Spis treści

[Switch 32 portowy (2 szt.) 2](#_Toc521933797)

[Macierz (1 szt.) 3](#_Toc521933798)

[Serwer typ 1 (3 szt.) 5](#_Toc521933799)

[SFP+ Optical Transceiver (16 szt.) 9](#_Toc521933800)

[Networking Cable SFP+ to SFP+ typ 1 (4 szt.) 9](#_Toc521933801)

[Networking Cable SFP+ to SFP+ typ 2 (14 szt.) 9](#_Toc521933802)

[Switch 24 portowy (3 szt.) 10](#_Toc521933803)

[Switch 48 portowy typ 1 (7 szt.) 12](#_Toc521933804)

[Switch 48 portowy typ 2 (8 szt.) 13](#_Toc521933805)

[Sieciowe urządzenie zabezpieczające - Firewall (1 szt.) 15](#_Toc521933806)

[Zasilanie awaryjne - UPS (1 szt.) 21](#_Toc521933807)

[Oprogramowanie wirtualizacyjne (2 szt.) 23](#_Toc521933808)

[Klimatyzator (1 szt.) 25](#_Toc521933809)

[Szafa RACK (1 szt.) 26](#_Toc521933810)

[Serwer typ 2 (2 szt.) 27](#_Toc521933811)

[Oprogramowanie backupowe (1 szt.) 32](#_Toc521933812)

[Licencje dla serwerów do obsługi backupów (3 szt.) 36](#_Toc521933813)

[Prace adaptacyjno instalacyjne/ montażowe 40](#_Toc521933814)

|  |
| --- |
| **Uwaga:**  Wszystkie podane parametry są wymogiem granicznym.  Tam gdzie nie podano warunku granicznego dla parametru, należy przyjąć go jako parametr minimalny.  Oferty które nie spełniają tych wymagań zostaną odrzucone jako niezgodne ze Specyfikacją Istotnych Warunków Zamówienia. |

# Switch 32 portowy (2 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Obudowa:** Do instalacji w szafie typu typu Rack 19", wysokość nie więcej niż 1U | |  |
| 2 | **Porty:** Przełącznik musi posiadać minimum 32 aktywne 10Gbitowe porty Minimum 24 porty Ethernet 10Gbase-T; Minimum 8 portów SFP+ 10Gbit; Porty wymienione wyżej nie mogą być współdzielone | |  |
| 3 | **Zarządzanie:** 1 port 100/1000 Mb zarządzający, dodatkowo możliwość zarządzania przez port RS232 | |  |
| 4 | **Funkcjonalności:** Przełącznik musi działać na warstwie 2 i 3 modelu OSI; Przełącznik musi obsługiwać protokoły: VLAN, STP, LAG, vLAG; Przełącznik musi posiadać agenta sprawdzającego dane telemetryczne; Przełącznik musi posiadać API typu REST API bądź podobne - o takiej samej albo większej możliwości programowania przełącznika. Funkcjonalność VM-aware przynajmniej dla Vmware i Nutanixa | |  |
| 5 | **Wydajność:** Przepustowość minimum 640GBps Opóźnienia portów: Maksymalnie 770ns dla SFP+; Maksymalnie 2.3mikrosekundy dla portów 10GBASE-T; Minimum prędkość przełączania – 470 milionów pakietów na sekundę; Wielkość bufora minimum 12MB; Ilość zapamiętywanych adresów MAC – minimum 205000 | |  |
| 6 | **Chłodzenie/zasilanie:** Redundantne i hot-swapowe chłodzenie i zasilanie. Możliwość zamówienia przełącznika w dwóch wariantach przepływu powietrza: RTF (rear to front) oraz FTR (front to rear). Zamawiany przełącznik ma mieć przepływ powietrza od tylnej ścianki w stronę portów (RTF) | |  |
| 7 | **Dokumenty:** zamawiający wymaga aby oferowany przełącznik:  - posiadał deklarację zgodności CE  - jest zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta) | |  |
| 8 | **Gwarancja:** 60 miesięcy gwarancji producenta. Gwarantowany czas reakcji – 4 godziny od zarejestrowania zgłoszenia.  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Macierz (1 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Obudowa:** Do instalacji w szafie typu Rack 19", wysokość nie więcej niż 2U | |  |
| 2 | **Kontrolery:** Macierz musi posiadać 2 kontrolery pracujące w trybie active/active; Każdy kontroler musi posiadać:  - Minimum 8 GB Cache wewnątrz kontrolera  - Minimum 2 porty 10GbE SFP+ oraz 16Gb FC. Zamawiający nie przewiduje używania portów 10Gbit i 16Gb FC w tym samym momencie. Kontroler więc musi posiadać albo dwa porty działające jako „omniporty” – zależnie od zainstalowanego Gbic, albo dwa porty 10Gbit + dwa porty 16Gb FC  - W momencie dostawy – wszystkie porty muszą być wyposażone w cztery kable 1 metrowe zgodne zarówno z macierzą, jak i z zamawianym przełącznikiem Ethernet  - Minimum 1 port zarządzający Ethernet  - Minimum 1 port zarządzający szeregowy  - Minimum 1 port rozszerzający macierz o kolejne półki | |  |
| 3 | **Liczba wspieranych dysków:** Min. 96 dysków | |  |
| 4 | **Poziomy RAID:** 0,1,5,6,10 | |  |
| 5 | **Funkcjonalności:** Macierz musi posiadać funkcjonalność tieringu z użyciem dysków SSD; Macierz musi posiadać możliwość użycia dysków SSD w celu rozbudowania Cache dyskowego (funkcjonalność osobna od tieringu) do minimum 4TB  Macierz musi mieć możliwość rozszerzenia ilości snapschotów do 1024 (w momencie zamawiania macierzy – minimum 128 snapschotów); Macierz musi posiadać funkcjonalność replikacji z inną macierzą. Licencja na tą funkcjonalność nie jest przedmiotem zamówienia. | |  |
| 6 | **Inne funkcjonalności:** Macierz musi mieć możliwość rozszerzenia do macierzy wyższego poziomu poprzez wymianę tylko kontrolerów macierzy (to jest, dyski, obudowa macierzy, zasilacze muszą pozostać te same); Macierz wyższego poziomu musi umożliwiać instalację minimum 240 dysków, możliwość wyprowadzenia 4 portów 10Gbit lub 4 portów 16Gb FC na kontroler | |  |
| 7 | **Możliwości:** Macierz musi umożliwiać budowę przestrzeni, umożliwiającej osiągnięcie:  100 tysięcy IOPS (random disk read)  3.5Gbps sekwencyjnego odczytu dysków  3.0Gbps sekwencyjnego zapisu dysków | |  |
| 8 | **Dyski:** Zainstalowane dyski:  18 dysków 1.8TB 10k rpm SAS  6 dysków 1.6TB SSD SAS 10 DWD | |  |
| 9 | **Chłodzenie/zasilanie:** Redundantne chłodzenie i zasilanie. Moc zasilaczy maksymalnie 600W | |  |
| 10 | **Dokumenty:**  - deklaracja zgodności CE  - zgodność ze standardem RoHS (oświadczenie producenta lub przedstawiciela producenta) | |  |
| 11 | **Gwarancja:** 60 miesięcy gwarancji producenta. Gwarantowany czas reakcji – 4 godziny od zarejestrowania zgłoszenia. W przypadku awarii dyski twarde zostają u Zamawiającego.  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu)  Oświadczenie producenta macierzy, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. | |  |

# Serwer typ 1 (3 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Obudowa:** Do instalacji w szafie typu Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz organizatorem kabli | |  |
| 2 | **Procesor:** Zainstalowane dwa procesory klasy x86, maksymalny TDP dla procesora 85W. Co najmniej 8 rdzeni w każdym procesorze. Dedykowany do pracy z oferowanym serwerem. Wynik wydajności procesora instalowanego w oferowanym serwerze, powinien być nie mniejszy niż 680 punktów Base w testach SPECint\_rate\_base2006 opublikowanych przez SPEC.org dla konfiguracji dwuprocesorowej.  Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.  Zamawiający dopuszcza procesory, których wynik testów wydajności jest równoważny. | |  |
| 3 | **Płyta główna:** Płyta główna dedykowana do pracy w serwerach, zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym, z możliwością zainstalowania co najmniej dwóch procesorów wykonujących 64-bitowe równoważne instrukcje AMD64 lub Intel 64 | |  |
| 4 | **Pamięć operacyjna:** Zainstalowane co najmniej 128GB, w kościach min. 32GB pamięci RAM DDR4 o taktowaniu co najmniej 2666MHz.  Minimum 12 slotów na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM. Pamięć o częstotliwości 2666MHz. | |  |
| 5 | **Zabezpieczenie pamięci:** ECC, Memory Mirroring, Memory Rank Sparing, Patrol Scrubbing oraz Demand Scrubbing. | |  |
| 6 | **Procesor graficzny:** Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz z głębią koloru co najmniej 16 bitów/piksel. | |  |
| 7 | **Dyski:** Serwer musi być wyposażony w dwa nośniki (zapewniającym redundancję) o pojemności min 32GB  Serwer musi być przygotowany do rozbudowy, o co najmniej 8 dysków 2,5” HotSwap w taki sposób, aby rozbudowa nie wymagała instalacji żadnego innego sprzętu niż dyski. | |  |
| 8 | **Zasilacz:** Minimum dwa identyczne zasilacze zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie przekraczającej 750W, z certyfikatem minimum Platinum. | |  |
| 9 | **Interfejsy sieciowe:** Zainstalowane i w pełni funkcjonalne interfejsy:  - co najmniej 2 portów 1 Gbps Ethernet RJ-45  - co najmniej 4 portów 10 Gbps Ethernet SFP+ wraz z przetwornikami SR | |  |
| 10 | **Dodatkowe porty:** z przodu obudowy: 1x USB 3.0, 1x USB 2.0 z dostępem dla podsystemu zarządzania (modułu administracyjnego) serwera, niezależnie od zainstalowanego systemu operacyjnego.  z tyłu obudowy: 2x USB 3.0, 1x DB-15 VGA. | |  |
| 11 | **Chłodzenie:** Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 | |  |
| 12 | **Zarządzanie:** Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania, umożliwiający:   * Zbieranie i przeglądanie informacji o systemie oraz inwentaryzacja * Monitorowanie statusu systemu oraz jego stanu * Podnoszenie alarmów oraz wysyłanie informacji * Zapisywanie zdarzeń w dzienniku * Konfigurowanie połączeń sieciowych * Konfigurowanie bezpieczeństwa * Aktualizowanie oprogramowania wewnętrznego (firmware) * Konfigurowanie ustawień serwera oraz urządzeń * Monitorowanie zużycia energii elektrycznej w czasie rzeczywistym * Zdalne kontrolowanie zasilania serwera (włączenie, wyłączenie, restart) * Zarządzanie kluczami aktywacyjnymi funkcji na żądanie (FoD) * Przekierowywanie konsoli szeregowej poprzez IPMI * Przechwytywanie treści wyświetlanej na konsoli w przypadku zawieszenia się systemu operacyjnego * Zdalny podgląd treści konsoli w rozdzielczości co najmniej 1920x1200 przy odświeżaniu z częstotliwością 60 Hz i głębią koloru co najmniej 16 bitów / piksel * Zdalny dostęp do serwera z użyciem klawiatury i myszy zdalnej stacji klienckiej * Zdalne instalowanie systemu operacyjnego * Alarmowanie za pośrednictwem Syslog * Przekierowanie konsoli szeregowej poprzez SSH * Wyświetlanie grafiki z danymi w czasie rzeczywistym oraz z danymi historycznymi na temat poboru mocy i temperatury * Ograniczanie poboru mocy * Mapowanie obrazu ISO i plików obrazów nośników, zlokalizowanych w lokalnej stacji klienckiej jako wirtualnych napędów, dostępnych do użycia przez serwer * Montowanie zdalnych obrazów ISO I plików obrazów nośników poprzez HTTPS, SFTP, CIFS i NFS * Współpraca co najmniej sześciu użytkowników konsoli wirtualnej * Kontrolowanie jakości i wykorzystania pasma komunikacyjnego * Obsługa co najmniej następujących interfejsów komunikacyjnych: IPMI v2.0, SNMP v3, CIM, DCMI v 1.5, REST API, WWW na bazie HTML 5, CLI (wiersz komend). * Dostęp przy pomocy smartfona z systemem Android oraz z systemem iOS, z zainstalowaną aplikacją, dostarczaną przez producenta serwera, poprzez port USB z przodu serwera, z możliwością co najmniej sprawdzenia stanu i statusu serwera, poziomu firmware, ustawień sieciowych i alarmów, a także z możliwością włączenia, wyłączenia i zrestartowania serwera. Ze względów bezpieczeństwa, nie dopuszcza się komunikacji bezprzewodowej pomiędzy serwerem a smartfonem.   **Funkcja punktowana (kryterium oceny):**   * **w przypadku zaofeowania Wykonawca otrzyma – 20 pkt.** * **za brak tej funkcji Wykonawca otrzyma – 0 pkt.** | |  |
| 13 | **Funkcje zabezpieczeń:** Hasło włączania, hasło administratora, moduł TPM z możliwością przełączania w UEFI pomiędzy wersją 1.2 a 2.0.; Możliwość zastosowania zamykanego na klucz panelu przedniego serwera. | |  |
| 14 | **Urządzenia hot swap:** Co najmniej dyski, zasilacze oraz wentylatory | |  |
| 15 | **Obsługa:** Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane’y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych. | |  |
| 16 | **Diagnostyka:** Wbudowany system analizy predykcyjnej, pozwalający na przewidywanie możliwości wystąpienia awarii serwera. Analiza musi obejmować co najmniej: procesory, regulatory napięcia, pamięć operacyjną (RAM), dyski wewnętrzne, wentylatory, zasilacze, kontrolery RAID  Możliwość użycia aplikacji mobilnej na smartfonie z systemem Android oraz iOS, podłączonym do serwera poprzez port USB z przodu obudowy, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. | |  |
| 17 | **Obsługiwane systemy operacyjne:** Microsoft Windows Server 2012 R2 i 2016, Red Hat Enterprise Linux 6 oraz 7, SUSE Linux Enterprise Server 11 oraz 12, VMware vSphere (ESXi) 6.0 oraz 6.5. | |  |
| 18 | **Waga:** Nie więcej niż 32 kg w maksymalnej możliwej konfiguracji serwera. | |  |
| 19 | **Dokumenty:**  - Deklaracja zgodności CE, z widocznym oznaczeniem na obudowie  - zgodność ze standardem RoHS (oświadczenie producenta lub przedstawiciela producenta) | |  |
| 20 | **Gwarancja:** 60 miesięcy gwarancji producenta z gwarantowanym czasem reakcji 4 godziny od zarejestrowania zgłoszenia; uszkodzone nośniki zostają u Zamawiającego  W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie „Diagnostyka” (tj. procesor, pamięć, VRM, dyski, zasilacze, wentylatory) wymagane jest rozszerzenie poziomu gwarancji do 60 miesięcy gwarantowanym czasem naprawy 4h oraz zainstalowania dodatkowego dla każdej lokalizacji systemu monitoringu (na dedykowanym serwerze o parametrach rekomendowanych przez producenta oprogramowania monitorującego).  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu)  Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem. | |  |

# SFP+ Optical Transceiver (16 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | 10GBase-SR- up to 300 m | |  |

# Networking Cable SFP+ to SFP+ typ 1 (4 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | 10GbE Copper Twinax Direct Attach Cable, CusKit - 5 m | |  |

# Networking Cable SFP+ to SFP+ typ 2 (14 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | 10GbE,Copper Twinax Direct Attach Cable,0.5 Meter | |  |

# Switch 24 portowy (3 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Rodzaj obudowy:** Montowany w szafie typu Rack 1U | |  |
| 2 | **Porty:** 24 x 10/100/1000 (PoE+) + 2 x combo 10 Gigabit SFP+ + 2 x 10 Gigabit SFP+ | |  |
| 3 | **Zasilanie przez Ethernet:** PoE+ | |  |
| 4 | **Moc dedykowana dla PoE:** 195W | |  |
| 5 | **Wykonanie:** Pojemność przełączania (rozmiar pakietu - 64 bajty): 95,23 Mp/s ¦ Zdolność przełączania:128 Gbps | |  |
| 6 | **Pojemność:** Instancje MSTP:16; Aktywnty VLAN:4096; Trasy IPv4 (statyczne): 8000; Trasy IPv6 (statyczne): 6000; Wpisy ACL: 2000 | |  |
| 7 | **Wielkość tablicy adresów MAC**: 64K wpisów | |  |
| 8 | **Obsługiwane ramki Jumbo**: 9000 bajtów | |  |
| 9 | **Protokół routing:** IGMP v2 , IGMP,IGMPv3,routing statyczny IPv4,routing statyczny IPv6,policy-based routing (PBR),MLDv2,MLD,CIDR | |  |
| 10 | **Protokół zdalnego zarządzania:** SNMP 2, SNMP, RMON, Telnet, SNMP 3, HTTP, HTTPS, T FTP, SSH, SSH-2, CLI, SCP | |  |
| 11 | **Cechy:** Sterowanie przepływem,przełączanie warstwy 3,obsługa DHCP,nasłuchiwanie I G M P,obsługa Syslog,zapobieganie atakom typu DoS,dublowanie portów,ważone cykliczne kolejkowanie (WRR),Broadcast Storm Control,obsługa IPv6,kontrola nad szturmem pakietów multicast,kontrola nad szturmem pakietów unicast,możliwość aktualizacji firmwaru,obsługa SNTP,sFlow,obsługa protokołu Spanning Tree (STP),obsługa protokołu Rapid Spanning Tree (RSTP),obsługa protokołu Multiple Spanning Tree Protocol (MSTP),nasłuchiwanie DHCP,obsługa list dostępu (ACL),Quality of Service (QoS),IP Precedence,serwer DHCP,MLD snooping,Dynamic ARP Inspection (DAI),reset button,Cable Diagnostics Function,Uni-Directional Link Detection (UDLD),obsługa IPv4,przekaźnik D H C P,Port Security,Remote Switch Port Analyzer (RSPAN),klient DHCP,Energy Efficient Ethernet,Management Information Base (MIB),Class of Service (CoS),Generic Attribute Registration Protocol (GARP),Generic VLAN Registration Protocol (GVRP),Duplicated Address Detection,Type of Service (ToS),obsługuje DiffServ Code Point (DSCP),2 wiatraki,bufor pakietów 1,5MB,kontrolowana czasowo obsługa ACL,Storm Control,zabezpieczenie źródła IP,inspekcja ARP,Bridge protocol data unit (BPDU),Internet Control Message Protocol (ICMP),Secure Copy (SCP),Cisco Discovery Protocol,querier IGMP,VLAN Double Tagging (Q-inQ),odzwierciedlanie VLAN,klient DNS,Voice VLAN,zarządzanie VLAN,Secure Core Technology (SCT),Private VLAN Edge (PVE),LLDP-MED,blokowanie portów (HOLB),IP/Mac/Port Binding (IPMB),Secure Sensitive Data (SSD),Private VLAN, obsługa tunelu ISA TA P,osłona RA | |  |
| 12 | **Zgodność z normami:** IEEE 802 .3, IEEE 802 .3u, IEEE 802 .3z, IEEE 802 .1D, IEEE 802 .1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3a f, IEEE 802 .3x, IEEE 802 .3ad (LACP), IEEE 802 .1w, IEEE 802 .1x, IEEE 802 .3ae, IEEE 802 .1s, IEEE 802 .1ab (LLDP), IEEE 802 .3an, IEEE 802 .3at, IEEE 802 .3az | |  |
| 13 | **Zasilanie:** AC 120/230 V (47 - 63 Hz) | |  |
| 14 | **Wymiary:** Suma wymiarów nie może przekroczyć 840 mm | |  |
| 15 | **Waga:** nie może przekroczyć 5 kg | |  |
| 16 | **Dokumenty:** zamawiający wymaga aby oferowany przełącznik:  - posiadał deklarację zgodności CE  - jest zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta) | |  |
| 17 | **Gwarancja:** 60 miesięcy producenta  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Switch 48 portowy typ 1 (7 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | Przełącznik powinien posiadać 48 portów 1 GbE RJ45 oraz minimum 4 porty SFP+ wspierające technologie 10 GbE | |  |
| 2 | Wymagane dostarczanie 2 przetworników (transceiver)10Gbs SR | |  |
| 3 | Minimalna przepustowość przełącznika to 176 Gbps ( full duplex ) i  131 Mpps | |  |
| 4 | Przepustowość bez blokowania przy maksymalnym obciążeniu wszystkich portów | |  |
| 5 | Przełącznik powinien być wyposażony w redundantne zasilanie | |  |
| 6 | Przełącznik powinien mieć wymienialne na gorąco wentylatory oraz zasilacze | |  |
| 7 | Przełącznik powinien wspierać sposób wentylacji tył-przód lub przód-tył | |  |
| 8 | Przełącznik musi mieć możliwość montażu w szafie 19”,wysokość nie większa niż 1RU | |  |
| 9 | Przełącznik musi wspierać przełączanie w warstwie 2 | |  |
| 10 | Przełącznik musi wspierać możliwość terminowania/agregacji fizycznych linków prowadzących do dwóch różnych przełączników ( np.vpc,vlag), przy czym przełączniki muszą być zarządzane osobno. | |  |
| 11 | Min. : 8,000 adresów MAC | |  |
| 12 | VLANs: 4,095 (512 active VLANs) | |  |
| 13 | Przełącznik musi wspierać następujące protokoły: 802.1s, 802.1w, PVRST+, LACP, QoS 802.1p, LDAP, RADIUS, TACACS+, SSH v1/v2, VRRP, IGMP v1/v2/v3, SNMP v1/v2c,v3, LLDP, 9k Jumbo Frames,sflow v5, OpenFlow | |  |
| 14 | **Dokumenty:** zamawiający wymaga aby oferowany przełącznik:  - posiadał deklarację zgodności CE  - jest zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta) | |  |
| 15 | **Gwarancja:** 60 miesięcy gwarancji producenta. Gwarantowany czas reakcji – 4 godziny od zarejestrowania zgłoszenia.  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Switch 48 portowy typ 2 (8 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Rodzaj obudowy:** Montowany w szafie typu Rack 1U | |  |
| 2 | **Porty:**  48 x 10/100/1000 (PoE+) + 2 x combo 10 Gigabit SFP+ + 2 x 10 Gigabit SFP+ | |  |
| 3 | **Zasilanie przez Ethernet:** PoE+ | |  |
| 4 | **Moc dedykowana dla PoE:** 382W | |  |
| 5 | **Wykonanie:** Pojemność przełączania (rozmiar pakietu- 64 bajty): 130.94 Mpps; Zdolność przełączania: 176 Gbps | |  |
| 6 | **Pojemność:** Instalacje MSTP: 16; Aktywnych VLAN: 4096; Trasy IPv4 (statyczne): 8000; Trasy IPv6 (statyczne): 6000; Wpisy ACL: 2000 | |  |
| 7 | **Wielkość tablicy adresów MAC:** 64k wpisów | |  |
| 8 | **Obsugiwane ramki Jumbo:** 9000 bajtów | |  |
| 9 | **Protokół routingu:** IGMP v2 , IGMP,IGMPv3,routing statyczny IPv4,routing statyczny IPv6,policy-based routing (PBR),MLDv2,MLD,CIDR | |  |
| 10 | **Protokół zdalnego zarządzania:** SNMP 2 ,SNMP,RMON ,Telnet,SNMP 3,HTTP,HTTPS ,T FTP,SSH ,SSH-2 ,CLI ,SCP | |  |
| 11 | **Cechy:** Sterowanie przepływem,przełączanie warstwy 3,obsługa DHCP,nasłuchiwanie I G M P,obsługa Syslog,zapobieganie atakom typu DoS,dublowanie portów,ważone cykliczne kolejkowanie (WRR),Broadcast Storm Control,obsługa IPv6,kontrola nad szturmem pakietów multicast,kontrola nad szturmem pakietów unicast,możliwość aktualizacji firmwaru,obsługa SNTP,sFlow,obsługa protokołu Spanning Tree (STP),obsługa protokołu Rapid Spanning Tree (RSTP),obsługa protokołu Multiple Spanning Tree Protocol (MSTP),nasłuchiwanie DHCP,obsługa list dostępu (ACL),Quality of Service (QoS),IP Precedence,serwer DHCP,MLD snooping,Dynamic ARP Inspection (DAI),reset button,Cable Diagnostics Function,Uni-Directional Link Detection (UDLD),obsługa IPv4,przekaźnik D H C P,Port Security,Remote Switch Port Analyzer (RSPAN),klient DHCP,Energy Efficient Ethernet,Management Information Base (MIB),Class of Service (CoS),Generic Attribute Registration Protocol (GARP),Generic VLAN Registration Protocol (GVRP),Duplicated Address Detection,Type of Service (ToS),obsługuje DiffServ Code Point (DSCP),4 wentylatory,kontrolowana czasowo obsługa ACL,bufor pakietów 3MB,Storm Control,zabezpieczenie źródła IP,inspekcja ARP,Bridge protocol data unit (BPDU),Internet Control Message Protocol (ICMP),Secure Copy (SCP),Cisco Discovery Protocol,querier IGMP,VLAN Double Tagging (Q-inQ),odzwierciedlanie VLAN,klient DNS,Voice VLAN,zarządzanie VLAN,Secure Core Technology (SCT),Private VLAN Edge (PVE),LLDP-MED,blokowanie portów (HOLB),IP/Mac/Port Binding (IPMB),Secure Sensitive Data (SSD),Private VLAN,obsługa tunelu ISA TA P,osłona RA | |  |
| 12 | **Zgodność z normami:** IEEE 802 .3 ,IEEE 802 .3u ,IEEE 802 .3z ,IEEE 802 .1D ,IEEE 802 .1Q ,IEEE 802.3ab,IEEE 802.1p,IEEE 802.3a f, IEEE 802 .3x ,IEEE 802 .3ad (LACP) ,IEEE 802 .1w ,IEEE 802 .1x ,IEEE 802 .3ae ,IEEE 802 .1s ,IEEE 802 .1ab (LLDP) ,IEEE 802 .3an ,IEEE 802 .3at ,IEEE 802 .3az | |  |
| 13 | **Zasilanie:** AC 120/230 V (47 - 63 Hz) | |  |
| 14 | **Wymiary:** Suma wymiarów nie może przekroczyć 940 mm | |  |
| 15 | **Waga:** nie może przekroczyć 6 kg | |  |
| 16 | **Dokumenty:** zamawiający wymaga aby oferowany przełącznik:  - posiadał deklarację zgodności CE  - jest zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta) | |  |
| 17 | **Gwarancja:** 60 miesięcy gwarancji producenta.  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Sieciowe urządzenie zabezpieczające - Firewall (1 szt.)

klaster (składający się z 2 sztuk urządzeń)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Obsługa sieci:** Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP. | |  |
| 2 | **Zapora korporacyjna (Firewall):**  - Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.  - Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.  - Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).  - Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.  - Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.  - Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall’u.  - Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).  - Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). | |  |
| 3 | **Intrusion Prevention System (IPS):**  - System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.  - Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy.  - Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.  - Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.  - Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej.  - Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.  - Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP | |  |
| 4 | **Kształtowanie pasma (Traffic Shapping):**  - Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.  - Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.  - Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).  - Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. | |  |
| 5 | **Ochrona antywirusowa:**  - Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).  - Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.  - Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.  - Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. | |  |
| 6 | **Ochrona Antyspam:**  - Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).  - Ochrona antyspam ma działać w oparciu o:  a.    białe/czarne listy,  b.    DNS RBL,  c.     heurystyczny skaner.  - W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.  - Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. | |  |
| 7 | **Wirtualne sieci prywatne (VPN):**  - Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).  - Odpowiednio kanały VPN można budować w oparciu o:  a.    PPTP VPN,  b.    IPSec VPN,  c.     SSL VPN  - SSL VPN musi działać w trybach Tunel i Portal.  - W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.  - Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).  - Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.  - Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. | |  |
| 8 | **Filtr dostępu do stron WWW:**  - Urządzenie ma posiadać wbudowany filtr URL.  - Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.  - Administrator musi mieć możliwość dodawania własnych kategorii URL.  - Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.  - Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.  - Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji:  a.    blokowanie dostępu do adresu URL,  b.    zezwolenie na dostęp do adresu URL,  c.     blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.  - Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.  - Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.  - Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.  - Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.  - Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane.  - Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http. | |  |
| 9 | **Uwierzytelnianie:**  - Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o:  a.    lokalną bazę użytkowników (wewnętrzny LDAP),  b.    zewnętrzną bazę użytkowników (zewnętrzny LDAP),  c.     usługę katalogową Microsoft Active Directory.  - Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.  - Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia  autoryzacje w oparciu o protokoły:  a.    SSL,  b.    Radius,  c.     Kerberos.  - Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.  - Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.  - Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. | |  |
| 10 | **Administracja łączami do Internetu (ISP):**  - Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).  - Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:  a.    równoważenie względem adresu źródłowego,  b.    równoważenie względem połączenia.  - Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.  - Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.  - Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.  - Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.  - Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.  - Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.  - Rozwiązanie powinno wspierać technologię Link Aggregation. | |  |
| 11 | **Pozostałe usługi I funkcję rozwiązania:**  - Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.  - Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.  - Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.  - Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS  - Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.  - Urządzenie musi posiadać usługę DNS Proxy. | |  |
| 12 | **Administracja urządzeniem:**  - Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.  - Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.  - Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.  - Komunikacja może odbywać się na porcie innym niż https (443 TCP).  - Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.  - Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.  - Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.  - Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).  - Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.  - Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.  - Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora. | |  |
| 13 | **Raportowanie:**  - Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.  - System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.  - System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.  - System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.  - System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.  - W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.  - Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy | |  |
| 14 | **Parametry sprzętowe:**  - Urządzenie ma być wyposażone w dysk twardy o pojemności co najmniej 320 GB.  - Liczba portów Ethernet 10/100/1000Mbps – min. 12.  - Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta.  - Przepustowość Firewalla – min. 5 Gbps  - Przepustowość Firewalla wraz z włączonym systemem IPS – min. 3 Gbps.  - Przepustowość filtrowania Antywirusowego – min. 850 Mbps  - Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1 Gbps.  - Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500  - Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100  - Obsługa min. VLAN 256  - Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 20 000 nowych sesji/sekundę.  - Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.  - Urządzenie jest nielimitowane na użytkowników. | |  |
| 15 | **Dokumenty:**  - posiadał deklarację zgodności CE  - jest zgodny z standardem RoHS (oświadczenie producenta lub przedstawiciela producenta) | |  |
| 16 | **Gwarancja:** 60 miesięcy producenta, czas reakcji w następnym dniu od zgłoszenia.  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Zasilanie awaryjne - UPS (1 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | Zasilacz UPS o moc minimum 9000 VA/7200 W, który musi zapewnić czas podtrzymania minimum 5 minut dla obciążenia 7200W. Maksymalna wysokość zestawu 6U. Zasilacz UPS wykonany w architekturze podwójnej konwersji on-line VFI z wejściem PFC i automatycznym by-passem z możliwością pracy redundantnej ze wspólną baterią.  Uniwersalna obudowa typu Rack. Zasilacz UPS elektronika oraz moduły baterii muszą być dostarczone wraz z kompletem kabli i zestawem szyn do montażu w szafie typu Rack. | |  |
| 2 | **Parametry wejściowe:**  - Napięcie: 230 V (1-fazowe) 181 – 280 V do 100 V przy 50% obciążenia  - Częstotliwość : 50 / 60 Hz + /-10% (ustawiana automatycznie)  - Współczynnik mocy/THDi : > 0,99 / < 5 %  - Zaciski | |  |
| 3 | **Parametry wyjściowe:**  - Napięcie (czysty przebieg sinusoidalny): 230 V (1-f) do wyboru 200 / 208 / 220 / 240V  - Częstotliwość :50 /60 Hz + /- 2 % (+/- 0,05 Hz w trybie pracy bateryjnej)  - Współczynnik mocy 0,9 przy 8000 VA  - Sprawność: min. 92 % w trybie on-line  - Przeciążalność: min. 105 % w sposób ciągły ; 125 % przez 5 min ; 150 % przez 30 s  - Gniazda wyjściowe: zaciski | |  |
| 4 | **Bateria:**  - Hermetyczne, bezobsługowe akumulatory o żywotności 3-5 lat wg klasyfikacji EUROBAT umieszczone w obudowie bateryjnej. Moduł baterii musi składać się z co najmniej 20 szt. akumulatorów 12V/9Ah.  - Możliwość dodania 9 szt. dodatkowych modułów baterii, które wydłużą czas podtrzymania do minimum 91 minut dla obciążenia 7200W  - Czas ładowania < 6 godz. do odzyskania 90 % wydajności po całkowitym rozładowaniu | |  |
| 5 | **Urządzenie musi posiadać alfanumeryczny wyświetlacz LCD wskazujący:**  - stan obciążenia,  - wyjścia programowalne,  - stan baterii,  - poziom obciążenia (5 poziomów),  - obciążenie obecne,  - awaria baterii/wymiana baterii,  - alarm ogólny,  - przeciążenia,  - wartość na wejściu,  - tryb normalny/praca z użyciem baterii | |  |
| 6 | **Zasilacz UPS musi posiadać diody LED sygnalizujące:**  - praca w trybie bypass  - brak zakłóceń w zasilaniu,  - stan obciążenia | |  |
| 7 | **Zasilacz UPS musi posiadać alarmy dźwiękowe sygnalizujące:**  - tryb bateryjny,  - przeciążenie,  - konieczność wymiany baterii | |  |
| 8 | Zasilacz UPS musi być wyposażony w wyłącznik alarmu akustycznego, port RS232 (do obsługi protokołu MODBUS), Wraz z zasilaczem UPS musi zostać dostarczony panel z gniazdami: IEC 320 C13 - 8 szt., IEC 320 C19 - 2szt. mocowanego na tyle UPS-a oraz karta komunikacyjna SNMP i oprogramowanie do monitorowania i wyłączania stacji roboczych działające w systemach operacyjnych Windows®, Linux® i Mac OS X® | |  |
| 9 | **Zasilacz UPS musi być zgodny z Normami**  **-** Parametry i topologia: IEC 62040-3 (VFI-SS-111)  - Bezpieczeństwo: IEC/EN 62040-1, AS 62040.1.1, AS 62040.1.2  - Kompatybilność elektromagnetyczna IEC/EN 62040-2, AS 62040.2  - Certyfikaty: RoHS, CE, RCM (E2376)  - Stopień ochrony IP: min. IP20 | |  |
| 10 | **Zasilacz UPS musi spełniać parametry środowiskowe co najmniej takie jak :**  - Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie temperatur od 15 °C do 25 °C)  - Wilgotność: 95 % bez kondensacji  - Poziom hałasu w odległości 1 m < 55 dB | |  |
| 11 | Wymiary zasilacza UPS (moduł elektroniki) nie mogą być większe niż suma (mm) 1195; 3U  Masa zasilacza UPS (moduł elektroniki) – nie większa niż 19,5 kg Wymiary modułu baterii EBM nie mogą być większe niż suma (mm) 1195; 3U. Masa modułu baterii nie może być większa niż 66 kg | |  |
| 12 | Urządzenie musi mieć możliwość dodania ręcznego bezprzerwowego bypassu serwisowego. Akcesoria dodatkowe muszą być wyprodukowane przez tego samego producenta co zasilacz UPS. | |  |
| 13 | **Gwarancja:** Urządzenie musi być objęte gwarancja producenta na okres co najmniej 24 miesięcy na moduł elektroniki oraz akumulatory.  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Oprogramowanie wirtualizacyjne (2 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. | |  |
| 2 | Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. | |  |
| 3 | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w dowolną liczbę rdzeni oraz do 2TB pamięci fizycznej RAM. | |  |
| 4 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych. | |  |
| 5 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 1 TB pamięci operacyjnej RAM. | |  |
| 6 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć 1-10 wirtualnych kart sieciowych. | |  |
| 7 | Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z których każda może mieć co najmniej 4 porty szeregowe i 3 porty równoległe i 20 urządzeń USB. | |  |
| 8 | Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. | |  |
| 9 | Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. | |  |
| 10 | Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). | |  |
| 11 | Polityka licencjonowania oprogramowania nie może wiązać licencji w żaden sposób ze środowiskiem na które zostało zakupione. | |  |
| 12 | Rozwiązanie musi wspierać systemy operacyjne zaproponowane przez Wykonawcę w ofercie. | |  |
| 13 | Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. | |  |
| 14 | Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. | |  |
| 15 | Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. | |  |
| 16 | Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. | |  |
| 17 | Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. | |  |
| 18 | Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. | |  |
| 19 | Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi (hierarchiczna baza danych). | |  |
| 20 | Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. | |  |
| 21 | System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. | |  |
| 22 | Pojedynczy ww. przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. | |  |
| 23 | Pojedynczy ww. wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. | |  |
| 24 | Ww. wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN). | |  |
| 25 | Wsparcie serwisowe producenta: 5lat.  Wsparcie realizowane będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Klimatyzator (1 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Wydajność chłodnicza Nominalna (min-max) kW:**  5,00 (0,98 - 6,00) | |  |
| 2 | **Współczynnik EER Nominalny (min-max) W/W:**  3,47 (3,50 - 3,02) A | |  |
| 3 | **Wydajność chłodnicza przy -10 °C Nominalna kW:** 6,00 | |  |
| 4 | **Współczynnik EER przy -10 °C Nominalny W/W:** 6,00 | |  |
| 5 | **Wydajność chłodnicza przy -20 °C Nominalna kW:** 5,82 | |  |
| 6 | **Współczynnik EER przy -20 °C Nominalny W/W:** 5,39 | |  |
| 7 | **Współczynnik SEER Nominalny W/W:** 6,90 (A++) | |  |
| 8 | **Moc projektowa Pdesign kW:** 5,0 | |  |
| 9 | **Pobór mocy w trybie chłodzenia Nominalny (min-max) kW:** 1,440 (0,280 - 1,990) | |  |
| 10 | **Roczne zużycie energii (tryb chłodzenia) kWh/rok:** 254 | |  |
| 11 | **Wydajność grzewcza Nominalna (min-max) kW:**  5,80 (0,98 - 8,00) | |  |
| 12 | **Wydajność grzewcza przy -7 °C Nominalna kW:** 4,98 | |  |
| 13 | **Współczynnik COP Nominalny (min-max) W/W:**  3,82 (2,88 - 3,11) A | |  |
| 14 | **Współczynnik SCOP Nominalny W/W:**  4,20 (A+) | |  |
| 15 | **Moc projektowa Pdesign przy -10 °C kW:** 4,4 | |  |
| 16 | **Pobór mocy w trybie ogrzewania Nominalny (min-max) kW:** 1,520 (0,340 - 2,570) | |  |
| 17 | **Roczne zużycie energii (tryb grzania) kWh/rok:** 1.467 | |  |
| 18 | **Napięcie zasilania V:** 230 | |  |
| 19 | **Gwarancja:** Urządzenie musi być objęte gwarancją producenta na okres 60 miesięcy co najmniej na sprężarkę.  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Szafa RACK (1 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Wymiary:**  - Wysokość wewnętrzna:42U  - Wysokość: 2030 mm  - Szerokość: 800 mm  - Głębokość: 1000 mm | |  |
| 2 | **Wymagania:**  - Drzwi przednie stalowe perforowane z zamkiem  - Drzwi tylne stalowe perforowane dwuskrzydłowe uchylne z zamkiem  - Drzwi boczne dwudzielne demontowane na zatrzaskach z możliwością montażu zamka  - Wyposażenie: 4 wentylatory, 2 półki, listwa zasilająca,  - Stalowa blacha zimnowalcowana  - Wykończenie pow.: odtłuszczanie, wytrawianie, fosfatowanie, malowanie proszkowe  - Zabezpieczona przed rdzą, utlenianiem, porysowaniem, korozją  - Dwa przepusty kablowe - szczotkowy w suficie , kablowy w podłodze  - Regulowane nóżki i kółka o dużej wytrzymałości  - Dobry poziom wentylacji i rozpraszania ciepła  - Dwa pionowe organizery kabli montowane do szyn typu Rackowych  - Zestaw kabli uziemiających w komplecie | |  |
| 3 | **Zgodność z normami:**   * - ANSI/EIA RS-310-D, DIN41491 PART1, IEC297-2 * - DIN41494 PART7, GB/T3047.2-92 * - Kompatybilne ze standardami: metrycznym, ETSI oraz międzynarodowym 19”   - Stopień ochrony: IP20 | |  |
| 4 | **Listwa zasilająca wymagania:**  - Typ gniazda wyjściowego: złącze IEC  - Liczba gniazd wyjściowych: 8 sztuk  - Prąd znamionowy: 10 A  - Częstotliwość: 50 Hz, 60 Hz | |  |

# Serwer typ 2 (2 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | **Obudowa:** Do instalacji w szafie typu Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych oraz organizatorem kabli | |  |
| 2 | **Procesor:** Zainstalowany 1 procesor klasy x86, maksymalny TDP dla procesora 85W. Co najmniej 8 rdzeni. Dedykowany do pracy z oferowanym serwerem. Wynik wydajności procesora instalowanego w oferowanym serwerze, powinien być nie mniejszy niż 680 punktów Base w testach SPECint\_rate\_base2006 opublikowanych przez SPEC.org dla konfiguracji dwuprocesorowej.  Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org.  Zamawiający dopuszcza procesory, których wynik testów wydajności jest równoważny. | |  |
| 3 | **Płyta główna:** Płyta główna dedykowana do pracy w serwerach, zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym, z możliwością zainstalowania co najmniej dwóch procesorów wykonujących 64-bitowe równoważne instrukcje AMD64 lub Intel 64 | |  |
| 4 | **Pamięć operacyjna:** Zainstalowane co najmniej 128GB, w kościach min. 32GB pamięci RAM DDR4 o taktowaniu co najmniej 2666MHz.  Minimum 12 slotów na pamięć, wsparcie pamięci typu RDIMM oraz LRDIMM. Pamięć o częstotliwości 2666MHz. | |  |
| 5 | **Zabezpieczenie pamięci:** ECC, Memory Mirroring, Memory Rank Sparing, Patrol Scrubbing oraz Demand Scrubbing. | |  |
| 6 | **Procesor graficzny:** Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz z głębią koloru co najmniej 16 bitów/piksel. | |  |
| 7 | **Dyski:** Zainstalowane dyski:  - co najmniej dwa identyczne dyski SSD Hot Swap o pojemności co najmniej 480GB każdy,  - serwer musi być przygotowany do rozbudowy o co najmniej 6 dysków 2,5” Hot Swap w taki sposób, aby rozbudowa nie wymagała instalacji żadnego innego sprzętu niż dyski. | |  |
| 8 | **Kontroler dyskowy:**  Dedykowany kontroler dyskowy, o parametrach nie gorszych niż:  - interfejs komunikacji z serwerem: PCIe 3.0 x8 lub szybszy  - interfejsy komunikacji z dyskami: SAS 12Gbps, z obsługą dysków SAS oraz SATA, co najmniej 8 portów  - pamięć podręczna (cache): co 2 najmniej GB pamięci nieulotnej (flash)  - funkcja zarzadzania kluczami dla dysków SED  - funkcja akceleracji komunikacji I/O z dyskami SSD  - obsługa RAID 0, 1, 10, 5, 50, 6 i 60  - rozbudowa pojemności systemu dyskowego on-line  - migracja wersji RAID on-line  - automatyczna przebudowa grupy RAID  - obsługa global hot spare  - kontrola spójności danych w grupie RAID | |  |
| 9 | **Zasilacz:** Minimum dwa identyczne zasilacze zainstalowane wewnątrz serwera, pracujące redundantnie, zapewniające możliwość wyłączenia i wyjęcia dowolnego z nich z serwera bez przerywania pracy serwera oraz bez ograniczania wydajności serwera, o mocy każdego zasilacza nie przekraczającej 750W, z certyfikatem minimum Platinum. | |  |
| 10 | **Interfejsy sieciowe:** Zainstalowane i w pełni funkcjonalne interfejsy:  - co najmniej 2 portów 1 Gbps Ethernet RJ-45  - co najmniej 4 portów 10 Gbps Ethernet SFP+ wraz z przetwornikami SR | |  |
| 11 | **Dodatkowe porty:** z przodu obudowy: 1x USB 3.0, 1x USB 2.0 z dostępem dla podsystemu zarządzania (modułu administracyjnego) serwera, niezależnie od zainstalowanego systemu operacyjnego.  z tyłu obudowy: 2x USB 3.0, 1x DB-15 VGA. | |  |
| 12 | **Chłodzenie:** Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 | |  |
| 13 | **Zarządzanie:** Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania, umożliwiający:   * Zbieranie i przeglądanie informacji o systemie oraz inwentaryzacja * Monitorowanie statusu systemu oraz jego stanu * Podnoszenie alarmów oraz wysyłanie informacji * Zapisywanie zdarzeń w dzienniku * Konfigurowanie połączeń sieciowych * Konfigurowanie bezpieczeństwa * Aktualizowanie oprogramowania wewnętrznego (firmware) * Konfigurowanie ustawień serwera oraz urządzeń * Monitorowanie zużycia energii elektrycznej w czasie rzeczywistym * Zdalne kontrolowanie zasilania serwera (włączenie, wyłączenie, restart) * Zarządzanie kluczami aktywacyjnymi funkcji na żądanie (FoD) * Przekierowywanie konsoli szeregowej poprzez IPMI * Przechwytywanie treści wyświetlanej na konsoli w przypadku zawieszenia się systemu operacyjnego * Zdalny podgląd treści konsoli w rozdzielczości co najmniej 1920x1200 przy odświeżaniu z częstotliwością 60 Hz i głębią koloru co najmniej 16 bitów / piksel * Zdalny dostęp do serwera z użyciem klawiatury i myszy zdalnej stacji klienckiej * Zdalne instalowanie systemu operacyjnego * Alarmowanie za pośrednictwem Syslog * Przekierowanie konsoli szeregowej poprzez SSH * Wyświetlanie grafiki z danymi w czasie rzeczywistym oraz z danymi historycznymi na temat poboru mocy i temperatury * Ograniczanie poboru mocy * Mapowanie obrazu ISO i plików obrazów nośników, zlokalizowanych w lokalnej stacji klienckiej jako wirtualnych napędów, dostępnych do użycia przez serwer * Montowanie zdalnych obrazów ISO I plików obrazów nośników poprzez HTTPS, SFTP, CIFS i NFS * Współpraca co najmniej sześciu użytkowników konsoli wirtualnej * Kontrolowanie jakości i wykorzystania pasma komunikacyjnego * Obsługa co najmniej następujących interfejsów komunikacyjnych: IPMI v2.0, SNMP v3, CIM, DCMI v 1.5, REST API, WWW na bazie HTML 5, CLI (wiersz komend). * Dostęp przy pomocy smartfona z systemem Android oraz z systemem iOS, z zainstalowaną aplikacją, dostarczaną przez producenta serwera, poprzez port USB z przodu serwera, z możliwością co najmniej sprawdzenia stanu i statusu serwera, poziomu firmware, ustawień sieciowych i alarmów, a także z możliwością włączenia, wyłączenia i zrestartowania serwera. Ze względów bezpieczeństwa, nie dopuszcza się komunikacji bezprzewodowej pomiędzy serwerem a smartfonem.   **Funkcja punktowana (kryterium oceny):**   * **w przypadku zaofeowania Wykonawca otrzyma – 10 pkt.** * **za brak tej funkcji Wykonawca otrzyma – 0 pkt.** | |  |
| 14 | **Funkcje zabezpieczeń:** Hasło włączania, hasło administratora, moduł TPM z możliwością przełączania w UEFI pomiędzy wersją 1.2 a 2.0.; Możliwość zastosowania zamykanego na klucz panelu przedniego serwera. | |  |
| 15 | **Urządzenia Hot Swap:** Co najmniej dyski, zasilacze oraz wentylatory | |  |
| 16 | **Obsługa:** Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane’y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych. | |  |
| 17 | **Diagnostyka:** Wbudowany system analizy predykcyjnej, pozwalający na przewidywanie możliwości wystąpienia awarii serwera. Analiza musi obejmować co najmniej: procesory, regulatory napięcia, pamięć operacyjną (RAM), dyski wewnętrzne, wentylatory, zasilacze, kontrolery RAID  Możliwość użycia aplikacji mobilnej na smartfonie z systemem Android oraz iOS, podłączonym do serwera poprzez port USB z przodu obudowy, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera. | |  |
| 18 | **Obsługiwane systemy operacyjne:** Microsoft Windows Server 2012 R2 i 2016, Red Hat Enterprise Linux 6 oraz 7, SUSE Linux Enterprise Server 11 oraz 12, VMware vSphere (ESXi) 6.0 oraz 6.5. | |  |
| 19 | **Waga:** Nie więcej niż 32 kg w maksymalnej możliwej konfiguracji serwera. | |  |
| 20 | **Dokumenty:**  - Deklaracja zgodności CE, z widocznym oznaczeniem na obudowie  - zgodność ze standardem RoHS (oświadczenie producenta lub przedstawiciela producenta) | |  |
| 21 | **Gwarancja:** 60 miesięcy gwarancji producenta z gwarantowanym czasem reakcji 4 godziny od zarejestrowania zgłoszenia; uszkodzone nośniki zostają u Zamawiającego  W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie „Diagnostyka” (tj. procesor, pamięć, VRM, dyski, zasilacze, wentylatory) wymagane jest rozszerzenie poziomu gwarancji do 60 miesięcy gwarantowanym czasem naprawy 4h oraz zainstalowania dodatkowego dla każdej lokalizacji systemu monitoringu (na dedykowanym serwerze o parametrach rekomendowanych przez producenta oprogramowania monitorującego).  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu)  Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem | |  |
| 22 | **Wymagania dodatkowe:**  **1. Obudowa:** Do instalacji w szafie typu Rack 19", wysokość nie więcej niż 1U  **2. Porty:** Minimum 24 porty Ethernet 10Gbase-T; Minimum 8 portów SFP+ 10Gbit; Porty wymienione wyżej nie mogą być współdzielone – to jest przełącznik musi posiadać minimum 32 aktywne 10Gbitowe porty  **3.** **Zarządzanie:** 1 port 100/1000 Mb zarządzający, dodatkowo możliwość zarządzania przez port RS232  4. **Funkcjonalności:** Przełącznik musi działać na warstwie 2 i 3 modelu OSI; Przełącznik musi obsługiwać protokoły: VLAN, STP, LAG, vLAG; Przełącznik musi posiadać agenta sprawdzającego dane telemetryczne; Przełącznik musi posiadać API typu REST API bądź podobne - o takiej samej albo większej możliwości programowania przełącznika. Funkcjonalność VM-aware przynajmniej dla Vmware i Nutanixa  **5.** **Wydajność:** Przepustowość minimum 640GBps  Opóźnienia portów: Maksymalnie 770ns dla SFP+; Maksymalnie 2.3mikrosekundy dla portów 10GBASE-T; Minimum prędkość przełączania – 470 milionów pakietów na sekundę; Wielkość bufora minimum 12MB; Ilość zapamiętywanych adresów MAC – minimum 205000  **6.** **Chłodzenie/zasilanie:** Redundantne i hot-swapowe chłodzenie i zasilanie. Możliwość zamówienia przełącznika w dwóch wariantach przepływu powietrza: RTF (rear to front) oraz FTR (front to rear). Zamawiany przełącznik ma mieć przepływ powietrza od tylnej ścianki w stronę portów (RTF)  **7.** Deklarację zgodności CE  Zgodność ze standardem RoHS (oświadczenie producenta lub przedstawiciela producenta)  **8. Gwarancja:** 60 miesięcy gwarancji producenta. Gwarantowany czas reakcji – 4 godziny.  Serwis gwarancyjny realizowany będzie przez:  (wpisać adres, nr telefonu i email do kontaktu).  **9.** 10GbE Copper Twinax Direct Attach Cable,- długość: 5 m- 2 sztuki | |  |

# Oprogramowanie backupowe (1 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | Rozwiązanie musi zapewniać dostępność wszystkich obciążeń- wirtualnych, fizycznych i chmurowych z poziomu jednej konsoli zarządzania. | |  |
| 2 | Rozwiązanie musi łączyć funkcję tworzenia kopii zapasowych, przywracania i replikacji | |  |
| 3 | Rozwiązanie musi obejmować funkcje monitorowania i raportowania przeznaczone dla narzędzi Agent dla Microsoft Windows i Agent dla Linux. | |  |
| 4 | Rozwiązanie musi obsługiwać znaczniki lokalizacji maszyn wirtualnych, hostów i komputerów skonfigurowane tak, aby przestrzegana była suwerenność danych. | |  |
| 5 | Rozwiązanie musi w pełni obsługiwać program Microsoft SQL Server 2017, Microsoft Windows Server 2016. | |  |
| 6 | Rozwiązanie musi monitorować zadania backupu skonfigurowane dla Agentów. | |  |
| 7 | Rozwiązanie musi monitorować zasady agentów. | |  |
| 8 | Rozwiązanie musi posiadać wbudowane mechanizmy alarmujące obciążenia serwera. | |  |
| 9 | Rozwiązanie musi zawierać liczniki, które pozwalają określić ilość miejsca zajmowanego magazynie danych przez maszynę wirtualną i związane z nią pliki. | |  |
| 10 | Rozwiązanie musi umożliwiać ustawienie ścieżki pamięci podręcznej wydajności. | |  |
| 11 | Rozwiązanie musi umożliwiać wygenerowanie raportu, który przedstawia listę wszystkich chronionych obiektów, kopii zapasowych i replik pogrupowaną według znacznika lokalizacji. | |  |
| 12 | Rozwiązanie musi umożliwiać wygenerowanie raportu, który przedstawia potencjalne naruszenia suwerenności danych dotyczące wszystkich chronionych obiektów. | |  |
| 13 | Rozwiązanie musi umożliwiać generowanie raportów na podstawie znaczników lokalizacji. | |  |
| 14 | Rozwiązanie musi umożliwiać raportowanie i monitorowanie hostów oraz serwera vCenter w wersji vSphere 6.5. | |  |
| 15 | Rozwiązanie musi przedstawiać zapotrzebowanie na pamięć operacyjną w przypadku maszyn wirtualnych, na których jest skonfigurowana pamięć statyczna. | |  |
| 16 | Rozwiązanie musi umożliwiać wygenerowanie raportu dotyczącego właściwości kopii zapasowych. | |  |
| 17 | Rozwiązanie musi umożliwiać wygenerowanie raportu dotyczącego filtrowania maszyn wirtualnych na podstawie zadań powielania kopii zapasowych. | |  |
| 18 | Rozwiązanie musi posiadać mechanizm udostępniania pulpitów, polegający na zapewnieniu innym użytkownikom systemu dostępu do określonych pulpitów- bez przyznawania kompleksowych praw dostępu do wszystkich pulpitów. | |  |
| 19 | Rozwiązanie musi posiadać wbudowany mechanizm alarmowania, polegający na ostrzeżeniu użytkownika, jeżeli na monitorowanych maszynach wirtualnych występuje nietypowe korzystanie z procesora i częste operacje zapisu w magazynie danych mogące wynikać z aktywności oprogramowania ransomware. | |  |
| 20 | Rozwiązanie musi posiadać wbudowany mechanizm alarmowania, dzięki któremu możliwe jest śledzenie błędów podczas operacji zapisu danych o wydajności w folderze dysku. | |  |
| 21 | Rozwiązanie musi umożliwiać pomijanie alarmów o opóźnieniu dotyczących wszystkich maszyn wirtualnych znajdujących się w tym samym magazynie danych co maszyna objęta operacją backupu. | |  |
| 22 | Rozwiązanie musi umożliwiać pomijanie alarmów na podstawie okresu i zadań backupu. | |  |
| 23 | Rozwiązanie musi zawierać mechanizm modelowania alarmów, który pozwala wybrać określony obiekt znajdujący się w jego zakresie – z uwzględnieniem alarmów zawierających wiele reguł – jednocześnie honorując ustawienia pomijania alarmów. | |  |
| 24 | Rozwiązanie musi umożliwiać przypisanie wszystkich alarmów dotyczących maszyn wirtualnych do obiektów magazynu danych i hosta. | |  |
| 25 | Rozwiązanie musi posiadać kartę przeglądu maszyn wirtualnych, która zawiera informację na temat miejsca wykorzystywanego przez dyski wirtualne maszyn w odniesieniu do każdego obiektu magazynu danych. | |  |
| 26 | Rozwiązanie musi umożliwiać wybór określonych maszyn wirtualnych do monitorowania. | |  |
| 27 | Rozwiązanie musi umożliwiać wygenerowanie raportu, w ramach tego raportu przeprowadzany jest audyt maszyn wirtualnych oraz ustalane są najdroższe i najtańsze maszyny na podstawie parametrów wydajności procesora i pamięci. | |  |
| 28 | Rozwiązanie musi umożliwiać wygenerowanie raportu, w ramach tego raportu przeprowadzany jest audyt kosztów infrastruktury oraz ustalane są najdroższe i najtańsze maszyny wirtualne na podstawie ceny sprzętu i bieżących konfiguracji maszyn. | |  |
| 29 | Rozwiązanie musi umożliwiać wprowadzenie zasad przechowywania, które zawierają osobne ustawienie dotyczące danych wydajności, zdarzeń i danych kopii zapasowych. | |  |
| 30 | Rozwiązanie musi posiadać wbudowany mechanizm alarmu, który eliminuje fałszywe zgłoszenia detekcji, gdy maszyna wirtualna zostanie przeniesiona z jednej grupy do drugiej. | |  |
| 31 | Rozwiązanie musi posiadać wbudowany mechanizm alarmu, dzięki temu alarmowi można otrzymać informację, gdy zadanie powielania kopii zapasowych przekroczy skonfigurowany czas na transfer danych. | |  |
| 32 | Rozwiązanie musi umożliwiać wygenerowanie raportu przedstawiającego informację na temat historycznych kopii zapasowych przechowywanych na pulach nośników taśmowych typu GFS. | |  |
| 33 | Rozwiązanie musi umożliwiać wygenerowanie raportu przedstawiającego współczynnik kompresji i deduplikacji każdego utworzonego pliku kopii zapasowej, umożliwiając analizowanie typów danych zawartych w kopiach zapasowych w całym łańcuchu plików kopii. | |  |
| 34 | Rozwiązanie musi umożliwiać wygenerowanie raportu dotyczące alokacji zasobów hosta (procesor, pamięć operacyjna, pamięć masowa). | |  |
| 35 | Rozwiązanie musi umożliwiać całodobowe monitorowanie, raportowanie i ostrzeganie w czasie rzeczywistym w środowisku wirtualnym i fizycznym. | |  |
| 36 | Rozwiązanie musi udostępniać funkcję monitorowania agentów kopii zapasowych, w tym przeglądów alarmów i stanów zadań, a także raport na temat chronionych agentów określających ich liczbę i typ, stan kopii zapasowych z łączną liczbą operacji zakończonych powodzeniem, ostrzeżeniem i niepowodzeniem oraz powodu braku ochrony agentów. | |  |
| 37 | Rozwiązanie musi umożliwiać wygenerowanie raportu dotyczącego zgodności kopii zapasowych. | |  |
| 38 | Rozwiązanie musi posiadać funkcję predefiniowania kategorii geolokalizacji, w której obiekty grupowane są według lokalizacji geograficznej, raport dotyczący geolokalizacji ochrony danych, czyli listę źródeł danych pogrupowanych według lokalizacji danych produkcyjnych oraz ich kopii i/lub replik, oraz raport dotyczący niezgodności geolokalizacji danych, czyli listę wszystkich źródeł danych, w przypadku których lokalizacja co najmniej jednej kopii różni się od lokalizacji danych produkcyjnych. | |  |
| 39 | Rozwiązanie musi posiadać funkcję oceny wydajności i konfiguracji. Dzięki tej funkcji, rozwiązanie musi określać m.in. elementy infrastruktury, które wykorzystują najwięcej zasobów, najmniej obciążone hosty, aktualne i skumulowane obciążenie magazynów danych operacjami we/wy oraz ich opóźnienia, a także wykorzystanie zasobów w odniesieniu do hostów, klastrów, pul zasobów i magazynów danych. | |  |
| 40 | Rozwiązanie musi zapewniać obsługę środowisk tj. Vmware vSphere 6.x, Vmware vSphere 5.x, Vmware vSphere 4.1, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 SP1. | |  |
| 41 | Rozwiązanie musi zapewnić dostępność serwerów dzięki następującym funkcjom:  - aktywne pełne kopie zapasowe  - przetwarzanie z uwzględnieniem specyfikacji aplikacji  - indeksowanie i wyszukiwanie plików  - funkcje harmonogramu i przechowywania odpowiednie dla serwerów  - syntetyczne pełne kopie zapasowe  - tworzenie kopii zapasowych dzienników transakcji baz danych | |  |
| 42 | Rozwiązanie po wykonaniu pierwszej pełnej kopii zapasowej musi tworzyć kopie przyrostowe, umieszczając w nich tylko nowe bloki danych lub bloki zmienione od czasu utworzenia ostatniej kopii. | |  |
| 43 | Rozwiązanie musi posiadać interfejs API zdalnego konfigurowania i zarządzania, który ułatwia wdrażanie i konfigurowanie agentów przy użyciu prostego interfejsu wiersza poleceń. | |  |
| 44 | Gwarancja: 60 miesięcy  serwis i wsparcie realizowane będzie przez:  (wpisać adres, nr telefonu i email do kontaktu) | |  |

# Licencje dla serwerów do obsługi backupów (3 szt.)

|  |  |  |  |
| --- | --- | --- | --- |
| Producent: | |  | |
| Pełna nazwa urządzenia / model / typ / wersja: | |  | |
| **Lp.** | **Minimalne parametry:** | | **Oferowane parametry:**  (wpisuje Wykonawca) |
| 1 | Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. | |  |
| 2 | System musi posiadać następujące, wbudowane cechy:  a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,  b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,  c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych,  d) 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,  e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,  f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,  g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,  h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),  i) wbudowane wsparcie instalacji i pracy na wolumenach, które:  I. pozwalają na zmianę rozmiaru w czasie pracy systemu,  II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),  j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,  k) wbudowane szyfrowanie dysków  l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,  m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,  n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,  o) graficzny interfejs użytkownika,  p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),  s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,  t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,  u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,  III. zdalna dystrybucja oprogramowania na stacje robocze,  IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,  V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:  1) dystrybucję certyfikatów poprzez http,  2) konsolidację CA dla wielu lasów domeny,  3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  VI. szyfrowanie plików i folderów,  VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),  VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,  IX. serwis udostępniania stron WWW,  X. wsparcie dla protokołu IP w wersji 6 (IPv6),  XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,  3) obsługi 4-KB sektorów dysków,  4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,  6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),  v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,  w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),  x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,  y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,  z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. | |  |

Uwagi końcowe dotyczące wszystkich pozycji asortymentowych w załączniku Przedmiot zamówienia – sprzęt:

**Oświadczamy, że oferowane, powyżej wyspecyfikowane urządzenia są kompletne, wolne od wad, pochodzą z bieżącej produkcji (min. 2018 r.), nie są wyposażeniem testowym, zastępczym, serwisowym ani powystawowym.**

**………………………………………………….**

**Podpis wykonawcy**

# Prace adaptacyjno instalacyjne/ montażowe

Celem projektu jest modernizacja infrastruktury serwerowej, sieciowej i macierzowej. Projekt ma na celu poprawę przepustowości sieci zarówno LAN jak i iSCSI SAN (zmiana z 1GbE na 10GbE na wszystkich poziomach – serwery, macierz, switche) oraz podniesienie ochrony poprzez wdrożenie nowego klastra wirtualnego w oparciu o oprogramowanie nadzorujące obie lokalizacje (lokalizacja główna oraz zapasowa).

W przypadku awarii serwerowni w lokalizacji głównej, umożliwi to uruchomienie kluczowych systemów szpitala, jak również automatyczne uruchomienie serwerów w przypadku awarii pojedynczych serwerów w klastrze nadzorującym.

W lokalizacji głównej zainstalowane zostaną trzy nowe serwery typ 1 na potrzebę nowego klastra wirtualnego. Serwery będą w konfiguracji bezdyskowej, z modułem SD oraz dwoma redundantnymi kartami SD. Na kartach SD serwerów zainstalowany zostanie hypervisor w najnowszej dostępnej wersji. Należy wdrożyć również serwer zarządzający klastrem – wirtualny appliance (również w najnowszej wersji). Należy wykonać konfigurację wysokiej dostępności dla serwerów wirtualnych (utworzenie klastra HA – High Availability). Dodatkowo, do nowego serwera zarządzającego podłączone zostaną również 3 stare serwery Fujitsu (po zainstalowaniu na nich hypervisorów w zgodnej z pozostałymi serwerami wersji).

W lokalizacjach głównej i zapasowej należy wdrożyć nowe switche 32-portowe. Część portów dedykowana będzie pod LAN, natomiast część pod ruch iSCSI SAN. Do switchy podłączone zostaną macierz oraz serwery (karty sieciowe w nowych serwerach, zarówno do LAN jak i do iSCSI SAN, za pomocą portów 10GbE).

W lokalizacji głównej należy wdrożyć nową macierz dyskową. Macierz musi być skonfigurowana z wykorzystaniem mechanizmu tieringu za pomocą dysków SSD. Macierz musi wykorzystywać 2 kontrolery pracujące w trybie active-active oraz 4 interfejsy iSCSI 10GbE. Do nowego klastra wirtualnego należy wystawić nowe LUN’y z macierzy na potrzebę uruchomienia maszyn wirtualnych zmigrowanych z posiadanych przez Zamawiającego serwerów Fujitsu RX300S6. Skonfigurować należy multipathing dla połączeń iSCSI na wszystkich poziomach dostępu do macierzy (serwery, switche, macierz).

Na potrzebę ochrony środowiska wirtualnego wdrożony zostanie system backupu i replikacji. Będzie on obejmował cykliczny backup maszyn wirtualnych znajdujących się na nowym klastrze wirtualnym w lokalizacji głównej. Backup realizowany będzie na obecny dysk NAS. Dodatkowo za pomocą mechanizmów oprogramowania backup’owego wdrożona zostanie replikacja kluczowych maszyn wirtualnych z lokalizacji głównej do lokalizacji zapasowej (na serwery Fujitsu RX300S6 i macierz ETHERNUS DX100 S3) – umożliwi to błyskawiczne uruchomienie replikowanych maszyn wirtualnych w przypadku awarii w serwerowni głównej (bez konieczności odzyskiwania maszyn/danych z backupu).

Backupem objęty zostanie także obecny fizyczny serwer Windows Asseco. Backup tego serwera również będzie realizowany na obecny dysk NAS.

Dodatkowo, w 2 lokalizacjach należy zainstalować po 1 nowym serwerze typ 2 na potrzebę klastra wysokiej dostępności dla systemu bazodanowego.

Możliwości obecnie wykorzystywanych przełączników (głównie Cisco SF300 i SG200) i uplinki między budynkami (1Gbps), są niewystarczające w stosunku do aktualnych wymagań aplikacji i systemów. Na styku sieci LAN/WAN brakuje też urządzenia chroniącego sieć szpitala.

Projekt modernizacji uwzględnia klaster urządzeń zabezpieczających-firewall, wymianę przełączników dostępowych na przełączniki wyposażone w porty 1GbE (zamiast FastEthernet) i 10GbE uplink oraz wymianę przełączników warstwy core (10GbE).

Na styku sieci LAN/WAN zostanie zainstalowany klaster wysokodostępny (HA) urządzeń zabezpieczających – firewall, który zapewni ochronę sieci przed zagrożeniami, optymalne wykorzystanie dwóch łączy internetowych (LB / Failover), dostęp VPN, routing między podsieciami szpitala i inne funkcje sieciowe (L3).

W obu lokalizacjach (głównej i zapasowej) elementy sieci o kluczowym znaczeniu dla zapewnienia ciągłości jej pracy mają zapewnioną redundancję sprzętową (układy podwójne switchy pracujące w konfiguracji Active-Active), użyte zostaną przełączniki core 32portowe, pracujące w stacku. Przełączniki te będą obsługiwać zarówno sieć LAN, jak i SAN (separacja na poziomie VLANów). Jako przełączniki dostępowe, zostaną użyte przełączniki 48portowe.

W lokalizacji głównej, będzie zainstalowanych 8 przełączników (zgrupowanych w 2 stacki) 48 portowych. Część z nich będzie wspierała funkcjonalność PoE/PoE+.

W lokalizacji zapasowej zlokalizowanej na oddziale kardiologicznym, zainstalowane będą 4 przełączniki 48 portowe zagregowane w 1 stack.

Punkt dystrybucyjny na Oddziale przewlekle chorych, będzie wyposażony w 2 przełączniki 48-portowe (stack).

W punkcie dystrybucyjnym w Diagnostyce, zainstalowany będzie 1 przełącznik 48portowy.

W pozostałych punktach będą zainstalowane przełączniki 24portowe.

Połączenia między lokalizacją główną a lokalizacją zapasową, Diagnostyką oraz punktem na Oddziale chorób przewlekłych, będą miały przepustowość 2x10GE (port-channel).

Pozostałe punkty dystrybucyjne, będą miały połączenia 1x10GE.

Punkty dystrybucyjne na oddziałach Kardiologicznym oraz chorób przewlekłych - z uwagi na ich rolę w topologii sieci - będą wyposażone w obecne zasilacze bezprzerwowe (UPS’y), umożliwią podtrzymanie działania przełączników w przypadku zaniku zasilania i zapewnienie działania sieci w puncie, oraz punktach podłączonych do nich.

Należy wymienić posiadane łącza miedziane i światłowodowe na wszystkich trasach na światłowód jednomodowy, aby możliwe było osiągnięcie prędkości 10Gb pomiędzy serwerownią i punktami dystrybucyjnymi.

Prace adaptacyjne obejmą m.in. przebudowę ściany z luksfer w serwerowni i ścianki w lokalizacji zapasowej oraz modernizacje wejść.

**………………………………………………….**

**Podpis wykonawcy**