • SMTP (z obsługą min. STARTTLS)  • SSH  • SYSLOG  • FTP  • SCP  • NTP | TAK/NIE |
| Gwarancja | Gwarancja producenta co najmniej 3 lata. | TAK/NIE |

## Szafa rack

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Typ | Szafa stojąca. Konstrukcja stalowa. | TAK/NIE |
| Wymiary | 42U, 800 x 1000. | TAK/NIE |
| Budowa | Szkielet szafy musi mieć możliwość demontażu co najmniej na:  • płytę górną,  • płytę dolną,  • 4 słupy,  • szkielet rack 19”  Drzwi przednie i tyle perforowane z zamkiem trzypunktowym  Panele boczne pełne z zamkiem jednopunktowym  Cokół o wysokości maksymalnej 100mm  Minimum dwa otwory o szerokości co najmniej 70 mm, umożliwiające wprowadzenie okablowania (w tym również kabli zasilających wraz z wtykami trójfazowymi). | TAK/NIE |
| Dopuszczalne obciążenie | 1350 kg lub więcej | TAK/NIE |
| Kolor | Odcienie szarości lub czarny | TAK/NIE |
| Wyposażenie | 2 szt. listwy zasilające PDU:  • montaż rack 19” o wysokości 1U  • kabel zasilający zakończony wtykiem IEC320-C14,  • co najmniej 8 szt. gniazd CEE7/5 | TAK/NIE |

## Macierz dyskowa

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Budowa | Urządzenie musi posiadać minimum dwa (2) kontrolery obsługujące dostęp do dysków, pracujące w trybie Active/Active.  Moduł kontrolerów musi umożliwiać instalację minimum 24 dysków 2,5”.  Urządzenie musi umożliwiać instalację w szafach rack 19” i musi być dostarczone z niezbędnym wyposażeniem do wykonania takiej instalacji.  Urządzenie musi umożliwiać rozbudowę do co najmniej 480 napędów dyskowych w obrębie pojedynczego urządzenia, bez potrzeby wymiany kontrolerów macierzy dostarczonych w ramach niniejszego postępowania. | TAK/NIE |
| Możliwości rozbudowy | Musi istnieć możliwość instalacji dodatkowych modułów dyskowych pozwalających na instalację w danym module co najmniej:  - 24 szt. dysków 2,5” w obudowie max 2U,  - 15 szt. dysków 3,5” w obudowie max 4U. | TAK/NIE |
| Redundancja | Urządzenie musi być wyposażone w system redundantnego zasilania i chłodzenia, zapewniające możliwość pracy i utrzymanie bez przerw funkcjonalności urządzenia, w tym działanie pamięci cache. | TAK/NIE |
| Zabezpieczenia danych | Urządzenie musi zapewniać w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez czas nieograniczony. | TAK/NIE |
| System magazynowania danych | Urządzenie musi umożliwiać utworzenie wolumenu LUN o rozmiarze minimum 64TB i systemu plików minimum 64TB. | TAK/NIE |
| Pamięć podręczna | Urządzenie musi zostać dostarczone z wyposażeniem pozwalającym na skonfigurowanie minimum 128 GB pamięci podręcznej, obsługującej jednocześnie odczyty i zapisy. Pamięć musi być dostępna jednocześnie dla wszystkich wolumenów i kontrolerów macierzy. Włączenie lub wyłączenie pamięci podręcznej nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. | TAK/NIE |
| Porty | Urządzenie musi być wyposażone w minimum następującą liczbę portów do podłączania hostów (Front-end):  - cztery (4) zewnętrzne porty, z autonegocjacją 1/10 Gbps NAS/iSCSI ze złączem Ethernet RJ45, dopuszcza się zastosowanie portów SFP+ wraz z dostarczeniem kompletu certyfikowanych wkładek SFP+ 4 szt. 1Gbp RJ45 i 4 szt. 10Gb RJ45,  - cztery (4) porty 10Gbps iSCSI SFP+.  Urządzenie musi wspierać architekturę bezpośredniego podłączania serwerów do macierzy (bez pośrednictwa przełączników SAN) przy pomocy protokołów FC i 10GbE iSCSI. | TAK/NIE |
| Zamontowane dyski | Pojemność surowa (ang. RAW) macierzy:  - minimum 4,50 TB, na minimum 6 dyskach SSD 12Gbps, 2,5”, DWPD 3  - minimum 19,00 TB, na minimum 11 dyskach SAS 12Gbps, 2,5”, 10K RPM.  Połączenia między dyskami, a kontrolerami muszą być wykonane w technologii SAS 12Gbps lub wydajniejszej.  Urządzenie musi być wyposażona w dyski posiadające podwójne interfejsy.  Urządzenie musi posiadać funkcjonalność globalnych dysków zapasowych lub globalnej przestrzeni Hot-Spare.  W wypadku zastosowania technologii globalnej przestrzeni Hot-Spare, wymagane jest dostarczenie o 10% większej surowej przestrzeni dyskowej niż wymagana powyżej, dla każdego rodzaju zaoferowanych dysków (dotyczy również dostarczanych ewentualnych dodatkowych modułów dyskowych). | TAK/NIE |
| RAID | Urządzenie musi umożliwiać równoczesną obsługę wielu poziomów RAID, minimum RAID 10, 5, 6. | TAK/NIE |
| Kopie migawkowe | Urządzenie musi posiadać funkcjonalność tworzenia lokalnych kopii migawkowych wewnętrznymi mechanizmami macierzy w technologii "redirect on write".  Dopuszcza się, aby macierz wykonywała lokalne kopie migawkowe z wykorzystaniem innych technologii, w takim wypadku wymaga się dostarczenia dodatkowych:  - minimum 4 dysków SSD każdy o pojemności minimum 1,6TB 12Gbps, 2,5”, Write Intensive, DWPD 3.  Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.  Urządzenie musi obsługiwać minimum 64 kopii migawkowych per dysk logiczny LUN oraz 64 kopii per system plików.  Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.  Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną.  W przypadku odtworzenia danych z dowolnej kopii migawkowej, urządzenie musi pozwalać na poprawne zachowanie także wcześniejszych jak i późniejszych snapshotów, z zachowaniem możliwości kolejnego odtworzenia danych ze wszystkich istniejących (starszych i nowszych) kopii dostępnych dla danego zasobu. | TAK/NIE |
| Pozostałe funkcje | Urządzenie musi obsługiwać LUN masking, LUN mapping i inicjowanie startu systemów operacyjnych. Należy dostarczyć licencje dla maksymalnej wspieranej liczby serwerów podłączonych do macierzy. | TAK/NIE |
| Urządzenie musi być wyposażone w funkcjonalność zarządzania poziomem usług (ang. Quality of Service) poprzez możliwość określania wartości „nie większej niż” (limit) dla następujących parametrów dostępu do dysku logicznego: a. Ilość operacji na sekundę (IOPS), b. Przepustowość (MB/s). Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy. | TAK/NIE |
| Urządzenie musi umożliwiać replikację synchroniczną i asynchroniczną danych blokowych oraz replikację asynchroniczną dla danych plikowych pomiędzy dwiema macierzami. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy. | TAK/NIE |
| Urządzenie musi posiadać funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych, w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Pojedynczy migrowany obszar nie może być większy niż 256MB. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy. | TAK/NIE |
| Funkcjonalność tieringu musi być możliwa pomiędzy wszystkimi typami stosowanych dysków (SSD, SAS, NLSAS). | TAK/NIE |
| Urządzenie musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych. | TAK/NIE |
| Urządzenie musi zapewniać jednoczesne zastosowanie różnych trybów protekcji RAID dla różnych typów dysków fizycznych obsługujących pojedynczy dysk logiczny objęty mechanizmem tieringu. | TAK/NIE |
| Urządzenie musi zapewniać mechanizm Thin Provisioning, który polega na udostępnianiu większej przestrzeni logicznej, niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała przydzielonej pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy. | TAK/NIE |
| Urządzenie musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (ang. Space reclamation). | TAK/NIE |
| Wirtualizacja | Urządzenie musi wspierać wirtualizację serwerową w zakresie:  VMware: VAAI, VASA, VVols 2.0, integracja macierzy z VMware vRealize Operations  oraz Hyper-V: Offloaded Data Transfer (ODX) and Offload Copy for File | TAK/NIE |
| Obsługiwane protokoły | Urządzenie musi obsługiwać co najmniej protokoły blokowe: FC i iSCSI, oraz protokoły plikowe: NFS v4.1(MS Windows 2016 i 2019), NFSv3, SMB 2, SMB 3 i VMware VVols (Virtual Volumes) 2.0. | TAK/NIE |
| Gwarancja, wsparcie techniczne | Co najmniej trzyletnia gwarancja producenta obejmująca urządzenie oraz jego oprogramowanie wewnętrzne.  W okresie gwarancji wymagane bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania.  Urządzenie musi oferować funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy.  Serwis musi zawierać usługę pozostawiania bez opłat u Zamawiającego uszkodzonych dysków w okresie obowiązywania gwarancji.  Musi być możliwość zgłaszania awarii poprzez linię telefoniczną producenta obsługiwaną w języku polskim. | TAK/NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Serwer typ C (backup)

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Typu rack o wysokości maksymalnie 2U z możliwością zamontowania minimum 8 dysków 3,5” Hot Plug, z kompletem szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli . | TAK/NIE |
| Płyta główna | Płyta główna pozwalająca na zainstalowanie minimum dwóch procesorów, zaprojektowana przez producenta. Chipset dedykowany przez producenta procesora do pracy w systemach dwuprocesorowych. | TAK/NIE |
| Procesor | Zainstalowany jeden procesor minimum ośmiordzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem uzyskujące w układzie dwuprocesorowym wynik co najmniej 150 punktów w teście SPECrate2017\_fp\_base dla oferowanego modelu serwera według wyników opublikowanych na stronie <http://spec.org>.  Do oferty należy załączyć wydruk z ww. strony, dopuszcza się wydruk w języku angielskim. | TAK/NIE  Procesor: …………………………………………………………….  (należy wpisać model procesora) |
| Pamięć RAM | Zainstalowane co najmniej 32 GB w modułach po co najmniej 16 GB każdy. Płyta główna w konfiguracji dwuprocesorowej musi obsługiwać do 1TB pamięci RAM lub więcej.  Zabezpieczenia pamięci RAM - Memory Mirror. | TAK/NIE |
| Grafika | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości co najmniej 1280x1024. | TAK/NIE |
| Sieć | Interfejsy sieciowe:   * minimum 2 porty typu Ethernet 1Gbps RJ45, * minimum 2 porty typu Ethernet 10Gbps SFP+. | TAK/NIE |
| Kontroler RAID | Sprzętowy kontroler dyskowy RAID z minimum 8 GB pamięci, obsługujący następujące poziomy RAID : 0, 1, 5, 6, 10, 50, 60.  Szybkość transmisji danych: 12Gbps | TAK/NIE |
| Kontroler SAS | Zewnętrzny kontroler SAS - karta SAS HBA 12Gbps z zewnętrznym portem pozwalającym podłączyć streamer dostarczany w ramach zamówienia | TAK/NIE |
| Przestrzeń dyskowa | Zainstalowane co najmniej 7 dysków SATA o pojemności co najmniej 4TB każdy. | TAK/NIE |
| Porty | Wbudowane porty:   * minimum 2 porty USB 2.0 * minimum 1 port USB 3.0, * 1 port RJ45 dedykowany do zarządzania, * 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), * minimum 1 port RS232. | TAK/NIE |
| Diagnostyka, bezpieczeństwo | Znajdujący się na froncie obudowy panel LCD, umożliwiający wyświetlanie informacji o stanie: temperatury, pamięci RAM, dysków, slotów PCIe, wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą.  Zintegrowany z płytą główną moduł TPM 2.0.  Wsparcie dla trybu blokady, polegającego na zapobieganiu przed wprowadzaniem modyfikacji i aktualizacji ustawień konfiguracji oraz oprogramowania wewnętrznego serwera. | TAK/NIE |
| Wentylacja | Redundantne wentylatory. | TAK/NIE |
| Zasilanie | Dwa redundantne zasilacze Hot Plug o mocy co najmniej 800 Wat. | TAK/NIE |
| Zarządzanie | Karta zarządzania, niezależna od zainstalowanego systemu operacyjnego, zintegrowana z płyta główną, posiadająca minimalną funkcjonalność :   * + komunikacja poprzez interfejs RJ45,   + podstawowe zarzadzanie poprzez protokół IPMI 2.0, DCMI 1.5, SNMP, VLAN tagging,   + wbudowana diagnostyka,   + dostęp poprzez interfejs graficzny Web karty oraz z linii poleceń,   + monitorowanie temperatury oraz zużycia energii w czasie rzeczywistym,   + lokalna oraz zdalna konfiguracja serwera,   + wsparcie dla IPv4 i IPv6,   + możliwość zdalnego dostępu do konsoli graficznej, zainstalowanego systemu operacyjnego serwera. | TAK/NIE |
| System operacyjny | Z serwerem należy dostarczyć licencje na system operacyjny taki sam jak dla serwera typ A.  Licencje na system operacyjny:   1. muszą obejmować najnowszą wersję systemu dostępną na dzień składania oferty, 2. muszą uprawniać do zainstalowania tego systemu na serwerze fizycznym – serwer typu C będący przedmiotem zamówienia, 3. nie mogą posiadać ograniczeń czasowych.   Do oferty należy załączyć potwierdzenie kompatybilności serwera z oferowanym systemem operacyjnym (wydruk ze strony producenta systemu operacyjnego, dopuszcza się wydruk w języku angielskim). | TAK / NIE  System operacyjny: …………………………………………………………………….  (należy wpisać producenta, nazwę i wersję systemu) |
| Warunki gwarancyjne, wsparcie techniczne | Co najmniej trzyletnia gwarancja producenta, obejmująca wszystkie komponenty serwera. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego.  Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Dedykowany portal techniczny producenta, umożliwiający Zamawiającemu zgłaszanie awarii oraz samodzielne zamawianie zamiennych komponentów.  Możliwość sprawdzenia kompletnych danych o urządzeniu na jednej witrynie internetowej prowadzonej przez producenta (automatyczna identyfikacja serwera, konfiguracja fabryczna, konfiguracja bieżąca, rodzaj gwarancji, data wygaśnięcia gwarancji, data produkcji komputera, aktualizacje, diagnostyka, dedykowane oprogramowanie, tworzenie dysku recovery systemu operacyjnego). | TAK/NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Streamer

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Obudowa | Do montażu w szafie rack.  Zewnętrzna z własnym zasilaniem i wyjściem zgodnym z protokołem SAS. | TAK/NIE |
| Technologia | Wykonany w technologii LTO-7 z interfejsem zewnętrznym SAS lub posiadającej większą wydajność, oraz pojemność nośników danych. | TAK/NIE |
| Wymagane wyposażenie | Akcesoria:  - kabel SAS 1m,  - 5 szt. nośników LTO-7 lub innych, zgodnych z dostarczanym streamerem,  - 1 szt. nośnika czyszczącego. | TAK/NIE |
| Zasilanie | Zasilanie 230V AC | TAK/NIE |
| Gwarancja | Gwarancja producenta co najmniej 3 lata. | TAK/NIE |
| Opcjonalnie wykonawca może zadeklarować nw. warunki świadczenia serwisu gwarancyjnego:   * usługi serwisu gwarancyjnego w miejscu instalacji urządzenia, * czas reakcji serwisu - do końca następnego dnia roboczego, czas naprawy - w ciągu 7 dni kalendarzowych licząc od dnia zgłoszenia.   Ww. opcjonalne warunki świadczenia serwisu gwarancyjnego będą stanowić kryteria oceny ofert. | Należy wskazać w formularzu oferty, czy wykonawca deklaruje opcjonalne warunki świadczenia serwisu gwarancyjnego. |

## Oprogramowanie do tworzenia kopii zapasowych

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, nazwa oprogramowania: ………………………………………………………………… |
| Licencjonowanie | Wymagane jest dostarczenie licencji bez ograniczeń czasowych, pozwalających na ochronę minimum:   * wirtualnych maszyn pracujących na oferowanej platformie wirtualizacji serwerów i pracujących pod kontrolą oferowanych systemów operacyjnych oraz systemów z rodziny Microsoft Windows Server i Linux, * serwerów fizycznych pracujących pod kontrolą oferowanych systemów operacyjnych oraz systemów z rodziny Microsoft Windows Server i Linux, * komputerów osobistych (laptop/desktop) pracujących pod kontrolą systemów operacyjnych Windows 10, * instancji serwera baz danych (minimum Oracle oraz Microsoft SQL Server).   Licencje muszą zapewnić ochronę minimum dziesięciu (10) instancji jednego z w/w typów lub kombinacji dowolnych instancji z w/w typów do łącznej liczby minimum dziesięciu (10). | TAK/NIE |
| Kompatybilność | Oprogramowanie musi współpracować z infrastrukturą VMware w wersjach 6.0, 6.5, 6.7, 7.0 oraz Microsoft Hyper-V 2012, 2012 R2, 2019 oraz 2022  Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.  Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.  Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manager, klastrami hostów oraz pojedynczymi hostami.  Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V.  Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. | TAK/NIE |
| Funkcjonalność | Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.  Oprogramowanie musi tworzyć “samowystarczalne” archiwa, do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.  Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental).  Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.  Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.  Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.  Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy aktualizowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania  Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania wykonania kopii migawkowej (snapshot).  Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)  Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania danych  Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API  Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji  Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji  Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania  Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).  Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.  Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej  Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.  Oprogramowanie musi oferować ten mechanizm z dokładnością do datastoru  Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora.  Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w oferowanym środowisku wirtualizacyjnym i być dostępna dla oferowanej macierzy.  Oprogramowanie musi posiadać wsparcie dla oferowanego środowiska wirtualizacyjnego potwierdzone odpowiednią certyfikacją.  Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn  Oprogramowanie musi posiadać wsparcie dla NDMP  Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)  Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.  Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.  Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.  Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.  Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.  Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.  Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)  Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V  Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)  Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere  Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)  Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.  Dodatkowo dla środowiska vSphere powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)  Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami  Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre  Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków  Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików  Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.  Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:   * Dla systemów Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs * Dla systemów Windows: NTFS, FAT, FAT32, ReFS   Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.  Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.  Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy AD Sites.  Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat.  Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.  Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.  Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN oraz SAP HANA.  Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN  Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.  Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.  Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere.  Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla dwóch dostawców.  Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. | TAK/NIE |
| Wsparcie techniczne | Oferowane oprogramowanie winno być dostarczone z minimum 1 rocznym wsparciem producenta oprogramowania. W ramach wsparcia musi istnieć możliwość zakładania zgłoszeń serwisowych przez stronę internetową producenta dostępną w trybie 24/7/365.  Zgłoszone problemy mają być rozwiązywane minimum w dni robocze (poniedziałek – piątek) w godzinach 8:00-20:00.  W ramach wsparcia, Zamawiający musi mieć prawo do pobierania plików aktualizacji oferowanego oprogramowania, jak również do nowych wersji, które zostaną wydane w czasie jego obowiązywania. | TAK/NIE |

## Klaster urządzeń UTM

|  |  |  |
| --- | --- | --- |
| **Obszar wymagań** | **Wymagania minimalne** | **Oferowane parametry – odpowiednio: uzupełnić wymagane informacje lub zaznaczyć: spełnia – TAK, nie spełnia – NIE** |
|  |  | Producent, model: ………………………………………………………………… |
| Praca w klastrze | Zamawiający wymaga dostarczenia klastra wysokiej dostępności urządzeń UTM (dwa węzły - urządzenia) działających co najmniej w trybie aktywny-pasywny (Active-Passive), w związku z czym każdy z węzłów klastra pełniąc rolę jako aktywny węzeł, musi spełniać poniższe wymagania. | TAK/NIE |
| Funkcjonalność firewall | Firewall musi umożliwiać zdefiniowanie co najmniej 3 stref bezpieczeństwa  Firewall musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF i BGP  Firewall musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPoE) na zewnętrznym interfejsie  Firewall musi obsługiwać DHPC v6 na zewnętrznym interfejsie  Firewall musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP, jako bridge (transpartent mode) lub z tym samym adresem IP na wszystkich portach.  Firewall musi mieć możliwość obsługi wielu łączy zewnętrznych z opcją balansowania ruchu i dynamiczną selekcją drogi routowania.  Firewall musi mieć możliwość obsługi łącza zapasowego typu LTE  Firewall musi obsługiwać Dynamic DNS  Firewall musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1  Firewall musi obsługiwać translację portów: PAT  Firewall musi obsługiwać IPSec NAT traversal  Firewall musi obsługiwać mechanizm policy-based NAT  Firewall musi obsługiwać VLAN 802.1Q  Firewall musi zapewniać ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów  Firewall musi obsługiwać pracę jako serwer DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.  Firewall musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP  Firewall musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.  Firewall musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników.  Firewall musi umożliwiać transparentne uwierzytelnianie użytkowników przez Active Directory.  Urządzenie musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z Microsoft Terminal Services i CitrixXenApp  Urządzenie nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.  Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji  Firewall musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.  Firewall musi obsługiwać mechanizmy Protocol Anomaly Detection (PAD) dla najpopularniejszych protokołów.  Firewall musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP  Firewall musi zapewniać ochronę z wykorzystaniem mechanizmów IPS  Firewall musi zapewniać ochronę antywirusową dla obsługiwanych protokołów  Firewall musi zapewniać możliwość filtrowania URL  Firewall musi zapewniać inspekcję ruchu szyfrowanego HTTPS  Firewall musi zapewniać ochronę przed niechcianą pocztą (AntySPAM)  Firewall musi zapewniać rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu.  Urządzenie musi mieć możliwość filtrowania treści według typu MIME  Urządzenie musi umożliwiać sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa, protokół, polisa, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji.  Firewall musi udostępniać mechanizmy limitowania dostępu do sieci użytkownikom w oparciu o kwoty czasowe lub transferu danych.  Firewall musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site  Firewall musi posiadać mechanizm blokujący szkodliwe żądania DNS, zapewniając ochronę użytkowników końcowych przed atakami typu phishing | TAK/NIE |
| Wydajność firewall | Firewall musi zapewnić obsługę na poziomie minimalnym:  17 Gbps dla pracy w trybie firewall (UDP 1518),  2.2 Gbps dla pracy w trybie UTM.  Firewall musi obsługiwać minimum 4 400 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 95 000 nowych połączeń na sekundę.  Ilość obsługiwanych sieci VLAN: minimum 200.  Minimalna ilość fizycznych portów:  - 8 portów 1Gbps RJ45. | TAK/NIE |
| Funkcje VPN | Urządzenie musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz TLS  Urządzenie musi w zakresie IPSec site-to-site VPN współpracować z rozwiązaniami innych producentów  Rozwiązanie musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256  Rozwiązanie musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, 3rd Party Cert.  Wsparcie dla Dead Peer Detection (DPD)  Urządzenie musi obsługiwać IKEv1 i IKEv2  Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman do wymiany kluczy przez email i web  Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego) z podtrzymaniem zestawionych połączeń TCP  Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu  Urządzenie musi obsługiwać statyczne i dynamiczne (routowane) połączenia VPN do dostawców chmury obliczeniowej (AWS i MS Azure)  Urządzenie musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP.  Połączenia client-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android  Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu  Urządzenie ma zapewnia funkcję portalu dostępowego chronionego przez szyfrowanie https (TLS) | TAK/NIE |
| Wydajność VPN | Przepustowość IPSec VPN (UDP 1518) nie mniejsza niż 5.0Gbps  Obsługa nie mniej niż: 200 tuneli IPSec site-to-site  Obsługa nie mniej niż: 200 tuneli client-to-site | TAK/NIE |
| Filtrowanie zawartości URL | Urządzenie musi umożliwiać filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji  Funkcjonalność filtrowania zawartości powinna dawać możliwość filtrowania stron według minimalnie 120 kategorii  Rozwiązanie musi pozwalać na tworzenie białych list wyjątków dla filtrowania zawartości  Baza zawartości URL powinna być dostępna on-line lub do ściągnięcia i zainstalowania miejscowo  Funkcja powinna filtrować treści w wielu językach, w tym w języku polskim  Filtrowanie musi obsługiwać również protokół https  Urządzenie musi umożliwiać wyłączenie inspekcji https dla wybranych kategorii stron www  System kategoryzacji stron musi posiadać kategorie: Command&control, Proxy avoidance, Botnets, Malicious sites, Phishing, Spyware | TAK/NIE |
| Kontrola aplikacyjna | System kontroli aplikacyjnej musi rozpoznawać aplikacje oraz kategorie aplikacji  Aplikacje muszą być rozpoznawana w oparciu o analizę ruchu a nie przez porty i protokoły  Ilość rozpoznawanych aplikacji nie mniejsza niż 1800  W ramach konkretnej aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe)  Kontrola aplikacyjna musi rozpoznawać co najmniej aplikacje: Tor, CryptoAdmin, Proxy service, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online | TAK/NIE |
| Antywirus | System musi mieć możliwość uruchomienia co najmniej 2 skanerów antywirusowych  Aktualizacja plików sygnatur antywirusowych musi się odbywać automatycznie  Aktualizacja plików sygnatur antywirusowych musi się odbywać nie rzadziej niż co 12 godzin.  Antywirus musi mieć możliwość przeprowadzania kwarantanny e-mail.  Jeden ze skanerów antywirusowych musi bazować na mechanizmach bezsygnaturowych  Rozwiązanie musi mieć możliwość tworzenia wyjątków w białej liście, aby umożliwić nieblokowany dostęp do poczty z określonych domen  Wykrywanie i blokowanie spyware’u  Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji  Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS  Przepustowość AV w urządzeniu nie mniejsza niż 3Gbps  W celu realizacji ochrony z wykorzystaniem 2 skanerów antywirusowych Zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia. | TAK/NIE |
| Antyspam | Antyspam ma zapewnić możliwość kwarantanny e-mail  Antyspam ma posiadać zintegrowaną antywirusową analizę spamu  Rozwiązanie ma umożliwić blokowanie spamu w wielu językach w tym w języku polskim  Możliwość blokowania spamu opartego na obrazach graficznych. | TAK/NIE |
| IPS | Automatyczna aktualizacja sygnatur IPS  IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy  Automatyczne blokowanie znanych źródeł ataków  System musi pozwalać na blokowanie ataków typu DoS i DDoS  Przepustowość IPS w urządzeniu nie mniejsza niż 3.2Gbps | TAK/NIE |
| WiFi | UTM musi mieć możliwość pełnienia funkcji kontrolera sieci WiFI.  Kontroler sieci wifi ma zapewniać centralne zarządzanie oraz serowanie punktami dostępowymi.  Sieć ma mieć możliwość jednoczesnej pracy w paśmie 2.4Ghz oraz 5Ghz.  Sieć ma mieć możliwość skonfigurowania co najmniej 8 SSID w każdym z zakresów (2.4GHz i 5GHz)  Sieć musi posiadać mechanizmy wykrywania innych punktów dostępu (ang. rogue access point)  Sieć musi mieć możliwość izolacji urządzeń końcowych  Sieć musi mieć możliwość uruchamiania poszczególnych SSID wg harmonogramu  Musi istnieć możliwość automatycznej aktualizacji oprogramowania punktów dostępowych przez kontroler sieci WiFi  Kontroler musi mieć funkcję graficznej prezentacji topologii sieci  Kontroler musi mieć funkcję analizy mapy konfliktów w kanałach transmisyjnych  Jako rozwiązanie równoważne Zamawiający dopuszcza realizację funkcji kontrolera sieci przez osobne, dedykowane urządzenie pełniące funkcję kontrolera sieci bezprzewodowej (1 szt.), spełniające nw. wymagania minimalne:  Obudowa do montażu w szafie RACK 19” – 1U wraz z zestawem montażowym.  Porty: 2 porty 1/10GBase-X SFP+, 2 porty COMBO (RJ45 lub SFP), 24 porty 10/100/1000Base-T, 1 port szeregowy konsoli (interfejs RJ-45), 1 port do zarządzania USB 2.0  Wydajność:   * obsługa minimum 16,000 adresów MAC. * pojemność tablicy ARP minimum 4000 wpisów. * możliwość jednoczesnej obsługi minimum 256 punktów dostępowych. * możliwość jednoczesnej obsługi minimum 10000 użytkowników bezprzewodowych w sieci.   Zasilanie 230V AC  Funkcje i protokoły: IEEE 802.1p (COS), IEEE 802.1x (Port Control), IEEE 802.1Q, IEEE802.3x, IEEE802.3ad, IGMP Snooping, MLD Snooping, GVRP, PVLAN, Port Mirror, QinQ,  Obsługa routingu: Routing statyczny, RIP v1/v2, OSPF, BGP, VRRP, Obsługa multicastów: IGMP v1/v2/v3, PIM-SM, PIM-DM, PIM-SSM, ARP, ARP Proxy,  Obsługa funkcji sieci bezprzewodowych: IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11d, IEEE 802.11h, IEEE 802.11i, IEEE 802.11e, IEEE 802.11k,  Obsługa protokołu CAPWAP:  Wsparcie dla tunelu CAPWAP między AC (kontroler sieci bezprzewodowej) i AP (punkt dostępowy),   * automatyczne wykrywanie dostępnego AC, * automatyczne pobieranie konfiguracji AP z AC, * automatyczna aktualizacja oprogramowania AP z AC, * obsługa roaming pomiędzy AP obsługiwanymi przez jeden AC,   Funkcje bezpieczeństwa:   * klucz WEP 64/128, dynamiczny WEP, TKIP, CCMP, * bezpieczna autentykacja użytkowników zgodna z IEEE 802.11i (możliwość zastosowania dwóch trybów: Enterprise i Personal), * szyfrowanie i autentykacja WAPI, * autentykacja LDAP, * autentykacja po adresie MAC, * autentykacja przez portal, * wbudowany portal, * zewnętrzny portal, * możliwość personalizacji portalu logowania, * autentykacja użytkowników PEAP, * okresowe włączanie i wyłączanie radia / SSID, * izolacja użytkowników bezprzewodowych, * filtrowanie ramek, * biała lista, * statyczna czarna lista i dynamiczna czarna lista, * klient RADIUS, * kontrola dostępu do różnych pakietów danych w tym po adresach MAC, IPv4 i IPv6, * bezpieczna kontrola dostępu do AP, taka jak uwierzytelnianie MAC, uwierzytelnianie hasłem lub uwierzytelnianie certyfikatu cyfrowego między AP i AC, - zapasowy serwer uwierzytelniający, * Wireless SAVI, * zabezpieczenie przed atakami typu flood, * zabezpieczenie przed spoofingiem, * wbudowany mechanizm WIDS oraz WIPS;   Obsługa QoS:   * IEEE 802.11e (WMM), * minimum 4 poziomy priorytetów kolejek danych, * mapowanie różnych sieci VLAN oraz SSID do różnych polityk QoS, * mapowanie różnych strumieni danych (na podstawie różnych pól pakietów) do rożnych polityk QoS, load balancing w oparciu o liczbę użytkowników/ilość ruchu/zakres częstotliwości, * limit przepustowości możliwy do zdefiniowania dla AP/SSID/terminali/strumieni danych, * tryb oszczędzania energii, * automatyczne odzyskiwanie komunikacji AP, * inteligentne identyfikowanie terminali, * funkcja Automatic emergency mechanism of APs (w przypadku braku komunikacji z którymkolwiek z AC, AP pracują jako niezależne urządzenia wciąż obsługując obecnych i nowych użytkowników), * mechanizm Multicast-to-unicast   Zarządzanie funkcjami radiowymi punktów dostępowych:   * ustawianie kodu kraju, * ręczne/automatyczne ustawianie mocy nadawania, * ręczne/automatyczne ustawianie kanału bezprzewodowego, * automatyczne ustawianie prędkości transmisji, * skanowanie przestrzeni radiowej, * ukrywanie SSID, * wykrywanie i unikanie zakłóceń RF, * ustawianie szerokości kanału bezprzewodowego (20MHz, 40 MHz, 80 MHz), * zapewnienie równych szczelin czasowych dla użytkowników pracujących w różnych standardach bezprzewodowych, * limitowanie użytkowników dla SSID oraz dla punktu dostępowego, * airtime protection w hybrydowym dostępie do terminali 11bg i 11n, * automatyczne starzenie się użytkowników bez ruchu, * zakaz dostępu klientów o słabych sygnałach, * wyświetlanie i zarządzanie wszystkimi punktami dostępu za pomocą jednego urządzenia fizycznego.   Funkcje podłączania punktów dostępowych: obsługa minimum trybów zabezpieczonego (autentykacja AP po adresie MAC lub przez cyfrowy certyfikat) i niezabezpieczonego (AC przyjmuje wszystkie AP, które się do niego zgłoszą).  Zarządzanie:   * możliwość zarządzania poprzez przeglądarkę internetową wykorzystując graficzny interfejs użytkownika (GUI), * tekstowy interfejs zarządzania z podpowiedziami kontekstowymi, * tekstowy plik konfiguracyjny możliwy do wyeksportowania, edytowania poza urządzeniem i ponownego zaimportowania do urządzenia, * możliwość zarządzania urządzeniem z wykorzystaniem protokołów SSHv2 oraz TELNET, * bezpośredni dostęp do interfejsu zarządzania z wykorzystaniem dedykowanego portu szeregowego lub jego emulacji, * wysyłanie powiadomień o zdarzeniach z użyciem protokołów SNMPv1, SNMPv2c oraz SNMPv3, * przesyłanie dzienników zdarzeń z wykorzystaniem protokołu SYSLOG, * synchronizacja czasu systemowego z użyciem protokołów SNTP lub NTP, * sprzętowy watchdog * mechanizm uprawnień użytkowników w oparciu o SSID.   Urządzenie musi być objęte co najmniej 3-letnią gwarancją producenta, z czasem reakcji serwisu do końca następnego dnia roboczego. | TAK/NIE  Jeżeli wykonawca oferuje dedykowany kontroler sieci bezprzewodowej, należy podać producenta i model urządzenia:  ……………………………………………………………………… |
| Ochrona przed phishingiem | System musi zapewniać dedykowaną (poza ochroną przed SPAMem) ochronę przed phishingiem  System winien blokować możliwość dostępu do spreparowanych stron.  System musi blokować dostęp niezależnie od użytego protokołu czy portu komunikacyjnego  Zablokowanie dostępu musi być odpowiednio notyfikowane użytkownikowi, którego dotyczy, niezależnie od logów i raportów  System musi chronić przed nadużyciem protokołu DNS | TAK/NIE |
| Zarządzanie | Administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania w czasie rzeczywistym.  Urządzenie musi umożliwiać zarządzanie za pomocą linii poleceń poprzez port szeregowy lub poprzez SSH.  Urządzenie musi umożliwiać zarządzanie za pomocą wbudowanego interfejsu www.  Interfejs WWW do zarządzania urządzeniem musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.  Urządzenie może być zarządzane jednocześnie z wielu platform przez różnych administratorów.  Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.  Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online.  Rozwiązanie musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji z wykorzystaniem dodatkowego oprogramowania producenta.  System musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.  Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.  System ma posiadać metodę porównywania różnych wersji konfiguracji.  Obsługa różnych ról administratorów.  Umożliwia monitorowanie logów ruchu w czasie rzeczywistym.  Serwer logów musi umożliwiać zapis do wbudowanej bazy danych lub do zewnętrznej bazy danych.  System ma posiadać możliwość stworzenia mapy sieci wewnętrznej zawierającej szczegółowe dane urządzenia (MAC, IP, System operacyjny, otwarte porty).  Urządzenie musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.  System zarządzania musi zapewniać korelację zdarzeń dotyczących konkretnych komputerów pochodzących z systemów ochrony sieciowej i z chronionych komputerów  System zarządzania musi posiadać graficzną konsolę do zarządzania systemem VPN działającą w trybie drag-and-drop | TAK/NIE |
| Dzienniki i raporty | Rozwiązanie musi umożliwiać zbieranie i przechowywanie dzienników i raportów.  Rozwiązanie musi umożliwiać przesyłanie logów do co najmniej 2 serwerów dziennika  Dzienniki transmisji muszą być szyfrowane.  Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.  Rozwiązanie musi udostępniać narzędzie analizy całości ruchu  Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa  Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów czy rozmiaru bazy danych  Rozwiązanie musi posiadać minimum 90 predefiniowanych typów raportów.  Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie  System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.  System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania tych sprawozdań pocztą e-mail.  Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.  System raportowania musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów i dzienników.  System musi wspierać automatyczne wysyłanie wszystkich typów raportów pocztą elektroniczną.  Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.  System musi umożliwiać pseudoanonimizację użytkowników z prawem do deanonimizacji tylko dla wybranych administratorów  System musi zapewniać wizualizację, opisującą w trybie graficznym stan przepustowości systemu. | TAK/NIE |
| Zaawansowana detekcja malware | Funkcja zaawansowanego wykrywania szkodliwego oprogramowania w tym samym urządzeniu.  Zaawansowany malware jest wykrywany przez uruchomienie plików w chmurze przy użyciu emulacji pełnego systemu.  Zaawansowana detekcja malware musi obsługiwać wszystkie pliki wykonywalne systemu Windows, pliki zip, pdf, Microsoft Office, oraz pliki Android APK.  Wymagane są szczegółowe raporty, oraz informacje wskazujące na powody, dla których plik jest uważany za zaawansowany malware  W celu realizacji ochrony „Zero Day” zamawiający dopuszcza wykorzystanie dodatkowego urządzenia spełanijącego powyższe założenia. | TAK/NIE |
| System blokowania i odpowiedzi na zaawansowane zagrożenia typu malware i ransomware | Rozwiązanie musi posiadać system blokowania i odpowiedzi na zaawansowane zagrożenia typu malware i ransomware o parametrach:   * musi posiadać agentów dedykowanych dla systemów operacyjnych co najmniej Windows 7, 8, 8.1, 10, 11, Windows Server 2008, 2012, 2016, 2019 Linux RedHat/CentOS, Mac OS 10.x, * musi zostać dostarczone z licencja na wsparcie minimum 150 hostów (stacji roboczych i serwerów), * musi posiadać możliwość prowadzenia analizy heurystycznej i behawioralnej pod kątem zagrożeń typu malware i ransomware, bezpośrednio na hostach i w trybie ciągłym wysyłać wyniki analizy do systemu centralnego w celu przeprowadzenia oceny zagrożeń dzięki korelacji i scoringu zagrożeń, * musi posiadać mechanizm automatycznej odpowiedzi na wykryte zagrożenie typu malware i ransomware, poprzez minimum takie działania jak, kwarantanna plików, zabijanie procesów (ang. kill) i usuwanie wpisów w rejestrach, * musi pozwalać na konfigurowalne powiadamianie poprzez e-mail minimum o wykrytych krytycznych zdarzeniach, incydentach, oraz akcjach podjętych aby im zapobiec które miały miejsce w sieci i na hostach. |  |
| Gwarancja, subskrypcje | Gwarancja producenta co najmniej 3 lata.  Urządzenie musi być dostarczone ze wszystkimi licencjami/subskrypcjami umożliwiającymi uzyskanie funkcjonalności wymienionymi w niniejszej specyfikacji. Długość trwania licencji/subskrypcji nie może być krótsza niż okres gwarancji.  W okresie gwarancji musi być zapewniona możliwość zgłaszania incydentów za pomocą e-mail, portalu - 24 godziny na dobę 7 dni w tygodniu.  Zamawiający wymaga, by wymiana urządzenia w przypadku zdiagnozowania awarii uniemożliwiającej funkcjonowanie, następowała na następny dzień roboczy od zdiagnozowania awarii. | TAK/NIE |

## Usługi wdrożenia sprzętu oraz oprogramowania

1. Montaż elementów szafy rack będącej przedmiotem zamówienia i jej instalacja w miejscu wyznaczonym przez Zamawiającego.
2. Wykonawca uwzględni w cenie oferty i dostarczy wszelkie elementy niezbędne do montażu, instalacji i uruchomienia sprzętu będącego przedmiotem zamówienia, w tym kable, listwy zasilające, akcesoria montażowe itp. W ramach powyższego wykonawca dostarczy nie mniej niż:
   1. Moduły SFP+ 10Gb UTP RJ45 – 4 6szt.
   2. Kable DAC QSFP+ to QSFP+ 40GbE, 0.5metra – 2 szt.
   3. Kable DAC SFP+ to SFP+ 10GbE, 1metry – 5 szt.
   4. Kable DAC SFP+ to SFP+ 10GbE, 3metry – 6 szt.
   5. Kable Ethernet Patchcord cat.6a RJ45, 3m – 16 szt.

oraz wszelkie inne elementy niezbędne do montażu, instalacji i uruchomienia sprzętu będącego przedmiotem zamówienia.

1. Instalacja, uruchomienie i konfiguracja w ww. szafie nw. elementów będących przedmiotem zamówienia:
   1. Serwerowy zasilacz awaryjny, w tym
      1. instalacja dodatkowych modułów bateryjnych jeśli dotyczy,
      2. weryfikacja poprawności działania,
      3. aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
      4. konfiguracja adresacji IP interfejsu zarządzania,
      5. konfiguracja protokołu synchronizacji czasu NTP,
      6. konfiguracja protokołu rozwiązywania nazw DNS,
   2. Przełączniki sieciowe typ A, w tym:
      1. okablowanie sieciowe urządzeń,
      2. podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
      3. uruchomienie i weryfikacja poprawności działania urządzeń,
      4. aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
      5. konfiguracja adresacji IP interfejsów zarządzania,
      6. konfiguracja protokołu synchronizacji czasu NTP,
      7. konfiguracja protokołu rozwiązywania nazw DNS,
      8. konfiguracja konstrukcji nadmiarowej,
      9. konfiguracja wymaganych połączeń VLAN,
      10. konfiguracja wymaganych połączeń agregujących – LAG
      11. konfiguracja wymaganych kont administracyjnych
      12. podłączenie urządzeń do dostarczanego klastra urządzeń UTM
   3. Przełączniki sieciowe typ B, w tym:
      1. okablowanie sieciowe urządzeń,
      2. podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
      3. uruchomienie i weryfikacja poprawności działania urządzeń,
      4. aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
      5. konfiguracja adresacji IP interfejsów zarządzania,
      6. konfiguracja protokołu synchronizacji czasu NTP lub SNTP,
      7. konfiguracja protokołu rozwiązywania nazw DNS,
      8. konfiguracja konstrukcji nadmiarowej,
      9. konfiguracja wymaganych połączeń VLAN,
      10. konfiguracja wymaganych połączeń agregujących – LAG,
      11. konfiguracja wymaganych kont administracyjnych,
      12. podłączenie urządzeń do nadmiarowej konstrukcji przełączników sieciowych typ A.
   4. Urządzenia UTM, w tym:
      1. okablowanie sieciowe urządzeń,
      2. podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
      3. uruchomienie i weryfikacja poprawności działania urządzeń,
      4. aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
      5. konfiguracja adresacji IP interfejsów zarządzania,
      6. konfiguracja protokołu synchronizacji czasu NTP,
      7. konfiguracja protokołu rozwiązywania nazw DNS,
      8. konfiguracja konstrukcji nadmiarowej,
      9. konfiguracja wymaganych połączeń VLAN,
      10. konfiguracja wymaganych połączeń agregujących – LAG,
      11. konfiguracja wymaganych sieci VPN,
      12. konfiguracja wymaganych kont administracyjnych,
      13. integracja z domeną usług katalogowych,
      14. konfiguracja polis bezpieczeństwa zgodnie z wymaganiami Zamawiającego,
      15. uruchomienie oraz konfiguracja zaawansowanych funkcjonalności zgodnie z wymaganiami Zamawiającego,
      16. weryfikacja poprawności działania klastra wysokiej dostępności.
   5. Access-pointy oraz kontroler sieci bezprzewodowej (jeśli dotyczy), w tym:
      1. okablowanie sieciowe urządzeń
      2. podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
      3. uruchomienie i weryfikacja poprawności działania urządzeń
      4. aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
      5. konfiguracja adresacji IP interfejsów zarządzania
      6. konfiguracja protokołu synchronizacji czasu NTP lub SNTP
      7. konfiguracja protokołu rozwiązywania nazw DNS
      8. konfiguracja konstrukcji nadmiarowej
      9. konfiguracja wymaganych połączeń VLAN
      10. konfiguracja wymaganych połączeń agregujących – LAG
      11. konfiguracja wymaganych kont administracyjnych
      12. podłączenie urządzeń do nadmiarowej konstrukcji przełączników sieciowych typ A
      13. integracja z dostarczanymi punktami dostępowymi (access-point)
      14. konfiguracja sieci bezprzewodowej zgodnie z wymogami Zamawiającego
   6. Macierz dyskowa, w tym:
      1. podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego
      2. okablowanie sieciowe urządzeń
      3. uruchomienie i weryfikacja poprawności działania urządzeń
      4. aktualizacja oprogramowania układowego do wersji zalecanej przez producenta
      5. konfiguracja adresacji IP interfejsów zarządzania
      6. konfiguracja protokołu synchronizacji czasu NTP
      7. konfiguracja protokołu rozwiązywania nazw DNS
      8. instalacje niezbędnych licencji do uruchomienia wymaganych funkcjonalności
      9. integracja uwierzytelniania macierzy z domeną MS Active Directory
      10. konfiguracja przestrzeni dyskowych zgodnie z wymaganiami Zamawiającego
      11. konfiguracja interfejsów Front-End zgodnie z wymaganiami Zamawiającego
      12. konfiguracja mechanizmów zabezpieczeń przestrzeni dyskowych (snapshot)
      13. integracja z Systemem Wirtualizacji Serwerów VMware vSphere
      14. wykonanie testów działania nadmiarowości komponentów i poprawności konfiguracji w zakresie połączeń Front-End i odporności na zanik napięcia w jednym źródle zasilania.
   7. Serwery (typ A, typ B i typ C - backup), w tym:
      1. okablowanie sieciowe urządzeń,
      2. podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
      3. uruchomienie i weryfikacja poprawności działania urządzeń,
      4. aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
      5. konfiguracja adresacji IP interfejsów zarządzania,
      6. konfiguracja protokołu synchronizacji czasu NTP,
      7. konfiguracja protokołu rozwiązywania nazw DNS,
      8. podłączenie kart sieciowych LAN (porty 10Gbps) urządzeń do przełączników sieciowych typ A,
      9. weryfikacja poprawności działania połączeń LAN,
      10. wykonanie testów działania nadmiarowości zasilania i odporności na zanik napięcia w jednym źródle zasilania.
   8. Streamer, w tym:
      1. podłączenie urządzeń do sieci zasilania zgodnie z wytycznymi Zamawiającego,
      2. uruchomienie i weryfikacja poprawności działania urządzenia,
      3. aktualizacja oprogramowania układowego do wersji zalecanej przez producenta,
      4. podłączenie urządzenia do zapisu kopii zapasowej do serwera typ C (backup).
2. Wdrożenie oprogramowania do tworzenia kopii zapasowych:
   1. instalacja ww. oprogramowania na serwerze typ C (backup),
   2. instalacja niezbędnych licencji w celu uruchomienia oprogramowania do wykonywania kopii zapasowej,
   3. zaprojektowanie polityk wykonywania kopii zapasowej dla wymaganych wirtualnych maszyn,
   4. wykonanie kopii zapasowej zgodnie z zaprojektowanymi politykami,
   5. weryfikacja poprawności działania wykonanych kopii zapasowych,
   6. wykonanie odtworzenia wybranej wirtualnej maszyny.
3. Usługi w zakresie wdrożenia systemu wirtualizacji serwerów:
   1. Instalacja systemu operacyjnego do wirtualizacji serwerów na urządzeniach serwer typ A i serwer typ B.
   2. Konfiguracja systemu operacyjnego do wirtualizacji serwerów, obejmująca co najmniej:
      1. konfigurację adresu(-ów) IP zarządzania,
      2. synchronizację czasu z serwerem NTP,
      3. konfigurację wirtualnych przełączników sieciowych,
      4. konfigurację przestrzeni dyskowej udostępnionej z dostarczonej macierzy,
      5. wykonanie testu poprawności konfiguracji namiarowości połączeń wirtualnego przełącznika sieciowego poprzez odłączenie jednego z fizycznych interfejsów LAN serwera.
   3. Wdrożenie i konfiguracja systemu zarządzania wirtualizacją serwerów, obejmująca m.in.:
      1. konfigurację adresu(-ów) IP,
      2. synchronizację czasu z serwerem NTP,
      3. konfigurację środowiska obejmującą instancję zainstalowanego oprogramowania serwera wirtualizacji,
      4. integracja uwierzytelniania systemu zarządzania z Active Directory,
   4. Przygotowanie dwóch wirtualnych maszyn zgodnie z wymaganiami Zamawiającego,
   5. Zapewnienie wsparcia podczas migracji aplikacji do nowego środowiska.
4. Usługi w zakresie wdrożenia domeny / usług katalogowych:
   1. Instalacja maszyny wirtualnej w systemie do wirtualizacji serwerów.
   2. Instalacja systemu operacyjnego, w oparciu o który mają być uruchomione usługi.
   3. Aktualizacja oprogramowania systemu operacyjnego do najwyższej rekomendowanej przez producenta wersji.
   4. Uruchomienia usługi domeny.
   5. Uruchomienie usługi serwera DNS.
   6. Uruchomienie usługi serwera DHCP.
   7. Dodanie do domeny dziesięciu (10) przykładowych stacji roboczych.
5. Wdrożenie rozproszonego systemu plików DFS (ang. Distributed File System):
   1. Instalacja dwóch maszyn wirtualnych w systemie do wirtualizacji serwerów.
   2. Instalacja systemu operacyjnego.
   3. Aktualizacja oprogramowania systemu operacyjnego do najwyższej rekomendowanej przez producenta wersji.
   4. Konfiguracja DFS.
6. Opracowanie dokumentacji powykonawczej wdrożonego rozwiązania, zawierającej co najmniej nw. elementy:
   1. Topologia fizyczna sieci LAN oraz SAN.
   2. Topologia logiczna sieci LAN oraz SAN.
   3. Adresacja IPv4.
   4. Konfiguracje protokołów sieciowych.
   5. Konfiguracje sieci VLAN.
   6. Konfiguracje sieci SAN.
   7. Konfiguracje dostarczanych serwerów.
   8. Konfiguracje przełączników sieciowych.
   9. Konfiguracje klastra urządzeń UTM.
   10. Konfiguracje systemu do wirtualizacji serwerów.
   11. Konfiguracje systemu do wykonywania kopii zapasowej.

## Szkolenie dla administratora w zakresie obsługi zakupionego sprzętu

Wykonawca zrealizuje szkolenie dla administratorów (dwie osoby) w siedzibie Zamawiającego. Wymiar czasowy szkolenia – 3 dni po 8 godzin. Szkolenie ma mieć charakter warsztatowy z naciskiem na praktyczne aspekty wykorzystania zakupionego sprzętu, wszelkie omawiane przykłady mają odnosić się do modeli sprzętu będących przedmiotem dostawy. Wykonawca zaproponuje i przedstawi Zamawiającemu szczegółowy program szkolenia uwzględniający nw. zagadnienia:

* Konfiguracja i funkcje administracyjne serwera;
* Konfiguracja i zarządzanie przełącznikiem sieciowym;
* Konfiguracja i zarządzanie urządzeniem dyskowym;
* Projektowanie i wdrażanie wirtualnych sieci lokalnych;
* Tworzenie klastrów wirtualizacyjnych;
* Instalacja, konfiguracja i zarządzanie serwerowym systemem operacyjnym;
* Instalacja, konfiguracja i zarządzanie systemem zarządzania wirtualizacją serwerów;
* Tworzenie i zarządzanie serwerami wirtualnymi;
* Migracja serwerów wirtualnych;
* Instalacja oprogramowania do tworzenia kopii zapasowych;
* Wdrażanie polityki tworzenia kopii zapasowych.

Szkolenie przeprowadzone w języku polskim. Wymagane dostarczenie materiałów zgodnych z programem szkolenia w języku polskim w postaci elektronicznej.