**WYKAZ OFEROWANEGO SPRZĘTU**

**„Dostawa i instalacja infrastruktury sprzętowej i oprogramowania dla Urzędu Gminy Lesznowola.”**

**…………………………………………………………………………………………………………………………………………………………………….…………………………………………………………….………**

*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, REGON Wykonawcy* */ każdego z Wykonawców w przypadku składania oferty wspólnej)*

1. **Firewall UTM (1 szt.) o parametrach nie gorszych niż:**Typ/model ……….……….……….……….………. producent ……….……….……….……….……….

|  |  |  |
| --- | --- | --- |
| **Kategoria** | **Opis** |  |
| Wymagania ogólne | 1. System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 2. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 3. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. 4. Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu. 5. System wspiera protokoły IPv4 oraz IPv6 w zakresie: - Firewall. - Ochrony w warstwie aplikacji. - Protokołów routingu dynamicznego. | ☐ TAK\* ☐ NIE\* |
| 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. | ☐ TAK\* ☐ NIE\* |
| Interfejsy, Dysk, Zasilanie: | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: - 8 portami Gigabit Ethernet RJ-45. - 4 gniazdami SFP 1 Gbps. - 8 gniazdami SFP+ 10 Gbps. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie 2xAC. | ☐ TAK\* ☐ NIE\* |
| Parametry wydajnościowe: | 1. W zakresie Firewall’a obsługa nie mniej niż 10 mln jednoczesnych połączeń oraz 380 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 35 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 9 Gbps. 6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6 Gbps. | ☐ TAK\* ☐ NIE\* |
| 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. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji  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. Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. 13. 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). | ☐ TAK\* ☐ NIE\* |
| Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: - Translację jeden do jeden oraz jeden do wielu. - Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. - Amazon Web Services (AWS). - Microsoft Azure. - Cisco ACI. - Google Cloud Platform (GCP). - OpenStack.  - VMware NSX.  - Kubernetes. | ☐ TAK\* ☐ NIE\* |
| Połączenia VPN | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: - Wsparcie dla IKE v1 oraz v2. - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). - Obsługa protokołu Diffie-Hellman grup 19, 20. - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. - Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. | ☐ TAK\* ☐ NIE\* |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewnia obsługę: 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. | ☐ TAK\* ☐ NIE\* |
| 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). | ☐ TAK\* ☐ NIE\* |
| 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. | ☐ TAK\* ☐ NIE\* |
| Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum. 4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w usłudze chmurowej realizowanej na terenie Unii Europejskiej. 8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. | ☐ TAK\* ☐ NIE\* |
| Ochrona przed atakami | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 8. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. | ☐ TAK\* ☐ NIE\* |
| 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). | ☐ TAK\* ☐ NIE\* |
| Kontrola WWW | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search - przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. | ☐ TAK\* ☐ NIE\* |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego. 3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | ☐ TAK\* ☐ NIE\* |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego. 4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. | ☐ TAK\* ☐ NIE\* |
| 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. | ☐ TAK\* ☐ NIE\* |
| Testy wydajnościowe oraz funkcjonalne | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub w przypadku braku parametrów wydajnościowych w dokumentacji, wymagane jest dostarczenie wyników testów wydajnościowych (wykonanych przez producenta rozwiązania w czasie ostatnich 90 dni. | ☐ TAK\* ☐ NIE\* |
| Serwisy i licencje | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:  - Kontrola Aplikacji, IPS, Antywirus , bazy reputacyjne adresów IP/domen na okres [12] miesięcy. Wymagana jest licencja Advanced Threat Protection - w tym przypadku koniecznym jest zastosowanie serwisu 24x7. | ☐ TAK\* ☐ NIE\* |
| Gwarancja oraz wsparcie | System jest objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania i wsparcie techniczne w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię. Wymagana licencja minimum FortiCare Premium.  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. | ☐ TAK\* ☐ NIE\* |

**II. Switch zarządzalny (3 szt.) o parametrach nie gorszych niż:**  
Typ/model ……….……….……….……….………. producent ……….……….……….……….……….  
pisz

|  |  |  |
| --- | --- | --- |
| **Kategoria** | **Opis** |  |
| Porty, protokoły, funkcje | Ilość portów 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne | ☐ TAK\* ☐ NIE\* |
| Chłodzenie od przodu do tyłu obudowy | ☐ TAK\* ☐ NIE\* |
| Możliwość instalacji redundantnego zasilacza | ☐ TAK\* ☐ NIE\* |
| Tablica MAC min. 16K | ☐ TAK\* ☐ NIE\* |
| Tablica ARP/NDP min. 888 | ☐ TAK\* ☐ NIE\* |
| Bufor 16Mb | ☐ TAK\* ☐ NIE\* |
| MTBF min. 578472 godzin | ☐ TAK\* ☐ NIE\* |
| Wydajność min. 130,9 Mp/s | ☐ TAK\* ☐ NIE\* |
| Przepustowość min. 176 Gb/s | ☐ TAK\* ☐ NIE\* |
| Port USB | ☐ TAK\* ☐ NIE\* |
| Port miniUSB | ☐ TAK\* ☐ NIE\* |
| Port zarządzania Out-of-band; | ☐ TAK\* ☐ NIE\* |
| Web GUI | ☐ TAK\* ☐ NIE\* |
| HTTPs | ☐ TAK\* ☐ NIE\* |
| CLI | ☐ TAK\* ☐ NIE\* |
| Telnet | ☐ TAK\* ☐ NIE\* |
| SSH | ☐ TAK\* ☐ NIE\* |
| SNMP | ☐ TAK\* ☐ NIE\* |
| MIB RSPAN | ☐ TAK\* ☐ NIE\* |
| Radius | ☐ TAK\* ☐ NIE\* |
| TACACS+ | ☐ TAK\* ☐ NIE\* |
| DiffServ | ☐ TAK\* ☐ NIE\* |
| Możliwość łączenia w stos za pomocą interfejsów 10Gb/s | ☐ TAK\* ☐ NIE\* |
| Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh | ☐ TAK\* ☐ NIE\* |
| Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram | ☐ TAK\* ☐ NIE\* |
| IPv4/IPv6 Multicast filtering | ☐ TAK\* ☐ NIE\* |
| IGMPv3 MLDv2 Snooping | ☐ TAK\* ☐ NIE\* |
| ASM & SSM | ☐ TAK\* ☐ NIE\* |
| IGMPv1,v2 Querier | ☐ TAK\* ☐ NIE\* |
| Auto-VoIP | ☐ TAK\* ☐ NIE\* |
| Auto-iSCSI | ☐ TAK\* ☐ NIE\* |
| Policy-based routing (PBR) | ☐ TAK\* ☐ NIE\* |
| LLDP-MED | ☐ TAK\* ☐ NIE\* |
| Spanning Tree | ☐ TAK\* ☐ NIE\* |
| Green Ethernet | ☐ TAK\* ☐ NIE\* |
| STP | ☐ TAK\* ☐ NIE\* |
| MTP | ☐ TAK\* ☐ NIE\* |
| RSTP | ☐ TAK\* ☐ NIE\* |
| PV(R)STP | ☐ TAK\* ☐ NIE\* |
| BPDU/STRG Root Guard | ☐ TAK\* ☐ NIE\* |
| EEE (802.3az) | ☐ TAK\* ☐ NIE\* |
| GVRP/GMRP | ☐ TAK\* ☐ NIE\* |
| Q in Q, | ☐ TAK\* ☐ NIE\* |
| Private VLAN | ☐ TAK\* ☐ NIE\* |
| DOT1X | ☐ TAK\* ☐ NIE\* |
| MAB | ☐ TAK\* ☐ NIE\* |
| Captive Portal | ☐ TAK\* ☐ NIE\* |
| DHCP Snooping | ☐ TAK\* ☐ NIE\* |
| Dynamic ARP | ☐ TAK\* ☐ NIE\* |
| Inspection | ☐ TAK\* ☐ NIE\* |
| IP Source Guard | ☐ TAK\* ☐ NIE\* |
| CPU min 800 Mhz | ☐ TAK\* ☐ NIE\* |
| Min 1GB RAM | ☐ TAK\* ☐ NIE\* |
| Min 256MB Flash | ☐ TAK\* ☐ NIE\* |
| Min ilość obsługiwanych VLAN 4K | ☐ TAK\* ☐ NIE\* |
| DHCP Server min 2K rezerwacji | ☐ TAK\* ☐ NIE\* |
| OSPFv3 min. sąsiadów 400 | ☐ TAK\* ☐ NIE\* |
| OSPFv3 min. sąsiadów na interfejs 100 | ☐ TAK\* ☐ NIE\* |
| UDLD | ☐ TAK\* ☐ NIE\* |
| LLPF | ☐ TAK\* ☐ NIE\* |
| DHCPv6 Snooping | ☐ TAK\* ☐ NIE\* |
| wysyłanie alertów na email | ☐ TAK\* ☐ NIE\* |
| MMRP | ☐ TAK\* ☐ NIE\* |
| Ilość ACL min. 100 | ☐ TAK\* ☐ NIE\* |
| Ilość reguł na listę min. 1023 na wejściu | ☐ TAK\* ☐ NIE\* |
| Zasilacz z certyfikatem 80+ | ☐ TAK\* ☐ NIE\* |
| CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014, | ☐ TAK\* ☐ NIE\* |
| Class A, EN 61000-3-3:2013, EN 55024:2010 | ☐ TAK\* ☐ NIE\* |
| VCCI : VCCI-CISPR 32:2016, Class A | ☐ TAK\* ☐ NIE\* |
| RCM: AS/NZS CISPR 32:2013 Class A | ☐ TAK\* ☐ NIE\* |
| FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014 | ☐ TAK\* ☐ NIE\* |
| ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014 | ☐ TAK\* ☐ NIE\* |
| BSMI: CNS 13438 Class A | ☐ TAK\* ☐ NIE\* |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **III. Serwer RACK (1 szt.). wraz z oprogramowaniem serwerowym i licencjami dla użytkowników o parametrach nie gorszych niż:**  Typ/model ……….……….……….……….………. producent ……….……….……….……….……….   |  |  |  | | --- | --- | --- | | **Kategoria** | **Opis** |  | | Obudowa | - Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.  - Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI. | ☐ TAK\* ☐ NIE | | Płyta główna | - Płyta główna z możliwością zainstalowania do dwóch procesorów.  - Obsługa procesorów 56 rdzeniowych.  - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  - Płyta główna powinna obsługiwać do 8TB pamięci RAM. | ☐ TAK\* ☐ NIE | | Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. | ☐ TAK\* ☐ NIE | | Procesor | Zainstalowany jeden procesor min. 36-rdzeniowy, min. 2GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 603 pkt w teście w teście SPECrate 2017 Integer, dostępnym na stronie https://www.spec.org/cpu2017/results/ dla konfiguracji dwuprocesorowej | ☐ TAK\* ☐ NIE | | RAM | - Minimum 256GB DDR5 RDIMM 5600MT/s,  - Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. | ☐ TAK\* ☐ NIE | | Funkcjonalność pamięci RAM | - Demand Scrubing,  - Patrol Scrubing,  - Permanent Fault Detection | ☐ TAK\* ☐ NIE | | Interfejsy sieciowe/FC/SAS | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) | ☐ TAK\* ☐ NIE | | Dyski twarde | Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug skonfigurowane fabrycznie w RAID 1. | ☐ TAK\* ☐ NIE | | Wbudowane porty | - 4x USB, w tym min. 1 porty USB 3.0  - 2x port VGA (jeden na panelu przednim)  - Możliwość rozbudowy o Serial Port | ☐ TAK\* ☐ NIE | | Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 | ☐ TAK\* ☐ NIE | | Zasilacze | Redundantne, Hot-Plug min. 700W każdy. | ☐ TAK\* ☐ NIE | | Bezpieczeństwo | - Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.  - Możliwość wyłączenia w BIOS funkcji przycisku zasilania.  - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła  - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.  - Moduł TPM 2.0 V3  - Możliwość dynamicznego włączania I wyłączania portów USB na obudowie - bez potrzeby restartu serwera  - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera - niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem | ☐ TAK\* ☐ NIE | | Diagnostyka | Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. | ☐ TAK\* ☐ NIE | | Karta Zarządzania | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:  - zdalny dostęp do graficznego interfejsu Web karty zarządzającej;  - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);  - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;  - możliwość podmontowania zdalnych wirtualnych napędów;  - wirtualną konsolę z dostępem do myszy, klawiatury;  - wsparcie dla IPv6;  - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;  - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;  - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;  - integracja z Active Directory;  - możliwość obsługi przez dwóch administratorów jednocześnie;  - wsparcie dla dynamic DNS;  - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.  - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera  - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera  oraz z możliwością rozszerzenia funkcjonalności o:  - Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej  - Przesyłanie danych telemetrycznych w czasie rzeczywistym  - Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze  - Automatyczna rejestracja certyfikatów (ACE) | ☐ TAK\* ☐ NIE | | Oprogramowanie do zarządzania | Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:  - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych  - integracja z Active Directory  - Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta  - Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish  - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram  - Szczegółowy opis wykrytych systemów oraz ich komponentów  - Możliwość eksportu raportu do CSV, HTML, XLS, PDF  - Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.  - Grupowanie urządzeń w oparciu o kryteria użytkownika  - Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji  - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach  - Szybki podgląd stanu środowiska  - Podsumowanie stanu dla każdego urządzenia  - Szczegółowy status urządzenia/elementu/komponentu  - Generowanie alertów przy zmianie stanu urządzenia.  - Filtry raportów umożliwiające podgląd najważniejszych zdarzeń  - Integracja z service desk producenta dostarczonej platformy sprzętowej  - Możliwość przejęcia zdalnego pulpitu  - Możliwość podmontowania wirtualnego napędu  - Kreator umożliwiający dostosowanie akcji dla wybranych alertów  - Możliwość importu plików MIB  - Przesyłanie alertów „as-is” do innych konsol firm trzecich  - Możliwość definiowania ról administratorów  - Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów  - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)  - Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta  - Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów  - Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.  - Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.  - Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile  - Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.  - Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.  - Zdalne uruchamianie diagnostyki serwera.  - Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.  - Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V. | ☐ TAK\* ☐ NIE | | Oprogramowanie systemowe | - Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nieograniczonej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  - Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.  - Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  - Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  - Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  - Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  - Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  - Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.  - Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  - Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  - Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.  - Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  - Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  - Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.  - Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej dwóch języków poprzez wybór z listy dostępnych lokalizacji.  - Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  - Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  - Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).  - Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  - Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. | ☐ TAK\* ☐ NIE | | Certyfikaty | - Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001  - Serwer musi posiadać deklaracja CE.  - Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - Wykonawca złoży dokument potwierdzający spełnianie wymogu.  - Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2025, Microsoft Windows Server 2022. | ☐ TAK\* ☐ NIE | | Dokumentacja użytkownika | - Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  - Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | ☐ TAK\* ☐ NIE | | Warunki gwarancji | - Gwarancja producenta: 3 lat  - Możliwość rozszerzenia gwarancji przez producenta do 7 lat.  - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji.  - Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  - Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.  - Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.  - Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  - Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  - Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.  - Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.  - Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  - Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  - Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  - Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  Możliwość rozszerzenia gwarancji o:  - Wyznaczonego przez wykonawcę Opiekuna Technicznego Klienta, do którego obowiązków będzie należało:   * Monitorowanie zdarzeń w obrębie infrastruktury * Zarządzanie eskalacjami i współpraca z kierownikiem eskalacji   - Przygotowywanie kwartalnych zaleceń dotyczące konserwacji infrastruktury sprzętowej (BIOS, firmware, patche)  - Zdalne lub na miejscu wdrażanie poprawek - 2x w roku  - Raportowanie realizacji kontraktów serwisowych i wykorzystania zasobów sprzętowych (na żądanie) | ☐ TAK\* ☐ NIE | | Serwerowy System Operacyjny: | Do serwera należy dołączyć licencję bezterminową na Serwerowy System Operacyjny – SSO. Dołączona licencja musi uprawniać do uruchamiania na serwerze min. 2 maszyn wirtualnych SSO w najnowszej dostępnej wersji. Dostarczona licencja musi obejmować wszystkie rdzenie procesora zainstalowanego w serwerze. Serwerowy System Operacyjny musi posiadać następujące, wbudowane cechy minimalne:  1. Współpraca z procesorami o architekturze x86-64 bit  2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.  3. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory po 8 rdzeni każdy.  4. Praca w roli klienta domeny Microsoft Active Directory.  5. System musi być wspierany przez producenta oprogramowania do 2030 r. (wsparcie techniczne, aktualizacje bezpieczeństwa)  6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2022.  7. Możliwość uruchomienia roli klienta i serwera czasu (NTP).  8. Możliwość uruchomienia roli serwera pliko w z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.  9. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.  10. Możliwość uruchomienia roli serwera stron WWW.  11. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.  12. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.  13. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania.  14. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  15. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  16. Wbudowane wsparcie instalacji i pracy na wolumenach, które:   * pozwalają na zmianę rozmiaru w czasie pracy systemu, * umożliwiają zdefiniowanie list kontroli dostępu (ACL).   17. Wbudowany mechanizm klasyfikowania i indeksowania pliko w (dokumentów) w oparciu o ich zawartość  18. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET.  19. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  20. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  21. Zlokalizowane w języku polskim lub angielskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.  22. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  23. Mechanizmy logowania w oparciu o:   * login i hasło, * karty z certyfikatami (smartcard), * wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).   24. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:   * określonych grup użytkowników. * zastosowanej klasyfikacji danych, * centralnych polityk dostępu w sieci, * centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.   25. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  26. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  27. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  28. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  29. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:   1. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. 2. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  * ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, * odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, * zdalna dystrybucja oprogramowania na stacje robocze, * Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  1. Dystrybucję certyfikatów poprzez http, 2. Konsolidację CA dla wielu lasów domeny 3. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, 4. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. 5. szyfrowanie plików i folderów, 6. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), 7. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi, 8. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail - over) oraz rozłożenia obciążenia serwerów, 9. serwis udostępniania stron WWW, 10. wsparcie dla protokołu IP w wersji 6 (IPv6), 11. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, 12. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera), 13. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (Hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 14. mechanizmy wirtualizacji mające wsparcie dla:     1. dynamicznego podłączania zasobów dyskowych typu hot plug do maszyn wirtualnych,     2. obsługi ramek typu jumbo frames dla maszyn wirtualnych.     3. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.     4. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.     5. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).     6. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.     7. mechanizm konfiguracji połączenia VPN do platformy Azure.     8. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.     9. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.     10. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard) | ☐ TAK\* ☐ NIE | | Licencje Użytkownika końcowego | Licencja CAL do SSO - 150 sztuk  Oprogramowanie: USER CAL lub równoważne do SSO  Sposób licencjonowania: Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. Licencja ma uprawniać do dostępu do zasobów serwera dla 150 użytkowników.  Kompatybilność: Zamawiający wymaga, aby licencja była kompatybilna z Serwerowym Systemem Operacyjnym SSO opisanym powyżej.  Licencje dostępowe CAL dla SSO - opis równoważności  Sposób licencjonowania: Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu. Licencja ma uprawniać do dostępu do zasobów serwera dla określonej liczby użytkowników.  Cechy: Licencja powinna zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także dostęp do zasobów serwera dla określonej liczby użytkowników.  Kompatybilność: Zamawiający wymaga, aby licencja była kompatybilna z systemem operacyjnym opisanym powyżej. | ☐ TAK\* ☐ NIE | |

|  |
| --- |
| **IV. Macierz do systemów wdrażanych w ramach projektu (1 szt.). o parametrach nie gorszych niż:**  Typ/model ……….……….……….……….………. producent ……….……….……….……….………. |

|  |  |  |
| --- | --- | --- |
| **Kategoria** | **Opis** |  |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U oraz możliwości instalacji 24 dysków 2.5”. | ☐ TAK\* ☐ NIE |
| Przestrzeń dyskowa | Zainstalowane:  2 dyski Dysk AG 1,92 TB SSD, do 24 Gb/s SAS ISE 512e 2,5″ do intensywnego odczytu wymieniany bez wyłączania systemu. | ☐ TAK\* ☐ NIE |
| Możliwość rozbudowy | Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych. | ☐ TAK\* ☐ NIE |
| Obsługa dysków | Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. | ☐ TAK\* ☐ NIE |
| Sposób zabezpieczenia danych | Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).  Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.  Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).  Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. | ☐ TAK\* ☐ NIE |
| Tryb pracy kontrolerów macierzowych | Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. | ☐ TAK\* ☐ NIE |
| Pamięć cache | Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.  Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.  Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat. | ☐ TAK\* ☐ NIE |
| Rozbudowa pamięci cache | Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem. | ☐ TAK\* ☐ NIE |
| Interfejsy | Macierz musi posiadać, co najmniej 8 portów FC Type-B 32Gb/s (4 porty na kontroler). | ☐ TAK\* ☐ NIE |
| Kable/wkładki | 2X wkładki SFP, FC16, 16GB | ☐ TAK\* ☐ NIE |
| Zarządzanie | Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. | ☐ TAK\* ☐ NIE |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.  Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. | ☐ TAK\* ☐ NIE |
| Thin Provisioning | Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.  Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. | ☐ TAK\* ☐ NIE |
| Tiering | Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.  Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.  Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych. | ☐ TAK\* ☐ NIE |
| Wewnętrzne kopie migawkowe | Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.  Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. | ☐ TAK\* ☐ NIE |
| Wewnętrzne kopie pełne | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. | ☐ TAK\* ☐ NIE |
| Migracja danych w obrębie macierzy | Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia. | ☐ TAK\* ☐ NIE |
| Podłączanie zewnętrznych systemów operacyjnych | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).  Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.  Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. | ☐ TAK\* ☐ NIE |
| Redundancja | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.  Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.  Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.  Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold. | ☐ TAK\* ☐ NIE |
| Dodatkowe wymagania | Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.  Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. | ☐ TAK\* ☐ NIE |
| Standardy bezpieczeństwa | Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International). | ☐ TAK\* ☐ NIE |
| Warunki gwarancji | Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat.  Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet.  Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania  Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki.  Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego.  Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.  Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki:  Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego.  Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.  Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową.  Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu.  Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu.  Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. | ☐ TAK\* ☐ NIE |
| Inne | Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca wraz z ofertą musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta.  Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.  Deklaracja zgodności CE. | ☐ TAK\* ☐ NIE |

|  |
| --- |
| **V. Macierz do kopii zapasowych wraz z oprogramowaniem do kopii zapasowych (1 szt.). o parametrach nie gorszych niż:**  Typ/model ……….……….……….……….………. producent ……….……….……….……….………. |

|  |  |  |
| --- | --- | --- |
| **Kategoria** | **Opis** |  |
| Zarządzanie i magazyny | 1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2025 r.  2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.  3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:  - Obudowa rack rozmiar: 1U  - Procesor: min. 6 rdzeni, min. 12 wątków. Minimalna częstotliwość bazowa procesora 2.6GHz  - Pamięć RAM: 16GB DDR4  - Przestrzeń dostępna na przechowywanie danych: Min. 14TB po RAID 5  - Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,  - Redundantne zasilanie,  - Interfejsy sieciowe: Min. 2szt. Ethernet 1Gb,  - Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania.  4. Produkt dostępny w polskiej wersji językowej.  5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej  6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków  7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów  8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych  9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT  10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft.  11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe.  12. System zarządzania nie może być oparty o relacyjne bazy danych.  13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).  14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).  15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn - serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.  16. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.  17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.  18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.  19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.  20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.  21. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.  22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.  23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych  24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.  25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.  26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).  27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.  28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.  29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika.  30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.  31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.  32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).  33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.  34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.  35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych.  36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.  37. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.  38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.  39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.  40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.  41. System musi pozwalać na automatyczne aktualizacje oprogramowania.  42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.  43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.  44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.  45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.  46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.  47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.  48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.  49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.  50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.  51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.  52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.  53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.  54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental.  55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).  56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance’u.  57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb,S3, nfs, iscsi, katalog lokalny.  58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).  59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.  60. Możliwość generowania raportów dobowych w oparciu o harmonogram.  61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter powinno być zlokalizowane na terenie Polski).  62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna).  63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.  64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu). | ☐ TAK\* ☐ NIE |
| Wspierane systemy | Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy: Alpine 3.10+, Debian: 9+, Ubuntu: 16.04+, Fedora: 29+, centOS: 7+, RHEL: 6+, openSUSE: 15+, SUSE Enterprise Linux(SLES): 12 SP2+, macOS: 10.13+, Windows: 7, 8.1, 10(1607+), Windows Server: 2016+, Środowisk wirtualnych: Hyper-V 2016+, VMware: 6.7+. | ☐ TAK\* ☐ NIE |
| Środowiska fizyczne i bazy danych | 1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.  2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.  3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.  4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.  5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.  6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.  7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.  8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.  9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.  10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.  11. Rozwiązanie powinno wspierać odtwarzanie danych w scenaruszach P2P, P2V, V2P, V2V.  12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).  13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.  14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows). | ☐ TAK\* ☐ NIE |
| Środowiska wirtualne | 1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.  2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.  3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.  4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.  5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.  6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).  7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.  8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku. | ☐ TAK\* ☐ NIE |
| Aplikacje SaaS | 1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.  2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji)  3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.  4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi  5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.  6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.  7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.  8. System musi umożliwiać zabezpieczenie środowisk Jira.  9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego. | ☐ TAK\* ☐ NIE |
| Licencjonowanie i wsparcie techniczne | 1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.  2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.  3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.  4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)  5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.  6. W ramach dostawy rozwiązania, dostawca musi wyznaczyć dedykowanego opiekuna technicznego od strony producenta rozwiązania backupowego.  7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do dedykowanego opiekuna technicznego od strony producenta rozwiązania backupowego.  8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.  9. Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.  10. Wsparcie techniczne producenta musi zostać dostarczone na min. 12 miesięcy.  11. Licencje powinny umożliwiać replikację na własne zasoby.  12. Licencje powinny umożliwiać korzystanie z przestrzeni chmurowej dostarczonej bezpośrednio przed producenta, min. 20 TB przez cały okres trwania wsparcia technicznego. | ☐ TAK\* ☐ NIE |
| Anty-ransomware i bezpieczeństwo | 1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").  2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System  3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.  4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu, ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.  5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczanym urządzeniu. | ☐ TAK\* ☐ NIE |
| Szkolenie | 1. Szkolenie musi zostać przeprowadzone w formie stacjonarnej w języku polskim.  2. Szkolenie jest realizowane bezpośrednio przez producenta oferowanego systemu backupowego.  3. Szkolenie musi zostać przeprowadzone przez dedykowanego inżyniera producenta systemu backupowego.  4. Szkolenie musi zakończyć się imiennym certyfikatem dla administratorów uczestniczących w szkoleniu.  5. Szkolenie musi trwać minimum 2 dni. | ☐ TAK\* ☐ NIE |
| Wdrożenie | 1. Wdrożenie stacjonarne musi zostać realizowane bezpośrednio przez producenta oferowanego systemu backupowego.  2. Wdrożenie musi zostać przeprowadzone przez dedykowanego inżyniera od producenta systemu backupowego.  3. Wdrożenie musi zakończyć się dostarczeniem dokumentacji powdrożeniowej, przygotowanej przez dedykowanego inżyniera od producenta systemu backupowego.  4. Zamawiający powinien móc skorzystać z przynajmniej 2 dniowej pomocy wdrożeniowej bezpośrednio świadczonej przez producenta rozwiązania.  5. Wdrożenie powinno być zrealizowane tak, aby dostosować się do preferencji zamawiającego. | ☐ TAK\* ☐ NIE |