**ZP.271.4.2025 Załącznik nr 8**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

Niniejszy załącznik stanowi szczegółowy opis przedmiotu zamówienia. Zaoferowany przez Wykonawcę sprzęt lub oprogramowanie musi spełniać minimalne wymagania postawione w niniejszym załączniku oraz zostać dostarczony na warunkach określonych poniżej i w projekcie umowy. Realizacja przedmiotu zamówienia składać się będzie z 4 poniżej opisanych etapów:

**ETAP 1 – bezpieczne zasilanie: dostawa, montaż, wdrożenie agregatu i centralnego UPS-a 30KVA**

1. Przygotowanie do instalacji agregatu i UPS-a

* Trasa kablowa w budynku:
* Poprowadzenie przewodu (YKY 5x16 mm2) 24 m
* Przekucie przez ścianę 1 szt.
* Trasa kablowa w terenie:
* Demontaż utwardzenia kostka/asfalt 16 m2
* Wykopy w terenie 33 m
* Podsypka piaskowa (gr. 15 cm) 33 m
* Poprowadzenie przewodu (YKY 5x16 mm2) 66 m
* Obsypanie kabla (gr. 15 cm) 33 m
* Zasypanie ziemią z wykopu z zagęszczeniem 33 m
* Odtworzenie nawierzchni kostka 16 m2
* Agregat:
* Fundament, kostka, uziemienie 1 szt.
* Podłączenie w rozdzielnicy 1 szt.
* UPS:
* Korytka kablowe PCV 70 m
* Poprowadzenie przewodu (YKY 5x16 mm2) 70 m
* Przekucie przez ścianę 4 szt.
* Agregat PDB40RST3 40kVA lub równoważny
* Dostawa oraz rozładunek
* Powiększony zbiornik na 12h
* Skrzynka do montażu zewnętrznego SZR 63A
* Podłączenie agregatu
* Rozszerzenie gwarancji do 36 miesięcy

|  |  |  |  |
| --- | --- | --- | --- |
| **Specyfikacja:** | | | |
|  | | | |
| 1. **Agregat stacjonarny**  |  |  | | --- | --- | | **Rodzaj obudowy** | **Stacjonarna, wyciszona obudowa wykonana z stali, malowana proszkowo z zintegrowanym zbiornikiem paliwa** | | Moc maksymalna (LTP) | Min. 88 kVA / 70 kW | | Moc znamionowa (PRP) | Min. 80 kVA / 64 kW | | Prąd znamionowy | Min. 115 A | | Napięcie znamionowe | 230 / 400 V | | Częstotliwość | Min. 50 Hz | | Pojemność zbiornika paliwa | Min. 150 l | | Czas pracy na pełnym zbiorniku przy 100% obciążeniu | Min. 7 godzin | | Zużycie paliwa przy 100% / 75% / 50% obciążenia w l/h | 18,3 / 13,7 / 9,1 | | Rodzaj oleju | SAE 15W40 | | Ilość oleju w układzie | 16 l | | Rodzaj płynu chłodzącego | Antyfreeze -38 stopni Celsiusa | | Ilość płynu chłodzącego | 23 l | | Liczba obrotów silnika na min. | Min. 1500 | | Ilość układów cylindrów | 4 rzędowe, turbo | | Układ zasilania silnika | Bezpośredni wtrysk | | Maksymalna temperatura gazów spalinowych | 600 stopni Celsiusa | | Stabilizacja obrotów silnika | Elektroniczna | | Rodzaj paliwa | Olej napędowy ON-DIESEL | | Pojemność skokowa silnika | Min, 7 litrów | | Moc silnika (PRP) | Min. 74 kW | | Rodzaj prądnicy | Samowzbudna synchroniczna bez szczotkowa | | Ilość biegunów / typ połączeń | 4 / gwiazda | | Uzwojenie odporne na środowisko | Wilgotne / słone | | Klasa izolacji uzwojeń | Min. H | | Stopień ochrony | Min. IP23 | | Regulacja napięcia | AVR, elektroniczna | | Stabilność napięcia | +/- 1% | | Zawartość THD | Maks. 2% | | Wydajność | Min. 90% | | Fizyczne zabezpieczenia | Wszystkie drzwi serwisowe oraz korek wlewu paliwa zamykane na klucz | | Inne | Kompatybilność z układem SZR/ATS (Samoczynne Załączanie Rezerwy) | | Wymiary | Maks. 266 x 101 x 130 cm | | Masa | Maks. 1450 kg | | Okres pomiędzy wymianami oleju silnikowego | Co 500 motogodzin | | Okres pomiędzy wymianami płynu chłodniczego | Co 1000 motogodzin | | Okres pomiędzy wymianami filtra paliwa | Co 500 motogodzin | | Okres pomiędzy wymianami filtra oleju | Co 500 motogodzin | | Okres pomiędzy wymianami filtra powietrza | Co 500 motogodzin | | Wyposażenie standardowe | - silnik DIESEL  - prądnica  - akumulator  - ładowarka akumulatorów  - zbiornik paliwa  - wibroizolatory silnika i prądnicy  - tłumik z kompensatorem drgań  - wyłącznik mocy  - wyłącznik awaryjny  - grzałka panelu sterowania  - oświetlenie wnętrza  - panel sterowania w języku polskim  - grzałka bloku silnika | | Gwarancja | 36 miesięcy pod warunkiem corocznego przeglądu wykonywanego przez serwis producenta.  Czynności jakie obejmuje przegląd:  - przyjazd serwisu  - wymiana oleju i filtrów oleju  - wymiana filtru powietrza  - wymiana filtrów paliwa  - kontrola i uzupełnienie płynu chłodzącego  - sprawdzenie akumulatorów i alternatora  - sprawdzenie połączeń silnik + prądnica  - kontrola układu: paliwowego, smarowania i chłodzenia  - sprawdzenie połączeń elektrycznych  - sprawdzenie-regulacja paska  - sprawdzenie działania układów sterowania  - pomiar rezystancji izolacji prądnicy  - kontrola układu podgrzewania silnika  - próbna praca zespołu, testy sprawności  - pomiary generowanego napięcia wyjściowego,  - oględziny zewnętrzne instalacji elektrycznej i sterowniczej  -sprawdzenie poprawności działania panelu sterowania | | Usługa wdrożenie | Usługa wdrożenia musi obejmować podłączenie, uruchomienie, testy sprawnościowe wykonana przez certyfikowanego inżyniera | | | | |
| 1. **Centralny UPS EVER POWERLINE GREEN PRO 3/3 30kVA lub równoważny** | | | |
| **Lp.** | **Nazwa komponentu** | **Wymagane parametry techniczne** |
| 1 | 2 | 3 |
| 1. | Model, symbol, producent urządzenia |  |
| 2. | Technologia | online, VFI-SS-111 |
| 3. | Moc wyjściowa | 40kVA/40kW; PF=1 |
| 4. | **Moc bierna pojemnościowa (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)** | **0 var** |
| 5. | **Napięcie wejściowe** | **173 ÷ 485 V AC ± 2 %** |
| 6. | Napięcie wyjściowe (wartość skuteczna) | 3x400 V AC |
| 7. | Częstotliwość napięcia wejściowego (oraz tolerancja) | 45 ÷ 55 Hz ± 1 Hz |
| 8. | Częstotliwość napięcia wyjściowego praca sieciowa / rezerwowa | Synchroniczne / 50Hz ± 0,1 Hz |
| 9. | **Współczynnik szczytu CF** | **4:1** |
| 10. | Parametry styków przekaźników wyjść programowalnych | 1A / 250 V AC / w standardzie NO i NC dla każdego wyjścia |
| 11. | Zniekształcenia prądu wejściowego THDi (bez zewnętrznych układów filtrujących, realizowane za pomocą układu prostownika) | < 3% |
| 12. | Zniekształcenia napięcia wyjściowego THDu | < 2% dla Pmax (liniowe)  < 5% (nieliniowe wg PN EN 62040-3 |
| 13. | **Współczynnik tg φ (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)** | **< 0,4** |
| 14. a | Czas podtrzymania dla obciążenia 40kW | Minimum 4 minuty (w oparciu o minimum 64 szt akumulatorów 12V10Ah zamontowanych wewnątrz UPS) |
| 15. | **Przeciążalność** | **130% - 10min / 160% - 1min / 300% 100ms** |
| 16. | EPO | Wymagane – standard NC |
| 17. | Bypass zewnętrzny | Wymagany (odpowiedni do oferowanego zasilacza, w obudowie naściennej) |
| 18. | Sygnalizacja | akustyczno-diodowa, wyświetlacz LCD, menu w języku polskim i angielskim (do wyboru przez użytkownika) |
| 19. | Język oprogramowania i menu | polski i angielski do wyboru z poziomu interfejsu użytkownika |
| 20. | **Wymagane certyfikaty** | **ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument)** |
| 21. | Komunikacja z urządzeniem | RS232, USB, MODBUS RTU, bezpotencjałowe wyjścia programowalne (min. 4), wejścia sterujące (min. 4), SNMP - dopuszczalna jako opcjonalna karta |
| 22. | Wymiary UPS (wys. x szer. x gł.) | **Nie więcej niż 1151 x 490 x 860 mm** |
| 23. | **Podłączenie zasilania** | **Umiejscowione z tyłu UPS’a, w dolnej części obudowy** |
| 24. | Oprogramowanie do monitorowania pracy zasilacza UPS | Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych w sieci; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów |
| 25. | **Dodatkowe wymagania** | **UPS musi pochodzić z autoryzowanego kanału sprzedaży, wyprodukowane na terenie Unii Europejskiej, nowe, nieużywane, wyprodukowane nie później niż na 2 miesiące przed dostawą** |
| 26. | Serwis producenta | wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty |
| 27. | Podłączenie systemu | Dowóz, rozładunek, transport do wskazanego pomieszczenia, podłączenie systemu zasilania gwarantowanego UPS do przygotowanej instalacji oraz pierwsze uruchomienie i testy rozwiązania. Wskazane usługi muszą zostać wykonane przez serwis producenta. |
| 28. | Inne wymagania gwarancyjne | w przypadku niemożności naprawy urządzenia w trakcie trwania gwarancji na miejscu u klienta podstawiony zostanie bezpłatnie UPS o minimum tych samych, a na pewno nie gorszych parametrach na czas naprawy (podmiana i dostawa na koszt dostawcy lub autoryzowanego serwisu producenta UPS) – oświadczenie producenta |
| 29.b | Gwarancja dodatkowa | Minimum 36 miesięcy elektronika, 18 miesięcy akumulatory, w cenie przegląd okresowy po 2 roku z dojazdem na obiekt |
| 30. | Dokumentacja | Instrukcja w języku polskim |
| 31. | Szkolenie | Przeszkolenie pracownika z zakresu obsługi urządzenia w dniu instalacji. Przedstawienie wykazu obowiązków pracownika w zakresie konserwacji oraz monitoringu urządzenia oraz postępowania na wypadek awarii. |
|  | | | |
| **ETAP 2 – modernizacja serwerowni: dostawa, montaż dodatkowej szafy Rack42U, wykonanie okablowania między szafami, wykonanie okablowania pod 4 dodatkowe AP**   1. Dostawa, montaż dodatkowej szafy Rack42U  * Szafa Rack42U o wymiarach 600x1000, czarna, perforowana wraz z podsufitowym panelem wentylacyjnym wraz z montażem - 2 szt. * Półki stałe, mocowane czteropunktowo, zespół jezdny w postaci 4 kół, listwa zasilająca z uziemieniem – 3 szt. * Dodatkowa listwa zasilająca 2 szt. * Konsola KVM + 8-portowy przełącznik (USB)KVM 1 szt. * Kable KVM USB (~2 m) 4 x * Kable KVM USB (~6 m) 4 x  1. Połączenie między szafami  * Patchpanel 24 porty 4 x * Organizer 4 x * Przewód UTP cat 5e (2000 m) * Koryto PCV 100 x 60 (15 m) * Instalacja okablowania  1. Porządkowanie istniejących szaf RACK 42U  * Patchory 1,5 m * Patchord 3 m 10 x * Organizer 10 x * Koryta PCV 100 x 60 (10m) * Okablowanie AP * Patchpanel 24 porty * Organizer * Patchord 1,5 m 4 x * Przewód UTP (140m)   **ETAP 3 – bezpieczna sieć komputerowa: dostawa i wdrożenie UTM, zarządzanych urządzeń sieci lokalnej (LAN i WiFi) oraz urządzeń do zarządzania i analizy sieci lokalnej**   1. przełącznik sieciowy zarządzalny (np.: FortiSwitch 124F lub równoważny) + wparcie Care i Hezo – **3 x**; 2. przełącznik sieciowy zarządzalny z POE (np.: FortiSwitch 124F POE lub równoważny) + wsparcie Care i Hezo – **1 x**; 3. acces point zarządzalny (np.: FortiAP 231G lub równoważny ) + wsparcie Care Hezo – **4 x;** 4. wdrożenie switch + AP; 5. sprzętowa platforma analiz i kontroli sieci, zarządzania logami, lokalnej (np.: FortiAnalyzer VM lub równoznaczny ) + wsparcie Care + upgrade for 5 GB;   6. UTM FireWall (np.: FortiGate 100F lub równoważny) + wparcie HEZO – **1 x**. Specyfikacja:Przełącznik sieciowy W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.  W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem realizującym funkcję Firewall. Parametry fizyczne platformy  * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. * Zasilanie AC 230V. * Maksymalny pobór mocy: 30 W. * Minimalny zakres temperatury pracy: 0-40ᵒC.  Interfejsy sieciowe - wymagania minimalne Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:   * 24 porty GE RJ-45. * 4 porty 10 GE SFP+.  Zarządzanie  * Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). * Wsparcie dla SNMP w wersjach 1-3 * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. * Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. * Automatycznie wykonywane rewizje konfiguracji.  Parametry wydajnościowe  * Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. * Tablica adresów MAC o pojemności co najmniej 32k wpisów. * Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.  Wymagane funkcje  * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. * Obsługa Jumbo Frames. * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). * Agregacja portów zgodna ze standardem 802.3ad. * Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. * Obsługa routingu statycznego. * Port-mirroring. * Uwierzytelnianie 802.1x na poziomie portu. * Uwierzytelnianie 802.1x w oparciu o adres MAC. * W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. * Obsługa protokołu sFlow.  Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC  1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:  * Centralne zarządzanie konfiguracją urządzenia * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania * Centralne zarządzanie sieciami VLAN. * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. * Automatyczna detekcja i rekomendacje konfiguracji. * Przesyłanie logów na zewnętrzny serwer syslog. * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. * Obsługa białych i czarnych list adresów MAC. * Wykrywanie aplikacji komunikujących się w sieci.  1. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.  Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa  * System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. * System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.  Gwarancja oraz wsparcie System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Rozszerzone wsparcie serwisowe  1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:  * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 podmiotu serwisującego.  Przełącznik sieciowy POE W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.  W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem realizującym funkcję Firewall. Parametry fizyczne platformy  * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. * Zasilanie AC 230V. * Budżet mocy dla portów PoE min.: 370 W. * Maksymalny pobór mocy bez budżetu dla PoE: 85 W. * Minimalny zakres temperatury pracy: 0-40ᵒC.  Interfejsy sieciowe - wymagania minimalne Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:   * 24 porty GE RJ-45.   W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.   * 4 porty 10 GE SFP+.  Zarządzanie  * Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). * Wsparcie dla SNMP w wersjach 1-3 * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. * Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. * Automatycznie wykonywane rewizje konfiguracji.  Parametry wydajnościowe  * Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. * Tablica adresów MAC o pojemności co najmniej 32k wpisów. * Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.  Wymagane funkcje  * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. * Obsługa Jumbo Frames. * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). * Agregacja portów zgodna ze standardem 802.3ad. * Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. * Obsługa routingu statycznego. * Port-mirroring. * Uwierzytelnianie 802.1x na poziomie portu. * Uwierzytelnianie 802.1x w oparciu o adres MAC. * W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. * Obsługa protokołu sFlow.  Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC  1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:  * Centralne zarządzanie konfiguracją urządzenia * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania * Centralne zarządzanie sieciami VLAN. * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. * Automatyczna detekcja i rekomendacje konfiguracji. * Przesyłanie logów na zewnętrzny serwer syslog. * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. * Obsługa białych i czarnych list adresów MAC. * Wykrywanie aplikacji komunikujących się w sieci.  1. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 2. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.  Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa  * System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. * System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.  Gwarancja oraz wsparcie System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Rozszerzone wsparcie serwisowe  1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:  * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 podmiotu serwisującego.   **Access Point**  Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.   1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:  * Temperatura 0–50°C, * Wilgotność 5–90%.  1. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington. 2. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:  * 2.4 GHz 802.11b/g/n, * 5 GHz 802.11a/n/ac/ax, * 2.4/5/6 GHz 802.11a/b/g/n/ac/ax  1. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID. 2. Urządzenie musi być wyposażone w moduł BLE. 3. Urządzenie musi być wyposażone w dwa interfejsy Ethernet: 10/100/1000 Base-TX oraz 100/1000/2500 Base-TX, 4. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. 5. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:  * Tunnel, * Bridge, * Mesh.  1. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. 2. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST). 3. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:    1. MIMO – 2x2,    2. Maksymalna przepustowość dla poszczególnych modułów radiowych:       1. 574 Mbps;       2. 1201 Mbps;       3. 2401 Mbps;    3. Wymagana moc nadawania:       1. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;       2. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;       3. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;    4. Wsparcie dla 802.11n 20/40Mhz HT,    5. Wsparcie dla kanałów 80 i 160MHz,    6. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz.    7. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy, 4. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512; 5. Funkcje dodatkowe:  * OFDMA UL i DL * Spatial Reuse (BSS Coloring) * UL-MU-MIMO * DL-MU-MIMO * Enhanced Target Wake Time (TWT) * Wbudowany analizator widma * Wbudowane mechanizmy WIPS/WIDS  Gwarancja oraz wsparcie Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.  Usługa wdrożenia musi obejmować montaż, podłączenie i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.  **Rozszerzone wsparcie serwisowe**   1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Oferent winien przedłożyć dokumenty:  * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 podmiotu serwisującego.   **Sprzętowa platforma analiz sieci:** Wymagania Ogólne W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.  Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP). Interfejsy, Dysk:  1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB.  Parametry wydajnościowe:  1. System musi być w stanie przyjmować minimum 5 GB logów na dzień. 2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.   W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje: Logowanie  1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:  * Listę najczęściej wykrywanych ataków. * Listę najbardziej aktywnych użytkowników. * Listę najczęściej wykorzystywanych aplikacji. * Listę najczęściej odwiedzanych stron www. * Listę krajów , do których nawiązywane są połączenia. * Listę najczęściej wykorzystywanych polityk Firewall. * Informacje o realizowanych połączeniach IPSec.  1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.  Raportowanie W zakresie raportowania system musi zapewniać:   1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.  Korelacja logów W zakresie korelacji zdarzeń system musi zapewniać:   1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:  * Malware. * Aplikacje sieciowe. * Email. * IPS. * Traffic. * Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.  1. Funkcję zarządzania zdarzeniami z automatyzacją zadań, która może być konfigurowalna za pomocą playbooków składających się z reakcji i sekwencji zautomatyzowanych działań.  Zarządzanie  1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.  * Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.  1. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.  Serwisy i licencje  1. System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. 2. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.  Opisy do wymagań ogólnych  1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.   **UTM FireWall** Wymagania Ogólne System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego.  Redundancja, monitoring i wykrywanie awarii  1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.  Interfejsy, Dysk, Zasilanie:  1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 16 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 2 gniazdami SFP+ 10 Gbps.  1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System jest wyposażony w zasilanie AC.  Parametry wydajnościowe:  1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B. 4. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. 6. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 Gbps. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.  Funkcje Systemu Bezpieczeństwa: W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Analiza ruchu szyfrowanego protokołem SSH. 13. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 14. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).  Polityki, Firewall  1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * Nuage Networks VSP. * OpenStack. * VMware vCenter (ESXi). * VMware NSX. * VMware NSX.Nutanix. * VMware NSX.IBM Cloud. * **Kubernetes.**  Połączenia VPN  1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:  * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20 oraz 21. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Dynamiczne zestawianie tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.  Routing i obsługa łączy WAN W zakresie routingu rozwiązanie zapewnia obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.  Funkcje SD-WAN  1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). 3. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu. 4. Rozwiązanie powinno wspierać funkcję Forward Error Correctionm na tunelach IPSec. 5. Funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.  Zarządzanie pasmem  1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.  Ochrona przed malware  1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS. 3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.  Ochrona przed atakami  1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.  Kontrola aplikacji  1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).  Kontrola WWW  1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 9. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 10. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. 11. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo. 12. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.  Uwierzytelnianie użytkowników w ramach sesji  1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.  Zarządzanie  1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.  Logowanie  1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4. Możliwość włączenia logowania per reguła w polityce firewall. 5. System zapewnia możliwość logowania do serwera SYSLOG. 6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.  Testy wydajnościowe oraz funkcjonalne Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. Serwisy i licencje Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:   * Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.  Gwarancja oraz wsparcie System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Rozszerzone wsparcie serwisowe AHB/SOS System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy.  System jest objęty usługą wsparcia technicznego świadczoną przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:   * Wsparcie telefoniczne zespołu certyfikowanych inżynierów. * Pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu. * Doradztwo w zakresie konfiguracji. * Zdalne wsparcie techniczne. * Pomoc w zakładaniu zgłoszeń serwisowych u producenta. * Pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą). * Przygotowanie urządzenia do zdalnej konfiguracji. * Zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika. * Minimum 5 zdalnych rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań użytkownika. * Minimum dwa razy w roku zdalny przegląd konfiguracji i logów urządzenia wraz z raportem zaleceń na bazie dobrych praktyk inżynierskich. * Minimum dwa razy w roku zdalna aktualizacja oprogramowania zgodnie z zaleceniami producenta i dobrych praktyk inżynierskich. * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 podmiotu serwisującego.   Usługa wdrożenia musi obejmować montaż, podłączenie i uruchomienie oferowanego sprzętu w siedzibie zamawiającego. Wdrożenie powinno być przeprowadzone przez certyfikowanego inżyniera Wykonawcy. Po wdrożeniu należy przeprowadzić szkolenie wskazanego pracownika Zamawiającego w czasie co najmniej 5 godzin.  Zakres wdrożenia UTM:   * Konfiguracja sieci (interfejsy i routing). * Konfiguracja firewalla (limit reguł – 20). * Konfiguracja NAT (limit reguł – 10). * Konfiguracja IPS – zgodnie z wymaganiami klienta. * Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy. * Konfiguracja dostawców Internetu (maksymalnie 2 dostawców). * Konfiguracja VPN: * IPSec Site-to-Site (limit 2 tuneli) – zgodnie z otrzymanymi od klienta parametrami tuneli. * Client-to-Site – konfiguracja urządzenia i jednej wzorcowej stacji klienckiej. * Integracja usługi Active Directory z urządzeniem FortiGate, integracja obejmująca [m.in](http://m.in/).: * Uwierzytelnianie użytkowników przy połączeniach VPN z konfiguracją 2FA na email. * Konfigurację profili bezpieczeństwa również dla ruchu zaszyfrowanego w celu pełnej analizy zagrożeń. * Konfigurację integracji pozwalającej na zarządzanie ruchem do zasobów sieci oraz Internetu w oparciu o przynależność do grup w Active Directory. Polityki powinny działać również w momencie przepinania się między sieciami fizycznymi np. LAN, WiFi   Zakres wdrożenia switch:   * Konfiguracja portu/agregacji. * Rejestracja oraz upgrade urządzenia. * Konfiguracja VLAN na interfejsie urządzenia. * Weryfikacja działania VLAN na portach urządzenia.   Zakres wdrożenia access point:   * Konfiguracja SecurityFabric; * Rejestracja oraz upgrade urządzenia; * Konfiguracja Profilu WiFi; * Konfiguracja SSID oraz zasad bezpieczeństwa. | | | |
| **ETAP 4 – bezpieczna chmura: dostawa i wdrożenie sprzętu, tj.: serwery (2 x), rozbudowa obecnej macierzy dyskowej, licencje serwerowe WS 2022 i SQL, licencje User Cal, wdrożenie „klastra pracy awaryjnej”, wdrożenie „domeny”, połączenie wszystkich komputerów i przeniesienie zasobów do nowego środowiska, rozbudowa systemu antywirusowego z centralnym zarządzaniem, dostawa dodatkowej macierzy i wdrożenie zintegrowanego backupu dla całych zasobów, dostawa i wdrożenie infrastruktury komputerowej do monitorowania i ewidencji zasobów.**  **Serwery, licencje**   1. Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń odnawianych, demonstracyjnych lub powystawowych. 2. Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta. 3. Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta serwera. 4. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta. 5. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej. 6. Urządzenia na etapie dostawy producent, a Zamawiający nie mogą podlegać modyfikacjom.   **Dwa serwery o poniższej konfiguracji:**   |  |  | | --- | --- | | **Nazwa elementu, parametru lub cechy** | **Opis wymagań Serwerów** | | **Obudowa** | Do instalacji w szafie Rack 19”, wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. | | **Procesor** | Zainstalowany jeden procesor 16-rdzeniowe, klasy x86, dedykowany do pracy z zaoferowanym serwerem, taktowane zegarem min. 2.9 GHz (częstotliwość bazowa) umożliwiające osiągnięcie wyniku minimum 35 250 punktów w teście PassMark dostępnym na stronie internetowej: <https://www.cpubenchmark.net/multi_cpu.html> z dnia 30.07.2024 lub nowszego. | | **Płyta główna** | Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon).  Wsparcie dla procesorów do 40 rdzeni o mocy do 270W. | | **Pamięć operacyjna** | Zainstalowane minimum 128GB pamięci RAM o częstotliwości 3200MHz w kościach 32 GB. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 1024GB RAM bez zmiany kości.  Możliwość instalacji pamięci nieulotnych Intel Optane PM200. | | **Zabezpieczenie pamięci** | Memory mirroring, ECC, SDDC, ADDDC | | **Procesor Graficzny** | Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz.  1 port VGA z tyłu serwera.  Opcjonalny 1 port VGA na przednim panelu serwera. | | **Rozbudowa dysków** | Możliwość instalacji min 8 dysków 2.5”.  Zainstalowane minimum dwa dyski SSD 2,5” hot swap, o pojemności min 480GB.  Kontroler RAID z obsługą poziomów 1,10,5,50,6,60 z min. 2 GB pamięci cache z podtrzymaniem typu flash. | | **Zasilacz** | Minimum dwa redundantne zasilacze o mocy minimum 1100W z certyfikatem Titanium. | | **Interfejsy sieciowe** | Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.  Dwie dwuportowe karty 10/25Gb SFP28  Dostarczone przez producenta serwera dwie wkładkami 10Gb SFP+ SR. | | **Dodatkowe sloty I/O** | Obudowa z obsługą do 2 slotów PCIe x16.  Dodatkowy port na kartę OCP. | | **Dodatkowe porty** | Min. 5x USB 3.2, VGA | | **Chłodzenie** | Redundantne wentylatory N+1 | | **Zarządzanie** | Możliwość zdalnego zarządzania serwerem, udostępniania zdalnej konsoli graficznej i podłączania zdalnych napędów.  Opcjonalna Licencja na zarządzanie farmą serwerów tego samego typu – pozwalająca na automatyzację zadań administratora. | | **Funkcje zabezpieczeń** | Hasło włączania, hasło administratora, moduł TPM (wspierający TPM 2.0). Możliwość użycia funcji Secure Boot. Opcjonalna przednia obudowa zamykana na klucz. Opcjonalny czujnik otwarcia obudowy. | | **Urządzenia hot swap** | Dyski twarde, zasilacze, wentylatory. | | **Diagnostyka** | Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, a także nietypowych temperatur serwera i komponentów wewnętrznych. | | **Systemy operacyjne** | Wsparcie dla systemów Windows Server 2016, 2019, 2022, VMware ESXi 7.0, 8.0 SUSE Linux 12 i 15, Redhat Linux (minimum w najnowszej i poprzedniej wersji systemu ) | | **Gwarancja** | 5 lat serwisu producenta on-site. Wymagana jest reakcja serwisu w trybie „NBD”. Dyski uszkodzone pozostają u Zamawiającego.  Serwis świadczony bezpośrednio przez producenta sprzętu. Możliwość rozszerzenia serwisu o serwis z 24h gwarantowanym czasem naprawy. Możliwość rozszerzenia serwisu o serwis z lepszym SLA (np. 8 lub 12h) – również jako serwis producenta. |   **Licencje:**  Serwery muszą zostać dostarczone z licencjami dołączonymi przez producenta oferowanych serwerów:   * dla każdego z serwerów osobna licencja Windows Server 2022 Standard pozwalająca na uruchomienie 4 maszyn wirtualnych * łącznie 70 licencji na użytkownika Windows Server 2022 (Windows Server 2022 User CAL) * jedną licencję Microsoft SQL Server 2022 Standard wraz z 50 licencjami Microsoft SQL Server 2022 CAL na użytkownika   **Rozbudowa posiadanej macierz:**  Dla posiadanej przez zamawiającego macierzy Lenovo ThinkSystem DE2000H Gen2 (4C57A14367)należy dostarczyć fabrycznie nowe, pochodzące z autoryzowanego kanału sprzedaży producenta Lenovo:   * 8 dysków Lenovo ThinkSystem DE Series 1.2TB 10K 2.5" HDD 2U24 (4XB7A14112) * 12 dysków Lenovo ThinkSystem DE Series 960GB 1DWD 2.5" SSD 2U24 (4XB7A74948) * 2 karty Lenovo ThinkSystem DE2000/4000 HIC, 10/25GbE iSCSI,4-ports (4C57A14369, po jednej na każdy kontroler) * 6 kabli Lenovo 3m Passive 25G SFP28 DAC Cable   **Montaż, konfiguracja, uruchomienie, wdrożenie:**   * Usługa musi obejmować instalację w posiadanej macierzy Lenovo dostarczonych dysków HDD oraz SSD, a także wymianę w kontrolerach portów na 10/25GbE iSCSI. * Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego, a także odpowiednie redundantne połączenie trzech serwerów z macierzą. * Na zaoferowanych urządzeniach oraz posiadanej macierzy musi zostać przeprowadzona aktualizacja firmware’u. Urządzenia (serwery oraz macierz) muszą zostać skonfigurowane zgodnie z najlepszymi praktykami (klaster HA na trzech serwerach i macierzy), a na dostarczonych serwerach zainstalowane zostanie oprogramowanie do wirtualizacji (Windows Server Hyper-V). * Wykonawca dokona migracji 3 maszyn wirtualnych zamawiającego z systemem Windows Server 2022 z obecnego serwera na utworzony z trzech dostarczonych serwerów i posiadanej przez zamawiającego macierzy klaster. * Wykonawca utworzy nową maszynę wirtualną z systemem Windows Server 2022 na której uruchomi usługę kontrolera domeny wraz z usługami wymaganymi do jej prawidłowego działania. * Wykonawca musi utworzyć konta dla wszystkich użytkowników (maksymalnie 70 kont) oraz skonfigurować politykę domenową z uwzględnieniem wytycznych Zamawiającego. * Wszystkie komputery zamawiającego z systemem w wersji Professional (maksymalnie 70 urządzeń) zostaną przez wykonawcę podłączone do domeny, a na każdym komputerze przeprowadzona zostanie migracja profilu lokalnego do domenowego połączona z konfiguracją dla tych urządzeń profili mobilnych. * Na posiadanym przez zamawiającego serwerze wykonawca zainstaluje wirtualizator (Hyper-V) oraz utworzy maszynę wirtualną z systemem Windows Serwer 2019/2022 (licencję posiada zamawiający) na której zostanie skonfigurowany zapasowy kontroler domeny. * Wszystkie wymienione prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym poza godzinami pracy urzędu oraz w weekendy. * Podczas wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów. * Po wdrożeniu zostanie przeprowadzone szkolenie z wdrożonych systemów obejmujące przynajmniej omówienie konfiguracji i funkcji Hyper-V, konsoli administracyjnej, zarządzania domeną oraz najlepszych praktyk.   Czas szkolenia minimum 8 godzin.  **Rozbudowa systemu antywirusowego**  Odnowienie i migracja obecnego oprogramowania antywirusowego ESET PROTECT Entry do poziomu ESET PROTECT Enterprise, w ilości 70 stanowisk na okres 30.06.2026.  Usługa wdrożenia musi obejmować instalację, uruchomienie i konfigurację oprogramowania antywirusowego w siedzibie zamawiającego. Usługa musi być wykonana przez certyfikowanego inżyniera wykonawcy.  Po wdrożeniu zostanie przeprowadzone szkolenie dla wskazanego pracownika zamawiającego w czasie co najmniej 5 godzin.  Zakres wdrożenia:   1. Instalacja i konfiguracja konsoli zdalnego zarządzania ESET Protect. 2. Przygotowanie paczek instalacyjnych oprogramowania klienckiego ESET wraz z agentem. 3. Konfiguracja maksymalnie trzech polityk. 4. Stworzenie przykładowych grup statycznych/dynamicznych. 5. Instalacja wcześniej przygotowanej paczki klienta wraz z agentem. 6. Skonfigurowanie usługi sandbox. 7. Instalacja i konfiguracja szyfrowania pełnej powierzchni dysku na maksymalnie jednej stacji (stacja robocza nie może być zaszyfrowana innym rozwiązaniem do szyfrowania). 8. Weryfikacja czy zostały przypisane odpowiednie polityki/konfiguracja. 9. Weryfikacja poprawności instalacji. 10. Wdrożenie serwera ESET Inspect. 11. Wdrożenie bazy danych na serwerze. 12. Konfiguracja bazy danych MySQL. 13. Wdrożenie konektorów ESET Inspect Connector. 14. Przygotowanie polityki połączeniowej i zaaplikowanie dla stacji końcowych z zainstalowanym konektorem. 15. Stworzenie maksymalnie 3 wyjątków dla rozwiązania ESET Inspect.   **Dostawa dodatkowej macierzy i wdrożenie zintegrowanego backupu**  Dostarczenie i wdrożenie rozwiązania do backupu składającego się z macierzy, oprogramowania do backupu oraz usługi montażu, instalacji, konfiguracji i wdrożenia.  System powinien umożliwić archiwizację 70 stacji roboczych oraz 4 hostów (Hyper-V). Licencja w formie subskrypcji na 2 lata.  Oferowane rozwiązania muszą spełnić poniższe minimalne wymagania.  **Macierz:**   1. Urządzenia muszą być fabrycznie nowe, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych. 2. Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta. 3. Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta serwera. 4. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta. 5. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej. 6. Urządzenia na etapie dostawy producent, a zamawiający nie mogą podlegać modyfikacjom**.**  |  |  |  | | --- | --- | --- | | **Lp.** | **Nazwa parametru** | **Minimalna wartość parametru** | |  | Obudowa | Macierz musi być dostarczona ze wszystkimi komponentami do instalacji w szafie rack 19''. Obudowa umożliwiająca instalację min. 12 dysków 3,5” z możliwością wkładania i wyjmowania, bez wyłączania macierzy (dyski typu Hot Swap) | |  | Pojemność: | Macierz musi zostać dostarczona w konfiguracji zawierającej minimum:  - 8 dysków 12 TB 7.2K 3.5" NL-SAS HDD.  Macierz musi wspierać dyski:  - SSD: od 960GB do 15.36TB  - SAS: od 1.2TB do 2.4TB  - NL-SAS: od 4TB do 22TB.  Macierz musi mieć możliwość rozbudowy do minimum 84 dysków hot-swap”.  Macierz musi być macierzą umożliwiającą jednoczesną konfigurację dysków SSD i SAS. | |  | Kontroler | Dwa kontrolery macierzy wyposażone w przynajmniej 8GB cache każdy. pracujące w trybie active-active i udostępniające jednocześnie dane blokowe za pośrednictwem protokołu SFP28 o przepustowości min. 25Gb. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników.  W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash. Zawartość cache musi być mirrorowana (kopia lustrzana) między kontrolerami. | |  | Interfejsy | Oferowana macierz musi posiadać minimum:  - 4 porty iSCSI 10/25 Gb/s- na kontroler, wraz z 2 kablami 25G SFP28 DAC min 3m dostarczonymi przez producenta.  - 1 porty RJ-45 1000 Mb Ethernet typu out-of-band management, na kontroler.  - 2 porty SAS 12Gb/s do podłączenia dodatkowych półek, na kontroler.  Macierz musi pozwalać na wymianę 4 portów 10/25Gb iSCSI SFP28 na 4 porty 16/32Gb FC SFP lub 4 porty SAS 12Gb bez potrzeby wymiany kontrolera macierzy. | |  | RAID | Kontrolery macierzy muszą umożliwiać konfigurację dysków w RAID: 0, 1, 5, 6, 10. Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 84 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych. | |  | Obsługiwane protokoły | Macierz musi obsługiwać protokół iSCSI. Możliwość zmiany karty HIC i obsługa SAS 12Gb, FC 8/16/32Gb | |  | Inne wymagania | Macierz musi posiadać wsparcie dla systemów:  Microsoft Windows Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); VMware vSphere.  Macierz musi posiadać funkcjonalność wykonywania minimum 128 kopii migawkowych typu copy-on-write, z możliwością rozbudowy do 512 kopii migawkowych na system. Macierz musi posiadać funkcjonalność replikacji asynchronicznej.  Macierz musi mieć możliwość replikacji danych po FC lub IP w trybie asynchronicznym.  Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.  Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 512 partycji.  Macierz musi posiadać funkcjonalność thin provisioning.  Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji.  Macierz musi posiadać oprogramowanie pozwalające na integrację z VMware vCenter.  Macierz musi zapewniać możliwość szyfrowania danych przy użyciu dysków typu FIPS SSD. Realizacja procesu szyfrowania i zarządzania kluczem może się odbywać przez kontrolery macierzy lub zewnętrzne urządzenia i oprogramowanie do zarządzania kluczami.  Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 4 TB z wykorzystaniem dysków SSD. | |  | Gwarancja i serwis | 5 lat serwisu producenta on-site. Wymagana jest reakcja serwisu w trybie „NBD”. Dyski uszkodzone pozostają u Zamawiającego.  Dostarczony system musi posiadać również 5 lat subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. |   **Rozbudowa posiadanego serwera:**  Dla posiadanego przez zamawiającego serwera Lenovo SR630 należy dostarczyć fabrycznie nową, pochodzącą z autoryzowanego kanału sprzedaży producenta Lenovo kartę sieciową ThinkSystem Broadcom 57414 10/25GbE SFP28 2-port Ethernet Adapter    **Oprogramowanie do backupu:**  Dostarczone oprogramowanie musi pozwalać na backup 70 stacji roboczych oraz 4 hostów Hyper-V.  Dostarczone oprogramowanie musi być w formie subskrypcji na 24 miesiące.  Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk stacji roboczych.   1. Oprogramowanie musi wspierać fizyczne komputery z systemem operacyjnym Windows XP i nowsze oraz systemy macOS. 2. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  * Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. * Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). * Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. * Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). * Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym Windows. * Zdalne uaktualniania agentów kopi zapasowych. * Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.  1. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  * Kopie zapasowe całych dysków i partycji. * Kopie zapasowe wybranych plików i folderów. * Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. * Zapis kopi zapasowych na udziały sieciowe. * Zapis kopi zapasowych na serwer SFTP. * Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana. * Szyfrowanie plików kopi zapasowych. * Wsparcie dla technologii VSS. * Kompresja plików kopi zapasowych. * Replikacja kopi zapasowych na kolejny nośnik (dysk, magazyn chmurowy).  1. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:  * Odtworzenie całej maszyny (Windows, Mac) – tzw. Bare Metal Restore. * Odtworzenie całej maszyny (Windows, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. * Odtworzenie poszczególnych plików i folderów.  1. Dodatkowe wymagania związane ochroną danych (dla poniższych funkcjonalności wymagane wsparcie dla systemu Windows 7 i nowsze):  * Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware  w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń. * Wbudowana ochrona antywirusowa i antymalware. * Mechanizm ochrony przed exploitami. * Filtrowanie adresów URL. * Zarządzanie produktem antywirusowym Windows Defender i Microsoft Security Essentials. * Funkcja otrzymywania informacji o nowych zagrożeniach wraz ze wskazaniem zadań do wykonania dla konkretnego zagrożenia (m.in instalacja poprawki, wykonanie skanowania stacji). * Mechanizm badania zdrowia dysku. * Mechanizm ciągłej ochrony (backupu) plików zapisywanych w wybranych aplikacji lub lokalizacji. Funkcja ta musi co najmniej wspierać aplikacje z kategorii dokumentów (m.in Office, LibreOffice), inżynierii (Autocad) oraz z możliwością wskazania niestandardowej aplikacji. * Filtrowanie stron na podstawie kategorii stron.  1. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem powinna spełniać poniższe wymagania:  * W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta. * W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu * Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich repliki muszą być przechowywane na terenie Polski. * Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie zapasowe) przy użyciu technik szyfrowania, minimum AES-256. * Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w środowiskach programistycznych lub testowych. * Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co najmniej raz w roku. * Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana zgodnie z podejściem N+1 (to, co niezbędne +1). * Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie. * Przestrzeń chmurowa dostarczana wraz z oprogramowaniem to minimum 50GB w ramach jednej licencji, na cały okres jej trwania.  1. Wymagania co do modelu licencjonowania rozwiązania:  * Model licencjonowania oparty na maszynach fizycznych – brak limitów na chronioną ilość danych  i aplikacji.   Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk wirtualizacyjnych.   1. Oprogramowanie musi wspierać co najmniej systemy operacyjne:  * Dla hosta: * VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0. * Hyper-V. * Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, * Red Hat Virtualization 4.0, 4.1. * Linux KVM. * Oracle VM Server 3.0, 3.3, 3.4. * Scale Computing Hypercore 8.8, 8.9, 9.0, 9.1, 9.2, 9.3 * Dla maszyn wirtualnych: Windows XP (SP3) i nowsze. * Windows Server 2003 i nowsze. * Windows SBS 2011/2008, 2003/2003R2. * Windows Storage Server 2012/2012R2, 2008R2/2008/2003. * Windows MultiPoint Server 2012/2011/2010. * Linux OS. * macOS.  1. Zarządzanie systemem kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności: Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z  * Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania systemem z poziomu urządzenia mobilnego). * Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT. * Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem). * Możliwość zdalnej instalacji agentów kopi zapasowych z poziomu konsoli cyberochrony na maszynach z systemem operacyjnym Windows. * Zdalne uaktualniania agentów kopi zapasowych. * Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych.  1. Wykonywanie kopii zapasowych musi posiadać, co najmniej poniższe funkcjonalności:  * Kopie zapasowe całych dysków i partycji. * Kopie zapasowe wybranych plików i folderów. * Kopia zapasowa udziałów sieciowych * Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi). * Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory). * Kopie zapasowe hostów Hyper-V i VMWare ESXi. * Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych. * Zapis kopi zapasowych na udziały sieciowe. * Zapis kopi zapasowych na serwer SFTP. * Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której * Wyszukiwanie plików w kopiach zapasowych. * Szyfrowanie plików kopi zapasowych. * Wsparcie dla technologii VSS. * Kompresja plików kopi zapasowych. * Replikacja kopii zapasowych na kolejny nośnik (dysk, magazyn chmurowy).  1. Oprogramowanie musi umożliwiać odtwarzanie kopii zapasowych w oparciu o co najmniej:    * Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore.    * Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie.    * Odtworzenie całej maszyny wirtualnej.    * Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej    * Odtworzenie poszczególnych plików i folderów.    * Granularne odtwarzanie baz danych Microsoft Exchange.    * Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości    * Wyszukiwanie i podgląd odtwarzanych wiadomości email.    * Granularne odtwarzanie baz danych Microsoft SQL.    * Granularne odtwarzanie witryn i plików Microsoft SharePoint.    * Odtwarzanie kontrolerów domeny Microsoft Active Directory.    * Przywracanie przyrostu względem danych, które już się znajdują na dysku na który przywracana jest kopia zapasowa.    * Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy. 2. Dodatkowe (obowiązkowe) wymagania związane ochroną danych:    * Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń.    * Wbudowana ochrona antywirusowa i antymalware.    * Mechanizm ochrony przed exploitami.    * Filtrowanie adresów URL.    * Zarządzanie produktem antywirusowym Windows Defender i Microsoft Security Essentials.    * Funkcja otrzymywania informacji o nowych zagrożeniach wraz ze wskazaniem zadań do wykonania dla konkretnego zagrożenia (m.in instalacja poprawki, wykonanie skanowania stacji).    * Mechanizm badania zdrowia dysku.    * Mechanizm ciągłej ochrony (backupu) plików zapisywanych w wybranych aplikacji lub lokalizacji. Funkcja ta musi co najmniej wspierać aplikacje z kategorii dokumentów (m.in Office, LibreOffice), inżynierii (Autocad) oraz z możliwością wskazania niestandardowej aplikacji.    * Skanowanie oprogramowania celem poszukiwania podatności. Podatności wypisane muszą być z minimum informacjami takimi jak nazwa produktu który zawiera podatność, maszyny na których znaleziono takie oprogramowanie, stopień ważności w skali CVSS.    * Filtrowanie stron na podstawie kategorii stron. 3. Przestrzeń chmurowa dostarczana wraz z oprogramowaniem musi spełniać poniższe   wymagania:   * W przypadku uzyskania uzasadnionej pewności, że doszło do naruszenia * bezpieczeństwa, producent oprogramowania bez zbędnej zwłoki dostarczy informacje o takowym naruszeniu na adres e-mail podany podczas rejestracji konta. * W przypadku wyżej wymienionego naruszenia, producent podejmie kroki, aby * udokumentować, naprawić i zminimalizować skutki naruszenia bezpieczeństwa w odniesieniu do danych osobowych oraz aby zapobiec jego powtórzeniu. * Kopie zapasowe wykonywane do dostarczonej przestrzeni chmurowej oraz ich * repliki muszą być przechowywane na terenie Polski. * Producent przechowuje dane osobowe klienta (dane osobowe oraz kopie * zapasowe) przy użyciu technik szyfrowania, minimum AES-256. * Producent nie wykorzystuje danych osobowych klienta bez anonimizacji w * środowiskach programistycznych lub testowych. * Producent oprogramowania przeprowadza okresowe oceny ryzyka i przeglądy co * najmniej raz w roku. * Infrastruktura (chmurowy magazyn kopii zapasowych) jest zaprojektowana * zgodnie z podejściem N+1 (to, co niezbędne +1). * Producent oprogramowania jest zgodny z standardem bezpieczeństwa ISO 27001 lub SOC 2, a magazyn kopii zapasowych musi być zgodny z certyfikatami ISO 9001, ISO 27001 oraz certyfikację DCOS na minimum 4 poziomie.  1. Wymagania co do modelu licencjonowania rozwiązania:  * Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji).   **Montaż, konfiguracja, uruchomienie:**   * Usługa wdrożenia musi obejmować montaż i uruchomienie oferowanego sprzętu w siedzibie zamawiającego lub jednostce wskazanej przez zamawiającego, * W posiadanym przez zamawiającego serwerze Lenovo wykonawca będzie musiał zainstalować dostarczoną kartę sieciową oraz połączyć serwer redundantnie z dostarczoną macierzą, * Na posiadanym przez zamawiającego serwerze wykonawca będzie musiał zainstalować wirtualizator (Hyper-V) oraz utworzyć maszynę wirtualną z systemem Windows Serwer 2019/2022 (licencję posiada zamawiający), * Na utworzonej maszynie wirtualnej wykonawca zainstaluje oraz skonfiguruje oferowane oprogramowanie do backupu (wraz z konsolą zarządzającą wdrażanym systemem) zgodnie z wytycznymi producenta oprogramowania, * Na zaoferowanej macierzy musi zostać przeprowadzona aktualizacja firmware’u. Urządzenie zostanie skonfigurowane zgodnie z najlepszymi praktykami, pod katem używania go jako miejsce przechowywania kopii dla zaoferowanego oprogramowaniem do backupu, * Wykonawca zainstaluje na wszystkich stacjach klienckich (do 70 stacji) dostarczane oprogramowanie do backupu oraz skonfiguruje na nich zadania backupu z uwzględnieniem wytycznych zamawiającego oraz najlepszych praktyk, * Wykonawca zainstaluje na wszystkich hostach wirtualizacji (4 hosty Hyper-V) dostarczane oprogramowanie do backupu oraz skonfiguruje na nich zadania backupu z uwzględnieniem wytycznych zamawiającego oraz najlepszych praktyk, * Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, poza godzinami pracy urzędu). * Po wdrożeniu zostanie przeprowadzone szkolenie z wdrożonych systemów obejmujące przynajmniej omówienie konfiguracji i funkcji konsoli administracyjnej oprogramowania do backupu, procesu odzyskiwania danych oraz najlepszych praktyk dla rozwiązań backupowych. Czas szkolenia minimum 4 godziny.   **Zakup i wdrożenie systemu do monitorowania i ewidencjonowania zasobów**  Oprogramowanie posiada budowę modułową, składa się z serwera zarządzającego, zdalnych konsoli oraz Agentów. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana jest przy użyciu szyfrowanego protokołu TLS 1.2. Program umożliwia zmianę portu komunikacyjnego wykorzystywanego przez konsolą zarządzającą.  Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwanym użytkownikiem. Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (PostgreSQL w wersji 12) dzięki czemu nie jest objęty limitem ilości danych, baza danych jest rozwiązaniem darmowym niewymagającym dodatkowego licencjonowania. Instalacja Serwera oraz Konsol zarządzających wymaga 64-bitowego systemu operacyjnego Windows.  Dane, które dotyczą działań pracownika na komputerze, a więc: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., są odseparowane od danych stricte technicznych tj. informacji o stacji roboczej. Są one również grupowane w osobnym, dedykowanym oknie. Pozwala to na, zgodne z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.  Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęty jest kontrolą na poziomie wybranych Administratorów – w programie można nadawać kontom administracyjnym różne poziomy dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników. Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do Opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym administratorów, może być synchronizowana z Active Directory, również przez szyfrowane połączenie LDAPS.  Program umożliwia konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityk pozawala na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.  Program zawiera mechanizmy uwierzytelniania logowań administratorów do konsoli z wykorzystaniem weryfikacji dwuskładnikowej (MFA). Kod autoryzacyjny może być wysyłany za pomocą e-mail i/lub SMS. W weryfikacji MFA można skonfigurować okres, po którym należy ponownie zautoryzować logowanie. W przypadku awarii autoryzacja logowania może być pominięta tylko w lokalnej konsoli serwera.  Producent został wyróżniony znakiem jakości CYBERSECURITY MADE IN EUROPE przyznawanym przez Europejską Organizację ds. Cyberbezpieczeństwa (ECSO).  MONITOROWANIE INFRASTRUKTURY (BEZAGENTOWO) obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:   * wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping * wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) * wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci * wizualizacji urządzeń na mapach z funkcją siatki umożliwiającej korygowanie pozycji ikon na mapie do najbliższej linii siatki * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. * wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku * wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze * wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie * wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny * zablokowania mapy urządzeń przed przypadkową edycją * serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów * serwerów pocztowych: * program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty * program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza zakresem) * program ma możliwość wykonywania operacji testowych * program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa * monitorowania serwerów WWW i adresów URL * cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS * obsługi szyfrowania SSL/TLS w powiadomieniach e-mail * obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID * obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych * monitoringu routerów i przełączników wg: * zmian stanu interfejsów sieciowych * ruchu sieciowego * podłączonych stacji roboczych – graficzna prezentacja panelu switcha * ruchu generowanego przez podłączone do portów stacje robocze * serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie * wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu * monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano * zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny * wydajności systemów Windows: * obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy   Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.  Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitowego, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0  Program ma możliwość integracji ze sprzętową bramką GSM w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP).  W ZAKRESIE INWENTARYZACJI program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:  1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp.  2. Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe.  3. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade.  4. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji.  5. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd.  6. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiejkolwiek zmiany konfiguracji sprzętowej komputera.  7. Umożliwia odczytanie numeru seryjnego (klucze licencyjne).  8. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych.  9. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp.  10. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu).  11. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane.  Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:   * przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, * przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, * tworzenia powiązań między zasobami a urządzeniami, * tworzenia powiązań między zasobami a kontami użytkowników (zarówno lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych, * wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, * definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, * np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, * określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, * określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, * masową edycję atrybutów zasobów, * definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, * importu danych z zewnętrznego źródła (.CSV), * przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., * tworzenia powiązań między zasobami a dokumentami w relacji 1:N, * oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., * ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, * generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, * przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, * konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, * konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, * archiwizacji i porównywania audytów zasobów, * tworzenia kodów kreskowych dla zasobów, * drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, * inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, * możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, * inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), * definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnie licencja/gwarancja”).   Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:  1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP.  2. Informacje o aplikacjach używanych w organizacji.  3. Tworzenie własnych wzorców aplikacji.  4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp.  5. Informacje o komputerach, na których aplikacja została wykryta.  6. Zarządzanie posiadanymi licencjami.  7. Wskazywanie osób odpowiedzialnych za licencję.  8. Wskazanie użytkowników licencji.  9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N.  10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu.  11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych.  12. Zarządzanie posiadanymi licencjami: raport zgodności licencji.  13. Możliwość przypisania do programów numerów seryjnych, wartości itp.  Okna audytowe posiadają możliwość filtrowania elementów per oddział.  PROGRAM UMOŻLIWIA REALIZACJĘ ZDALNEJ POMOCY UŻYTKOWNIKOM. W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połączenia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.  W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.  Moduł ten zawiera również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na:  ✓ zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej  ✓ rozmowy również między „zwykłymi” użytkownikami  ✓ przesyłanie plików między rozmówcami w trybie online  ✓ tworzenie pokojów tematycznych, rozmów grupowych  ✓ oznaczanie kontaktów jako „ulubionych” na liście kontaktów  ✓ uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku  ✓ może być wyświetlany w trybie jasnym lub ciemnym  W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.  Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym.  Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.  Moduł pomocy zdalnej umożliwia również:   * pobieranie listy użytkowników z Active Directory, * wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, * zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, * zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, * zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, * zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, * tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO, * automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, * definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, * przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, * procesowanie zgłoszeń użytkowników z wiadomości e-mail, * eksportowania listy zgłoszeń do plików CSV i XLSX, * integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, * tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych * kategorii zgłoszeń, * wykonywanie operacji na wielu zgłoszeniach równocześnie, * dołączanie załączników do zgłoszeń, * rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, * szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, * wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, * zrzuty ekranowe (podgląd pulpitu), * zdalną modyfikację rejestrów, * dystrybucję oprogramowania przez Agenty, * definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami, * przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników, * dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), * zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, * możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, * możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, * planowanie nieobecności pracowników helpdesk, * obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, * generowanie raportów obsługi helpdesk, * zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), * zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), * wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.   Wdrożenie, uruchomienie i szkolenie musi być przeprowadzone w siedzibie Zamawiającego. Wdrożenie powinien wykonać certyfikowany inżynier wykonawcy. Po wdrożeniu należy przeprowadzić szkolenie dla wskazanego pracownika zamawiającego w czasie co najmniej 5 godzin.  Zakres wdrożenia:   1. Instalacja oprogramowania 2. Konfiguracja bezpiecznego dostępu administratora. 3. Ustawienie czasu przechowywania danych w bazie danych. 4. Konfiguracja i uruchomienie wykonywania automatycznych kopii zapasowych bazy danych. 5. Wdrożenie polityki monitorowania oraz paczki instalacyjnej agenta. 6. Instalacja agenta na wskazanych stacjach roboczych. 7. Konfiguracja polityki inwentaryzacji sprzętu i oprogramowywania. 8. Ustawienie alarmowania w ramach zasobów dla wskazanych przez Zamawiającego zasobów. 9. Opisanie wybranych przez Zamawiającego zasobów wraz z omówieniem możliwych opcji, procesowania cyklu życia zasoby, czy rejestru czynności administracyjnych na zasobie. 10. Stworzenie wzorców aplikacji - zasady pracy i aktualizacji. 11. Konfiguracja powiadomień o zmianach, w krytycznych dla Klienta obszarach zmian, konfiguracji sprzętowej i programowej. 12. Omówienie dostępnych ról i konsekwencji wynikających z roli dla użytkownika HelpDesk. 13. Omówienie i zdefiniowanie drzewa kategorii zgłoszeń, formularzy zgłoszeń, reguł widoczności i przypisywania zgłoszeń. 14. Zdefiniowanie reguł w zakresie działania metryk SLA.   Przeszkolenie wskazanego pracownika u Zamawiającego musi być przeprowadzone przez certyfikowanego inżyniera | | | |