**Załącznik 1b do zapytania ofertowego 1/12/2024/CUS**

**Specyfikacja techniczna zamówienia (STZ)**

**Część 2: Serwery i urządzenia bezpieczeństwa sieci i cyberbezpieczeństwa**

**Spis treści**

[1. Urządzenie do ochrony brzegowej typu UTM- 1 szt. 2](#_Toc185453759)

[2. Serwer NAS z dyskami i backupem w chmurze – 1 szt. 3](#_Toc185453760)

[3. Serwer – 1 szt. 5](#_Toc185453761)

[4. Przełącznik (switch) – 2 szt. 14](#_Toc185453762)

[5. UPS serwerowy – 1 szt. 15](#_Toc185453763)

Do:

Gmina Mrocza

działająca poprzez realizatora:

Miejsko-Gminny Ośrodek Pomocy Społecznej w Mroczy

przekształcony w Centrum Usług Społecznych w Mroczy

ul. Łąkowa 7, 89-115 Mrocza

**WYKONAWCA:**

|  |  |
| --- | --- |
| Pełna nazwa albo  imię i nazwisko Wykonawcy  (wpisz dane zgodne z dokumentami rejestrowymi): |  |
| Siedziba albo miejsce zamieszkania i adres Wykonawcy  (wpisz dane zgodne z dokumentami rejestrowymi) |  |
| Nr telefonu/faksu: |  |
| Adres e-mail: |  |
| NIP/REGON/PESEL (jeśli dotyczy): |  |
| Osoba upoważniona do kontaktów (imię, nazwisko, tel. adres e-mail): |  |

# Urządzenie do ochrony brzegowej typu UTM- 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry (potwierdź spełnienie poprzez skreślenie niepoprawnej odpowiedzi) oraz wpis wymagane dane według wskazań** |
|  | Funkcje modułu Firewall | 1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).  2. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).  3. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.  4. Musi obsługiwać Multicast routing.  5. Musi obsługiwać Policy Based routing.  6. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.  7. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.  8. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.  9. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).  10. Musi obsługiwać Dynamic DNS.  11. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.  12. Musi obsługiwać translację portów: PAT.  13. Musi obsługiwać IPSec NAT traversal.  14. Musi obsługiwać mechanizm Policy Based NAT.  15. Musi obsługiwać VLAN 802.1Q.  16. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.  17. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.  18. Musi mieć możliwość obsługi zapasowego łącza typu 4G LTE/5G poprzez podłączenie zewnętrznego modemu USB.  19. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.  20. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.  21. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza, minimum dla wartości: utrata pakietów, opóźnienie, jitter.  22. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.  23. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.  24. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.  25. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.  26. Musi posiadać co najmniej dwie metody transparentnej autoryzacji nie wymagające instalacji dedykowanego agenta na stacjach roboczych użytkowników.  27. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.  28. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.  29. Musi dostarczać mechanizm identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.  30. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.  31. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.  32. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.  33. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.  34. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.  35. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.  36. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.  37. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.  38. Musi ochraniać przed minimum: atakami DoS, pofragmentowanymi i zniekształconymi pakietami, zagrożeniami mieszanymi (Blended threats).  39. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.  40. VPN site-to-site musi wspierać minimum: IKEv2, IPSec, tunele oparte na politykach i routingu, TLS hub and spoke.  41. VPN client-to-site musi wspierać minimum: IKEv2, IPSec, L2TP, TLS | **Producent**  **Nazwa /model**  SPEŁNIA  TAK /NIE |
|  | Specyfikacja UTM | 1. Firewall musi zapewnić obsługę na poziomie minimalnym:  3.94 Gbps dla pracy w trybie firewall,  557 Mbps dla pracy w trybie full scan (włączone mechanizmy bezpieczeństwa takie jak: AV, IPS)  2. Ilość obsługiwanych sieci VLAN: 50  3. Firewall musi obsługiwać 3 850 000 jednoczesnych połączeń TCP oraz przyjmować nowe połączenia z wydajnością minimalną 26 500 połączeń na sekundę.  4. Minimalna ilość portów 10/100/1000 BaseT: 5  5. Wsparcie połączeń VPN site-to-site lub client-to-site dla minimum 30 użytkowników. | SPEŁNIA  TAK /NIE |
|  | Wymagane funkcje VPN systemu | 1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.  2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.  3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.  4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.  5. Obsługa Dead Peer Detection (DPD).  6. Wsparcie dla IKEv1 i IKEv2.  7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.  8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).  9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.  10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.  11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.  12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows. | SPEŁNIA  TAK /NIE |
|  | Zarządzanie | 1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.  2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.  3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.  4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).  5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.  6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.  7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.  8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania. | SPEŁNIA  TAK /NIE |
|  | Gwarancja i wsparcie | Wykonawca ma obowiązek dostarczyć urządzenie z 3 letnia gwarancja Serwis z czasem reakcji na poziomie do 4 godzin. | SPEŁNIA  TAK /NIE |

# Serwer NAS z dyskami i backupem w chmurze – 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry (potwierdź spełnienie poprzez skreślenie niepoprawnej odpowiedzi) oraz wpis wymagane dane według wskazań** |
|  | Przeznaczenie | Serwer NAS z przeznaczeniem do wdrożenia kopi danych Zamawiającego celem zwiększenia bezpieczeństwa i integralności danych | **Producent**  **Nazwa /model** |
|  | Procesor | Wielordzeniowy procesor o architekturze 64-bit. | SPEŁNIA  TAK /NIE |
|  | Obudowa | Typu desktop (wolnostojąca). | SPEŁNIA  TAK /NIE |
|  | Pamięć RAM | Minimum 4GB pamięci RAM DDR4 ECC. | SPEŁNIA  TAK /NIE |
|  | Interfejsy sieciowe | Minimum 2 porty 1GbE RJ-45 z obsługą agregacji łączy. | SPEŁNIA  TAK /NIE |
|  | Ilość obsługiwanych dysków | Minimum 4 dyski o maksymalnej pojemności nie mniejszej niż 18TB każdy, po podłączeniu modułów rozszerzających minimum 9 dysków. | SPEŁNIA  TAK /NIE |
|  | Zainstalowane dyski | 4 dyski o pojemności 6TB każdy zgodne z listą kompatybilności oferowanego serwera NAS oraz charakteryzujące się następującymi parametrami: - prędkość obrotowa: minimum 5400 RPM, - pamięć cache: minimum 256 MB, - MTBF: minimum 1 milion, - gwarancja: minimum 36 miesięcy. | **Producent**  **Model i wersja** |
|  | Wskaźniki LED | Status, HDD 1-4, zasilanie, LAN 1-2 | SPEŁNIA  TAK /NIE |
|  | Obsługa RAID | Podstawowy, RAID 0, 1, 5, 6, 10 wraz z obsługa dysków typu hot spare. | SPEŁNIA  TAK /NIE |
|  | Funkcje RAID | Możliwość zwiększania pojemności i migracja między poziomami RAID online. | SPEŁNIA  TAK /NIE |
|  | Szyfrowanie | Możliwość szyfrowania wybranych udziałów sieciowych. | SPEŁNIA  TAK /NIE |
|  | Protokoły | SMB, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP | SPEŁNIA  TAK /NIE |
|  | Usługi | 1. Serwer VPN, Stacja monitoringu, Windows ACL, Integracja z Windows ADS, Firewall, Serwer WWW, Serwer plików, Manager plików przez WWW, Szyfrowana replikacja zdalna na kilka serwerów w tym samym czasie, Antyvirus, Klient VPN, Usługa DDNS, Serwer i klient LDAP, Możliwość utworzenia kilku wolumenów  w obrębie jednej macierzy RAID, migawki (min. 65 tys. w cały systemie), możliwość tworzenia i uruchamiania maszyn wirtualnych bezpośrednio w systemie bez wykorzystywania zewnętrznych wirtualizatorów.  2. Wykonywanie kopii zapasowych typu bare-metal komputerów lokalnych z systemem Windows 7 lub nowszym według harmonogramu z centralnej konsoli zarządzania dostępnej lokalnie oraz zdalnie, z możliwością przywracania pojedynczych plików, folderów oraz całych obrazów dysku. Kopia musi być wykonywana w trybie przyrostowym z możliwością przechowywania minimum 32 wersji i zarządzania ich przechowywaniem w sposób automatyczny poprzez dedykowany algorytm. Bez ograniczenia liczby podłączanych komputerów do systemu kopii zapasowej.  3. Możliwość utworzenia klastra wysokiej dostępności (HA) z dwóch identycznych urządzeń pracującego minimum w trybie aktywny-pasywny. Wymagane jest, aby klaster obsługiwał w pełni automatyczne przełączanie awaryjne bez ingerencji administratora. | SPEŁNIA  TAK /NIE |
|  | Zarządzanie dyskami | SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów. | SPEŁNIA  TAK /NIE |
|  | Język GUI | Polski | SPEŁNIA  TAK /NIE |
|  | Gwarancja i serwis | Minimum 36 miesięcy gwarancji producenta . | SPEŁNIA  TAK /NIE |
|  | Pobór mocy | Maksymalnie 45W w trybie pracy. | SPEŁNIA  TAK /NIE |
|  | Certyfikaty | CE, FCC | SPEŁNIA  TAK /NIE |
|  | System plików | Dyski wewnętrzne: BTRFS.  Dyski zewnętrzne: FAT, NTFS, EXT3, EXT4, HFS+. | SPEŁNIA  TAK /NIE |
|  | Zasilanie | Zasilacz zewnętrzny o mocy minimum 100W. | SPEŁNIA  TAK /NIE |

| **Usługa przechowywania danych i synchronizacji w chmurze** | | | |
| --- | --- | --- | --- |
|  | Pojemność przechowywania | Minimalna przestrzeń przechowywania danych w chmurze wynosząca 2 TB. | **Producent**  **nazwa usługi** |
|  | Okres świadczenia usługi | Usługa musi być dostępna przez co najmniej 3 lata. | SPEŁNIA  TAK /NIE |
|  | Tworzenie kopii zapasowych | Możliwość automatycznego wykonywania kopii zapasowych co godzinę. | SPEŁNIA  TAK /NIE |
|  | Dostosowanie strategii przechowywania | Możliwość dostosowywania strategii przechowywania danych, w tym konfiguracja rotacji kopii zapasowych. | SPEŁNIA  TAK /NIE |
|  | Optymalizacja przechowywania danych | Wbudowany mechanizm deduplikacji danych na poziomie bloków, eliminujący duplikaty i redukujący zużycie przestrzeni dyskowej. | SPEŁNIA  TAK /NIE |
|  | Udostępnianie i synchronizacja | Funkcjonalność umożliwiająca synchronizację i udostępnianie plików między różnymi lokalizacjami z możliwością jednoczesnej pracy wielu użytkowników na wspólnych plikach. | SPEŁNIA  TAK /NIE |
|  | Lokalna pamięć podręczna | Pamięć podręczna dla często używanych danych, zapewniająca szybki dostęp do informacji przy ograniczonym dostępie do internetu. | SPEŁNIA  TAK /NIE |
|  | Przypinanie plików i folderów | Możliwość przypinania plików lub folderów w celu zagwarantowania ich dostępności offline na lokalnych urządzeniach. | SPEŁNIA  TAK /NIE |
|  | Szyfrowanie danych | Zastosowanie szyfrowania danych algorytmem AES-256 lub równoważnym, zapewniającego ochronę przed nieautoryzowanym dostępem. | SPEŁNIA  TAK /NIE |
|  | Sprawdzanie integralności | Mechanizm pozwalający na zaplanowanie sprawdzania integralności danych w celu wykrycia ewentualnych uszkodzeń oraz zapewnienia ciągłości działania kopii zapasowych. | SPEŁNIA  TAK /NIE |
|  | Dostępność danych | Możliwość szybkiego dostępu do danych oraz ich pobierania za pomocą platformy internetowej dostępnej przez przeglądarkę internetową. | SPEŁNIA  TAK /NIE |
|  | Elastyczne plany użytkowania | Możliwość dostosowania planów rozliczeniowych do potrzeb użytkownika bez ukrytych opłat za przesyłanie lub pobieranie danych. | SPEŁNIA  TAK /NIE |
|  | Wsparcie techniczne | Zapewnienie wsparcia technicznego w zakresie konfiguracji usługi, rozwiązywania problemów i aktualizacji zabezpieczeń. | SPEŁNIA  TAK /NIE |
|  | Obsługa transferu dużych danych | Możliwość przenoszenia dużych ilości danych początkowych do usługi chmurowej w sposób szybki i bezpieczny, minimalizując opóźnienia w transferze danych. | SPEŁNIA  TAK /NIE |
|  | Zgodność z przepisami | Usługa musi spełniać wymogi zgodne z obowiązującymi przepisami prawa, w tym ochrony danych osobowych oraz przepisami dotyczącymi zamówień publicznych. | SPEŁNIA  TAK /NIE |

# Serwer – 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry (potwierdź spełnienie poprzez skreślenie niepoprawnej odpowiedzi) oraz wpis wymagane dane według wskazań** |
|  | **Obudowa** | * Obudowa Rack o wysokości 2U. * 12 kieszeni na dyski 3.5”. * Możliwość instalacji dysków SAS/SATA/NVMe. Obudowa musi umożliwiać instalację 4 dysków NVMe równolegle z pozostałymi typami dysków. | **Producent**  **Model i wersja serwera** |
|  | **Płyta główna** | * Płyta główna w architekturze dwuprocesorowej z możliwością zainstalowania procesorów 64 rdzeniowych. * Płyta główna musi umożliwiać instalacje minimum 32 kości DDR5 z możliwością wyskalowania pamięci do minimum 8TB. | SPEŁNIA  TAK /NIE |
|  | **Procesor** | * Zainstalowany jeden procesor min. 16-rdzeniowy, min. 3.4GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 273 w teście SPECrate2017\_int\_base w konfiguracji dwuprocesorowej, dostępnym na stronie [www.spec.org](http://www.spec.org) **- wynik należy dołączyć na etapie umowy z Wykonawcą.** | SPEŁNIA  TAK /NIE |
|  | **RAM** | * 128GB DDR5 RDIMM 4800MHz. * Pamięć RAM musi wspierać wczesne wykrywanie błędów poprawialnych (CE) w pamięci i przeprowadzanie operacji izolacji. Pamięć musi wspierać typowe technologie ochrony m.in. ECC, Address/Command Parity, PPR, Write Data CRC Protection, ADC-SR, ADDDC-MR, SDDC. | SPEŁNIA  TAK /NIE |
|  | **Kontroler RAID** | * Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 00, 1, 5, 6, 10, 50 i 60. | SPEŁNIA  TAK /NIE |
|  | **Dyski twarde** | * Zainstalowane:   + 2x dysk SSD SATA o pojemności min. 1,92TB   + 2x dysk HDD SATA 12TB * Możliwość zainstalowania dwóch dysków M.2 SSD o pojemności 480GB Hot-Plug z możliwością konfiguracji RAID 1. | SPEŁNIA  TAK /NIE |
|  | **Gniazda PCIe** | * 1x PCIe 5.0 16X * 2x PCIe 4.0 8X | SPEŁNIA  TAK /NIE |
|  | **Interfejsy sieciowe/FC/SAS** | * Min. 2 interfejsy sieciowe 10GE BASE-T (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) | SPEŁNIA  TAK /NIE |
|  | **Wbudowane porty oraz wskaźniki** | * 5 portów USB w tym min:   + 2 porty USB 3.0 z tyłu obudowy,   + 2 port USB 3.0 z przodu obudowy   + 1 port USB 2.0 zainstalowany wewnętrznie * 1 porty VGA * 3 dedykowane, wbudowane poty umożliwiające zarządzanie serwerem, z czego co najmniej jeden umożliwiający połączenie z graficznym interfejsem zarządzającym, przynajmniej jeden port na przodzie obudowy umożliwiający połączenie za pomocą USB Type-C. * Przyciski i wskaźniki:   + Diagnostyczny panel LED – panel musi wyświetlać informacje na temat aktualnego stanu serwera. W przypadku awarii, panel LED musi wskazywać odpwiedni kod błędu, a w sytuacji wystąpienia więcej niż jednego błędu, system musi wyświetlać odpowiednie kody błędów w pętli.   + Wskaźnik aktualnego stanu urządzenia – wskaźnik musi za pomocą stosownego koloru oraz określonej czestotliwości odświeżania wyświetlać w jakim stanie znajduje się urządzenie.   + Wskaźnik stanu karty OCP NIC. Wskaźnik musi informować czy:     - Karta została wykryta     - Karta została wykryta ale nie jest włączona     - Karta została zainstalowana, wykryta i działa poprawnie   + Wskaźnik stanu zasilania zintegrowany z przyciskiem zasilania informujący czy:     - Urządzenie jest włączone.     - Urządzenie jest wyłączone.     - Urządzenie zostało uruchomione, a moduł zarządzania się uruchamia. W tej sytuacji wciśnięcie przycisku zasilania nie może spowodować wyłączenia serwera.   + Wskaźnik UID zintegrowany z przyciskiem, umożliwiający zlokalizowanie urządzenia, udostępniający następnujące funkcje:     - Przycisk migający lub świeciący ciągłbym swiatłem niebieskim umożliwia zlokalizowanie serwera.     - Włączenie/wyłączenie funkckcji lokalizacji urządzenia musi być możliwe zarówno z poziomu przycisku jak i z poziomu interfejsu zarządzania.   + Wskaźnik statusu bezpośredniego połączenia z interfejsem zarządzania. Musi informować o aktualnym stanie połączenia z interfejsem zarządzania umieszczonym na przednim panelu urządzenia. | SPEŁNIA  TAK /NIE |
|  | **Video** | * Zintegrowana karta graficzna z minimum 32MB pamięci osiągająca rozdzielczość 1920x1200 60Hz | SPEŁNIA  TAK /NIE |
|  | **Wentylatory** | * Redundantne | SPEŁNIA  TAK /NIE |
|  | **Zasilacze** | * Minimum dwa redundantne zasilacze o mocy minimum 900W z certyfikatem minimum Titanium. | SPEŁNIA  TAK /NIE |
|  | **Elementy montażowe** | * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |  |
|  | **Bezpieczeństwo** | * Moduł TPM 2.0 * Secure boot * Ochrona przed atakami. Urządzenie musi udostępniać minimalną wymaganą liczbę portów usług sieciowych. Domyślnie, zbędne usługi muszą być wyłączone, porty usług sieciowych do debugowania i diagnozy muszą być wyłączone podczas normalnej pracy serwera. | SPEŁNIA  TAK /NIE |
|  | **Moduł zarządzania** | * Niezależny od zainstalowanego na serwerze systemu operacyjnego, moduł zarządzania, posiadająca dedykowany port Gigabit Ethernet RJ45. * NC-SI * Zarządzanie certyfikatami. Moduł musi obsługiwać szyfrowanie i wymianę certyfikatów SSL. Wymiana samych certyfikatów musi być możliwa z poziomu GUI. * Moduł musi umożliwiać import certyfikatu LDAP (Lightweight Directory Access Protocol. * Wsparcie dla DCMI 1.5. * Wsparcie dla IMPI 1.5 oraz 2.0. * Moduł zarządzania musi posiadać certyfikacje CC EAL4+. * Wymagana jest funkcjonalność zarządzania diagnostyką błędów (FDM. Funkcjonalność musi obejmować zbieranie i analizę danych o błędach, diagnozowanie i lokalizowanie błędów, wczesne ostrzeganie o błędach oraz analizę kondycji urządzeń. Podczas rutynowej obsługi i konserwacji można wyświetlać informacje o wadliwych komponentach oraz związanych z nimi zdarzeniami historycznymi. Wymagana funkcjonalność musi być możliwa do włączenia/wyłączenia z poziomu BIOS. * Moduł musi oferować precyzyjne powiadomienia o niekrytycznych, niekorygowalnych błędach (UCE) w pamięci w sposób umożliwiający zlokalizowanie uszkodzonego modułu. * Wymagana jest obsługa szczegółowych alarmów dotyczących dysków twardych, które mogą rozróżniać trzy typy alarmów: oprogramowania układowego dysku twardego, konfigurację i usterki fizyczne. * Musi umożliwiać przeglądanie w formie graficznego modelu 3D rozkładu temperatury. Mapa temperatury musi umożliwić lokalizowanie anomalii związanych z temperaturą wewnątrz urządzenia w dowolnym jego punkcie. * Moduł musi umożliwiać włączenie funkcji szyfrowania KVM i VNC (Virtual Network Console), które szyfrują dane przesyłane do i z zdalnej konsoli wirtualnej.   Wymagania dotyczące portu bezpośredniego połączenia z modułem zarządzania serwera   1. Lokalizacja portu:    * Serwer musi być wyposażony w dedykowany port do bezpośredniego zarządzania, umieszczony na przednim panelu urządzenia, zapewniający łatwy dostęp bez konieczności manipulacji tylnym panelem. 2. Sposób połączenia:    * Port zarządzania musi umożliwiać podłączenie komputera administracyjnego za pomocą przewodu USB-C lub przewodu sieciowego Ethernet.    * Połączenie musi działać niezależnie od głównej sieci LAN. 3. Funkcjonalność graficznego interfejsu zarządzania:    * Port musi zapewniać dostęp do graficznego interfejsu użytkownika za pośrednictwem przeglądarki internetowej.    * Interfejs zarządzania musi umożliwiać:      + Monitorowanie statusu serwera, w tym zużycia zasobów, stanu komponentów oraz historii zdarzeń.      + Przeprowadzanie diagnostyki sprzętowej, w tym odczytywanie kodów błędów i ich interpretację.      + Zarządzanie zasilaniem serwera, w tym włączanie, wyłączanie i restartowanie urządzenia. 4. Funkcje diagnostyczne i zarządzania:    * Port musi umożliwiać zdalne ładowanie obrazów ISO w celu instalacji systemów operacyjnych lub narzędzi diagnostycznych.    * Musi być możliwe monitorowanie stanu komponentów sprzętowych, takich jak dyski, pamięci czy zasilacze. 5. Izolacja od głównej sieci:    * Port zarządzania musi być niezależny od głównej infrastruktury sieciowej, umożliwiając pełną izolację operacji administracyjnych od środowiska produkcyjnego. 6. Bezpieczeństwo dostępu:    * Port musi wymagać uwierzytelnienia przy użyciu nazwy użytkownika i hasła.    * Musi być możliwość konfiguracji danych uwierzytelniających w celu zwiększenia bezpieczeństwa. 7. Wsparcie dla różnych metod dostępu:    * Port musi wspierać lokalne zarządzanie za pomocą USB-C oraz alternatywnie możliwość konfiguracji sieciowej. | SPEŁNIA  TAK /NIE |
|  | **BIOS** | * Oferowany serwer musi być wyposażony w BIOS zapewniający następujące funkcjonalności:   + Inicjalizacja sprzętu: BIOS musi wspierać pełne testowanie i uruchamianie kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde oraz interfejsy sieciowe.   + Zarządzanie konfiguracją systemu: BIOS musi umożliwiać konfigurację ustawień systemowych, w tym kolejności bootowania, konfiguracji RAID oraz ustawień zasilania.   + Bezpieczeństwo systemu: BIOS musi wspierać funkcję Secure Boot, chroniącą przed uruchamianiem nieautoryzowanego oprogramowania. Musi również posiadać opcję zabezpieczenia hasłem dostępu. * Aktualizacje oprogramowania: BIOS musi umożliwiać aktualizację firmware’u oraz zapewniać wsparcie dla aktualizacji zdalnych. | SPEŁNIA TAK /NIE |
|  | **System operacyjny** | **Windows Server 2022 Standard – licencja dobrana tak, aby przy oferowanych procesorach umożliwić uruchomienie minimum 2 maszyny wirtualne. Oraz 5 licencji Cal na użytkownika**  Microsoft Windows Server 2022 Standard lub równoważny spełniający min. poniższe wymagania:  Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowiskach serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.  Możliwość wykorzystywania 64 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 uruchamianie 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 2 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.  Możliwość migracji konfiguracji systemu Microsoft Windows Serwer 2021/2016. | **Producent**  **Nazwa i wersja oprogramowania**  SPEŁNIA  TAK /NIE |
|  | **System do zarządzania serwerem** | Oferowany serwer musi być wyposażony w zaawansowane oprogramowanie do zarządzania i monitorowania, które umożliwia centralne zarządzanie oraz optymalizację pracy serwera. Oprogramowanie musi spełniać następujące wymagania:  1. Centralne zarządzanie serwerami   * Oprogramowanie do zarządzania serwerami musi zapewniać:   + Monitorowanie infrastruktury w czasie rzeczywistym: Oprogramowanie musi umożliwiać śledzenie wydajności serwerów, stanu komponentów oraz zużycia zasobów, prezentując dane w formie graficznej.   + Automatyzacja aktualizacji: Musi wspierać zdalne i automatyczne aktualizowanie oprogramowania układowego oraz sterowników, z możliwością planowania aktualizacji.   + Diagnostyka i analiza stanu sprzętu: System musi umożliwiać analizę kondycji serwerów, gromadząc dane diagnostyczne i identyfikując potencjalne problemy przed ich wystąpieniem.   + Zarządzanie wieloma serwerami jednocześnie: Oprogramowanie musi umożliwiać zarządzanie co najmniej 50 serwerami z jednej platformy zarządzającej.   2. Moduł zarządzania płytą główną   * Serwer musi być wyposażony w moduł zarządzania, który oferuje następujące funkcjonalności:   + Dostęp do zdalnej konsoli serwera: Moduł musi umożliwiać pełną kontrolę nad serwerem poprzez zdalny dostęp do konsoli, niezależnie od stanu systemu operacyjnego.   + Monitorowanie sprzętu: Moduł musi zapewniać monitorowanie parametrów sprzętowych, takich jak temperatura, prędkość wentylatorów, napięcia oraz stan kluczowych komponentów.   + Obsługa wirtualnych nośników: Moduł musi umożliwiać montowanie obrazów dysków zdalnie, co ułatwia instalację systemów operacyjnych oraz aktualizacje oprogramowania.   + Bezpieczne zarządzanie: Moduł musi wspierać szyfrowanie komunikacji oraz integrację z systemami uwierzytelniania, takimi jak LDAP, oraz zarządzanie certyfikatami.   + Wsparcie dla standardowych protokołów zarządzania: Moduł musi obsługiwać popularne protokoły zarządzania sprzętem, umożliwiając integrację z zewnętrznymi systemami zarządzania.   3. System zarządzania zasobami serwera   * Serwer musi być wyposażony w oprogramowanie do zarządzania zasobami, które zapewnia:   + Monitorowanie obciążenia w czasie rzeczywistym: Oprogramowanie musi umożliwiać śledzenie wykorzystania procesora, pamięci oraz przestrzeni dyskowej, prezentując dane w formie wykresów i raportów.   + Automatyczna optymalizacja zasobów: System musi posiadać funkcję automatycznego dostosowywania przydziału zasobów, aby maksymalizować wydajność serwera.   + Zarządzanie cyklem życia sprzętu: Oprogramowanie musi wspierać planowanie konserwacji, aktualizacje oprogramowania układowego oraz zarządzanie konfiguracją serwera.   + Integracja z zewnętrznymi systemami zarządzania: System musi obsługiwać standardowe interfejsy API, co umożliwia integrację z narzędziami do automatyzacji i zarządzania infrastrukturą.   4. Oprogramowanie do zarządzania serwerem lokalnie i zdalnie   * Oferowane oprogramowanie musi umożliwiać zarządzanie serwerami zarówno lokalnie, jak i zdalnie, zapewniając:   + Automatyzację konfiguracji i monitorowania: Oprogramowanie musi umożliwiać automatyczną konfigurację serwerów, monitorowanie ich stanu oraz zarządzanie zasobami.   + Integrację z popularnymi platformami chmurowymi: Musi wspierać integrację z rozwiązaniami używanymi w środowiskach chmurowych, takimi jak narzędzia do wirtualizacji oraz systemy zarządzania centrami danych.   + Monitorowanie zużycia energii: Oprogramowanie musi oferować funkcje monitorowania zużycia energii oraz zarządzania profilami energetycznymi serwerów, co pozwala na optymalizację kosztów energii.   5. Otwarte standardy zarządzania sprzętem   * Oprogramowanie musi wspierać otwarte standardy zarządzania sprzętem, takie jak nowoczesny interfejs API, który zapewnia:   + Zdalne zarządzanie sprzętem: API musi umożliwiać programistyczne zarządzanie serwerem, monitorowanie jego parametrów oraz automatyzację zadań administracyjnych.   + Bezpieczną komunikację: API musi wspierać szyfrowanie danych oraz integrację z narzędziami do zarządzania certyfikatami. * Integrację z narzędziami do automatyzacji: API musi umożliwiać integrację z popularnymi narzędziami automatyzacji, takimi jak systemy zarządzania konfiguracją i orkiestracji. | **Producent**  **Nazwa i wersja**  **Należy podać pełną nazwę oferowanego oprogramowania**  SPEŁNIA  TAK /NIE |
|  | **Wymagania dotyczące systemu diagnostycznego** | Oferowany serwer musi być wyposażony w zaawansowany system diagnostyczny, który zapewnia kompleksowe monitorowanie stanu sprzętu oraz precyzyjną diagnostykę problemów. Wymagane są następujące funkcjonalności:  1. Funkcja diagnostyki błędów   * System musi zapewniać pełną funkcjonalność diagnostyki błędów, obejmującą:   + Zbieranie i analizę danych o błędach: Automatyczne gromadzenie danych diagnostycznych dotyczących kluczowych komponentów serwera, takich jak procesory, pamięć RAM, dyski twarde, zasilacze oraz wentylatory.   + Diagnozowanie i lokalizowanie usterek: System musi umożliwiać automatyczne wykrywanie i lokalizowanie usterek sprzętowych, wskazując precyzyjnie wadliwe komponenty.   + Wczesne ostrzeganie o błędach: Wymagane jest wsparcie dla funkcji wczesnego ostrzegania, które informuje użytkownika o potencjalnych problemach jeszcze przed ich wystąpieniem, co minimalizuje ryzyko awarii.   + Analiza historii zdarzeń: System diagnostyczny musi umożliwiać przeglądanie pełnej historii zdarzeń oraz błędów, co ułatwia analizę przyczyn awarii i planowanie działań naprawczych.   2. Zaawansowane monitorowanie dysków twardych   * System musi oferować szczegółowe monitorowanie stanu dysków twardych z podziałem na:   + Alarmy dotyczące oprogramowania układowego dysku (firmware): Wykrywanie błędów związanych z oprogramowaniem układowym dysków oraz informowanie o konieczności aktualizacji firmware’u.   + Alarmy dotyczące konfiguracji dysków: Monitorowanie nieprawidłowej konfiguracji dysków, takich jak problemy z RAID, oraz informowanie o konieczności interwencji.   + Alarmy dotyczące usterek fizycznych: Wykrywanie błędów fizycznych dysków, takich jak problemy mechaniczne lub sektory uszkodzone, z możliwością precyzyjnego wskazania wadliwego dysku.   3. Monitoring temperatury i zarządzanie termiczne   * System diagnostyczny musi zapewniać:   + Graficzną mapę temperatury: Wymagana jest funkcjonalność przeglądania rozkładu temperatury wewnątrz serwera w formie graficznego modelu 3D. Mapa temperatury musi umożliwiać szybkie lokalizowanie anomalii termicznych.   + Alerty dotyczące przekroczenia temperatur: Automatyczne powiadamianie o przekroczeniu dopuszczalnych wartości temperatury dla kluczowych komponentów, takich jak procesory, pamięć RAM czy zasilacze.   + Dynamiczne zarządzanie chłodzeniem: System musi wspierać dynamiczne dostosowywanie prędkości wentylatorów na podstawie aktualnych odczytów temperatury, co zapewnia optymalną pracę serwera i minimalizuje zużycie energii.   4. Szyfrowane powiadomienia o błędach   * Wymagane jest wsparcie dla szyfrowanych powiadomień o niekrytycznych i niekorygowalnych błędach (UCE), które umożliwiają precyzyjną identyfikację wadliwego modułu pamięci lub dysku. * System musi wspierać funkcję wysyłania powiadomień o błędach do administratora poprzez e-mail oraz protokoły zarządzania (np. SNMP, Redfish API).   5. Integracja z modułem zarządzania   * System diagnostyczny musi być w pełni zintegrowany z modułem zarządzania iBMC, co umożliwia dostęp do danych diagnostycznych z poziomu interfejsu zarządzania. * Wymagana jest możliwość przeglądania szczegółowych raportów diagnostycznych oraz uruchamiania testów diagnostycznych w czasie rzeczywistym z poziomu konsoli zarządzającej. | **Producent**  **Nazwa i wersja**  SPEŁNIA  TAK /NIE |
|  | **Certyfikaty** | * Producent serwera musi posiadać certyfikację:   + QC 080000.   + ISO 14001.   + SA8000.   + Certyfikat EPEAT minimum Bronze dla oferowanego serwera.   + Serwer musi posiadać deklaracja CE. * Proces produkcji oferowanego urządzenia musi być zgodny z wytycznymi postawionymi przez:   + ISO-9001.   + ISO-50001. | SPEŁNIA  TAK /NIE |
|  | **Parametry środowiskowe i efektywność energetyczna** | * Oferowane urządzenie musi udostępniać narzędzie, które zapewni możliwość bieżącej analizy poboru prądu. * Serwer musi być przystosowany do pracy w temperaturze od 5 do 50 stopni Celsjusza w sposób kompatybilny z wytycznymi ASHRAE A1 do A4. * Oferowane urządzenie musi być przystosowane do pracy w środowisku określonym normą ISO 14644-1. Informacja na ten temat musi znajdować się w oficjalnej dokumentacji oferowanego serwera. * Zasilacze muszą posiadać certyfikat 80 Plus Titanium, zapewniający sprawność energetyczną na poziomie co najmniej 96% przy obciążeniu 50%. | SPEŁNIA  TAK /NIE |
|  | **Dokumentacja użytkownika** | * Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim oraz dostęp do oprogramowania wymaganego do poprawnego funkcjonowania serwera. |  |
|  | **Dodatkowe oprogramowanie zabezpieczające** | System chroniący przed zagrożeniami, posiadający certyfikaty: OPSWAT Platinum, AV-Test ‘Top Product’, AV Comperative Advance +, ISO 27001 .  Szyfrowanie danych:  •Oprogramowanie do szyfrowania, chroniące dane rezydujące na punktach końcowych za pomocą silnych algorytmów szyfrowania takich jak AES, RC6, SERPENT i DWAFISH. Pełne szyfrowanie dysków działających m.in. na komputerach z systemem Windows.  •Zapobiegające utracie danych z powodu utraty / kradzieży punktu końcowego. Oprogramowanie szyfruje całą zawartość na urządzeniach przenośnych, takich jak Pen Drive’y, dyski USB i udostępnia je tylko autoryzowanym użytkownikom.  Oprogramowanie umożliwia blokowanie wybranych przez administratora urządzeń zewnętrznych podłączanych do stacji końcowej.  Oprogramowanie umożliwia zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączanie do stacji końcowej.  Istnieje możliwość blokady zapisywanie plików na zewnętrznych dyskach USB oraz blokada możliwości uruchamiania oprogramowania z takich dysków. Blokada ta powinna umożliwiać korzystanie z pozostałych danych zapisanych na takich dyskach.  Interfejs zarządzania wyświetla monity o zbliżającym się zakończeniu licencji, a także powiadamia o zakończeniu licencji.  Dodatkowy moduł chroniący dane użytkownika przed działaniem oprogramowania ransomware. Działanie modułu polega na ograniczeniu możliwości modyfikowania chronionych plików, tylko procesom systemowym oraz zaufanym aplikacjom.  Możliwość dowolnego zdefiniowania dodatkowo chronionych folderów zawierających wrażliwe dane użytkownika.  Możliwość zdefiniowania zaufanych folderów. Aplikacje uruchamiane z zaufanych folderów mają możliwość modyfikowania plików objętych dodatkową ochroną any ransomware.  Zaawansowane monitorowanie krytycznych danych użytkownika zapewniające zapobiegające prze niezamierzonymi manipulacjami – ataki ransomware  Centralna konsola zarządzająca zainstalowana na serwerze musi umożliwiać co najmniej:  • Przechowywanie danych w bazie typu SQL, z której korzysta funkcjonalność raportowania konsoli  • Zdalną instalację lub deinstalację oprogramowania ochronnego na stacjach klienckich, na pojedynczych punktach, zakresie adresów IP lub grupie z ActiveDirectory  • Tworzenie paczek instalacyjnych oprogramowania klienckiego, z rozróżnieniem docelowej platformy systemowej (w tym 32 lub 64bit dla systemów Windows i Linux), w formie plików .exe lub .msi dla Windows oraz formatach dla systemów Linux  • Centralną dystrybucję na zarządzanych klientach uaktualnień definicji ochronnych, których źródłem będzie plik lub pliki wgrane na serwer konsoli przez administratora, bez dostępu do sieci Internet.  • Raportowanie dostępne przez dedykowany panel w konsoli, z prezentacją tabelaryczną i graficzną, z możliwością automatycznego czyszczenia starych raportów, z możliwością eksportu do formatów CSV i PDF, prezentujące dane zarówno z logowania zdarzeń serwera konsoli, jak i dane/raporty zbierane ze stacji klienckich, w tym raporty o oprogramowaniu zainstalowanym na stacjach klienckich  • Definiowanie struktury zarządzanie opartej o role i polityki, w których każda z funkcjonalności musi mieć możliwość konfiguracji  Zarządzanie przez Chmurę:  1. Musi być zdolny do wyświetlania statusu bezpieczeństwa konsolidacyjnego urządzeń końcowych zainstalowanych w różnych biurach  2. Musi posiadać zdolność do tworzenia kopii zapasowych i przywracania plików konfiguracyjnych z serwera chmury  3. Musi posiadać zdolność do promowania skutecznej polityki lokalnej do globalnej i zastosować ją globalnie do wszystkich biur  4. Musi mieć możliwość tworzenia wielu poziomów dostępu do hierarchii aby umożliwić dostęp do Chmury zgodnie z przypisaniem do grupy  5. Musi posiadać dostęp do konsoli lokalnie z dowolnego miejsca w nagłych przypadkach  6. Musi posiadać możliwość przeglądania raportów podsumowujących dla wszystkich urządzeń  7. Musi posiadać zdolność do uzyskania raportów i powiadomień za pomocą poczty elektronicznej  Centralna konsola do zarządzania i monitorowania użycia zaszyfrowanych woluminów dyskowych, dystrybucji szyfrowania, polityk i centralnie zarządzanie informacjami odzyskiwania, niezbędnymi do uzyskania dostępu do zaszyfrowanych danych w nagłych przypadkach.  Aktualizacja oprogramowania w trybie offline, za pomocą paczek aktualizacyjnych ściągniętych z dedykowanej witryny producenta oprogramowania.  1.Serwer: centralna konsola zarządzająca oraz oprogramowanie chroniące serwer  2.Oprogramowanie klienckie, zarządzane z poziomu serwera.  System musi umożliwiać, w sposób centralnie zarządzany z konsoli na serwerze, co najmniej:  • różne ustawienia dostępu dla urządzeń: pełny dostęp, tylko do odczytu i blokowanie  • funkcje przyznania praw dostępu dla nośników pamięci tj. USB, CD  • funkcje regulowania połączeń WiFi i Bluetooth  • funkcje kontrolowania i regulowania użycia urządzeń peryferyjnych typu: drukarki, skanery i kamery internetowe  • funkcję blokady lub zezwolenia na połączenie się z urządzeniami mobilnymi  • funkcje blokowania dostępu dowolnemu urządzeniu  • możliwość tymczasowego dodania dostępu do urządzenia przez administratora  • zdolność do szyfrowania zawartości USB i udostępniania go na punktach końcowych z zainstalowanym oprogramowaniem klienckim systemu  • możliwość zablokowania funkcjonalności portów USB, blokując dostęp urządzeniom innym niż klawiatura i myszka  • możliwość zezwalania na dostęp tylko urządzeniom wcześniej dodanym przez administratora  • możliwość zarządzani urządzeniami podłączanymi do końcówki, takimi jak iPhone, iPad, iPod, Webcam, card reader, BlackBerry  • możliwość używania tylko zaufanych urządzeń sieciowych,w tym urządzeń wskazanych na końcówkach klienckich  • funkcję wirtualnej klawiatury  • możliwość blokowania każdej aplikacji  • możliwość zablokowania aplikacji w oparciu o kategorie  • możliwość dodania własnych aplikacji do listy zablokowanych  • zdolność do tworzenia kompletnej listy aplikacji zainstalowanych na komputerach klientach poprzez konsole administracyjna na serwerze  • dodawanie innych aplikacji  • dodawanie aplikacji w formie portable  • możliwość wyboru pojedynczej aplikacji w konkretnej wersji  • dodawanie aplikacji, których rozmiar pliku wykonywalnego ma wielkość do 200MB  • kategorie aplikacji typu: tuning software, toolbars, proxy, network tools, file sharing application, backup software, encrypting tool  • możliwość generowania i wysyłania raportów o aktywności na różnych kanałach transmisji danych, takich jak wymienne urządzenia, udziały sieciowe czy schowki.  • możliwość zablokowania funkcji Printscreen  • funkcje monitorowania przesyłu danych między aplikacjami zarówno na systemie operacyjnym Windows jak i Osx  • funkcje monitorowania i kontroli przepływu poufnych informacji  • możliwość dodawania własnych zdefiniowanych słów/fraz do wyszukania w różnych typów plików  • możliwość blokowania plików w oparciu o ich rozszerzenie lub rodzaj  • możliwość monitorowania i zarządzania danymi udostępnianymi poprzez zasoby sieciowe  • ochronę przed wyciekiem informacji na drukarki lokalne i sieciowe  • ochrona zawartości schowka systemu  • ochrona przed wyciekiem informacji w poczcie e-mail w komunikacji SSL  • możliwość dodawania wyjątków dla domen, aplikacji i lokalizacji sieciowych  • ochrona plików zamkniętych w archiwach  • Zmiana rozszerzenia pliku nie może mieć znaczenia w ochronie plików przed wyciekiem  • możliwość tworzenia profilu DLP dla każdej polityki  • wyświetlanie alertu dla użytkownika w chwili próby wykonania niepożądanego działania  • ochrona przez wyciekiem plików poprzez programy typu p2p  Monitorowanie zmian w plikach:  • Możliwość monitorowania działań związanych z obsługą plików, takich jak kopiowanie, usuwanie, przenoszenie na dyskach lokalnych, dyskach wymiennych i sieciowych.  • Funkcje monitorowania określonych rodzajów plików.  • Możliwość wykluczenia określonych plików/folderów dla procedury monitorowania.  • Generator raportów do funkcjonalności monitora zmian w plikach.  • możliwość śledzenia zmian we wszystkich plikach  • możliwość śledzenia zmian w oprogramowaniu zainstalowanym na końcówkach  • możliwość definiowana własnych typów plików  Optymalizacja systemu operacyjnego stacji klienckich:  • usuwanie tymczasowych plików, czyszczenie niepotrzebnych wpisów do rejestru oraz defragmentacji dysku  • optymalizacja w chwili startu systemu operacyjnego, przed jego całkowitym uruchomieniem  • możliwość zaplanowania optymalizacje na wskazanych stacjach klienckich  • instruktaż stanowiskowy pracowników Zamawiającego  • dokumentacja techniczna w języku polskim  Wspierane platformy i systemy operacyjne:  1.Microsoft Windows XP/7/8/10/ Professional (32-bit/64-bit)  2.Microsoft Windows Server Web / Standard / Enterprise/ Datacenter (32-bit/64-bit)  3.Mac OS X, Mac OS 10  4.Linux 64-bit, Ubuntu, openSUSE, Fedora 14-25, RedHat  Platforma do zarządzania dla Android i iOS:  • Musi zapewnić kompleksowy system ochrony i zarządzania urządzeniami mobilnymi z systemami Android oraz iOS a także ich ochronę  • Funkcjonalność musi być realizowana za pomocą platformy w chmurze bez infrastruktury wewnątrz sieci firmowej.  Zarządzanie użytkownikiem  • Musi umożliwiać zarządzanie użytkownikami przypisanymi do numerów telefonów oraz adresów email  • Musi umożliwiać przypisanie atrybutów do użytkowników, co najmniej: Imię, Nazwisko, adres email, Departament, numer telefonu stacjonarnego, numer telefonu komórkowego, typ użytkownika  • Musi posiadać możliwość sprawdzenia listy urządzeń przypisanych użytkownikowi  • Musi posiadać możliwość eksportu danych użytkownika  Zarządzanie urządzeniem  • Musi umożliwiać wdrożenie przez Email, SMS, kod QR oraz ADO  • Musi umożliwiać import listy urządzeń z pliku CSV  • Musi umożliwiać dodanie urządzeń prywatnych oraz firmowych  • Musi umożliwiać podgląd co najmniej następujących informacji konfiguracji: Data wdrożenia, typ wdrożenia, status wdrożenia, status urządzenia, numer telefonu, właściciel, typ właściciela, grupa, reguły, konfiguracja geolokacji, wersja agenta  • Musi umożliwiać podgląd co najmniej następujących informacji sprzętowych: model, producent, system, IMEI, ID SIM, dostawca SIM, adres MAC, bluetooth, Sieć, wolna przestrzeń na dysku, całkowita przeszłość na dysku, bateria, zużycie procesora, sygnał  • Musi umożliwiać podgląd lokacji w zakresach czasu: dzisiaj, wczoraj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  • Musi zawierać podgląd aktualnie zainstalowanych aplikacji  • Musi zawierać informacje o zużyciu łącza danych, a w tym: Ogólne zużycie danych, zużycie danych według aplikacji, wykres zużycia danych,  • Musi zawierać moduł raportowania aktywności, skanowania oraz naruszenia reguł  • Moduł raportowania musi umożliwiać podgląd w zakresie: dzisiaj, ostatnie 7 dni, ostatnie 15 dni, ostatnie 30 dni, własny zakres  Oprogramowanie pozwalające na wykrywaniu oraz zarządzaniu podatnościami bezpieczeństwa:  Wymagania dotyczące technologii:  1. Dostęp do rozwiązania realizowany jest za pomocą dedykowanego portalu zarządzającego dostępnego przez przeglądarkę internetową  2. Portal zarządzający musi być dostępny w postaci usługi hostowanej na serwerach producenta.  3. Dostęp do portalu zarządzającego odbywa się za pomocą wspieranych przeglądarek internetowych:  - Microsoft Internet Explorer  - Microsoft Edge  - Mozilla Firefox  - Google Chrome  - Safari  4. Rozwiązanie realizuje skany podatności za pomocą dedykowanych nodów skanujących  5 Nod skanujący musi być dostępny w postaci usługi hostowanej na serwerach producenta oraz w postaci aplikacji instalowanej lokalnie  6. Nod skanujący w postaci aplikacji instalowanej lokalnie dostępny jest na poniższe systemy operacyjne:  - Windows 2008 R2  - Windows 2012  - Windows 2012 R2  - Windows 2016  7. Portal zarządzający musi umożliwiać:  a) przegląd wybranych danych na podstawie konfigurowalnych widgetów  b) zablokowania możliwości zmiany konfiguracji widgetów  c) zarządzanie skanami podatności (start, stop), przeglądanie listy podatności oraz tworzenie raportów.  d) tworzenie grup skanów z odpowiednią konfiguracją poszczególnych skanów podatności  e) eksport wszystkich skanów podatności do pliku CSV  Backup i przywracanie danych  - Deduplikacja danych,  - Backup przyrostowy i różnicowy,  - Wersjonowanie plików – możliwość zdefiniowania dowolnej ilości wersji,  - Backup danych lokalnych – plikowy oraz poczty Outlook,  - Backup otwartych plików (VSS),  - Filtr plików oraz folderów,  - Domyślne wykluczenia zbędnych plików (pliki tymczasowe etc.),  - Wyłączanie komputera po wykonaniu backupu,  - Przywracanie danych do wskazanej lokalizacji,  - Możliwość backup-u z wykorzystaniem dowolnej ilości rdzeni procesora,  - Wyszukiwanie plików w repozytorium użytkownika,  Ustawienia  - Automatyczne logowanie,  - Zapamiętywanie danych logowania,  - Automatyczne uruchamianie programu przy starcie systemu,  - Ustawianie priorytetu dla procesu backupu,  - Zmiana klucza szyfrującego,  - Ustawienia przepustowości/zajętości pasma,  - Konfiguracja wydajności procesu backupu,  Bezpieczeństwo  - Zastępowanie nazwy pliku GUID-em,  - Szyfrowanie danych algorytmem AES 256 CBC, zawsze po stronie komputera użytkownika,  - Kompresja danych,  - Transmisja po bezpiecznym protokole TLS,  - Deklaracja klucza szyfrującego dane użytkownika,  - Szczegółowy dziennik zdarzeń dostępny z poziomu aplikacji,  - Obliczanie sumy kontrolnej,  - Kopie zapasowe są przechowywane w profesjonalnych, certyfikowanych data center, na terenie Polski.  WSPIERANE SYSTEMY OPERACYJNE Microsoft Windows 7 i nowsze, Mac OS,Licencje przypisywane do jednego urządzenia z limitem pojemności przestrzeni w chmurze – minimum 50 GB. Wsparcie techniczne, świadczone jest bezpośrednio od producenta, w języku polskim, zawarte jest w cenie licencji.   * Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 oraz 27001 w zakresie świadczenia usług wsparcia technicznego oraz usług związanych z cyberbezpieczeństwem. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. | **Producent**  **Nazwa i wersja**  **Należy też podać pełną nazwę oferowanego oprogramowania**  SPEŁNIA  TAK /NIE |
|  | **Warunki gwarancji** | * Zamawiający wymaga zapewnienia oficjalnego wsparcia Producenta w ramach oferowanej technologii na okres 3 lat świadczone na miejscu u klienta. * Zamawiający wymaga przynajmniej dwóch podstawowych form kontaktu serwisowego tj. całodobowej infolinii oraz formularza online. * Oferowane wsparcie musi być świadczone w języku polskim bezpośrednio przez Producenta. * Wymagane dołączenie do oferty oświadczenia potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.   Usługi serwisowe obejmują:   * Diagnozowanie problemów sprzętowych i programowych. * Aktualizacje firmware oraz dostęp do najnowszych wersji sterowników przez okres trwania wsparcia. * Naprawy na miejscu w siedzibie zamawiającego. * Czas reakcji serwisu do następnego dnia roboczego. * Naprawy muszą być przeprowadzone przez certyfikowany personel Producenta lub partnera serwisowego posiadającego certyfikację ISO 9001, ISO 27001 **– dokumenty należy dołączyć na etapie umowy z Wykonawcą.** | SPEŁNIA  TAK /NIE |

# Przełącznik (switch) – 2 szt.

| **L.P.** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
| --- | --- | --- | --- |
| 1 | Liczba portów | Minimum 8 portów 10/100/1000 Mbps oraz 2 porty combo 10/100/1000BASE-T/SFP. | Producent  Model i wersja |
| 2 | Przepustowość przełączania | Przepustowość przełączania co najmniej 20 Gbps. | SPEŁNIA  TAK /NIE |
| 3 | Szybkość przekierowań pakietów | Minimum 14,88 Mpps dla 64-bajtowych pakietów. | SPEŁNIA  TAK /NIE |
| 4 | Bufor pamięci | Co najmniej 512 KB pamięci buforowej. | SPEŁNIA  TAK /NIE |
| 5 | Tablica adresów MAC | Obsługa minimum 8 000 adresów MAC. | SPEŁNIA  TAK /NIE |
| 6 | Obsługiwane standardy | Zgodność z IEEE 802.3, 802.3u, 802.3ab, 802.3x, 802.3az. | SPEŁNIA  TAK /NIE |
| 7 | Zarządzanie | Możliwość zarządzania przez przeglądarkę WWW (GUI), wiersz poleceń (CLI), SNMP v1/v2c/v3, RMON, Telnet. | SPEŁNIA  TAK /NIE |
| 8 | Funkcje warstwy 2 | Obsługa IGMP Snooping, Port Mirroring, Spanning Tree Protocol (STP), Link Aggregation Control Protocol (LACP). | SPEŁNIA  TAK /NIE |
| 9 | QoS (Quality of Service) | Możliwość definiowania priorytetów ruchu sieciowego z co najmniej 8 kolejkami na port. | SPEŁNIA  TAK /NIE |
| 10 | VLAN | Obsługa co najmniej 256 grup VLAN oraz zaawansowanych funkcji VLAN, takich jak Auto Voice VLAN i Auto Surveillance VLAN. | SPEŁNIA  TAK /NIE |
| 11 | Bezpieczeństwo | Funkcje takie jak Access Control List (ACL), 802.1X, ARP Spoofing Prevention, D-Link Safeguard Engine lub równoważne. | SPEŁNIA  TAK /NIE |
| 12 | Zasilanie | Zasilanie zewnętrzne z maksymalnym poborem mocy nieprzekraczającym 13,6 W. | SPEŁNIA  TAK /NIE |
| 13 | Wymiary | Szerokość: 280 mm, Wysokość: 44 mm, Głębokość: 180 mm. | SPEŁNIA  TAK /NIE |
| 14 | Waga | Maksymalnie 1,84 kg. | SPEŁNIA  TAK /NIE |
| 15 | Gwarancja | Gwarancja producenta minimum 36 m-cy lub równoważna. | SPEŁNIA  TAK /NIE |

# UPS serwerowy – 1 szt.

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry (potwierdź spełnienie poprzez skreślenie niepoprawnej odpowiedzi) oraz wpis wymagane dane według wskazań** |
|  | Przeznaczenie | Urządzenie przeznaczone dla urządzeń serwerowych do jednostek podległych Zamawiającemu , celem podtrzymywania zasilania na wypadek przerw dostawie prądu | **Producent**  **Nazwa i model oferowanego sprzętu** |
|  | Moc pozorna | minimum 2000VA | SPEŁNIA  TAK /NIE |
|  | Moc rzeczywista | minimum 2000W | SPEŁNIA  TAK /NIE |
|  | Technologia | on-line (VFI), podwójna konwersja | SPEŁNIA  TAK /NIE |
|  | Sprawność przy pracy sieciowej i w pełni naładowanych bateriach | ˃ 91 % | SPEŁNIA  TAK /NIE |
|  | Sprawność w trybie ECO i w pełni naładowanych bateriach | ˃ 96 % | SPEŁNIA  TAK /NIE |
|  | Typ obudowy | rack/tower | SPEŁNIA  TAK /NIE |
| **Wejście** | | | |
|  | Napięcie wejściowe | minimum 220/230/240 V AC | SPEŁNIA  TAK /NIE |
|  | Częstotliwość napięcia wejściowego | 40Hz - 70Hz | SPEŁNIA  TAK /NIE |
|  | Zakres napięcia wejściowego | minimum 160-300 VAC ± 5% @ 100% obciążenia | SPEŁNIA  TAK /NIE |
|  | Współczynnik odkształceń prądu wejściowego THDi | < 5% | SPEŁNIA  TAK /NIE |
| **Wyjście** | | | |
|  | Zakres napięcia wyjściowego | minimum 200 / 208 / 220 / 230 / 240 V AC ± 1 % | SPEŁNIA  TAK /NIE |
|  | Regulacja napięcia w trybe bateryjnym | ± 1% | SPEŁNIA  TAK /NIE |
|  | Częstotliwość napięcia wyjściowego | minimum 50/60 Hz ± 0,1Hz | SPEŁNIA  TAK /NIE |
|  | Kształt napięcia wyjściowego | sinusoidalny | SPEŁNIA  TAK /NIE |
|  | Współczynnik szczytu | 3:1 | SPEŁNIA  TAK /NIE |
|  | Czas przełączania sieć – bateria | 0ms | SPEŁNIA  TAK /NIE |
|  | Współczynnik odkształceń prądu wejściowego THD | ≦ 2 % (obciążenie liniowe); ≦ 4 % (obciążenie nieliniowe) | SPEŁNIA  TAK /NIE |
|  | Kształt napięcia wyjściowego na pracy bateryjnej | sinusoidalny | SPEŁNIA  TAK /NIE |
|  | Baterie wewnętrzne w UPS | minimum 12V 9Ah; szczelne, bezobsługowe | SPEŁNIA  TAK /NIE |
|  | Czas podtrzymania (90 % Pmax) - przy zastosowaniu wyłącznie wewnętrznych baterii | minimum 5 minut | SPEŁNIA  TAK /NIE |
| **Pozostałe** | | | |
|  | Regulowany prąd ładowania baterii | od 2A do 8A | SPEŁNIA  TAK /NIE |
|  | Wejście zasilania | 1 x IEC 320 C20 (16 A) | SPEŁNIA  TAK /NIE |
|  | Ilość i typ gniazd wyjściowych | min 8x IEC 320 C13 (10 A), z czego minimum sekcja 4 gniazda sterowalna | SPEŁNIA  TAK /NIE |
|  | Sygnalizacja | Dźwiękowa, Wyświetlacz LCD (obracany) | SPEŁNIA  TAK /NIE |
|  | Informacje wyświetlane na panelu LCD | * minimum poziom obciążenia (w %), * poziom naładowania baterii (w %), * praca z sieci/baterii/ładowanie baterii, * przeciążenie, * niski poziom baterii, * bateria nie podłączona, * tryb ECO/Bypass, * napięcie wej/wyj, * czętotliwość wej/wyj, * napięcie baterii, * temperatura otoczenia, * wyłączenie dźwięku, |  |
|  | Dostępne ustawienia z panelu LCD | * minimum ustawienie napięcia wyjściowego, * ustawienie częstotiwości wyjściowej, włączenie trybu ECO, * ustawienie zakresu napięcia w trybie ECO, * włączenie/wyłączenie trybu Bypass, ustawienie zakresu napięcia w trybie Bypass, * ustawienie zakresu częstotliwości w trybie Bypass, * włączenie/wyłączenie sterowalnych gniazd, ustawienie czasu zasilania sterowalnych gniazd, ustawienie pojemności zainstalowanych baterii, ustawienie prądu ładowania ładowarki, * ustawienie logiki EPO, włączenie auto testu | SPEŁNIA  TAK /NIE |
|  | Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych (producenta) | wymagane | SPEŁNIA  TAK /NIE |
|  | Możliwość podłączenia dodatkowych, zewnętrznych baterii o pojemności powyżej 9Ah za pomocą kabla dostarczanego przez producenta. Kabel powinien być wyposażony z jednej strony we wtyk pasujący do UPSa a z drugiej strony w tulejki oczkowe. | wymagane | SPEŁNIA  TAK /NIE |
|  | Interfejs komunikacyjny - każdy jako osobne gniazdo/złącze | RS232, USB, SNMP | SPEŁNIA  TAK /NIE |
|  | Karta SNMP | wymgana uniwersalna karta dla UPS 1-fazowych i 3-fazowych tego samego producenta | SPEŁNIA  TAK /NIE |
|  | Wsporniki do montażu w szafie RACK | wymagane | SPEŁNIA  TAK /NIE |
|  | Zabezpieczenia | minimum przeciwzwarciowe, przeciwprzepięciowe,  przeciążeniowe | SPEŁNIA  TAK /NIE |
|  | Złącze EPO | wymagane | SPEŁNIA  TAK /NIE |
|  | Waga UPS | do 21 kg | SPEŁNIA  TAK /NIE |
|  | Wymiary UPS - wersja RACK | nie większe niż: wysokość 2U; głębokość 510 mm | SPEŁNIA  TAK /NIE |
|  | Gwarancja | minimum 12 miesięcy na elektronikę i 12 miesięcy na akumulatory; | SPEŁNIA  TAK /NIE |
|  | Serwis | autoryzowany serwis producenta zlokalizowany w Polsce.  naprawa w maksymalnie 5 dni roboczych  serwis realizowany w systemie door to door | SPEŁNIA  TAK /NIE |
|  | Oprogramowanie | * oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS * jedno wspólne oprogramowanie do zarzadzania UPSami 1-fazowymi i 3-fazowymi tego samego producenta * wsparcie dla systemów: Windows, Linux * wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe) | SPEŁNIA  TAK /NIE |
|  | Oświadczenia / dokumenty | dla gwarancji standardowej lub rozszerzonej wymagane jest by realizowana była wyłącznie przez autoryzowany serwis producenta - **należy przedstawić odpowiednie oświadczenie producenta/lub wyłącznego Dystrybutora certyfikat lub oświadczenie producenta o posiadaniu przez oferenta statusu Autoryzowanego Partnera** - mającego wiedzę w zakresie doboru i sprzedaży zasilaczy UPS jeżeli oferent nie jest producentem danego urządzenia  deklaracja zgodności CE  **(wymagane dokumenty/oświadczenia należy dołączyć na etapie umowy z Wykonawcą.** | SPEŁNIA  TAK /NIE |
|  |

…………………………………….

Data, czytelny podpis i pieczęć Oferenta