Spis treści

[1. Macierz dyskowa 1 szt. 1](#_Toc518473594)

[2. Dodatkowy serwer fizyczny 1szt. 3](#_Toc518473595)

[3. Oprogramowanie serwerów do wykonywania kopii zapasowej 1szt. 7](#_Toc518473596)

[4. Kontroler SFP (karta sieciowa światłowodowa) 1 szt. 12](#_Toc518473597)

[5. Oprogramowanie do zarządzania maszynami wirtualnymi 1szt. 12](#_Toc518473598)

[6. System operacyjny serwera 4szt. 13](#_Toc518473599)

[7. Przełącznik sieciowy rdzeniowy (główny) 1szt. 16](#_Toc518473600)

[8. Przełącznik dostępowy wyposażony w 24 porty 3szt. 19](#_Toc518473601)

[9. Przełącznik sieciowy dostępowy wyposażony w 48 portów 3szt. 22](#_Toc518473602)

[10. Przewód do połącznia przełączników dostępowych 6szt. 25](#_Toc518473603)

[11. Moduł do podłączenia światłowodu do przełączników sieciowych dostępowych i rdzeniowych 13 szt. 25](#_Toc518473604)

[12. Usługa wdrożenia 25](#_Toc518473605)

# Macierz dyskowa 1 szt.

|  |  |
| --- | --- |
| Nazwa parametru | Minimalna wartość parametru |
| Obudowa  | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''  |
| Pojemność:  | System musi zostać dostarczony w konfiguracji zawierającej minimum:12 dysków 4TB NL-SAS oraz posiadać możliwość rozbudowy o kolejne dyski.System musi wspierać dyski: * SAS 900GB, 1200GB, 1800GB
* SATA/NL-SAS od 4TB do 8TB
* SSD od 400GB do min 3800GB

Budowa systemu musi umożliwiać rozbudowę do modeli wyższych bez potrzeby kopiowania/migrowania danych (zamawiający przez model wyższy rozumie inny model macierzy danego producenta z większą pamięcią cache oraz mocniejszymi procesorami).System musi mieć możliwość rozbudowy do 300 dysków |
| Kontroler  | Dwa kontrolery wyposażone w przynajmniej 24GB cache (oparty o RAM) każdy z dodatkową pamięcią Flash min 1TB na kontroler (wbudowana w kontroler lub formie dodatkowych dysków Flash skonfigurowanych jako Cache w RAID 10).W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub za pomocą zrzutu pamięci cache na flash.System musi pozwalać na rozbudowę do klastra 6 kontrolerów. Macierz musi pozwalać na poszerzenie pamięci Cache za pomocą dysków SSD do 4TB Zamawiający nie dopuszcza zastosowania dysków SSD w formie Tieringu zamiast funkcjonalności SSD cache. |
| Interfejsy  | Oferowana macierz musi posiadać minimum 4 porty FC 16GB4 porty 10GbE SFP+4 porty SAS,  |
| RAID  | System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID  |
| Kopie Migawkowe  | Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności macierzy +/-5%  |
| Obsługiwane protokoły  | Macierz musi obsługiwać jednocześnie protokoły FC, FCoE, iSCSi, CIFS i NFS - jeśli wymagane są licencje do aktywowania ww. protokołów Zamawiający wymaga dostarczenia ich wraz z macierzą. Licencje muszą być udzielone na czas nieoznaczony, umożliwiać prawidłowe funkcjonowanie oprogramowania oraz umożliwiać Zamawiającemu lub osobom przez niego upoważnionym nieograniczone użytkowanie programu. |
| Inne wymagania  | Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych, którą można stosować na macierzy/danych produkcyjnej dla wszystkich rodzajów danych. Macierz powinna mieć możliwość czynności odwrotnej tzn. cofnięcia procesu deduplikacji na zdeduplikowanym wolumenie. Macierz musi posiadać funkcjonalność kompresji danych. Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2012/2016, Linux, Vmware, Unix.Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie. Macierz musi posiadać funkcjonalność priorytetyzacjii zadań. Macierz musi posiadać funkcjonalność replikacji danych z inną macierzą tego samego producenta w trybie asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów. Macierz musi posiadać funkcjonalność klonowania danych bez potrzeby wykonywania fizycznej kopii danych na dyskach. Macierz musi posiadać możliwość automatycznego informowania i przesyłania przez pocztę elektroniczną raportów o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy. Zamawiający wymaga dostarczenia licencji na czas nieoznaczony dla oprogramowania z macierzą lub oprogramowania zewnętrznego, na pełną pojemność macierzy, która pozwala na: - monitoring wykorzystania przestrzeni na macierzy- monitoring grup RAIDowych- monitoring wykonywanych backupów/replikacji danych między macierzami- monitoring wydajności macierzy- analizę i diagnozę spadku wydajnościWszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy  |
| Gwarancja i rękojmia | Min. 12 miesięcy gwarancji i rękojmi na sprzęt i oprogramowanie. Termin naprawy elementów lub dostawy i wymiany uszkodzonych elementów na nowe - następny dzień roboczy po dniu zgłoszenia. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta sprzętu i oprogramowania (gwarancja poparta gwarancją Producenta), na sprzęt i oprogramowanie. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ.**Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert** |

# Dodatkowy serwer fizyczny 1szt.

|  |  |
| --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych. Bez dodatkowego przedniego panela. 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 (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| **Procesor** | Zainstalowane dwa procesory min. ośmiordzeniowe, szesnastowątkowe klasy x86 dedykowane do pracy z zaoferowanym serwerem. Częstotliwość pracy każdego z procesorów min 1.8GHz, 3.8GHz w trybie turbo. |
| **RAM** | 256GB DDR4 RDIMM 2666MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512GB pamięci RAM. |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Lockstep |
| **Gniazda PCI** | Min. dwa sloty PCIe Gen 3 o prędkości min. x16. |
| **Interfejsy sieciowe/FC** | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T. Dodatkowo zainstalowana jedna karta dwuportowa typu 10GbE SFP+ porty muszę być obsadzone modułami SFP+  |
| **Napęd optyczny** | Wbudowany DVD-RW |
| **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD.Zainstalowane 2x600GB SAS 12Gb/s 10k.Możliwość instalacji wewnętrznego modułu dedykowany dla hypervisora wirtualizacyjnego, możliwość wyposażenia w 2 jednakowe nośniki typu flash o pojemności minimum 64GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samo szyfrujących. |
| **Wbudowane porty** | min. 3 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232 |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200. |
| **Wentylatory** | Redundantne |
| **Zasilacze** | Redundantne, Hot-Plug maksymalnie 550W. |
| **Bezpieczeństwo** | Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |
| **System operacyjny** | System operacyjny opisany w pkt 6 |
| **Diagnostyka** | Panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **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.
* 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 (licencja dla Zamawiającego na czas nieoznaczony) 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 zaoferowanego 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) |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z zachowaniem norm jakości ISO-9001:2008 oraz ISO-14001.Serwer musi posiadać deklarację CE.Z uwagi na posiadaną infrastructurę zamawiającego, oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Windows Server 2008, Windows Server 2008 R2, Microsoft Windows 2012, Microsoft Windows 2012 R2, Windows Server 2016. |
| **Warunki gwarancji i rękojmi** | Min. 12 miesięcy gwarancji i rękojmi. Gwarancja i rękojmia realizowane w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przekazania zgłoszenia. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta sprzętu i oprogramowania (gwarancja poparta gwarancją Producenta), na sprzęt i oprogramowanie. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ, z zastrzeżeniem, że Zamawiający musi mieć dodatkowo zapewnioną możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną Producenta.Zamawiający wymaga także, aby Producent sprzętu zapewniał możliwość rozszerzenia gwarancji do siedmiu lat.**Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert** |
| **Dodatkowa przestrzeń dyskowa** | Wraz z dostawą serwera należy dostarczyć dodatkową przestrzeń dyskową na potrzeby wykonywania kopii danych w postaci urządzenia typu NAS o minimalnych parametrach:Rack 1U8GB pamięci Ram4 dyski twarde 6TB 7.2K Hot-plug4 interfejsy 1GbE Base-T2 interfejsy 10Gbit SFP/SFP+ obsadzone modułami 10GB MM4 USB 3.0Redundantne zasilanieObsługa RAID 0/1/5/6/10 + hot spareObsługa protokołów: CIFS/SMB, NFS, FTP, iSCSI, SNMPMin. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta sprzętu (gwarancja poparta gwarancją Producenta), na sprzęt. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ.**Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert** |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |

# Oprogramowanie serwerów do wykonywania kopii zapasowej 1szt.

**Wymagania ogólne**

1. Licencja na czas nieoznaczony na 2 serwery dwuprocesorowe.
2. Min. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji
i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta oprogramowania (gwarancja poparta gwarancją Producenta), na oprogramowanie. Wykonawca
w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ, z zastrzeżeniem, że gwarancja Producenta musi umożliwiać także aktualizację oprogramowania do najnowszej wersji bez dodatkowych opłat oraz zapewniać pomoc Producenta w rozwiązywaniu problemów (tel.,
e-mail lub zdalną sesję). **Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert**.
3. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
4. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
5. Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
6. Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V

**Całkowite koszty posiadania**

1. Oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone,
2. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej,
3. Oprogramowanie musi tworzyć “samowystarczalne” archiwa, do odzyskania których nie jest wymagana osobna baza danych z metadanymi deduplikowanych bloków,
4. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji,
5. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu,
6. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania,
7. Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,
8. Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość akutalizacji pola „notatki” na wirtualnej maszynie,
9. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware,
10. Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 5.5, 5.6, 8.0, 8.10 i archiwizować również metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD,
11. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji,
12. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji,
13. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX),
14. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

**Wymagania RPO**

1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
2. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
3. Oprogramowanie musi wspierać kopiowanie plików na taśmy
4. Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server
5. Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej
6. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
7. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.
8. Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio
z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
9. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
10. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
11. Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V
12. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
13. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere
14. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

**Wymagania RTO**

1. Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania
2. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na zasoby dyskowe produkcyjne.
3. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji
i dysków
4. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure.
5. Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
6. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
7. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików:
	1. **Linux**
		* ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs
	2. **BSD**
		* UFS, UFS2
	3. **Solaris**
		* ZFS, UFS
	4. **Mac**
		* HFS, HFS+
	5. **Windows**
		* NTFS, FAT, FAT32, ReFS
	6. **Novell OES**
		* NSS
8. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
9. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
10. Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD.
11. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").
12. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze.
13. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze.
14. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.
15. Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.
16. Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows
17. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

**Monitoring**

1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 4.1, 5.x oraz 6.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 oraz 2016 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
4. System musi mieć możliwość instalacji na systemach operacyjnych w wersjach 64 bitowych:
	1. Microsoft Windows 2008 SP2
	2. Microsoft Windows 2008 R2 SP1
	3. Microsoft Windows 7 SP1
	4. Microsoft Windows 8
	5. Microsoft Windows 2012
	6. Microsoft Windows 2012 R2
	7. Microsoft Windows 8.1
	8. Microsoft Windows 10
	9. Microsoft Windows 2016
5. System musi obsługiwać następujące bazy danych w wersjach 32 i 64 bitowych:
	1. Microsoft SQL Server 2008
	2. Microsoft SQL Server 2008 R2
	3. Microsoft SQL Server 2012 R2
	4. Microsoft SQL Server 2014
	5. Microsoft SQL Server 2016
6. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
7. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
8. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
9. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
10. Silnik raportowania powinien być oparty o SQL Server Reporting Services w celu zapewnienia bezpiecznego dostępu do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji
11. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
12. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
13. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
14. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
15. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio
z narzędzia monitorującego
16. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
17. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
18. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
19. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 5.5, 5.6, 8.0 oraz 8.10

**Raportowanie**

1. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 4.1, 5.x oraz 6.0, vCenter Server 4.1, 5.x oraz 6.0 jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2i 2016.
2. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
3. System musi instalować się na następujących systemach operacyjnych:
	1. Microsoft Windows 2008 SP2
	2. Microsoft Windows 2008 R2 SP1
	3. Microsoft Windows 7 SP1
	4. Microsoft Windows 8
	5. Microsoft Windows 2012
	6. Microsoft Windows 2012 R2
	7. Microsoft Windows 8.1
	8. Microsoft Windows 10
	9. Microsoft Windows 2016
4. System musi wspierać jako silnik bazodanowy następujące bazy danych:
	1. Microsoft SQL Server 2008
	2. Microsoft SQL Server 2008 R2
	3. Microsoft SQL Server 2012
	4. Microsoft SQL Server 2014
	5. Microsoft SQL Server 2016
5. System do prezentacji raportów musi umożliwiać jednoczesny dostępu do raportów wielu użytkownikom z określonymi przez administrator systemu uprawnieniami.
6. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
7. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
8. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
9. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
10. Minimalny interwał czasowy dla zadań kolekcjonowania i raportowania musi wynosić min. 1 godzinę
11. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
12. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
13. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
14. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
15. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
16. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn wirtualnych, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
17. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
18. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy witalizacyjnej.
19. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
20. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

# Kontroler SFP (karta sieciowa światłowodowa) 1 szt.

Zamawiający wymaga dostarczenia i instalacji kontrolera Ethernet wyposażonego w dwa porty 10GB SFP+ (porty muszą być obsadzone wkładkami 10GBASE-SR) oraz 192 GB RAM do posiadanego już przez Zamawiającego serwera Dell Poweredge R420.

Min. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji
i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta sprzętu
(gwarancja poparta gwarancją Producenta), na sprzęt. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ.

Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert

# Oprogramowanie do zarządzania maszynami wirtualnymi 1szt.

1. Licencja na czas nieoznaczony na 2 serwery dwuprocesorowe.
2. Min. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji
i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta oprogramowania (gwarancja poparta gwarancją Producenta), na oprogramowanie. Wykonawca
w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ, z zastrzeżeniem,
że gwarancja Producenta musi umożliwiać także aktualizację oprogramowania do najnowszej wersji bez dodatkowych opłat oraz zapewniać pomoc Producenta w rozwiązywaniu problemów (tel., e-mail lub zdalną sesję). **Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert**.
3. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
4. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
5. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
6. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 480 logicznych wątków oraz do 6TB pamięci fizycznej RAM.
7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
8. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.
9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 4 TB pamięci operacyjnej RAM.
10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
11. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe.
12. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
13. Rozwiązanie powinno być niezależne od producenta platformy sprzętowej.
14. 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). Licencjonowanie nie może odbywać się w trybie OEM.
15. Rozwiązanie musi wspierać następujące systemy operacyjne: MS-DOS 6.22, Windows 3.1, Windows 95, Windows 98, Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 14, Ubuntu 12, SCO OpenServer, SCO Unixware, Mac OS X.
16. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
17. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
18. 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.
19. 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.
20. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
21. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
22. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
23. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.
24. 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. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
25. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
26. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).
27. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych.
28. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.
29. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
30. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

# System operacyjny serwera 4szt.

|  |
| --- |
| **Wymagania minimalne** |
| Licencja na serwerowy system operacyjny musi zapewnić poniżej opisane funkcjonalności dla jednego serwera posiadającego dwa procesory. Każdy z procesorów posiada 8 rdzeni fizycznych. 3szt. licencji będą zainstalowane na dostarczonym serwerze, 1 szt. licencji będzie instalowana na posiadanym serwerze Dell PowerEdge R420. |
| Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i **dwóch wirtualnych środowisk serwerowego systemu operacyjnego** za pomocą wbudowanych mechanizmów wirtualizacji. |
| Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy. |
| 1. Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym |
| 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. |
| 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.  |
| 4. Możliwość migracji maszyn wirtualnych z możliwością  kompresji danych, bez zatrzymywania ich pracy, między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. |
| 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. |
| 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. |
| 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. |
| 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. |
| 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: |
| a. pozwalają na zmianę rozmiaru w czasie pracy systemu, |
| b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, |
| c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, |
| d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). |
| 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. |
| 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. |
| 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET |
| 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. |
| 14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. |
| 15. Graficzny interfejs użytkownika. |
| 16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, |
| 17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. |
| 18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). |
| 19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. |
| 20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. |
| 21. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). |
| 22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: |
| a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, |
| b. 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: |
| * Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
 |
| * Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
 |
| * Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
 |
| * Ustanawianie praw dostępu do określonych zasobów dla użytkowników nie dołączonych do domeny
 |
| c. Zdalna dystrybucja oprogramowania na stacje robocze. |
| d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej |
| e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: |
| -Dystrybucję certyfikatów poprzez http |
| -Konsolidację CA dla wielu lasów domeny, |
| -Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. |
| f. Szyfrowanie plików i folderów. |
| g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). |
| h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. |
| i. Serwis udostępniania stron WWW. |
| j. Wsparcie dla protokołu IP w wersji 6 (IPv6), |
| k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, |
| l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 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: |
| - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, |
| - Obsługi ramek typu jumbo frames dla maszyn wirtualnych. |
| - Obsługi 4-KB sektorów dysków  |
| - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra |
| - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. |
| - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) |
| 23. 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. |
| 24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). |
| 25. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |
| 26. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| 27. Oprogramowanie musi być dostarczone w najnowszej wersji na dzień wszczęcia postępowania, z zastrzeżeniem, że jeżeli po tym dniu na rynku pojawią się nowsze wersje, Zamawiający dopuszcza złożenie oferty obejmującej nowszą wersję.  |

# Przełącznik sieciowy rdzeniowy (główny) 1szt.

**Wymagania podstawowe**

1. Przełącznik posiadający 16 portów 10Gigabit Ethernet SFP+, mogących pracować z prędkością 100 MB, 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+
2. Wysokość urządzenia 1U.
3. Przełącznik musi posiadać min. dwa zasilacze do realizacji redundancji zasilania.
4. Przełącznik musi mieć możliwość montażu zasilaczy AC lub DC w zależności od potrzeb (dostarczany przełącznik musi być wyposażony w min. dwa zasilacze AC)
5. Przełącznik musi posiadać możliwość instalacji zestawu wentylatorów zapewniających chłodzenie przód-tył lub tył-przód (dostarczany przełącznik musi być wyposażony w układ chłodzenia przód-tył)
6. Zarówno zasilacze jak i wentylatory muszą mieć możliwość wymiany podczas pracy urządzenia (hot-swap)
7. Nieblokująca architektura o wydajności przełączania minimum 320 Gb/s
8. Szybkość przełączania minimum 238 Milionów pakietów na sekundę
9. Średnie opóźnienia na portach maksimum 900ns (pakiety 64 bitowe)
10. Konstrukcja pozwalająca na łączenie do 8 przełączników w stos.
11. Tablica MAC adresów minimum 16k
12. Pamięć operacyjna: minimum 1GB pamięci DRAM
13. Pamięć flash: minimum 4GB pamięci Flash
14. Pojemność bufora pakietów minimum 2MB
15. Obsługa sieci wirtualnych IEEE 802.1Q – minimum 4094
16. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
17. Wsparcie dla ramek Jumbo Frames (minimum 9216 bajtów)
18. Obsługa Q-in-Q IEEE 802.1ad
19. Obsługa Quality of Service
	1. IEEE 802.1p
	2. DiffServ
	3. 8 kolejek priorytetów na każdym porcie wyjściowym
20. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
21. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
22. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
23. Wbudowany DHCP serwer i klient
24. Instalacja minimum dwóch wersji oprogramowania - firmware
25. Przechowywanie minimum kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
26. Monitorowanie zajętości CPU
27. Lokalny i zdalny monitoring pakietów (Local and Remote Mirroring)
28. Obsługa Wirtualnych Routerów - uruchamiania oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami.
29. Gwarancja użycia tych samych podsieci w różnych wirtualnych routerach.
30. Wbudowany dodatkowy port Gigabit/ Ethernet do zarządzania poza pasmem - out of band management.
31. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

**Obsługa Routingu IPv4**

1. Sprzętowa obsługa routingu IPv4 – forwarding
2. Pojemność tabeli routingu  minimum 480 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
	1. RIPv1/v2
	2. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
5. Policy Based Routing dla IPv4
6. Obsługa DHCP/BootP Relay dla IPv4

**Obsługa Routingu IPv6**

1. Sprzętowa obsługa routingu IPv6 – forwarding
2. Pojemność tabeli routingu minimum 240 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
	1. RIPng
	2. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
5. Obsługa MLDv1 (Multicast Listener Discovery version 1)
6. Obsługa MLDv2 (Multicast Listener Discovery version 2)
7. Policy Based Routing dla IPv6
8. Obsługa DHCP/BootP Relay dla IPv6
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

**Obsługa Multicastów**

1. Statyczne przyłączenie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa Multicast VLAN Registration - MVR
4. Obsługa IGMP v1 (RFC 1112)
5. Obsługa IGMP v2 (RFC 2236)
6. Obsługa IGMP v3 (RFC 3376)
7. Obsługa IGMP v1/v2/v3 snooping

**Bezpieczeństwo**

1. Obsługa Network Login
	1. IEEE 802.1x
	2. Web-based Network Login
	3. MAC based Network Login
2. Obsługa wielu klientów (minimum 4) Network Login na jednym porcie (Multiple supplicants)
3. Funkcja integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
4. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
5. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
6. Obsługa Guest VLAN dla IEEE 802.1x
7. Obsługa funkcjonalności przechwytywania autoryzacji użytkowników z wykorzystaniem odpowiedniego protokołu
8. Wbudowana obrona procesora urządzenia przed atakami DoS
9. Obsługa TACACS+ (RFC 1492)
10. Obsługa RADIUS Authentication (RFC 2865)
11. Obsługa RADIUS Accounting (RFC 2866)
12. RADIUS and TACACS+ per-command Authentication
13. Bezpieczeństwo MAC adresów
	* + - 1. ograniczenie liczby MAC adresów na porcie
				2. zatrzaśnięcie MAC adresu na porcie
				3. wpisywanie statycznych MAC adresów na port/vlan Funkcja wyłączenia MAC learning Obsługa SNMPv1/v2/v3
14. Klient SSH2
15. Zabezpieczenie przełącznika przed atakami DoS
	1. Networks Ingress Filtering RFC 2267
	2. SYN Attack Protection
	3. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
16. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
17. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
18. Obsługa bezpiecznego transferu plików SCP/SFTP
19. Obsługa DHCP Option 82
20. Obsługa Gratuitous ARP Protection
21. Obsługa Trusted DHCP Server
22. Obsługa DHCP Snooping
23. Obsługa DHCP Secured ARP/ARP Validation
24. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s

**Bezpieczeństwo sieciowe**

1. Obsługa redundancji routingu VRRP (RFC 2338)
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
5. Obsługa PVST+
6. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
7. Obsługa G.8032
8. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
9. Obsługa  rozwiązania umożlwiającego połączenie dwóch niezależnych od siebie przełączników za pomocą 2 lub więcej linków umożliwiających zagregowanie prędkości połącznia pomiędzy przełącznikami

**Zarządzanie**

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
2. Obsługa synchronizacji czasu NTP
3. Zarządzanie przez SNMP v1/v2/v3
4. Zarządzanie przez przeglądarkę WWW – protokół  http i https
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON minimum 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)

**Inne**

1. Wsparcie dla technologii Data Center Bridging (802.1Qaz & 802.1Qbb)
	1. DCBx Data Center Bridging Exchange Protocol
	2. Priority Flow Control (PFC)
	3. Enhanced Transmission Selection (ETS)
2. Obsługa OpenFlow
3. Obsługa skryptów CLI
4. Edycja skryptow i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plikow tekstowych)
5. Uruchamianie skryptów
6. Ręcznie
7. O określonym czasie lub co wskazany okres czasu
8. Na podstawie wpisów w logu systemowym
9. Gwarancja i rękojmia: min. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta (gwarancja i rękojmia poparte gwarancją Producenta), na sprzęt
i oprogramowanie. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ. **Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert**

# Przełącznik dostępowy wyposażony w 24 porty 3szt.

**Wymagania podstawowe**

1. Przełącznik 24 portów 1G 10/100/1000BASE-T oraz dodatkowo minimum 4 porty 1/10 Gigabit Ethernet SFP+
2. Wysokość urządzenia 1U.
3. Możliwość zainstalowania dodatkowego zasilacza w celu uzyskania redundancji.
4. Nieblokująca architektura o wydajności przełączania minimum 128 Gb/s
5. Szybkość przełączania minimum 95 Milionów pakietów na sekundę
6. Konstrukcja pozwalająca na łączenie do 8 przełączników w stos.
7. Tablica MAC adresów minimum 16k
8. Pamięć operacyjna: minimum 1GB pamięci DRAM
9. Pamięć flash: minimum 4GB pamięci Flash
10. Pojemność bufora pakietów minimum 1,5MB
11. Obsługa sieci wirtualnych IEEE 802.1Q – minimum 4094
12. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
13. Wsparcie dla ramek Jumbo Frames (minimum 9216 bajtów)
14. Obsługa Q-in-Q IEEE 802.1ad
15. Obsługa Quality of Service
	1. IEEE 802.1p
	2. DiffServ
	3. 8 kolejek priorytetów na każdym porcie wyjściowym
16. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
17. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
18. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
19. Wbudowany DHCP serwer i klient
20. Instalacja minimum dwóch wersji oprogramowania - firmware
21. Przechowywania minimum kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
22. Monitorowanie zajętości CPU
23. Lokalny i zdalny monitoring pakietów (Local and Remote Mirroring)
24. Obsługa Wirtualnych Routerów - uruchamiania oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami.
25. Gwarancja użycia tych samych podsieci w różnych wirtualnych routerach.
26. Wbudowany dodatkowy port Gigabit/ Ethernet do zarządzania poza pasmem - out of band management.
27. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

**Obsługa Routingu IPv4**

1. Sprzętowa obsługa routingu IPv4 – forwarding
2. Pojemność tabeli routingu  minimum 450 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
	1. RIPv1/v2
	2. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
5. Policy Based Routing dla IPv4
6. Obsługa DHCP/BootP Relay dla IPv4

**Obsługa Routingu IPv6**

1. Sprzętowa obsługa routingu IPv6 – forwarding
2. Pojemność tabeli routingu minimum 225 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
	1. RIPng
	2. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
5. Obsługa MLDv1 (Multicast Listener Discovery version 1)
6. Obsługa MLDv2 (Multicast Listener Discovery version 2)
7. Policy Based Routing dla IPv6
8. Obsługa DHCP/BootP Relay dla IPv6
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

**Obsługa Multicastów**

1. Statyczne przyłączenie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa Multicast VLAN Registration - MVR
4. Obsługa IGMP v1 (RFC 1112)
5. Obsługa IGMP v2 (RFC 2236)
6. Obsługa IGMP v3 (RFC 3376)
7. Obsługa IGMP v1/v2/v3 snooping

**Bezpieczeństwo**

1. Obsługa Network Login
2. IEEE 802.1x
3. Web-based Network Login
4. MAC based Network Login
5. Obsługa wielu klientów (minimum 4) Network Login na jednym porcie (Multiple supplicants)
6. Funkcja integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
7. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
8. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
9. Obsługa Guest VLAN dla IEEE 802.1x
10. Obsługa funkcjonalności przechwytywania autoryzacji użytkowników z wykorzystaniem odpowiedniego protokołu
11. Wbudowana obrona procesora urządzenia przed atakami DoS
12. Obsługa TACACS+ (RFC 1492)
13. Obsługa RADIUS Authentication (RFC 2865)
14. Obsługa RADIUS Accounting (RFC 2866)
15. RADIUS and TACACS+ per-command Authentication
16. Bezpieczeństwo MAC adresów
	* + - 1. ograniczenie liczby MAC adresów na porcie
				2. zatrzaśnięcie MAC adresu na porcie
				3. wpisywanie statycznych MAC adresów na port/vlan Funkcja wyłączenia MAC learning Obsługa SNMPv1/v2/v3
17. Klient SSH2
18. Zabezpieczenie przełącznika przed atakami DoS
19. Networks Ingress Filtering RFC 2267
20. SYN Attack Protection
21. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
22. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
23. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
24. Obsługa bezpiecznego transferu plików SCP/SFTP
25. Obsługa DHCP Option 82
26. Obsługa Gratuitous ARP Protection
27. Obsługa Trusted DHCP Server
28. Obsługa DHCP Snooping
29. Obsługa DHCP Secured ARP/ARP Validation
30. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s

**Bezpieczeństwo sieciowe**

1. Obsługa redundancji routingu VRRP (RFC 2338)
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
5. Obsługa PVST+
6. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
7. Obsługa G.8032
8. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
9. Obsługa  rozwiązania umożlwiającego połączenie dwóch nie zależnych od siebie przełączników za pomocą 2 lub więcej linków umożliwiających zagregowanie prędkości połącznia pomiędzy przełącznikami

**Zarządzanie**

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
2. Obsługa synchronizacji czasu NTP
3. Zarządzanie przez SNMP v1/v2/v3
4. Zarządzanie przez przeglądarkę WWW – protokół  http i https
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON minimum 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)

**Inne**

1. Obsługa skryptów CLI
2. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
3. Możliwość uruchamiania skryptów
4. Ręcznie
5. O określonym czasie lub co wskazany okres czasu
6. Na podstawie wpisów w logu systemowym
7. Gwarancja i rękojmia: min. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta (gwarancja i rękojmia poparte gwarancją Producenta), na sprzęt
i oprogramowanie. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ. **Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert**

# Przełącznik sieciowy dostępowy wyposażony w 48 portów 3szt.

**Wymagania podstawowe**

1. Przełącznik 48 portów 1G 10/100/1000BASE-T oraz dodatkowo minimum 4 porty 1/10 Gigabit Ethernet SFP+
2. Wysokość urządzenia 1U.
3. Możliwość zainstalowania dodatkowego zasilacza w celu uzyskania redundancji.
4. Nieblokująca architektura o wydajności przełączania minimum 175 Gb/s
5. Szybkość przełączania minimum 130 Milionów pakietów na sekundę
6. Konstrukcja pozwalająca na łączenie do 8 przełączników w stos.
7. Tablica MAC adresów minimum 16k
8. Pamięć operacyjna: minimum 1GB pamięci DRAM
9. Pamięć flash: minimum 4GB pamięci Flash
10. Pojemność bufora pakietów minimum 1,5MB
11. Obsługa sieci wirtualnych IEEE 802.1Q – minimum 4094
12. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
13. Wsparcie dla ramek Jumbo Frames (minimum 9216 bajtów)
14. Obsługa Q-in-Q IEEE 802.1ad
15. Obsługa Quality of Service
	1. IEEE 802.1p
	2. DiffServ
	3. 8 kolejek priorytetów na każdym porcie wyjściowym
16. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
17. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
18. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
19. Wbudowany DHCP serwer i klient
20. Instalacja minimum dwóch wersji oprogramowania - firmware
21. Przechowywania minimum kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
22. Monitorowanie zajętości CPU
23. Lokalny i zdalny monitoring pakietów (Local and Remote Mirroring)
24. Obsługa Wirtualnych Routerów - uruchamiania oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami.
25. Gwarancja użycia tych samych podsieci w różnych wirtualnych routerach.
26. Wbudowany dodatkowy port Gigabit/ Ethernet do zarządzania poza pasmem - out of band management.
27. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika

**Obsługa Routingu IPv4**

1. Sprzętowa obsługa routingu IPv4 – forwarding
2. Pojemność tabeli routingu  minimum 450 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego IPv4
	1. RIPv1/v2
	2. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
5. Policy Based Routing dla IPv4
6. Obsługa DHCP/BootP Relay dla IPv4

**Obsługa Routingu IPv6**

1. Sprzętowa obsługa routingu IPv6 – forwarding
2. Pojemność tabeli routingu minimum 225 wpisów
3. Routing statyczny
4. Obsługa routingu dynamicznego dla IPv6
	1. RIPng
	2. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
5. Obsługa MLDv1 (Multicast Listener Discovery version 1)
6. Obsługa MLDv2 (Multicast Listener Discovery version 2)
7. Policy Based Routing dla IPv6
8. Obsługa DHCP/BootP Relay dla IPv6
9. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

**Obsługa Multicastów**

1. Statyczne przyłączenie do grupy multicast
2. Filtrowanie IGMP
3. Obsługa Multicast VLAN Registration - MVR
4. Obsługa IGMP v1 (RFC 1112)
5. Obsługa IGMP v2 (RFC 2236)
6. Obsługa IGMP v3 (RFC 3376)
7. Obsługa IGMP v1/v2/v3 snooping

**Bezpieczeństwo**

1. Obsługa Network Login
2. IEEE 802.1x
3. Web-based Network Login
4. MAC based Network Login
5. Obsługa wielu klientów (minimum 4) Network Login na jednym porcie (Multiple supplicants)
6. Funkcja integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
7. Obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
8. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
9. Obsługa Guest VLAN dla IEEE 802.1x
10. Obsługa funkcjonalności przechwytywania autoryzacji użytkowników z wykorzystaniem odpowiedniego protokołu
11. Wbudowana obrona procesora urządzenia przed atakami DoS
12. Obsługa TACACS+ (RFC 1492)
13. Obsługa RADIUS Authentication (RFC 2865)
14. Obsługa RADIUS Accounting (RFC 2866)
15. RADIUS and TACACS+ per-command Authentication
16. Bezpieczeństwo MAC adresów

a. ograniczenie liczby MAC adresów na porcie

b. zatrzaśnięcie MAC adresu na porcie

c. wpisywanie statycznych MAC adresów na port/vlan Funkcja wyłączenia MAC learning Obsługa SNMPv1/v2/v3

1. Klient SSH2
2. Zabezpieczenie przełącznika przed atakami DoS
3. Networks Ingress Filtering RFC 2267
4. SYN Attack Protection
5. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
6. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
7. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
8. Obsługa bezpiecznego transferu plików SCP/SFTP
9. Obsługa DHCP Option 82
10. Obsługa Gratuitous ARP Protection
11. Obsługa Trusted DHCP Server
12. Obsługa DHCP Snooping
13. Obsługa DHCP Secured ARP/ARP Validation
14. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s

**Bezpieczeństwo sieciowe**

1. Obsługa redundancji routingu VRRP (RFC 2338)
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
5. Obsługa PVST+
6. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
7. Obsługa G.8032
8. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
9. Obsługa  rozwiązania umożlwiającego połączenie dwóch nie zależnych od siebie przełączników za pomocą 2 lub więcej linków umożliwiających zagregowanie prędkości połącznia pomiędzy przełącznikami

**Zarządzanie**

1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
2. Obsługa synchronizacji czasu NTP
3. Zarządzanie przez SNMP v1/v2/v3
4. Zarządzanie przez przeglądarkę WWW – protokół  http i https
5. Telnet Serwer/Klient dla IPv4 / IPv6
6. SSH2 Serwer/Klient dla IPv4 / IPv6
7. Ping dla IPv4 / IPv6
8. Traceroute dla IPv4 / IPv6
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów
10. Sprzętowa obsługa sFlow
11. Obsługa RMON minimum 4 grupy: Status, History, Alarms, Events (RFC 1757)
12. Obsługa RMON2 (RFC 2021)

**Inne**

1. Obsługa skryptów CLI
2. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
3. Możliwość uruchamiania skryptów
4. Ręcznie
5. O określonym czasie lub co wskazany okres czasu
6. Na podstawie wpisów w logu systemowym
7. Gwarancja i rękojmia: min. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta (gwarancja i rękojmia poparte gwarancją Producenta), na sprzęt
i oprogramowanie. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ. **Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert.**

# Przewód do połącznia przełączników dostępowych 6szt.

6 szt. przewodów typu DAC SFP+ o długości 1 metra kompatybilnych z dostarczanymi przełącznikami dostępowymi umożlwiające połączenie przełączników w stos (wydajność stosu min. 40GB).

Gwarancja i rękojmia: min. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta (gwarancja i rękojmia poparte gwarancją Producenta), na sprzęt. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ. **Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert.**

# Moduł do podłączenia światłowodu do przełączników sieciowych dostępowych i rdzeniowych 13 szt.

15szt. modułów SFP+ 10GBASE-SR kompatybilnych z dostarczanymi przełącznikami rdzeniowymi i dostępowymi.

Gwarancja i rękojmia: min. 12 miesięcy gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta (gwarancja i rękojmia poparte gwarancją Producenta), na sprzęt. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji i rękojmi wymaganych w SIWZ. **Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert.**

# Usługa wdrożenia

1. Instalacja:
2. Instalacja dostarczonego sprzętu w szafie rack w siedzibie Zamawiającego
3. Podłączenie przełącznika sieci SAN, macierzy dyskowej i serwerów z posiadaną przez Zamawiającego infrastrukturą
4. Konfiguracja:
5. Przed przystąpieniem do prac wdrożeniowych Wykonawca przedstawi do zaakceptowania Zamawiającemu koncepcję wdrożenia wszystkich elementów objętych zamówieniem.
6. Konfiguracja dostarczonych serwerów, przełącznika SAN, posiadanej macierzy dyskowej, w celu uruchomienia protokołu SAN iSCSI – wymagana jest pełna konfiguracja hypervisora oraz dostarczonych systemów operacyjnych
i sprzętu (patchcordy, moduły SFP+, przełączniki sieciowe). Wszystkie elementy muszą być podłączone interfejsami optycznymi do przełącznika sieciowego SAN. Zamawiający wymaga takiej konfiguracji, aby zapewnić wielościeżkowość dla serwera i macierzy dyskowej. System musi działać w klastrze wysokiej dostępności.
7. Instalacja i konfiguracja dostarczonego oprogramowania do tworzenia kopii zapasowej.
8. Podłączenie wszystkich elementów zgodnie z zaakceptowaną przez Zamawiającego koncepcją wdrożenia.
9. Uruchomienie kanału zdalnego zarządzania całą dostarczoną infrastrukturą na posiadanym przez Zamawiającego urządzeniu UTM Sonicwall NSA 2600
10. Konfiguracja wirtualizacji
11. Środowisko oparte o 2 serwery fizyczne oraz współdzielony zasób macierzowy.
12. Konfiguracja klastra HA dla maszyn virtualnych na 2 maszynach fizycznych
13. Automatyczne przenoszenie i uruchomienie maszyn virtualnych podczas awarii jednego z serwerów fizycznych na host nieuszkodzony.
14. Konfiguracja virtualnych switchy (podział na 4 podsieci: BACKUP, DMZ, LAN, MGMT)
15. Migracja systemów:
16. Migracja oprogramowania i systemów operacyjnych znajdującego się na posiadanych przez Zamawiającego serwerach na dostarczone środowisko.
17. Warunki wdrożenia:
18. Wdrożenie musi być przeprowadzone w taki sposób, aby nie zakłócało bieżącej działalności Zamawiającego. Wszystkie urządzenia muszą pochodzić z legalnego źródła oraz zostać zakupione w autoryzowanym kanale sprzedaży producenta na terenie Unii Europejskiej. Sprzęt musi być fabrycznie nowy i nie może pochodzić z dostawy do realizacji projektu u innego klienta.

# Wymagania dodatkowe

Na wszystkie elementy przedmiotu zamówienia Zamawiający wymaga min. 12 miesięcznej gwarancji i rękojmi. W okresie i w ramach udzielonej przez Wykonawcę gwarancji i rękojmi Wykonawca zobowiązany jest zapewnić Zamawiającemu także gwarancję Producenta (gwarancja i rękojmia poparte gwarancją Producenta), na poszczególne elementy przedmiotu zamówienia. Wykonawca w dniu odbioru przekaże Zamawiającemu dokumenty gwarancyjne. Warunki gwarancji Producenta muszą być nie gorsze od warunków gwarancji
i rękojmi wymaganych w niniejszej SIWZ. Ilekroć w niniejszej SIWZ wskazano dodatkowe, szczególne wymogi związane z gwarancją, rękojmią lub gwarancją Producenta, są one wiążące. **Termin gwarancji i rękojmi stanowi jedno z kryteriów oceny ofert.**

W ramach udzielonej gwarancji i rękojmi, Wykonawca zapewni usługę wsparcia technicznego w zakresie eksploatacji wdrożonej infrastruktury, w wymiarze 30 godzin, do wykorzystania w terminie 12 miesięcy od daty podpisania protokołu odbioru końcowego. Dopuszcza się wsparcie realizowane zdalnie (e-mail, tel., zdalna sesja). Usługa wsparcia technicznego polegać będzie na udzielaniu odpowiedzi i porad technicznych związanych
z eksploatacją sprzętu i oprogramowania oraz rozwiązywaniu zgłoszonych problemów. Usługa świadczona będzie w dni robocze, w godz. od 8.00 do 16.00. W ramach usługi wsparcia technicznego Zamawiający wymaga udzielenia odpowiedzi na zgłoszony problem, porady technicznej lub rozwiązywania zgłoszonego problemu najpóźniej następnego dnia po dniu przekazania zgłoszenia.