**Załącznik nr 1**

**Macierz dyskowa**

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany PODAĆ** |
| **Obudowa** | Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje 24 dysków 2.5”. | PODAĆ |
|  | Urządzenie fabrycznie nowe - nie powystawowe, ani niepotestowe | PODAĆ |
| **Kontrolery** | Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów iSCSI 10Gb/s BASE-T. | PODAĆ |
| **Cache** | 8GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii. | PODAĆ |
| **Dyski** | Zainstalowane 12 dysków 2,5” Hot-Plug SSD SAS do intensywnego odczytu o pojemności 960GB, możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych do łącznie minimum 276 dysków. Możliwość mieszania typów dysków w obrębie macierzy oraz pojedynczej półki. | PODAĆ |
| **Oprogramowanie/Funkcjonalności** | Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. Powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Macierz powinna zostać dostarczona z licencją umożliwiającą utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz.  Licencja zaoferowanej macierzy powinna umożliwiać podłączanie minimum 8 hostów bez konieczności zakupu dodatkowych licencji.  Konieczne jest posiadanie automatycznego, bez interwencji człowieka, rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane miedzy rożnymi typami dysków.  Możliwość wykorzystania dysków SSD jako cache macierzy, możliwość rozbudowy pamięci cache do min. 4TB poprzez dyski SSD.  Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie asynchronicznym. | PODAĆ |
| **Wsparcie dla systemów operacyjnych** | Windows Server 2012 R2, Windows Server 2016, Red Hat Enterprise Linux (RHEL), SLES, Vmware ESXi. | PODAĆ |
| **Bezpieczeństwo** | Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne. | PODAĆ |

|  |  |  |
| --- | --- | --- |
| **Warunki gwarancji dla macierzy** | Min. 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  W przypadku awarii dysków pozostają one własnością Zamawiającego.  Autoryzowany serwis gwarancyjny i pogwarancyjny. Wpisać lub podać w formie załącznika ilość punktów serwisowych, nazwa serwisu, adres, nr telefonu , fax. , adres e-mail. W przypadku zaprzestania działalności dotychczasowego serwisanta wskazanie innego, autoryzowanego serwisu.  Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji macierzy.   * Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu. * Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części I transportu. * W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych). | PODAĆ WARUNKI GWARANCJI |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim dostarczonej najpóźniej w dniu podpisania Protokołu Instalacji i Odbioru | PODAĆ |
| **Certyfikaty** | Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2008. | PODAĆ |

Przełączniki iSCSI – 2 sztuki

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany PODAĆ** |
| **Rodzaj urządzenia:** | Przełącznik zarządzalny L2 i L3 z możliwością łączenia w stos | PODAĆ |
|  | Urządzenie fabrycznie nowe - nie powystawowe, ani niepotestowe | PODAĆ |
| **Rodzaj obudowy:** | Montowany w szafie rack 1U | PODAĆ |
| **Porty:** | 8 x 10GBase-T + 8 x 10 Gigabit SFP+ | PODAĆ |
| **Wydajność:** | Przekazywanie pakietów min. 230Mpps  Szybkość przełączania min. 320 Gbps | PODAĆ |
| **VLAN** | Obsługa co najmniej 4094 VLAN | PODAĆ |
| **Protokoły routingu** | RIP-2, IGMPv2, IGMP, IGMPv3, policy-based routing (PBR), MLDv2, MLD, VRRPv2, VRRPv3, CIDR  Co najmniej 7100 tras statycznych IPv4i co najmniej 250 interfejsów IPv4  Co najmniej 1700 tras statycznych IPv6 i co najmniej 250 interfejsów IPv6 | PODAĆ |
| **Listy kontroli dostępy** | Co najmniej 2000 wpisów | PODAĆ |
| **QoS** | Co najmniej 8 kolejek, obsługa co najmniej Strict priority and Weighted Round-Robin (WRR) | PODAĆ |
| **Tablica MAC** | Co najmniej 32000 wpisów | PODAĆ |
| **Obsługa ramek Jumbo** | Co najmniej 9000 bajtów | PODAĆ |
| **Protokoły zdalnego zarządzania** | SNMP 1, SNMP, RMON, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH, SSH-2, CLI, SCP | PODAĆ |
| **Protokoły autentykacji** | RADIUS, TACACS, TACACS+ | PODAĆ |
| **Cechy i funkcje** | FlowControll, obsługa DHCP, IGMPsnooping, obsługa Syslog, zapobieganie atakom typu DoS, obsługa DiffServ, Broadcast Storm Control, obsługa IPv6, możliwość aktualizacji firmweru, obsługa sFlow, obsługa protokołu SpanningTree (STP), obsługa protokołu Rapid Spanning Tree (RSTP), obsługa protokołu Multiple Spanning TreeProtocol (MSTP), DHCPsnooping, serwer DHCP, Dynamic ARP Inspection (DAI), STP Root Guard, Uni-Directional Link Detection (UDLD), Remote Switch Port Analyzer (RSPAN), klient DHCP, podwójne obrazy oprogramowania, Class of Service (CoS), Generic Attribute Registration Protocol (GARP), Generic VLAN Registration Protocol (GVRP), Duplicated Address Detection, obsługujeDiffServ Code Point (DSCP), kontrolowana czasowo obsługa ACL, Storm Control, inspekcja ARP, Internet Control Message Protocol (ICMP), querier IGMP, VLAN DoubleTagging (Q-in-Q), klient DNS, Voice VLAN, Secure Core Technology (SCT), LLDP-MED, IP/Mac/Port Binding (IPMB), Private VLAN, obsługatunelu ISATAP, Guest VLAN, STP BPDU Guard | PODAĆ |
| **Stos urządzeń** | Musi mieć możliwość łączenia w stos min. 8 urządzeń | PODAĆ |
| **Pamięć RAM** | Co najmniej 512 MB | PODAĆ |
| **Pamięć Flash** | Co najmniej 256 MB | PODAĆ |
| **Bufor pakietów** | Co najmniej 3 MB | PODAĆ |
| **Zasilanie** | Przełącznik musi mieć możliwość dołączenia drugiego zasilacza w celu redundancji zasilania – dopuszczalne jest dołączenie zasilacza zewnętrznego | PODAĆ |
| **Dodatkowe porty** | Min. 1 port konsoli RJ-45  Min. 1 port USB Typ A  Min. 1 port zarządzania LAN o prędkości min 1 Gb/s | PODAĆ |
| **MTBF** | Co najmniej 400 000 godzin | PODAĆ |
| **Gwarancja** | Min. 36 miesięcy gwarancji producenta z wymianą sprzętu na następny dzień roboczy oraz dostępem do portalu producenta z pomocą techniczną oraz pobieraniem nowej wersji oprogramowania.  Autoryzowany serwis gwarancyjny i pogwarancyjny. Wpisać lub podać w formie załącznika ilość punktów serwisowych, nazwa serwisu, adres, nr telefonu , fax. , adres e-mail. W przypadku zaprzestania działalności dotychczasowego serwisanta wskazanie innego, autoryzowanego serwisu. | PODAĆ WARUNKI GWARANCJI |

Serwery do wirtualizacji wraz z systemem operacyjnym – 2 sztuki

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa musi mieć możliwość 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 NFC/ BLE/ WIFI. | PODAĆ |
|  | Urządzenie fabrycznie nowe - nie powystawowe, ani niepotestowe | PODAĆ |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. | PODAĆ |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych | PODAĆ |
| **Procesor** | Zainstalowane min. dwa procesory szesnasto-rdzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 180 punktów w teście SPECint\_rate\_base2017dostępnym na stronie www.spec.org dla dwóch procesorów. | PODAĆ |
| **RAM** | Minimum 512 GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 24 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 3 TB pamięci RAM. | PODAĆ |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Lockstep | PODAĆ |
| **Gniazda PCI** | - minimum trzy sloty x16 generacji 3 połowy wysokości | PODAĆ |
| **Interfejsy sieciowe/FC/SAS** | Dostępne cztery interfejsy sieciowe 10 Gb/s Ethernet w standardzie BASE-T.  Dostępne dwa interfejsy sieciowe 10Gb/S Ethernet w standardzie SFP+.  Możliwość instalacji wymiennie modułów udostępniających:  - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie BaseT.  - dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz dwa interfejsy sieciowe 10Gb Ethernet ze złączami w standardzie SFP+.  - cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT.  - dwa interfejsy sieciowe 25Gb Ethernet ze złączami SFP28. | PODAĆ |
| **Napęd optyczny** | Brak | PODAĆ |
| **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD.  Możliwość instalacji modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia modułu w 2 jednakowe nośniki typu flash o pojemności min. 64GB z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.  Zainstalowane dwa dyski M.2 SATA o pojemności min. 240GB w konfiguracji w RAID 1 na dedykowanej karcie producenta serwera z podtrzymaniem bateryjnym i cache.  Jako opcja Zamawiający dopuszcza dostarczenie dwóch dysków 2,5” SSD o pojemności min 240GB wraz z dedykowanym kontrolerem posiadającym min 2GB nieulotnej pamięci cache. | PODAĆ |
| **Kontroler RAID** | Posiada możliwość instalacji sprzętowego kontrolera dyskowego, posiadającego min. 8GB nieulotnej pamięci cache oraz możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfujących. | PODAĆ |
| **Wbudowane porty** | min. 3 porty USB 2.0 oraz 2 porty USB 3.0, 4 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 | PODAĆ |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 | PODAĆ |
| **Wentylatory** | Redundantne | PODAĆ |
| **Zasilacze** | Redundantne, Hot-Plug maksymalnie 750W każdy. | PODAĆ |
| **Bezpieczeństwo** | Zintegrowany z płytą główną moduł TPM 2.0.  Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. | PODAĆ |
| **Diagnostyka** | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o adresacji IP modułu zarządzania, adresach MAC, nazwie hosta, numerze seryjnym urządzenia, wydzielanej mocy urządzenia w jednostkach BTU/hr lub w Watach oraz temperaturze wewnątrz urządzenia |  |
| **System Operacyjny** | Zamawiający wymaga dostarczenia systemu operacyjnego Windows Server Standard 16CORE wraz z pełną licencją na oferowany serweroraz ilość procesorów oraz zestawem nośników.  Lub równoważnie:  Zainstalowany dostępny na rynku licencjonowany 64-bitowy serwerowy system operacyjny z gwarantowanym podstawowym wsparciem producenta do min. 31.12.2024 r. umożliwiający automatyczne poświadczenie i zalogowanie się do domeny Active Directory akceptujący zasady grupowe, polityki GPO obowiązujące w tej domenie; który pozwoli na uruchomienie co najmniej 4 maszyn wirtualnych z systemem operacyjnym umożliwiającym uruchomienie serwera Active Directory, licencjonowany zgodnie z zaproponowanymi procesorami wraz z zestawem nośników. | PODAĆ |
| **Oprogramowanie do wirtualizacji** | Licencje muszą umożliwić budowę środowiska wirtualizacyjnego Zamawiającego składającego się z dwóch dwuprocesorowych serwerów pracujących w klastrze HA wraz z centralną konsolą zarządzającą.  Wszystkie licencje muszą być dostarczone wraz z 12 miesięcznym wsparciem producenta.  Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym.  Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i musi charakteryzować się maksymalnym możliwym stopniem konsolidacji sprzętowej.  Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do min 1TB pamięci operacyjnej.  Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych min. 8 procesorów wirtualnych każda z krokiem co jeden.  Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.  Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.  Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7, , Windows Server 2008R2, Windows Server 2012R2, Windows Server 2016, Windows Server 2019, SLES Debian, CentOS, FreeBSD,  Ubuntu posiadane lub wykorzystywane przez Zamawiajacego  Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i usługami.  Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.  Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.  Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.  Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory.  Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane.  Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.  Rozwiązanie musi zapewnić ciągłą pracę usług.  Usługi krytyczne biznesowo muszą działać bez przestoju, czas niedostępności innych usług nie może przekraczać kilkunastu minut.  Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały przełączone na inne serwery infrastruktury.  Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.  Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej, hostowanych systemów operacyjnych (np. wgrywania patch-y) i aplikacji tak aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zmian.  Rozwiązanie musi zapewnić możliwość szybkiego wykonywania kopi zapasowych oraz odtwarzania usług. Proces ten nie może mieć wpływu na utylizację zasobów fizycznych infrastruktury wirtualnej.  Oprogramowanie nie może zawierać rozwiązań opartych o rozwiązania opensource z powodu konieczności zapewnienia dostępu do aktualizacji oraz wsparcia gwarancyjnego. | PODAĆ |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet 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 (SSLv3) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH * 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 podłączenia lokalnego poprzez złącze RS-232. * Producent systemu musi posiadać dedykowane rozwiązanie które będzie przeciwdziałało automatycznym skryptom konfiguracyjnym działającym w sieci. Jest niedopuszczalne aby konsole zarządzające serwerów miały identyczne dane dostępowe. * możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. * możliwość konfiguracji przepływu powietrza na każdym slocie PCIe, jak również musi posiadać możliwość konfiguracji wyłączania lub włączania poszczególnych wentylatorów. * możliwość zablokowania konfiguracji oraz odnowienia oprogramowania  karty zarządzającej poprzez jednego z administratorów. Podczas trwania blokady musi być ona wyświetlana dla wszystkich administratorów którzy obecnie korzystają z karty.   Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:   * Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych * Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta * Wsparcie dla protokołów– WMI, SNMP, IPMI, , Linux SSH * Możliwość oskryptowywania procesu wykrywania urządzeń * Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram * Szczegółowy opis wykrytych systemów oraz ich komponentów * Możliwość eksportu raportu do CSV, HTML, XLS * Grupowanie urządzeń w oparciu o kryteria użytkownika * Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach * Automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń * 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 * Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu * 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 sterowników i oprogramowania wewnętrznego serwerów * Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) * Możliwość instalacji sterowników i 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 gwarancji, adresy IP kart sieciowych * Możliwość automatycznego przywracania ustawień serwera ,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej). | PODAĆ |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.  Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Windows Server 2008 R2 x64, Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016 posiadane przez Zamawiającego | PODAĆ |
| **Warunki gwarancji** | Min 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego.  Autoryzowany serwis gwarancyjny i pogwarancyjny. Wpisać lub podać w formie załącznika ilość punktów serwisowych, nazwa serwisu, adres, nr telefonu , fax. , adres e-mail. W przypadku zaprzestania działalności dotychczasowego serwisanta wskazanie innego, autoryzowanego serwisu. | PODAĆ WARUNKI GWARANCJI |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim dostarczonej najpóźniej w dniu podpisania Protokołu Instalacji i Odbioru  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. | PODAĆ |

Klaster HA Active-Pasive system zapory sieciowej następnej generacji

|  |  |  |
| --- | --- | --- |
| Parameter | Charakterystyka (wymagania minimalne) | **Parametr oferowany** |
| **Wymagania podstawowe** | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym w postaci dwóch urządzeń pracujących w klasterze wysokiej dostępności (High Availability) w trybie active-pasive (urządzenie zapasowe w trybie DFak). | PODAĆ |
|  | Urządzenie fabrycznie nowe - nie powystawowe, ani niepotestowe | PODAĆ |
| **Tryb pracy** | System ochrony sieci powinien wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako routing, część jako bridge). | PODAĆ |
| **Minimalne wymagania sprzętowe i wydajnościowe** | 1. Obsługa nielimitowanej ilości hostów w sieci chronionej. 2. Typ procesora: minimum 4 rdzenie w architekturze x86 3. Pamięć RAM: co najmniej 12 GB 4. Metalowa obudowa o wysokości 1U przeznaczona do montażu w szafie RACK. 5. Minimalna liczba i typ interfejsów fizycznych: 8x GbE RJ45 (IEEE 1000Base-T), 2x GbE SFP, 2x 10GbE SFP+, 2x USB 3.0, 1x microUSB, 1x port konsoli zarządzania (RJ-45), 1x HDMI 6. Wymagany minimum 1 slot rozbudowy o dodatkowy moduł interfejsów GBE BaseT, w tym z PoE, lub SFP lub SFP+ lub QSFP. 7. Minimalna liczba nowych połączeń na sekundę: 140 000 8. Minimalna liczba jednoczesnych połączeń: 10 000 000 9. Minimalna przepustowość Firewall: 36 000 Mbps 10. Minimalna przepustowość IPS: 10 000 Mbps 11. Minimalna przepustowość z wszystkimi modułami ochrony: 2 000 Mbps 12. Minimalna przepustowość IPSec: 3 900 Mbps 13. Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 120 GB. 14. Zintegrowany zasilacz 100-240V, z opcją zastosowania zewnętrznego zasilacza redundantnego. 15. Zintegrowany wielofunkcyjny wyświetlacz LCD. | PODAĆ |
| **Zarządzanie urządzeniem** | 1. Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI). 2. Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup. 3. Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. 4. Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz protokołu SSH z autoryzacją za pośrednictwem kluczy RSA, DSA lub ECDSA o długości min. 4096 bitów. 5. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności. 7. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 8. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. 9. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). | PODAĆ |
| **Tryb pracy – klaster** | 1. System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive. 2. W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie). | PODAĆ |
| **Funkcjonalność** | 1. System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polityki bezpieczeństwa. 2. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. 3. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji. 4. Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej. 5. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem DFaking SMTP lub SNMP. 6. Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpowiednik). 7. System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. 8. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze (on-cloud). 9. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP lub via email. 10. Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu. 11. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich. 12. Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polityk zapory sieciowej. 13. Zarządzanie licencjami subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud a synchronizacja subskrypcji on-line powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami. 14. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). 15. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 16. Rozwiązanie powinno umożliwiać budowanie polityk w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas. 17. System powinien umożliwiać budowanie polityk bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe. 18. Polityki zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług. 19. Rozwiązanie powinno zapewniać możliwość tworzenia polityk w oparciu o relacje między strefami zapory sieciowej. 20. System ochrony sieci powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN. 21. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. 22. Rozwiązanie powinno pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading. 23. System powinien zapewniać ochronę przed atakami DoS czy DdoS (DFa protection). 24. System powinien zapewniać ochronę przed skanowaniem portów (portscan DFaki). 25. System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 26. Rozwiązanie powinno zapewniać obsługę routingu statycznego. 27. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). 28. Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). 29. System powinien oferować DFakingla IGMP snooping. 30. Rozwiązanie powinno zapewniać możliwość przekserowania ruchu do nadrzędnego serwera DFa (upstream/DFakin DFa). 31. Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. 32. Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). 33. System powinien oferować funkcjonalność serwera DHCP dla Ipv4 oraz Ipv6 i DHCP Relay. 34. System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP. 35. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 36. Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów. 37. Rozwiązanie powinn oferować wsparcie dla Policy Based Routing oraz Multipath Rules. 38. Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta. 39. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 40. System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP. 41. System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub innych oferowanych przez producenta rozwiązania. 42. Rozwiązanie powinno zapewniać wsparcie dla Ipv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz Ipv6 rapid deployment (6rd). 43. System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników. 44. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub DFa. Limity powinny być przyznawane cykliczne lub niecykliczne. 45. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. 46. System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania. 47. Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater. 48. Wdrożenie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu. 49. Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej. 50. Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej. 51. Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej. 52. Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise. 53. Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication). 54. Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition). 55. System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów. 56. Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości. 57. System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden. 58. System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe. 59. Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection). 60. Wymagana praca dla autoryzacji użytkowników w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication. 61. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. 62. System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+. 63. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory. 64. Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password). 65. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server. 66. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, DF, Android. 67. Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 68. Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal. 69. System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:     1. Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)     2. Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika). 70. Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 71. Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows. 72. Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, DF, Android. 73. Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła. 74. Rozwiązanie powinno pozwalać na podgląd statystyk ruchu generowanego przez użytkownika. 75. System powinien zapewniać minimum następujące moduły ochronne: 76. Dodatkowy moduł ochrony klasy IPS z bazą minimum 7000 sygnatur. 77. Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS. 78. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. 79. Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów. 80. System powinien generować alerty w przypadku wykrycia ataku. 81. System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control. 82. Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów NP. i HTTPS. 83. Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP). 84. System oferujący inspekcję i ochronę przed DFakin dla protokołów NP., HTTPS oraz FTP. 85. System powinien oferować możliwość uruchomienia drugiego niezależnego silnika antywirusowego. 86. Rozwiązanie powinno automatycznie odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups). 87. Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (DF-time) lub partiami (batch). 88. Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. Walidacją certyfikatów. 89. System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma. 90. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. 91. Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , DFaki. 92. System powinien zapewniać możliwość emulacji skryptów JavaScript. 93. Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 94. Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 95. Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez NP. i HTTPS. 96. Rozwiązanie powinno umożliwiać blokadę stron HTTPS. 97. Rozwiązanie powinno blokować anonimowe DFa działające poprzez NP. i HTTPS. 98. Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do DFaking w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników. 99. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji. 100. Rozwiązanie powinno oferować bazę danych opisująca co najmniej 2500 aplikacji. 101. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. 102. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. 103. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania. 104. Rozwiązanie powinno umożliwiać blokowanie:      1. aplikacji, które pozwalają na transfer plików (np. P2P).      2. komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.      3. DFa uruchamianych poprzez przeglądarki internetowe.      4. DFaking media (radio internetowe, Youtube, Vimeo). 105. Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo. 106. Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie. 107. Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. 108. Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared). 109. Dodatkowy moduł ochrony klasy on-cloud sandbox:      1. Rozwiązanie umożliwiające dodatkową inspekcję plików wykonywalnych w tym .exe, .com, .dll.      2. Rozwiązanie umożliwiające dodatkową inspekcję plików dokumentów w tym .doc, .docx, .docm, .rtf.      3. Rozwiązanie umożliwiające dodatkową inspekcję plików .pdf.      4. Rozwiązanie umożliwiające dodatkową inspekcję plików archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. 110. System zapewniający dynamiczną analizę behawioralną kodu uruchamianego w realnych środowiskach testowych Windows i MacOS. 111. System powinien oferować szczegółowe raporty wyników analizy. 112. System ochrony sieci musi zapewniać funkcje generowania logów i raportowania: 113. System powinien umożliwiać składowanie oraz archiwizację logów. 114. System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 115. System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali. 116. System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 117. System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długo terminowe przechowywanie danych). 118. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. 119. Rozwiązanie powinno generować raporty w PDF, HTML i XLS. 120. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. 121. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza 122. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację 123. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. 124. System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora. 125. System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji. | PODAĆ |
| **Wymagane certyfikacje dla systemu** | CE, FCC Class A, ISED, VCCI, RCM, CCC | PODAĆ |
| **Pozostałe wymagania** | 1. Subskrypcje dla wszystkich wymaganych modułów dla klastera HA active-pasive na okres nie krótszy niż 5 lat, 2. Wsparcie techniczne w trybie 8x5 na okresie nie krótszy niż 3 lata, 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji i wsparcia technicznego. | PODAĆ |
| **Warunki gwarancji** | Min 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, z usługą przyspieszonej wymiany w przypadku awarii na sprawny sprzęt. Autoryzowany serwis gwarancyjny i pogwarancyjny. Wpisać lub podać w formie załącznika ilość punktów serwisowych, nazwa serwisu, adres, nr telefonu , fax. , adres e-mail. W przypadku zaprzestania działalności dotychczasowego serwisanta wskazanie innego, autoryzowanego serwisu. | PODAĆ |

System podtrzymania zasilania UPS 8Kva 3-fazowy

|  |  |  |
| --- | --- | --- |
| Parameter | Charakterystyka (wymagania minimalne) | **Parametr oferowany** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Typ zasilacza | Zasilacz musi pracować w topologii on-line VFI-SS-111 wg normy IEC 62040-3 | PODAĆ |  |  |
| Bypass | Musi być wyposażony w wewnętrzny, bezprzerwowy bypass elektroniczny. Musi posiadać zabezpieczenie przed zwrotnym podawaniem energii do sieci zasilającej (backfeedprotection, zgodnie z normą IEC 62040).  Urządzenie powinno posiadać tryb oszczędzania energii, zapewniający automatyczne, bezprzerwowe przełączanie w tryb online (w czasie do 2ms) w przypadku wystąpienia nieprawidłowości w torze bypassu statycznego. Opis technologii powinien być materiałem firmowym producenta. | PODAĆ |  |  |
| Sposób zasilania | UPS musi być zasilany dwutorowo – przez tor główny (układ prostownik-falownik) oraz tor rezerwowy (bypass elektroniczny). Dodatkowo musi być wyposażony w wewnętrzny tor obejściowy (serwisowy, mechaniczny). | PODAĆ |
|  | Urządzenie fabrycznie nowe - nie powystawowe, ani niepotestowe | PODAĆ |
| Baterie | Baterie akumulatorów muszą zapewniać czas podtrzymania co najmniej 10 minut dla obciążenia 8kW i muszą być umieszczone wewnątrz zasilacza UPS  Urządzenie powinno być wyposażone w system nieciągłego ładowania baterii. Należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta. |  |
| Zarządzanie i monitorowanie pracy zasilacza | Zasilacz musi posiadać oprogramowanie do zarządzania i monitorowania pracy zasilacza. Oprogramowanie musi komunikować się poprzez sieć Ethernet. Musi przekazywać informacje o stanach pracy UPS, parametrach zasilania oraz parametrach elektrycznych na wyjściu zasilacza. Musi udostępniać informacje o alarmach sygnalizowanych przez urządzenie, zużyciu energii oraz aktualnym czasie podtrzymania bateryjnego w zależności od obciążenia. Musi posiadać dziennik zdarzeń. | PODAĆ |
| Moc zasilacza | Moc wyjściowa co najmniej 8 kVA/8 kW  Możliwość rozbudowy do mocy 10kVA/10kW bez ingerencji w strukturę fizyczną urządzenia (upgrade na poziomie software). | PODAĆ |
| System zasilania | Co najmniej ilość faz 3/3 – trzy fazy wejściowe i trzy fazy wyjściowe. | PODAĆ |
| Sprawność w trybie on-line | Co najmniej 95,5% dla obciążenia w zakresie 75-100%  Co najmniej 98,5% w trybie oszczędzania energii | PODAĆ |
| Tolerancja napięcia wejściowego prostownika, bez przejścia na pracę z baterii | W zakresie od min. 187 V do max. 276 V | PODAĆ |
| Częstotliwość wejściowa | 50 Hz lub 60 Hz z tolerancją 40Hz do 72Hz | PODAĆ |
| Wahania napięcia wyjściowego | Nie więcej niż 1% | PODAĆ |
| Wahania częstotliwości wyjściowej | Nie więcej niż +/- 0,1 Hz | PODAĆ |
| Zabezpieczenia | Musi posiadać zabezpieczenie przed zwrotnym podaniem energii do sieci zasilającej (backfeedprotection, zgodnie z normą IEC 62040) w torze bypassu statycznego UPS. | PODAĆ |
| Komunikacja | Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:  - gniazdo komunikacji RS-232,  - gniazdo wyłącznika awaryjnego p.poż.  Urządzenie musi posiadać komunikację SNMP poprzez kartę sieciową Gigabit Ethernet - zgodność ze standardem cyberbezpieczeństwa UL 2900-2-2, szyfrowanie TLS 1.2  Urządzenie musi posiadać graficzny dotykowy wyświetlacz LCD z komunikatami w języku polskim. | PODAĆ |
| Oprogramowanie do zarządzania | W wyposażeniu musi znajdować się oprogramowanie umożliwiające monitorowanie UPS oraz zamykanie systemów operacyjnych pracujących pod nast. systemami: Windows, Windows Server, Linux, VMWare, Citrix.  Oprogramowanie musi posiadać funkcjonalność integracji (plug-in) z platformą wirtualizacyjną Vmware vCenter Server | PODAĆ |
| Gwarancja | Gwarancja producenta na okres min. 36 miesięcy zawierająca przeglądy serwisowe producenta po 2, 3 latach od momentu uruchomienia.  Autoryzowany serwis gwarancyjny i pogwarancyjny. Wpisać lub podać w formie załącznika ilość punktów serwisowych, nazwa serwisu, adres, nr telefonu , fax. , adres e-mail. W przypadku zaprzestania działalności dotychczasowego serwisanta wskazanie innego, autoryzowanego serwisu. |  |
| Zakres pracy – wykonanie instalacji zasilania do oferowanego zasilacza | Zamawiający wymaga wykonania linni przyłącza zasilania 3-fazowego w celu uruchomienia zasilacza w serwerowni u Zamawiającego.  W ramach tych prac Wykonawca musi wykonać pełną instalację wraz z ułożeniem kabla zasilającego, systemu rozdzielni, listwy i gniazda w celu podłączenia i uruchomienia zasilacza.  Potrzebne materiały:   |  |  | | --- | --- | | Przewód YLY 5X25 mm 0,6/1kV | 60 m | | Przewód LV 50 mm 450/750 V czerwony | 1 m | | Przewód LV 50 mm 450/750 V czarny | 1 m | | Przewód LV 50 mm 450/750 V brązowy | 1 m | | Końcówka rurowa nieizolowana 50 x fi 12 | 10 szt. | | Końcówka rurowa nieizolowana 25 x fi 8 | 10 szt. | | Końcówka tulejkowa na przewód 25 mm | 20 szt. | | Rozłącznik izolacyjny RBK na wkładki 32A | 1 szt. | | Rozdzielnia elektryczna nadtynkowa 3x24 | 1 szt. | | Rozłącznik izolowany główny czteromodułowy 100A | 1 szt. | | Wyłącznik nadprądowy B32A 3-fazowy | 1 szt. | | Szyna izolowana łączeniowa 3FS-12/12W | 1 szt. | | Listwa zaciskowa w korpusie 1x50mm żółto-zielona | 1 szt. | | Listwa zaciskowa w korpusie 1x50mm żółto-zielona | 1 szt. | | Rura karbowana ziemna śr. 40 | 1 m |   Zakres robót:   1. Ułożenie przewodu zasilającego UPS z Rozdzielni Głównej do serwerowni odległość 60m na całej długości występują przepusty oraz kanały techniczne. Rozdzielnia oraz serwerownia są na tym samym piętrze 2. Wstawienie rozłącznika bezpiecznikowego RBK zabezpieczającego kabel w Rozdzielni Głównej 3. Podłączenie kabla w Rozdzielni Głównej 4. Zamontowanie i uzbrojenie w zabezpieczenie elektryczne skrzynki rozdzielczej w Serwerowni 5. Podłączenie przewodu do rozdzielni zamontowanej w serwerowni i podłączenie UPS-a w Serwerowni 6. Wyprowadzenie obwodów zasilających dostarczony sprzęt z UPS-a 7. Uruchomienie i sprawdzenie działania UPS | PODAĆ |