

**Załącznik nr 1A do formularza ofertowego**

**– Formularz cenowy –**

**kalkulacja kosztów dla Części Nr I**

**Specyfikacja warunków zamówienia**

**I część: dostawa sprzętu komputerowego**

1. Serwer – szt 1

………………………………………………………………………………………………………………………………

*(wykonawca winien opisać oferowany sprzęt, Producent/typ/model/opis)*

OFEROWANA CENA BRUTTO :……………………………. ZŁ/ 1 SZTUKĘ

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Opis parametrów oferowanego sprzętu** |
| 1. | Charakterystyka ogólna | Serwer będzie przeznaczony do instalacji oprogramowania zwiększającego poziom cyberbezpieczeństwa w środowisku Zamawiającego. Na serwerze będą instalowane i dostępne narzędzia do ochrony sieci, takie jak system do skanowania aktywów Zamawiającego, inwentaryzacja sieci , systemy DLP do ochrony przed wyciekiem danych, domena do zarzadzania siecią i zwiększenie wpływów nad zarzadzaniem użytkownikami . Jego przeznaczenie to ochrona infrastruktury IT przed zagrożeniami, zarządzaniem dostępem do zasobów oraz zapewnieniem bezpieczeństwa | **SPEŁNIA**  **TAK/NIE** |
| 2. | **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji min. 8 dysków 2.5”  Obudowa wyposażona w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. 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. | **SPEŁNIA**  **TAK/NIE** |
| 3. | **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych.  Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.  Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.  Płyta główna powinna obsługiwać do 1TB pamięci RAM. | **SPEŁNIA**  **TAK/NIE** |
| 4. | **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. | **SPEŁNIA**  **TAK/NIE** |
| 5. | **Procesor** | Zainstalowane dwa procesory 12-rdzeniowy, min. 2.0GHz, umożliwiający osiągnięcie wyniku min. 214 w teście SPECrate2017\_int\_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej | **SPEŁNIA**  **TAK/NIE** |
| 6. | **RAM** | Minimum 256GB DDR5 RDIMM 5600MT/s, ECC osiągnięte za pomocą 4 modułów 64GB | **SPEŁNIA**  **TAK/NIE** |
| 7. | **Funkcjonalność pamięci RAM** | Demand Scrubing, Patrol Scrubing, Permanent Fault Detection | **SPEŁNIA**  **TAK/NIE** |
| 8. | **Gniazda PCI** | minimum dwa sloty PCIe | **SPEŁNIA**  **TAK/NIE** |
| 9. | **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) | **SPEŁNIA**  **TAK/NIE** |
| 10. | **Dyski twarde** | Zainstalowane:  3x dysk SSD SATA o pojemności min. 960GB, 6Gbps, 2,5“ Hot-Plug. 2x dysk M.2 NVME o pojemności min. 480GB | **SPEŁNIA**  **TAK/NIE** |
| 11. | **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający  Min. 8GB nieulotnej pamięci cache,  Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących | **SPEŁNIA**  **TAK/NIE** |
| 12. | **Moduł NVME**  **do instalacji systemu operacyjnego** | Karta rozszerzeń umożliwiająca instalację systemu operacyjnego na redundantnych dyskach NVMe M.2 w konfiguracji RAID 1.  PCIe Gen3 x4 lub złącze dedykowane zgodne z architekturą serwera. Obsługiwane dyski: Minimum 2 × NVMe M.2. Obsługa RAID: RAID 1. | **SPEŁNIA**  **TAK/NIE** |
| 13. | **Wbudowane porty** | 4 x USB z czego nie mniej niż 1x USB 3.0,  2x VGA | **SPEŁNIA**  **TAK/NIE** |
| 14. | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 | **SPEŁNIA**  **TAK/NIE** |
| 15. | **Zasilacze** | Redundantne, Hot-Plug min. 700W klasy Titanium | **SPEŁNIA**  **TAK/NIE** |
| 16. | **Elementy montażowe** | Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych | **SPEŁNIA**  **TAK/NIE** |
| 17. | **System operacyjny** | Microsoft Windows Server 2022 Standard lub równoważny spełniający min. poniższe wymagania:  Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i minimum 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. | **SPEŁNIA**  **TAK/NIE** |
| 18. | **Licencje dostępowe** | Licencje dostępowe CAL , dla użytkowników w ilości 40 szt. | **SPEŁNIA**  **TAK/NIE** |
| 19. | **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  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  Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). | **SPEŁNIA**  **TAK/NIE** |
| 20. | **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) | **SPEŁNIA**  **TAK/NIE** |
| 21. | **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. | **SPEŁNIA**  **TAK/NIE** |
| 22. | **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO14001  Serwer musi posiadać deklaracja CE.  Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami.  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 25gramowe 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](http://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 2019, Microsoft Windows Server 2022. | **SPEŁNIA**  **TAK/NIE** |
| 23. | **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. | **SPEŁNIA**  **TAK/NIE** |
| 24. | **Wsparcie techniczne i oprogramowanie** – w formularzu oferty należy podać pełną nazwę oferowanego  oprogramowania | Oprogramowanie producenta połączone z oficjalnym działem wsparcia technicznego, automatycznie tworzące zgłoszenia serwisowe w przypadku awarii.  Zgłoszenia serwisowe zgłaszane przez aplikację muszą być traktowane na równi z tradycyjnym zgłoszeniem serwisowym przez dział techniczny producenta serwera. Oprogramowanie powinno być dostępne w postaci aplikacji na systemy Windows lub linux lub w postaci maszyny wirtualnej potrafiącej obsłużyć jednocześnie wiele serwerów.  Konfiguracja i zaoferowany poziom wsparcia powinien po wystąpieniu awarii urządzenia automatycznie zakładać zlecenie serwisowe w dziale wsparcia producenta, poinformować o tym za pomocą wiadomości e-mail, a następnie dział wsparcia powinien się kontaktować z klientem w celu rozwiązania problemu.  Oprogramowanie musi współpracować z kartą do zarządzania w urządzeniu, która będzie działać niezależnie od zainstalowanego systemu operacyjnego, posiadająca dedykowane port RJ-45 Gigabit. Karta musi umożliwiać podmontowanie zdalnych wirtualnych napędów, oraz wirtualną konsolę z dostępem do myszy, klawiatury. Oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :  Proaktywne, zautomatyzowane wykrywanie problemów, tworzenie zgłoszeń i wysyłanie powiadomień.  Predykcyjna analiza i wykrywanie awarii dysków twardych i płyt głównych serwerów. Szybsze rozwiązywanie problemów dzięki zdalnemu dostępowi i bezpiecznej dwukierunkowej komunikacji między serwisem producenta serwera, a środowiskiem klienta.  upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji, możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :  o poprawkach i usprawnieniach dotyczących aktualizacji  dacie wydania ostatniej aktualizacji priorytecie aktualizacji  zgodność z systemami operacyjnymi  jakiego komponentu sprzętu dotyczy aktualizacja wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.  wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.  - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty ( ddmm-rrrr ) sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą ( dd-mm-rrrr ) i wersją ( rewizja wydania )  dokładny wykaz wymaganych sterowników, aplikacji, BIOS’u z informacją o zainstalowanej obecnie wersji dla oferowanego komputera z możliwością exportu do pliku o rozszerzeniu \*.xml  raport uwzględniający informacje o: sprawdzaniu aktualizacji, znalezionych aktualizacjach, ściągniętych aktualizacjach , zainstalowanych aktualizacjach z dokładnym rozbiciem jakich komponentów to dotyczyło, błędach podczas sprawdzania, instalowania oraz możliwość exportu takiego raportu do pliku \*.xml od razu spakowany z rozszerzeniem \*.zip. Raport musi zawierać z dokładną datą ( dd-mm- rrrr ) i godziną z podjętych i wykonanych akcji/zadań w przedziale czasowym do min. 1 roku. | **SPEŁNIA**  **TAK/NIE** |

1. UTM - **ZAPORA SIECIOWA UTM OCHRONA STYKU SIECI LAN /WAN - szt 2**

………………………………………………………………………………………………………………………………

*(wykonawca winien opisać oferowany sprzęt, Producent/typ/model/opis)*

OFEROWANA CENA BRUTTO :……………………………. ZŁ/ 2 SZTUKI

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Opis parametrów oferowanego sprzętu** |
| **1.** | Wymagania Ogólne | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzwanego dytrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS,  Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły IPv4 oraz IPv6 w zakresie:  Firewall.  Ochrony w warstwie aplikacji.  Protokołów routingu dynamicznego. Redundancja, monitoring i wykrywanie awarii  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.  Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  Monitoring stanu realizowanych połączeń VPN.  System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP.  Ponadto daje możliwość tworzenia interfejsów redundantnych.  Interfejsy, Dysk, Zasilanie:  System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  5 portami Gigabit Ethernet RJ-45.  System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.  System jest wyposażony w zasilanie AC.  Parametry wydajnościowe:  W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.  Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.  Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.  Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1 Gbps.  Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.  Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.  Systemu Bezpieczeństwa:  W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:  Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  Kontrola Aplikacji.  Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.  Ochrona przed malware.  Ochrona przed atakami - Intrusion Prevention System.  Kontrola stron WWW.  Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.  Zarządzanie pasmem (QoS, Traffic shaping).  Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 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.  Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.  Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).  Polityki, Firewall  Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  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.  W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.  Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.  Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.  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.  Połączenia VPN  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 zasobó wsystemu. 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.  System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.  Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.  Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.  Routing i obsługa łączy WAN  W zakresie routingu rozwiązanie zapewnia obsługę:  Routingu statycznego.  Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).  Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.  Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.  ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.  BFD (Bidirectional Forwarding Detection).  Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.  Funkcje SD-WAN  System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).  Zarządzanie pasmem  System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  System daje możliwość określania pasma dla poszczególnych aplikacji.  System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.  System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. Ochrona przed malware  Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.  System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.  System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.  System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.  Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.  Ochrona przed atakami  Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  System chroni przed atakami na aplikacje pracujące na niestandardowych portach.  Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.  System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).  Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.  Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.  Kontrola aplikacji  Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np.  dopuszczenie tylko HTTP na porcie 80).  Kontrola WWW  Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 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.  Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).  Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.  Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania  WWW.  System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.  Uwierzytelnianie użytkowników w ramach sesji  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.  System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  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.  Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.  Zarządzanie  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.  Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.  Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.  System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.  System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).  Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.  Logowanie  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.  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.  Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.  Możliwość włączenia logowania per reguła w polityce firewall.  System zapewnia możliwość logowania do serwera SYSLOG.  Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.  Testy wydajnościowe oraz funkcjonalne  Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.  Serwisy i licencje  Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:  a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, bazy reputacyjne adresów IP/domen na okres [24 miesięcy.  Gwarancja oraz wsparcie  System jest objęty serwisem gwarancyjnym producenta przez okres [12] miesiące polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Obsługa zgłoszenia w tym zwrot uszkodzonego urządzenia do producenta, bez dodatkowych kosztów po stronie zamawiającego, realizowana przez producenta lub autoryzowanego dystrybutora w języku polskim przez okres wymaganej gwarancji.  Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji.  Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta w języku polskim w zakresie:  obsługa procesu RMA u producenta, zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta, jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej producenta, dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.  Dostęp do usługi powinien być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres).  Usługa ta ma być świadczona prze podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.  Do oferty należy załączyć oświadczenie producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001 oraz certyfikat potwierdzający posiadany najwyższy poziom certyfikacji technicznej producenta .  Rozszerzone wsparcie serwisowe AHB/SOS  a) System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesiące Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7  System 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 jest objęty usługą wsparcia technicznego świadczoną przez.  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.  Dla zapewnienia wysokiego poziomu usług, podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Czas reakcji jest nie dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.  Wymagania powinny być potwierdzone dokumentami: Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).  Certyfikat ISO 9001 podmiotu serwisującego. Załączyć do oferty | SPEŁNIA  TAK/NIE |

1. Macierz dyskowa – 1 szt + dyski – 6 szt

………………………………………………………………………………………………………………………………

*(wykonawca winien opisać oferowany sprzęt, Producent/typ/model/opis)*

MACIERZ DYSKOWA OFEROWANA CENA BRUTTO :……………………………. ZŁ/ 1 SZTUKĘ

Dyski – 6 szt

………………………………………………………………………………………………………………………………

*(wykonawca winien opisać oferowany sprzęt, Producent/typ/model/opis)*

DYSKI OFEROWANA CENA BRUTTO :……………………………. ZŁ/ 6 SZTUKĘ

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr** | **Wymagania minimalne** | **Opis parametrów oferowanego sprzętu** |
|  | Obudowa | Do instalacji w standardowej szafie RACK 19” z kompletem szyn przesuwnych w zestawie. Macierz musi zajmować wysokość maksymalnie 2U i pozwalać na instalacje min. 12 dysków. Nie dopuszcza się zastosowania rozwiązania złożonego z macierzy wraz z jednostką rozszerzającą o takiej samej wysokości maksymalnej. | SPEŁNIA  TAK/NIE |
|  | Rozbudowa | Do minimum 440 dysków poprzez dołożenie jednostek rozszerzających. | SPEŁNIA  TAK/NIE |
|  | Obsługiwane dyski | Minimum:  • 2.5" 12Gb/s SAS SSD,  • 2.5" 12Gb/s SAS 10,000 RPM HDD,  • 3.5" 12Gb/s NL-SAS 7,200 RPM HDD.  Macierz musi umożliwiać zastosowanie dysków rożnych producentów bez ograniczeń do dysków tego samego producenta co macierz (brak tzw. „vendor lock”). | SPEŁNIA  TAK/NIE |
|  | Zainstalowane dyski | Minimum 6 dysków zgodnych z listą kompatybilności oferowanej macierzy oraz charakteryzujących się następującymi parametrami:   * pojemność: minimum 3.84TB, * odczyt sekwencyjny: do 4000 MB/s, * zapis sekwencyjny: do 3500 MB/s, * losowy odczyt: do 760 tys. IOPS, * losowy zapis: do 130 tys. IOPS, * interfejs: SAS 12Gb/s lub SAS 24Gb/s, * gwarancja: minimum 60 miesięcy, * wytrzymałość: minimum 1 DWPD. | SPEŁNIA  TAK/NIE |
|  | Kontrolery | Dwa sprzętowe kontrolery pracujące w trybie active-active. | SPEŁNIA  TAK/NIE |
|  | Cache kontrolera | Minimum 16GB DDR4 ECC z możliwością rozbudowy do minimum 128GB. | SPEŁNIA  TAK/NIE |
|  | Zabezpieczenie pamięci cache | Moduł podtrzymania pamięci cache oparty o kondensator wraz dyskiem flash, który w przypadku awarii zasilania macierzy zabezpieczy dane przechowywane w pamięci podręcznej cache, które nie zostały zapisane na dyskach. | SPEŁNIA  TAK/NIE |
|  | Wentylatory | Wentylatory lub moduły wentylatora z możliwością wymiany podczas pracy macierzy. | SPEŁNIA  TAK/NIE |
|  | Zasilanie | Redundantny zasilacz o mocy minimalnej pozwalającej na bezproblemową pracę macierzy w przypadku awarii jednego modułu zasilacza, potwierdzony certyfikatem sprawności 80 PLUS Platinum lub wyższym. | SPEŁNIA  TAK/NIE |
|  | Obsługiwane typy RAID | Minimum RAID 0, 1, 5, 6, 10, 50, 60 | SPEŁNIA  TAK/NIE |
|  | Interfejsy kontrolera | Minimum:   * 1 port 1GbE RJ-45 LAN (zarządzanie), * 2 porty 12Gb SAS 12Gb/s (do podłączania jednostek rozszerzających) * 4 porty 10GbE SFP+ iSCSI (z kompletem modułów 10Gb/s SFP+ SR) | SPEŁNIA  TAK/NIE |
|  | Rozbudowa interfejsów kontrolera | Możliwość zamontowania dodatkowych rozszerzeń, minimum:   * 4 portowych 10GbE SFP+ iSCSI, * 2 lub 4 portowych 25GbE SFP28 iSCSI, * 2 lub 4 portowych 16Gb SFP+ Fibre Channel, * 2 portowych 32Gb SFP28 Fibre Channel. | SPEŁNIA  TAK/NIE |
|  | Oprogramowanie i funkcjonalności | * Migawki blokowe (minimalnie 4096 migawek na cały system), * Thin provisioning z odzyskiwaniem miejsca, * zdalna replikacja asynchroniczna, * zdalna replikacja synchroniczna (opcja), * Konfiguracja Quality of Service (QoS), * Automatyczne warstwowanie danych (opcja), * Pamięć podręczna SSD Cache (opcja), * Obsługa LACP, Multi-pathing, Trunking oraz Jumbo frame, * wsparcie dla RESTful API.   Jeżeli którakolwiek funkcjonalność wymaga aktywacji poprzez dodatkową licencję wymagana jest możliwość zakupu takiej licencji osobno po zakupie macierzy. Nie jest wymagane dostarczenie licencji na etapie dostawy macierzy. | SPEŁNIA  TAK/NIE |
|  | Wsparcie dla systemów operacyjnych i środowisk wirtualizacji | Minimum Windows Server 2022, VMware vSphere ESXI 8 | SPEŁNIA  TAK/NIE |
|  | Certyfikaty | CE, Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2015 i ISO 14001:2015. | SPEŁNIA  TAK/NIE |
|  | Dokumentacja | Zamawiający wymaga dokumentacji w języku polskim lub angielskim. | SPEŁNIA  TAK/NIE |
|  | Gwarancja | Minimum 36 miesięcy gwarancji Next Business Day producenta. W przypadku potwierdzonej awarii sprzętowej dostarczone zostaną sprawne, pojedyncze elementy macierzy (np. moduł zasilacza, kontroler). Wymianę uszkodzonych podzespołów realizuje klient we własnym zakresie. Obowiązuje od poniedziałku do piątku w dni robocze. Nie dotyczy dysków.  Wymagana jest możliwość sprawdzenia typu i ważności gwarancji, a także szczegółowej konfiguracji sprzętowej poprzez dedykowaną stronę producenta. Strona ta po podaniu unikalnego numeru identyfikacyjnego macierzy powinna udostępniać informacje dotyczące modelu macierzy, wersji oprogramowania, zamontowanych dodatkowych kart rozszerzeń, pamięci RAM, aktywowanych licencji oraz modelu i wersji oprogramowania zainstalowanych dysków HDD i SSD. | SPEŁNIA  TAK/NIE |

1. zarządzane urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X – 2 szt.

………………………………………………………………………………………………………………………………

*(wykonawca winien opisać oferowany sprzęt, Producent/typ/model/opis)*

OFEROWANA CENA BRUTTO :……………………………. ZŁ/ 2 SZTUKI

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Opis parametrów oferowanego sprzętu** |
| 1. | Cechy zarządzania | Warstwa przełącznika: L2/L3  Obsługa jakości usług (QoS): Tak  Zarządzanie przez stronę WWW: Tak  Inspekcja ARP: Tak  Porty Poe: Tak  Konfigurowanie ustawień lokalizacji (CLI): Tak  Obsługa MIB: Tak | SPEŁNIA  TAK/NIE |
| 2. | Porty i interfejsy | Liczba portów Ethernet RJ-45: 48  Liczba portów PoE: 48  Typ portów Ethernet RJ-45: Gigabit Ethernet (10/100/1000)  Liczba zainstalowanych modułów SFP+: 4 | SPEŁNIA  TAK/NIE |
| 3. | Sieć | Obsługiwane standardy: IEEE 802.1Q, IEEE 802.1ab, IEEE 802.1ad, IEEE 802.1w, IEEE 802.1x, IEEE 802.3, IEEE 802.3ad, IEEE 802.3u, IEEE 802.3x, IEEE 802.3z  Dublowanie portów: Tak  Blokowanie head-of-line (HOL): Tak  Prędkość transferu danych: 1000 Mbit/s  Kontrola wzrostu natężenia ruchu: Tak  Protokół drzewa rozpinającego: Tak  Podpora kontroli przepływu: Tak  Obsługa sieci VLAN: Tak  Obsługa Multicast: Tak | SPEŁNIA  TAK/NIE |
| 4. | Przesyłanie danych | Trasa statyczna: Tak  Zgodność z Jumbo Frames: Tak  Rozszerzenie Jumbo Frames: 9000 | SPEŁNIA  TAK/NIE |
| 5. | Ochrona | Lista kontrolna dostępu (ACL): Tak  IGMP snooping: Tak  Obsługa SSH/SSL: Tak  Szyfrowanie / bezpieczeństwo: HTTPS, SSH, SSL/TLS  Filtrowanie adresów MAC: Tak | SPEŁNIA  TAK/NIE |
| 6. | Konstrukcja | Kolor: Biały  Materiał obudowy: Metal  Przycisk reset: Tak  Diody LED: Tak  Szerokość: 350 mm  Głębokość: 444,5 mm  Wysokość: 43,9 mm | SPEŁNIA  TAK/NIE |
| 7. | Wydajność | Taktowanie procesora: 1400 MHz  Pamięć wewnętrzna: 1024 MB  Wielkość pamięci flash: 512 MB | SPEŁNIA  TAK/NIE |
| 8. | Zasilanie | Źródło zasilania: Prąd przemienny  Typ wtyczki: Typu C | SPEŁNIA  TAK/NIE |
| 9. | Oprogramowanie | Dostęp do najnowszych aktualizacji firmware bezpośrednio ze strony producenta | SPEŁNIA  TAK/NIE |

**ŁĄCZNA CENA OFERTOWA BRUTTO za Część NR I zamówienia:: …………………………… ZŁ**

***UWAGA:***

***Formularz cenowy składa się, pod rygorem nieważności, w formie elektronicznej (tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym przez osobę lub osoby uprawnione do reprezentowania wykonawcy wraz z dokumentami potwierdzającymi prawo do reprezentacji wykonawcy przez osobę lub osoby podpisujące ofertę.***