*Załącznik nr 3a do SIWZ*

*Załącznik nr 1 do umowy*

*pieczęć Wykonawcy*

**FORMULARZ TECHNICZNY**

**Parametry techniczne sprzętu oraz oprogramowania oferowanego przez Wykonawcę**Wykonawca zobowiązany jest do wypełnienia kolumny ***„Parametry techniczne sprzętu oferowanego przez Wykonawcę” / „Parametry techniczne oprogramowania oferowanego przez Wykonawcę”***  oraz podania nazwy, modelu i wersji produktów.

1. **Obudowa blade (klatka) – 2 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Obudowa, o wysokości maksymalnie 10U, musi być przystosowana do montażu w szafie typu rack 19”, umożliwiająca obsadzenie minimum 16 serwerów dwuprocesorowych bez konieczności rozbudowy o kolejne elementy sprzętowe. |  |
| 2 | Możliwość umieszczania w ramach pojedynczej obudowy wszystkich typów serwerów blade danego producenta. |  |
| 3 | Sposób agregacji/wyprowadzeń sygnałów LAN dla pojedynczej obudowy.Minimum dwa przełączniki LAN. Urządzenia te muszą umożliwiać agregację połączeń LAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów LAN z infrastruktury z zachowaniem redundancji połączeń. Każdy z modułów musi posiadać minimum 16 wewnętrznych portów 20Gb lub minimum 32 wewnętrzne porty 10Gb do serwerów (sumaryczne pasmo portów wewnętrznych pojedynczego modułu LAN do serwerów, musi wynosić minimum 320Gb).Każdy z modułów musi posiadać porty zewnętrzne:* Minimum 4 porty 40Gb QSFP+
* Minimum 8 portów dual personality 1/10Gb RJ45/SFP+ z możliwością zamontowania modułów SFP 10Gb SFP+ oraz 1Gb RJ45 – nie dopuszcza się zastosowania kabli typu „splitter” QSFP+ do 4xSFP+.

Sumaryczna przepustowość portów zewnętrznych (porty 40Gb oraz porty 10Gb, nie dopuszcza się samych portów 40Gb) musi wynosić minimum 240Gb dla pojedynczego modułu LAN.Wraz z modułami należy dostarczyć sumarycznie:* 8 wkładek 40Gb QSFP+
* 6 wkładek 10Gb SFP+ SR
* 4 wkładki 1Gb SFP RJ45.

Wszystkie dostępne, fizyczne porty (wewnętrzne oraz zewnętrzne) każdego modułu LAN (niezależnie od minimalnej wymaganej ilości portów) muszą być aktywne i gotowe do obsługi ruchu sieciowego bez konieczności dokupowania elementów sprzętowych lub dodatkowych licencji. Należy dostarczyć wszystkie niezbędne licencje do aktywacji wszystkich portów urządzeń. |  |
| 4 | Każda obudowa musi posiadać minimum dwa moduły typu switch 16Gb Fibre-Channel wyprowadzające sygnały z minimum 2 portów FC na serwerach. Urządzenia te muszą umożliwiać agregację połączeń SAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów SAN z infrastruktury z zachowaniem redundancji połączeń. Każdy moduł musi posiadać minimum 12 zewnętrznych portów obsadzonych modułami 16Gb SFP+ SW.Wszystkie dostępne, fizyczne porty każdego modułu Fibre-Channel muszą być aktywne i gotowe do obsługi ruchu sieciowego SAN bez konieczności dokupowania elementów sprzętowych lub dodatkowych licencji.Każdy moduł powinien umożliwiać (posiadać licencje):• ISL Trunking• Fabric Watch• Extended Fabric• Zaawansowane zarządzanie wydajnością |  |
| 5 | Możliwość przydzielania adresów MAC i WWN predefiniowanych przez producenta rozwiązania blade dla poszczególnych wnęk na serwery w obudowie. Przydzielenie adresów musi powodować zastąpienie fizycznych adresów kart Ethernet i Fibre-Channel na serwerze. Musi istnieć także możliwość przenoszenia przydzielonych adresów pomiędzy wnękami w obudowie. Funkcjonalność ta może być realizowana zarówno poprzez moduły LAN i SAN w infrastrukturze jak i poprzez dodatkowe oprogramowanie producenta serwerów blade. Dodatkowo dla sieci LAN musi istnieć możliwość stworzenia niezależnych połączeń VLAN tak aby między wydzielonymi sieciami nie było komunikacji. Wymagana jest możliwość boot’owania systemów operacyjnych zainstalowanych na poszczególnych serwerach blade bezpośrednio z macierzy w środowisku SAN. Wymagane wszystkie niezbędne licencje na opisaną funkcjonalność dla całej infrastruktury blade.W przypadku sieci LAN, musi istnieć możliwość określenia pasma przepustowości pojedynczego portu LAN na serwerze od 100Mb/s do 10Gb/s. |  |
| 6 | Każda z obudów na serwery wyposażona w zestaw redundantnych wentylatorów (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie blade. Wentylatory niezależne od zasilaczy, wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia zasilacza (zasilaczy). |  |
| 7 | Każda z obudów wyposażona w zestaw zasilaczy redundantnych typu Hot Plug. System zasilania zdolny do obsługi awarii połowy z zainstalowanych zasilaczy (dowolne N zasilaczy przy założeniu konfiguracji N + N), wymagane ciągłe dostarczenie mocy niezbędnej do zasilenia maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie. Procesory serwerów winny pracować z nominalną, maksymalną częstotliwością. Wymiana zasilacza nie może powodować konieczności odłączenia zewnętrznej infrastruktury zasilania (kabla zasilającego), jak również nie może powodować konieczności wyjęcia lub odłączenia wentylatorów (pojedynczego wentylatora lub modułu wentylatorów). |  |
| 8 | Możliwość instalacji switchy w standardzie InfiniBand oraz switchy SAS. |  |
| 9 | Dwa redundantne, sprzętowe moduły zarządzające, moduły typu Hot Plug. Moduł KVM, umożliwiający podłączenie klawiatury, myszy i monitora. |  |
| 10 | Każda z obudów wchodzących w skład infrastruktury musi posiadać identyczną konfigurację sprzętową w zakresie zasilaczy, wentylatorów oraz modułów I/O. |  |
| 11 | Wraz z infrastrukturą blade, należy dostarczyć odpowiednią ilość modułów PDU do prawidłowego, redundantnego podłączenia infrastruktury blade do zasilania w szafach Zamawiającego. PDU muszą spełniać minimalne wymagania:-minimum 32A-minimum dwa redundantne moduły (należy uwzględnić odpowiednią ilość modułów dla redundantnego podłączenia całej infrastruktury blade)-ilość gniazd zapewniająca podłączenie dostarczonej infrastruktury blade |  |
| 12 | Podstawowe funkcje: Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera |  |
| 13 | Zdalne udostępnianie napędu CD-ROM/DVD/ISO na potrzeby każdego serwera z możliwością bootowania z w/w napędów. |  |
| 14 | Zdalny sposób zarządzania z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu. |  |
| 15 | W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów w ramach infrastruktury |  |
| 16 | Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego |  |
| 17 | Automatyzowana konfiguracja sprzętowa każdego serwera niezależnie oraz wielu serwerów równocześnie za pomocą skryptów |  |
| 18 | Zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci)  |  |
| 19 | Zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. Plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego |  |
| 20 | Zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu |  |
| 21 | Zdalna dystrybucja oprogramowania,  |  |
| 22 | Automatyczne wykrywanie i identyfikacja urządzeń zainstalowanych w ramach infrastruktury (serwery, obudowy blade, karty zarządzające) i prezentacja infrastruktury w postaci graficznej |  |
| 23 | Monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć, dyski twarde, interfejsy sieciowe |  |
| 24 | Integracja z oprogramowaniem do wirtualizacji, w zakresie wykrywania hostów, wirtualnych maszyn na nich pracujących, możliwości sterowania wirtualnymi maszynami (start, stop, przejęcie konsoli graficznej) |  |
| 25 | Licencje na powyższą funkcjonalność na wszystkie serwery blade możliwe do obsadzenia w oferowanej infrastrukturze blade. |  |

1. **Serwery blade – 26 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Zainstalowane 2 procesory, minimum 14 rdzeni każdy, x86 - 64 Bit osiągające w testach SPECint\_rate2006 wynik nie gorszy niż 1290 punktów w konfiguracji dwuprocesorowej. |  |
| 2 | Zainstalowane 1TB RAM DDR4 Registred DIMMs w modułach min. 64GB. Minimum 16 slotów na pamięć. Możliwość rozbudowy do 2TB RAM. |  |
| 3 | Minimum jeden wewnętrzny port USB umożliwiający instalację pamięci Flash. |  |
| 4 | Minimum 2 sloty PCI-Express x16 (szybkość slotu). |  |
| 5 | Dwa Interfejsy SAN FC 16Gb. |  |
| 6 | Minimum 2 Interfejsy sieciowe 20GbE z możliwością podzielenia każdego interfejsu na 4 karty sieciowe (posiadające własne adresy MAC oraz będące widoczne z poziomu systemu operacyjnego jako fizyczne karty sieciowe). Podział musi być niezależny od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej. |  |
| 7 | Wspierane systemy operacyjne: MS Windows 2008 R2, MS Windows 2012 R2, Red Hat Enterprise Linux ,SUSE Linux Enterprise Server, VMware 6.0. |  |

1. **Serwery RACK typ A – 8 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Zainstalowane 2 procesory, maksimum 6 rdzeni każdy, x86 - 64 Bit osiągające w testach SPECint\_rate2006 wynik nie gorszy niż 1250 punktów w konfiguracji dwuprocesorowej. |  |
| 2 | Zainstalowane minimum 1TB RAM DDR4 Registred DIMMs w modułach min. 64GB. |  |
| 3 | 2 dyski SSD typu Hot Swap, każdy o pojemności minimum 1TB. |  |
| 4 | Kontroler dysków obsługujący poziomy RAID 0/1. |  |
| 5 | 2 redundantne zasilacze typu Hot-plug. |  |
| 6 | Zestaw redundantnych wentylatorów. |  |
| 7 | Minimum 2 sloty PCI-Express x16 (szybkość slotu). |  |
| 8 | Dwa Interfejsy SAN FC 16Gb. |  |
| 9 | Minimum 2 Interfejsy sieciowe 1GbE i 2 Interfejsy sieciowe 10GbE. |  |
| 10 | Wsperane systemy operacyjne: MS Windows 2008 R2, MS Windows 2012 R2, Red Hat Enterprise Linux. |  |
| 11 | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.Wraz z serwerem należy dostarczyć oprogramowanie do zarządzania serwerem, pozwalające na:• Inwentaryzację sprzętu serwerowego, monitoring zdrowia - „health status”• zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci)• zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego• zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu• monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć, dyski twarde, interfejsy sieciowe i zasilania• integrację z oprogramowanie wirtualizacyjnym, możliwość zarządzania maszynami wirtualnymi oraz hostami z jednej wspólnej konsoli oprogramowania producenta serwera |  |

1. **Serwery RACK typ B - 4 szt.**

| ID | Wymaganie |  |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Zainstalowane 1 procesor, maksimum 6 rdzeni, x86 - 64 Bit osiągający w testach SPECint\_rate2006 wynik nie gorszy niż 625 punktów. |  |
| 2 | Zainstalowane minimum 512GB RAM DDR4 Registred DIMMs w modułach min. 64GB. |  |
| 3 | 2 dyski SSD typu Hot Swap, każdy o pojemności minimum 1TB. |  |
| 4 | Kontroler dysków obsługujący poziomy RAID 0/1. |  |
| 5 | 2 redundantne zasilacze typu Hot-plug. |  |
| 6 | Zestaw redundantnych wentylatorów. |  |
| 7 | Minimum 2 sloty PCI-Express x16 (szybkość slotu). |  |
| 8 | Dwa Interfejsy SAN FC 16Gb. |  |
| 9 | Minimum 2 Interfejsy sieciowe 1GbE i 2 Interfejsy sieciowe 10GbE. |  |
| 10 | Wsperane systemy operacyjne: MS Windows 2008 R2, MS Windows 2012 R2, Red Hat Enterprise Linux. |  |
| 11 | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.Wraz z serwerem należy dostarczyć oprogramowanie do zarządzania serwerem, pozwalające na:• Inwentaryzację sprzętu serwerowego, monitoring zdrowia - „health status”• zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci)• zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego• zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu• monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć, dyski twarde, interfejsy sieciowe i zasilania• integrację z oprogramowanie wirtualizacyjnym, możliwość zarządzania maszynami wirtualnymi oraz hostami z jednej wspólnej konsoli oprogramowania producenta serwera |  |

1. **Konsola zarządzająca - 2 szt.**

|  |  |  |
| --- | --- | --- |
| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Konsola składająca się z monitora (minimum 17’’), klawiatury i urządzenia wskazującego (track ball, touchpad, itp...). Zajmująca w szafie nie więcej niż 1U. |  |
| 2 | Zainstalowany wraz z konsolą przełącznik KVM zapewniający możliwość podłączenia minimum 8 oferowanych serwerów RACK, dostarczony komplet wymaganych adapterów/interfejsów. Całość rozwiązania ma zajmować w szafie 1U. |  |

1. **Macierz blokowa typ A - 2szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Oferowane urządzenie musi być dostarczone ze wszystkimi niezbędnymi komponentami do instalowania w szafie rack 19''. |  |
| 2 | Oferowane urządzenie musi posiadać kontrolery pracujące w trybie Active-Active z funkcją Mirrored cache. |  |
| 3 | Macierz musi być wyposażona w minimum 1024GB pamięci Cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy (nie może to być funkcjonalność tieringu), musi być możliwość włączenia lub wyłączenia buforowania on-line (bez konieczności migracji bądź przenoszenia zawartości wolumenów). |  |
| 4 | Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych. |  |
| 5 | Macierz musi obsługiwać dyski 2,5” jak i 3,5”. |  |
| 6 | Macierz dyskowa musi umożliwiać stosowanie w niej dysków SSD, HDD 15k, HDD 10k i HDD 7,2k rpm wyposażonych w interfejsy SAS 12Gbps (SAS, NL-SAS).  |  |
| 7 | Macierz musi być wyposażona w dyski posiadające podwójne interfejsy. |  |
| 8 | Macierz musi mieć możliwość instalacji dysków SSD, SAS, NL-SAS w tej samej półce dyskowej. |  |
| 9 | Oferowana macierz musi posiadać dla każdego kontrolera minimum 2 porty FC, obsadzone modułami światłowodowymi SFP+ 16 Gb/s  |  |
| 10 | RAID w macierzy: obsługa poziomów RAID 1 lub 10, 5, 6. |  |
| 11 | Macierz musi obsługiwać protokół FC - jeśli wymagane są licencje Wykonawca dostarczy je wraz z macierzą.  |  |
| 12 | Brak pojedynczego punktu awarii.  |  |
| 13 | Redundantne zasilanie, chłodzenie, kontrolery, dwie ścieżki dostępu do każdego dysku. |  |
| 14 | Graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie. |  |
| 15 | Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.  |  |
| 16 | Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI. |  |
| 17 | Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, z jednej konsoli administracyjnej. |  |
| 18 | Wymagane jest aby dostarczona macierz posiadała interfejs zarządzający GUI, CLI, oraz umożliwiała tworzenie skryptów użytkownika. |  |
| 19 | Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie w oparciu o użytkowników z przypisanymi uprawnieniami (role-based). |  |
| 20 | Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. |  |
| 21 | W pełni nadmiarowe wentylatory i zasilacze z możliwością wymiany podczas pracy. |  |
| 22 | Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. |  |
| 23 | Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji. |  |
| 24 | Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli. |  |
| 25 | Macierz musi posiadać funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych (SSD, SAS/FC, NLSAS/SATA), w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji. |  |
| 26 | Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych. |  |
| 27 | Macierz musi obsługiwać LUN Masking i Lun mapping. |  |
| 28 | Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu mają być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych |  |
| 29 | Macierz musi posiadać funkcjonalność zwiększania rozmiaru wolumenów. |  |
| 30 | Macierz powinna zapewniać wykonywanie kopii migawkowych w ilości minimum 256 dla wolumenu logicznego. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest obecnie przedmiotem zamówienia. |  |
| 31 | Macierz musi wspierać mechanizm zdalnej replikacji w trybie synchronicznym i asynchronicznym. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.  |  |
| 32 | Obsługiwane systemy operacyjne: Microsoft Windows 2008/2008R2/2012/2012R2, Suse 11/12, Redhat 5/6/7, Solaris 11, VMware 5.0/5.1/5.5/6.0, vVOL. |  |
| 33 | Wymagane jest dostarczenie macierzy dyskowej spełniającej wymagania pojemnościowe:Macierz dyskowa składająca się z 3 obszarów dyskowych:I - zapewniającego bardzo wysoką wydajność - musi zawierać dyski SSD w ilości minimum 27 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 27TB w konfiguracji RAID 5\*\*II - zapewniającego wysoką wydajność - musi zawierać dyski SAS o prędkości obrotowej nie mniejszej niż 10k RPM w ilości minimum 90 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 128TB w konfiguracji RAID 5\*\*III - zapewniającego wysoką pojemność - musi zawierać dyski SAS/NL-SAS o prędkości obrotowej nie mniejszej niż 7,2k RPM w ilości minimum 40 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 161TB w konfiguracji RAID 6\*\*Należy wyposażyć macierz w niezbędne dyski zapasowe (spare) zgodnie z zaleceniami producenta macierzy (nie mniej niż 1 sztuka na 30 dysków).Wszystkie dyski oferowanej i dostarczonej macierzy muszą pracować w trybie „Hot-Plug”.W każdym z obszarów wszystkie dyski muszą być tego samego typu i pojemnościNie dopuszcza się stosowania dysków cMLC a jedynie dyski klasy eMLC.\*\* - Należy przyjąć, że 1 TB=1024GB, 1 GB=1024MB, 1MB=1024kB, 1kB=1024B i grupy dyskowe RAID nie większe niż 9 dysków dla RAID 5 oraz 8 dysków dla RAID 6. |  |
| 34 | Oferowana macierz ma więcej niż 1024GB pamięci cache. |  |
| 35 | Oferowane rozwiązanie musi umożliwiać wirtualizację zasobów dyskowych macierzy dyskowych pochodzących od różnych dostawców, m. in. HP, IBM, EMC, HDS. Wymagane jest dostarczenie licencji na maksymalną pojemność oferowanych macierzy. |  |
| 36 | Oferowane rozwiązanie musi umożliwiać prezentacje zwirtualizowanych zasobów dyskowych do aplikacji pracujących na różnych platformach OS, mi. In: IBM AIX, HP-UX, Linux, MS Windows, Solaris, VMware. |  |
| 37 | Oferowane rozwiązanie musi umożliwiać prezentowanie do aplikacji wolumenów logicznych wystawionych z macierzy dyskowych w sposób nienaruszający zawartości tych wolumenów (prezentacja 1 do 1). Oferowane rozwiązanie musi umożliwiać połączenie macierzy w dwóch oddalonych od siebie centrach przetwarzania danych (ośrodkach) w celu umożliwienia wirtualizacji zasobów dyskowych pomiędzy tymi centrami – rozwiązanie separowane geograficznie. |  |
| 38 | Wymagane jest, aby oferowane rozwiązanie umożliwiało transmisję danych pomiędzy ośrodkami w trybie synchronicznym. Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało oddalenie pary wirtualizatorów na odległość, dla której opóźnienie transmisji danych RTT dochodzi do 5ms. |  |
| 39 | Wirtualny wolumen logiczny prezentowany jednocześnie w trybie zapisu/odczytu w obu lokalizacjach zbudowany jest w oparciu o parę fizycznych wolumenów logicznych połączonych ze sobą zdalną replikacją danych (kopia lustrzana realizowana pomiędzy lokalizacjami). Wymagane jest zapewnienie spójności danych dla synchronicznego trybu replikacji. |  |
| 40 | Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało zastosowanie arbitra, znajdującego się w trzeciej lokalizacji, w celu uniknięcia zjawiska split-brain w przypadku awarii komunikacji pomiędzy centrami przetwarzania danych. |  |
| 41 | Oferowane rozwiązanie separowane geograficznie musi posiadać mechanizmy umożliwiające pracę, przy zachowaniu pełnej funkcjonalności oraz bezpieczeństwa i spójności danych także bez stosowania arbitra. |  |
| 42 | Oferowane rozwiązanie wirtualizujące musi posiadać wsparcie dla protokołów VAAI (CompareAndWrite SCSI Command) oraz VASA. |  |
| 43 | Oferowane rozwiązanie musi być odporne na awarię pojedynczego elementu. |  |
| 44 | Oferowane rozwiązanie musi umożliwiać naprawę, rozbudowę, aktualizacje oprogramowania wewnętrznego w sposób nieprzerywający dostępu do danych. Awaria dowolnego pojedynczego kontrolera rozwiązania nie może wymuszać konieczności przełączenia pracy aplikacji do drugiego ośrodka lub ręcznej rekonfiguracji środowiska. |  |
| 45 | W celu zapewnienia dostępności oraz wydajności oferowane rozwiązanie musi umożliwiać prezentowanie każdego wirtualnego wolumenu logicznego do serwerów poprzez wszystkie kontrolery oferowanego rozwiązania jednocześnie, także po rozbudowie do maksymalnej liczby kontrolerów |  |
| 46 | Oferowany rozwiązanie wirtualizacyjne (dla pojedynczej lokalizacji) ma być wyposażone w co najmniej:* 2 kontrolery z możliwością rozbudowy do co najmniej 8.
* 8 portów FC 16 Gb/s służących do komunikacji z serwerami, z możliwością rozbudowy do co najmniej 32.
* 8 portów FC 16 Gb/s służących do komunikacji z macierzami dyskowymi, z możliwością rozbudowy do co najmniej 32.
* 256 GB pamięci podręcznej brutto, z możliwością rozbudowy do co najmniej 1024 GB.
* 4 porty FC 16 Gb/s służące do komunikacji pomiędzy lokalizacjami, z możliwością rozbudowy do co najmniej 16.
 |  |
| 47 | Dla rozwiązania wirtualizacyjnego wsparcie dla operacji vMotion dla parametrów łącza pomiędzy site RTT=10ms |  |

1. **Macierz blokowa typ B – 1 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Oferowane urządzenie musi być dostarczone ze wszystkimi niezbędnymi komponentami do instalowania w szafie rack 19''. |  |
| 2 | Oferowane urządzenie musi posiadać kontrolery pracujące w trybie Active-Active z funkcją Mirrored cache. |  |
| 3 | Macierz musi być wyposażona w minimum 1024GB pamięci Cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy (nie może to być funkcjonalność tieringu), musi być możliwość włączenia lub wyłączenia buforowania on-line (bez konieczności migracji bądź przenoszenia zawartości wolumenów). |  |
| 4 | Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych. |  |
| 5 | Macierz musi obsługiwać dyski 2,5” jak i 3,5”. |  |
| 6 | Macierz dyskowa musi umożliwiać stosowanie w niej dysków SSD, HDD 15k, HDD 10k i HDD 7,2k rpm wyposażonych w interfejsy SAS 12Gbps (SAS, NL-SAS). |  |
| 7 | Macierz musi być wyposażona w dyski posiadające podwójne interfejsy. |  |
| 8 | Macierz musi mieć możliwość instalacji dysków SSD, SAS, NL-SAS w tej samej półce dyskowej. |  |
| 9 | Oferowana macierz musi posiadać dla każdego kontrolera minimum 2 porty FC, obsadzone modułami światłowodowymi SFP+ 16 Gb/s |  |
| 10 | RAID w macierzy: obsługa poziomów RAID 1 lub 10, 5, 6. |  |
| 11 | Macierz musi obsługiwać protokół FC - jeśli wymagane są licencje Wykonawca dostarczy je wraz z macierzą. |  |
| 12 | Brak pojedynczego punktu awarii. |  |
| 13 | Redundantne zasilanie, chłodzenie, kontrolery, dwie ścieżki dostępu do każdego dysku. |  |
| 14 | Graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie. |  |
| 15 | Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. |  |
| 16 | Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI. |  |
| 17 | Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, z jednej konsoli administracyjnej. |  |
| 18 | Wymagane jest aby dostarczona macierz posiadała interfejs zarządzający GUI, CLI, oraz umożliwiała tworzenie skryptów użytkownika. |  |
| 19 | Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie w oparciu o użytkowników z przypisanymi uprawnieniami (role-based). |  |
| 20 | Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. |  |
| 21 | W pełni nadmiarowe wentylatory i zasilacze z możliwością wymiany podczas pracy. |  |
| 22 | Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. |  |
| 23 | Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji. |  |
| 24 | Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli. |  |
| 25 | Macierz musi posiadać funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych (SSD, SAS/FC, NLSAS/SATA), w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji. |  |
| 26 | Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych. |  |
| 27 | Macierz musi obsługiwać LUN Masking i Lun mapping. |  |
| 28 | Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu mają być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych |  |
| 29 | Macierz musi posiadać funkcjonalność zwiększania rozmiaru wolumenów. |  |
| 30 | Macierz powinna zapewniać wykonywanie kopii migawkowych w ilości minimum 256 dla wolumenu logicznego. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest obecnie przedmiotem zamówienia. |  |
| 31 | Macierz musi wspierać mechanizm zdalnej replikacji w trybie synchronicznym i asynchronicznym. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia. |  |
| 32 | Obsługiwane systemy operacyjne: Microsoft Windows 2008/2008R2/2012/2012R2, Suse 11/12, Redhat 5/6/7, Solaris 11, VMware 5.0/5.1/5.5/6.0, vVOL. |  |
| 33 | Wymagane jest dostarczenie macierzy dyskowej spełniającej wymagania pojemnościowe:Macierz dyskowa składająca się z 2 obszarów dyskowych:I - zapewniającego bardzo wysoką wydajność - musi zawierać dyski SSD w ilości minimum 38 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 91TB w konfiguracji RAID 5\*\*II - zapewniającego wysoką wydajność - musi zawierać dyski SAS o prędkości obrotowej nie mniejszej niż 10k RPM w ilości minimum 121 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 111TB w konfiguracji RAID 5\*\*Należy wyposażyć macierz w niezbędne dyski zapasowe (spare) zgodnie z zaleceniami producenta macierzy (nie mniej niż 1 sztuka na 30 dysków).Wszystkie dyski oferowanej i dostarczonej macierzy muszą pracować w trybie „Hot-Plug”.W każdym z obszarów wszystkie dyski muszą być tego samego typu i pojemnościNie dopuszcza się stosowania dysków cMLC a jedynie dyski klasy eMLC.\*\* - Należy przyjąć, że 1 TB=1024GB, 1 GB=1024MB, 1MB=1024kB, 1kB=1024B i grupy dyskowe RAID nie większe niż 9 dysków dla RAID 5. |  |
| 34 | Oferowana macierz ma więcej niż 1024GB pamięci cache |  |
| 35 | Oferowane rozwiązanie musi umożliwiać wirtualizację zasobów dyskowych macierzy dyskowych pochodzących od różnych dostawców, m. in. HP, IBM, EMC, HDS. Wymagane jest dostarczenie licencji na maksymalną pojemność oferowanych macierzy. |  |
| 36 | Oferowane rozwiązanie musi umożliwiać prezentacje zwirtualizowanych zasobów dyskowych do aplikacji pracujących na różnych platformach OS, mi. In: IBM AIX, HP-UX, Linux, MS Windows, Solaris, VMware. |  |
| 37 | Oferowane rozwiązanie musi umożliwiać prezentowanie do aplikacji wolumenów logicznych wystawionych z macierzy dyskowych w sposób nienaruszający zawartości tych wolumenów (prezentacja 1 do 1). Oferowane rozwiązanie musi umożliwiać połączenie macierzy w dwóch oddalonych od siebie centrach przetwarzania danych (ośrodkach) w celu umożliwienia wirtualizacji zasobów dyskowych pomiędzy tymi centrami – rozwiązanie separowane geograficznie. |  |
| 38 | Wymagane jest, aby oferowane rozwiązanie umożliwiało transmisję danych pomiędzy ośrodkami w trybie synchronicznym. Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało oddalenie pary wirtualizatorów na odległość, dla której opóźnienie transmisji danych RTT dochodzi do 5ms. |  |
| 39 | Wirtualny wolumen logiczny prezentowany jednocześnie w trybie zapisu/odczytu w obu lokalizacjach zbudowany jest w oparciu o parę fizycznych wolumenów logicznych połączonych ze sobą zdalną replikacją danych (kopia lustrzana realizowana pomiędzy lokalizacjami). Wymagane jest zapewnienie spójności danych dla synchronicznego trybu replikacji. |  |
| 40 | Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało zastosowanie arbitra, znajdującego się w trzeciej lokalizacji, w celu uniknięcia zjawiska split-brain w przypadku awarii komunikacji pomiędzy centrami przetwarzania danych. |  |
| 41 | Oferowane rozwiązanie separowane geograficznie musi posiadać mechanizmy umożliwiające pracę, przy zachowaniu pełnej funkcjonalności oraz bezpieczeństwa i spójności danych także bez stosowania arbitra. |  |
| 42 | Oferowane rozwiązanie wirtualizujące musi posiadać wsparcie dla protokołów VAAI (CompareAndWrite SCSI Command) oraz VASA. |  |
| 43 | Oferowane rozwiązanie musi być odporne na awarię pojedynczego elementu. |  |
| 44 | Oferowane rozwiązanie musi umożliwiać naprawę, rozbudowę, aktualizacje oprogramowania wewnętrznego w sposób nieprzerywający dostępu do danych. Awaria dowolnego pojedynczego kontrolera rozwiązania nie może wymuszać konieczności przełączenia pracy aplikacji do drugiego ośrodka lub ręcznej rekonfiguracji środowiska. |  |
| 45 | W celu zapewnienia dostępności oraz wydajności oferowane rozwiązanie musi umożliwiać prezentowanie każdego wirtualnego wolumenu logicznego do serwerów poprzez wszystkie kontrolery oferowanego rozwiązania jednocześnie, także po rozbudowie do maksymalnej liczby kontrolerów |  |
| 46 | Oferowany rozwiązanie wirtualizacyjne (dla pojedynczej lokalizacji) ma być wyposażone w co najmniej:• 2 kontrolery z możliwością rozbudowy do co najmniej 8.• 8 portów FC 16 Gb/s służących do komunikacji z serwerami, z możliwością rozbudowy do co najmniej 32.• 8 portów FC 16 Gb/s służących do komunikacji z macierzami dyskowymi, z możliwością rozbudowy do co najmniej 32.• 256 GB pamięci podręcznej brutto, z możliwością rozbudowy do co najmniej 1024 GB.• 4 porty FC 16 Gb/s służące do komunikacji pomiędzy lokalizacjami, z możliwością rozbudowy do co najmniej 16. |  |
| 47 | Dla rozwiązania wirtualizacyjnego wsparcie dla operacji vMotion dla parametrów łącza pomiędzy site RTT=10ms |  |

1. **Macierz blokowa typ C – 1 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Oferowane urządzenie musi być dostarczone ze wszystkimi niezbędnymi komponentami do instalowania w szafie rack 19''. |  |
| 2 | Oferowane urządzenie musi posiadać kontrolery pracujące w trybie Active-Active z funkcją Mirrored cache. |  |
| 3 | Macierz musi być wyposażona w minimum 1024GB pamięci Cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy (nie może to być funkcjonalność tieringu), musi być możliwość włączenia lub wyłączenia buforowania on-line (bez konieczności migracji bądź przenoszenia zawartości wolumenów). |  |
| 4 | Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych. |  |
| 5 | Macierz musi obsługiwać dyski 2,5” jak i 3,5”. |  |
| 6 | Macierz dyskowa musi umożliwiać stosowanie w niej dysków SSD, HDD 15k, HDD 10k i HDD 7,2k rpm wyposażonych w interfejsy SAS 12Gbps (SAS, NL-SAS).  |  |
| 7 | Macierz musi być wyposażona w dyski posiadające podwójne interfejsy. |  |
| 8 | Macierz musi mieć możliwość instalacji dysków SSD, SAS, NL-SAS w tej samej półce dyskowej. |  |
| 9 | Oferowana macierz musi posiadać dla każdego kontrolera minimum 2 porty FC, obsadzone modułami światłowodowymi SFP+ 16 Gb/s  |  |
| 10 | RAID w macierzy: obsługa poziomów RAID 1 lub 10, 5, 6. |  |
| 11 | Macierz musi obsługiwać protokół FC - jeśli wymagane są licencje Wykonawca dostarczy je wraz z macierzą.  |  |
| 12 | Brak pojedynczego punktu awarii.  |  |
| 13 | Redundantne zasilanie, chłodzenie, kontrolery, dwie ścieżki dostępu do każdego dysku. |  |
| 14 | Graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie. |  |
| 15 | Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje.  |  |
| 16 | Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI. |  |
| 17 | Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, z jednej konsoli administracyjnej. |  |
| 18 | Wymagane jest aby dostarczona macierz posiadała interfejs zarządzający GUI, CLI, oraz umożliwiała tworzenie skryptów użytkownika. |  |
| 19 | Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie w oparciu o użytkowników z przypisanymi uprawnieniami (role-based). |  |
| 20 | Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. |  |
| 21 | W pełni nadmiarowe wentylatory i zasilacze z możliwością wymiany podczas pracy. |  |
| 22 | Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji. |  |
| 23 | Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji. |  |
| 24 | Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli. |  |
| 25 | Macierz musi posiadać funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych (SSD, SAS/FC, NLSAS/SATA), w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji. |  |
| 26 | Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych. |  |
| 27 | Macierz musi obsługiwać LUN Masking i Lun mapping. |  |
| 28 | Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu mają być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych |  |
| 29 | Macierz musi posiadać funkcjonalność zwiększania rozmiaru wolumenów. |  |
| 30 | Macierz powinna zapewniać wykonywanie kopii migawkowych w ilości minimum 256 dla wolumenu logicznego. Przepełnienie przestrzeni dla kopii migawkowych nie może powodować błędów zapisu na przestrzeń produkcyjną. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest obecnie przedmiotem zamówienia. |  |
| 31 | Macierz musi wspierać mechanizm zdalnej replikacji w trybie synchronicznym i asynchronicznym. Licencja umożliwiająca wykorzystanie powyższej funkcjonalności jest przedmiotem zamówienia.  |  |
| 32 | Obsługiwane systemy operacyjne: Microsoft Windows 2008/2008R2/2012/2012R2, Suse 11/12, Redhat 5/6/7, Solaris 11, VMware 5.0/5.1/5.5/6.0, vVOL. |  |
| 33 | Wymagane jest dostarczenie macierzy dyskowej spełniającej wymagania pojemnościowe:Macierz dyskowa składająca się z 1 obszaru dyskowego:I - zapewniającego wysoką wydajność - musi zawierać dyski SAS o prędkości obrotowej nie mniejszej niż 10k RPM w ilości minimum 224 sztuk udostępniając użytkownikowi powierzchnię użytkową (dla której nie wliczają się dyski parzystości i dyski hot spare) minimum 206TB w konfiguracji RAID 5\*\*Należy wyposażyć macierz w niezbędne dyski zapasowe (spare) zgodnie z zaleceniami producenta macierzy (nie mniej niż 1 sztuka na 30 dysków).Wszystkie dyski oferowanej i dostarczonej macierzy muszą pracować w trybie „Hot-Plug”.W każdym z obszarów wszystkie dyski muszą być tego samego typu i pojemności\*\* - Należy przyjąć, że 1 TB=1024GB, 1 GB=1024MB, 1MB=1024kB, 1kB=1024B i grupy dyskowe RAID nie większe niż 9 dysków dla RAID 5. |  |
| 34 | Oferowana macierz ma więcej niż 1024GB pamięci cache |  |
| 35 | Oferowane rozwiązanie musi umożliwiać wirtualizację zasobów dyskowych macierzy dyskowych pochodzących od różnych dostawców, m. in. HP, IBM, EMC, HDS. Wymagane jest dostarczenie licencji na maksymalną pojemność oferowanych macierzy. |  |
| 36 | Oferowane rozwiązanie musi umożliwiać prezentacje zwirtualizowanych zasobów dyskowych do aplikacji pracujących na różnych platformach OS, mi. In: IBM AIX, HP-UX, Linux, MS Windows, Solaris, VMware. |  |
| 37 | Oferowane rozwiązanie musi umożliwiać prezentowanie do aplikacji wolumenów logicznych wystawionych z macierzy dyskowych w sposób nienaruszający zawartości tych wolumenów (prezentacja 1 do 1). Oferowane rozwiązanie musi umożliwiać połączenie macierzy w dwóch oddalonych od siebie centrach przetwarzania danych (ośrodkach) w celu umożliwienia wirtualizacji zasobów dyskowych pomiędzy tymi centrami – rozwiązanie separowane geograficznie. |  |
| 38 | Wymagane jest, aby oferowane rozwiązanie umożliwiało transmisję danych pomiędzy ośrodkami w trybie synchronicznym. Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało oddalenie pary wirtualizatorów na odległość, dla której opóźnienie transmisji danych RTT dochodzi do 5ms. |  |
| 39 | Wirtualny wolumen logiczny prezentowany jednocześnie w trybie zapisu/odczytu w obu lokalizacjach zbudowany jest w oparciu o parę fizycznych wolumenów logicznych połączonych ze sobą zdalną replikacją danych (kopia lustrzana realizowana pomiędzy lokalizacjami). Wymagane jest zapewnienie spójności danych dla synchronicznego trybu replikacji. |  |
| 40 | Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało zastosowanie arbitra, znajdującego się w trzeciej lokalizacji, w celu uniknięcia zjawiska split-brain w przypadku awarii komunikacji pomiędzy centrami przetwarzania danych. |  |
| 41 | Oferowane rozwiązanie separowane geograficznie musi posiadać mechanizmy umożliwiające pracę, przy zachowaniu pełnej funkcjonalności oraz bezpieczeństwa i spójności danych także bez stosowania arbitra. |  |
| 42 | Oferowane rozwiązanie wirtualizujące musi posiadać wsparcie dla protokołów VAAI (CompareAndWrite SCSI Command) oraz VASA. |  |
| 43 | Oferowane rozwiązanie musi być odporne na awarię pojedynczego elementu. |  |
| 44 | Oferowane rozwiązanie musi umożliwiać naprawę, rozbudowę, aktualizacje oprogramowania wewnętrznego w sposób nieprzerywający dostępu do danych. Awaria dowolnego pojedynczego kontrolera rozwiązania nie może wymuszać konieczności przełączenia pracy aplikacji do drugiego ośrodka lub ręcznej rekonfiguracji środowiska. |  |
| 45 | W celu zapewnienia dostępności oraz wydajności oferowane rozwiązanie musi umożliwiać prezentowanie każdego wirtualnego wolumenu logicznego do serwerów poprzez wszystkie kontrolery oferowanego rozwiązania jednocześnie, także po rozbudowie do maksymalnej liczby kontrolerów |  |
| 46 | Oferowany rozwiązanie wirtualizacyjne (dla pojedynczej lokalizacji) ma być wyposażone w co najmniej:• 2 kontrolery z możliwością rozbudowy do co najmniej 8.• 8 portów FC 16 Gb/s służących do komunikacji z serwerami, z możliwością rozbudowy do co najmniej 32.• 8 portów FC 16 Gb/s służących do komunikacji z macierzami dyskowymi, z możliwością rozbudowy do co najmniej 32.• 256 GB pamięci podręcznej brutto, z możliwością rozbudowy do co najmniej 1024 GB.• 4 porty FC 16 Gb/s służące do komunikacji pomiędzy lokalizacjami, z możliwością rozbudowy do co najmniej 16. |  |
| 47 | Dla rozwiązania wirtualizacyjnego wsparcie dla operacji vMotion dla parametrów łącza pomiędzy site RTT=10ms |  |

1. **Rozwiązanie NAS typ A - 1szt.**

|  |  |  |
| --- | --- | --- |
| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Pojemność użyteczna oferowanego rozwiązania pamięci dyskowej na dane użytkowników musi wynosić nie mniej niż 2000TiB w obrębie jednego systemu plików przy zachowaniu dostępu do danych w przypadku awarii, co najmniej trzech dowolnych półek jednocześnie składających się z nie mniej niż 35 dysków każda, albo trzech dowolnych dysków. |  |
| 2 | Pojemność ma być zbudowana na dyskach NLSAS nie większych niż 4TB oraz dyskach SSD nie mniejszych niż 1.6TB. |  |
| 3 | Co najmniej 19 kontrolerów gdzie każdy realizuje dostęp plikowy do danych. |  |
| 4 | Rozwiązanie musi umożliwiać rozbudowę, do co najmniej 140 kontrolerów w ramach tego samego systemu dyskowego. |  |
| 5 | W celu zapewnienia odpowiedniej wydajności oferowany system pamięci masowej musi posiadać nie mniej niż 38 CPU. |  |
| 6 | Dla maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, półka dyskowa lub węzeł stanowiący element rozwiązania pamięci dyskowej musi mieścić nie mniej, niż 8 dysków typu NL-SAS lub SAS w przeliczeniu na 1U (tj. np. nie mniej, niż 32 dyski w obudowie 4U). |  |
| 7 | Rozwiązanie pamięci dyskowej musi udostępniać całkowitą dostępną przestrzeń́ w ramach jednego ciągłego systemu plików.  |  |
| 8 | Rozwiązanie pamięci dyskowej musi zapewniać dostępną̨, łączną̨ pojemność pamięci cache typu RAM nie mniejszą niż 1200 GB. Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci w oparciu o dyski SSD.  |  |
| 9 | Oferowane rozwiązanie musi zawierać nie mniej niż 19 dysków SSD o pojemności nie mniejszej niż 1.6TB każdy. Musi istnieć możliwość użycia tych dysków do przechowywania metadanych systemu plików. |  |
| 10 | Rozwiązanie musi umożliwiać zwiększenie trzykrotne pojemności i wydajności bez wprowadzania zmian do zaproponowanych kontrolerów. |  |
| 11 | Oferowane urządzenie musi umożliwiać dynamiczne rozszerzanie pojemności systemu plików w oparciu o całą pojemność fizyczną dodawaną do klastra bez konieczności:- modyfikacji już zainstalowanych kontrolerów,- restartu systemu,- ręcznej migracji/dystrybucji danych na nowe dyski systemu. |  |
| 12 | System plików zawarty w oferowanym rozwiązaniu musi być skalowalny, do co najmniej 10 PiB powierzchni netto. |  |
| 13 | System musi obsługiwać następujące protokoły plikowe: NFS V3 i V4, CIFS 2.0 i 3.0, FTP, HTTP |  |
| 14 | System musi zapewniać dostęp z różnych systemów operacyjnych (UNIX, Mac, Linux, Windows) z wykorzystaniem wszystkich standardowych protokołów: NFS, SMB (CIFS), HTTP, FTP. Wszystkie protokoły muszą być włączone bez dodatkowych licencji i sprzętu. |  |
| 15 | Rozwiązanie musi zapewniać wsparcie dla SMB 3.0 multi-channel pozwalając na korzystanie z kilku kanałow komunikacji dla zwiększenia przepustowości, tolerancje awarii jednego z połączeń I automatycznego wychwycenia tego typu awarii. |  |
| 16 | Oferowane rozwiązanie pamięci dyskowej musi obsługiwać protokół NDMP w wersji 3 oraz 4 dla kopii zapasowych na taśmach, z dowolnego obszaru systemu plików. |  |
| 17 | Oferowane rozwiązanie pamięci dyskowej musi zapewnić gwarantowaną ochronę przed „cichym uszkodzeniem dysków” (silent data corruption) dla wszystkich technologii dyskowych (w tym SATA). |  |
| 18 | Oferowane rozwiązanie pamięci dyskowej musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia innych elementów urządzenia. Musi istnieć możliwość jasnego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej lub wyświetlenia numeru pojedynczej zatoki/kieszeni. |  |
| 19 | Rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych. |  |
| 20 | W przypadku awarii jednego dysku, czas od momentu jego wymiany do odzyskania pierwotnego poziomu ochrony danych nie może być dłuższy niż 12 godzin – w sytuacji braku obciążenia przez urządzenia klienckie. |  |
| 21 | Użytkownicy sieci muszą uzyskiwać dostęp do systemu pamięci masowej przy wykorzystaniu wewnętrznego load balancingu bez konieczności stosowania zewnętrznych urządzeń równoważących obciążenie. |  |
| 22 | Rozwiązanie pamięci masowej musi posiadać mechanizm równoważenia nowych połączeń pomiędzy kontrolerami zgodnie z polityką wyboru kontrolera: kontroler o najmniejszej liczbie połączeń, kontroler o najmniejszym wykorzystaniu CPU, polityka roundrobin. |  |
| 23 | Rozwiązanie pamięci dyskowej musi posiadać funkcjonalność replikacji asynchronicznej danych. |  |
| 24 | Każde z rozwiązań pamięci masowej musi realizować replikację asynchroniczną danych na poziomie pojedynczego katalogu celem dystrybucji treści i zapewnienia kopii danych z oferowanym "rozwiązaniem typu NAS typ B". |  |
| 25 | Każde z rozwiązań pamięci masowej musi zapewniać synchronizacje shareów SMB oraz NFS między ośrodkiem podstawowym a zapasowym |  |
| 26 | Każde z rozwiązań pamięci masowej musi zapewnić automatyczną detekcje zmian na określonych share’ach czy exportach (SMB,NFS) dotyczącą zabezpieczeń oraz synchronizacji. |  |
| 27 | Rozwiązanie pamięci dyskowej musi zawierać funkcjonalność deduplikacji na poziomie bloków o wielkości nie większej, niż 8KiB dla wyznaczonych katalogów. |  |
| 28 | Rozwiązanie pamięci dyskowej musi umożliwiać wykonanie kopii migawkowej (snapshot). |  |
| 29 | Administracja systemem musi odbywać się poprzez Web GUI oraz Command Line Interface. |  |
| 30 | Rozwiązanie musi zapewniać dostęp do danych przy jednoczesnym wykorzystaniu portów/interfejsów typu 1 Gigabit Ethernet oraz 10 Gigabit Ethernet. |  |
| 31 | Rozwiązanie pamięci dyskowej musi posiadać nie mniej niż 38 portów 1 Gigabit Ethernet oraz nie mniej niż 38 portów typu 10 Gigabit Ethernet. Sumaryczna przepustowość portów zapewniających dostęp do danych (od strony serwerów i sieci LAN) musi być nie mniejsza niż 380 Gbps |  |
| 32 | System pamięci masowej musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. |  |
| 33 | Komunikacja pomiędzy kontrolerami/półkami dyskowymi musi odbywać się za pośrednictwem osobnych (niewspółdzielonych z portami dostępowymi) interfejsów. Każdy kontroler musi posiadać interfejsy o łącznej przepustowości nie mniejszej, niż 40Gbitps/kontroler. Sumaryczna przepustowość interfejsów wszystkich kontrolerów musi być nie mniejsza, niż 760Gbitps. |  |
| 34 | Urządzenie musi zapewniać przegląd statystyk historycznych jak i w czasie rzeczywistym w postaci graficznych raportów w zakresie:• Wydajności: klastra, dysków, kontrolerów, portów Ethernet oraz systemu plików rozbiciu na ścieżkę dostępu.• Użycia systemu plików: użycie pojemności klastra oraz prognoza użycia, histogram wielkości składowanych plików, lista plików o największym rozmiarze, najstarszych w sensie utworzenia, dostępu, modyfikacji.Należy dostarczyć licencję na cała pojemność systemu. |  |
| 35 | Rozwiązanie pamięci dyskowej pozwala na ochronę wybranych danych przed ich utratą z dynamiczną (na życzenie administratora) zmianą ich protekcji na poziomie plików i katalogów. |  |
| 36 | Rozwiązanie pamięci dyskowej oferuje zabezpieczenie chroniące je przed jednoczesną utratą minimalnie 4 dowolnych dysków lub 4 dowolnych półek dyskowych(węzłów) jednocześnie oferując mirroring określonych katalogów i plików od 1x do 8x. |  |
| 37 | Rozwiązanie pamięci masowej musi obsługiwać REST APIs (Restull Access to Namespace) dla aplikacji zewnętrznych. |  |
| 38 | Rozwiązanie pamięci masowej musi mieć możliwość rozbudowy o mechanizmy dotyczące szyfrowania danych oraz bezpieczeństwa takie jak HIPPA, PCI DSS, FIPS 140-2. |  |
| 39 | System pamięci masowej musi mieć możliwość skalowania pojemności zachowując pełny dostęp do danych i bez konieczności ich manualnej migracji na nowo przyłączane dyski/półki w celu ich redystrybucji. |  |
| 40 | "Rozwiązaniem typu NAS typ A" musi posiadać dedykowane oprogramowanie z portfolio produktu pamięci masowej służące do replikacji z oferowanym "rozwiązaniem typu NAS typ B". |  |
| 41 | System plików zaproponowanego rozwiązania zapewnia dostęp dla nieograniczonej liczby klientów bez względu na rodzaj użytego protokołu czy systemu operacyjnego. |  |
| 42 | System pamięci masowej nie opiera się na zabezpieczeniu danych znajdujących się na dyskach przy pomocy technologii RAID. |  |

1. **Rozwiązanie NAS typ B - 1szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Pojemność użyteczna oferowanego rozwiązania pamięci dyskowej na dane użytkowników musi wynosić nie mniej niż 2100 TiB w obrębie jednego systemu plików przy zachowaniu dostępu do danych w przypadku awarii, co najmniej trzech dowolnych dysków jednocześnie, lub jednoczesnej awarii dysku i półki składającej się z nie mniej niż 35 dysków. |  |
| 2 | Pojemność ma być zbudowana na dyskach NLSAS oraz dyskach SSD nie mniejszych niż 1.6TB. |  |
| 3 | Rozwiązanie pamięci masowej musi posiadać co najmniej 10 kontrolerów gdzie każdy realizuje dostęp plikowy do danych. |  |
| 4 | Rozwiązanie musi umożliwiać rozbudowę, do co najmniej 140 kontrolerów w ramach tego samego systemu dyskowego. |  |
| 5 | W celu zapewnienia odpowiedniej wydajności oferowany system pamięci masowej musi posiadać nie mniej niż 10 CPU. |  |
| 6 | Dla maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, półka dyskowa lub węzeł stanowiący element rozwiązania pamięci dyskowej musi mieścić nie mniej, niż 8 dysków typu NL-SAS lub SAS w przeliczeniu na 1U (tj. np. nie mniej, niż 32 dyski w obudowie 4U). |  |
| 7 | Rozwiązanie pamięci dyskowej musi udostępniać całkowitą dostępną przestrzeń́ w ramach jednego ciągłego systemu plików. |  |
| 8 | Rozwiązanie pamięci dyskowej musi zapewniać dostępną̨, łączną̨ pojemność pamięci cache typu RAM nie mniejszą niż 480 GB. Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci w oparciu o dyski SSD. |  |
| 9 | Oferowane rozwiązanie musi zawierać nie mniej niż 10 dysków SSD o pojemności nie mniejszej niż 1.6TB każdy. Musi istnieć możliwość użycia tych dysków do przechowywania metadanych systemu plików. |  |
| 10 | Rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych. |  |
| 11 | Musi umożliwiać zwiększenie trzykrotne pojemności i wydajności bez wprowadzania zmian do zaproponowanych kontrolerów. |  |
| 12 | Oferowane urządzenie musi umożliwiać dynamiczne rozszerzanie pojemności systemu plików w oparciu o całą pojemność fizyczną dodawaną do klastra bez konieczności:- modyfikacji już zainstalowanych kontrolerów,- restartu systemu,- ręcznej migracji/dystrybucji danych na nowe dyski systemu. |  |
| 13 | System plików zawarty w oferowanym rozwiązaniu musi być skalowalny, do co najmniej 30 PiB powierzchni netto. |  |
| 14 | Rozwiązanie pamięci masowej musi zapewniać dostęp z różnych systemów operacyjnych (UNIX, Mac, Linux, Windows) z wykorzystaniem wszystkich standardowych protokołów: NFS, SMB (CIFS), HTTP, FTP. Wszystkie protokoły muszą być włączone bez dodatkowych licencji i sprzętu. |  |
| 15 | Rozwiązanie pamięci masowej musi obsługiwać protokoły plikowe: NFS V3 i V4, CIFS 2.0 i 3.0, FTP, http. |  |
| 16 | Oferowane rozwiązanie pamięci dyskowej musi obsługiwać protokół NDMP w wersji 3 oraz 4 dla kopii zapasowych na taśmach, z dowolnego obszaru systemu plików. |  |
| 17 | Oferowane rozwiązanie pamięci dyskowej musi zapewnić gwarantowaną ochronę przed „cichym uszkodzeniem dysków” (silent data corruption) dla wszystkich technologii dyskowych (w tym SATA). |  |
| 18 | Rozwiązanie musi zapewniać wsparcie dla SMB 3.0 multi-channel pozwalając na korzystanie z kilku kanałów komunikacji dla zwiększenia przepustowości, tolerancje awarii jednego z połączeń I automatycznego wychwycenia tego typu awarii. |  |
| 19 | Oferowane rozwiązanie pamięci dyskowej musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia innych elementów urządzenia. Musi istnieć możliwość jasnego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej lub wyświetlenia numeru pojedynczej zatoki/kieszeni. |  |
| 20 | W przypadku awarii jednego dysku, czas od momentu jego wymiany do odzyskania pierwotnego poziomu ochrony danych nie może być dłuższy niż 12 godzin – w sytuacji braku obciążenia przez urządzenia klienckie. |  |
| 21 | Rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych. |  |
| 22 | Użytkownicy sieci muszą uzyskiwać dostęp do systemu pamięci masowej przy wykorzystaniu wewnętrznego load balancingu bez konieczności stosowania zewnętrznych urządzeń równoważących obciążenie. |  |
| 23 | Rozwiązanie pamięci dyskowej musi posiadać funkcjonalność replikacji asynchronicznej danych. |  |
| 24 | Rozwiązanie pamięci masowej musi realizować replikację asynchroniczną danych na poziomie pojedynczego katalogu celem dystrybucji treści i zapewnienia kopii danych w innym ośrodku. |  |
| 25 | Rozwiązanie pamięci masowej musi zapewniać synchronizacje shareów SMB oraz NFS między oferowanym "rozwiązaniem typu NAS typ A" a "rozwiązaniem typu NAS typ B". |  |
| 26 | Rozwiązanie pamięci masowej musi zapewnić automatyczną detekcje zmian na określonych share’ach czy exportach (SMB,NFS) dotyczącą zabezpieczeń oraz synchronizacji. |  |
| 27 | Rozwiązanie pamięci dyskowej musi umożliwiać wykonanie kopii migawkowej (snapshot). |  |
| 28 | Rozwiązanie pamięci dyskowej musi zawierać funkcjonalność deduplikacji na poziomie bloków o wielkości nie większej, niż 8KiB dla wyznaczonych katalogów. |  |
| 29 | Rozwiązanie pamięci masowej musi posiadać mechanizm równoważenia nowych połączeń pomiędzy kontrolerami zgodnie z polityką wyboru kontrolera: kontroler o najmniejszej liczbie połączeń, kontroler o najmniejszym wykorzystaniu CPU, polityka roundrobin. |  |
| 30 | Administracja systemem musi odbywać się poprzez Web GUI oraz Command Line Interface. |  |
| 31 | Zapewniać dostęp do danych przy jednoczesnym wykorzystaniu portów/interfejsów typu 1 Gigabit Ethernet oraz 10 Gigabit Ethernet. |  |
| 32 | Rozwiązanie pamięci masowej musi posiadać nie mniej niż 20 portów 1 Gigabit Ethernet oraz nie mniej niż 20 portów typu 10 Gigabit Ethernet. Sumaryczna przepustowość portów zapewniających dostęp do danych (od strony serwerów i sieci LAN) musi być nie mniejsza niż 200 Gbps. |  |
| 33 | Komunikacja pomiędzy kontrolerami/półkami dyskowymi musi odbywać się za pośrednictwem osobnych (niewspółdzielonych z portami dostępowymi) interfejsów. Każdy kontroler musi posiadać interfejsy o łącznej przepustowości nie mniejszej, niż 20Gbitps/kontroler. Sumaryczna przepustowość interfejsów wszystkich kontrolerów musi być nie mniejsza, niż 200Gbitps. |  |
| 34 | Urządzenie musi zapewniać przegląd statystyk historycznych jak i w czasie rzeczywistym w postaci graficznych raportów w zakresie:* Wydajności: klastra, dysków, kontrolerów, portów Ethernet oraz systemu plików rozbiciu na ścieżkę dostępu.
* Użycia systemu plików: użycie pojemności klastra oraz prognoza użycia, histogram wielkości składowanych plików, lista plików o największym rozmiarze, najstarszych w sensie utworzenia, dostępu, modyfikacji.

Należy dostarczyć licencję na cała pojemność systemu. |  |
| 35 | Rozwiązanie pamięci masowej musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. |  |
| 36 | Rozwiązanie pamięci dyskowej pozwala na ochronę wybranych danych przed ich utratą z dynamiczną (na życzenie administratora) zmianą ich protekcji na poziomie plików i katalogów. |  |
| 37 | Rozwiązanie pamięci dyskowej oferuje zabezpieczenie chroniące je przed jednoczesną utratą minimalnie 4 dowolnych dysków lub czterech dowolnych półek dyskowych(węzłów) jednocześnie oferując mirroring określonych katalogów i plików od 1x do 8x. |  |
| 38 | Rozwiązanie pamięci masowej musi obsługiwać REST APIs (Restull Access to Namespace) dla aplikacji zewnętrznych. |  |
| 39 | Rozwiązanie pamięci masowej musi mieć możliwość rozbudowy o mechanizmy dotyczące szyfrowania danych oraz bezpieczeństwa takie jak HIPPA, PCI DSS, FIPS 140-2. |  |
| 40 | System pamięci masowej musi mieć możliwość skalowania pojemności zachowując pełny dostęp do danych i bez konieczności ich manualnej migracji na nowo przyłączane dyski/półki w celu ich redystrybucji. |  |
| 41 | "Rozwiązaniem typu NAS typ B" musi posiadać dedykowane oprogramowanie z portfolio produktu pamięci masowej służące do replikacji z oferowanym "rozwiązaniem typu NAS typ A". |  |
| 42 | System plików zaproponowanego rozwiązania zapewnia dostęp dla nieograniczonej liczby klientów bez względu na rodzaj użytego protokołu czy systemu operacyjnego. |  |
| 43 | System pamięci masowej nie opiera się na zabezpieczeniu danych znajdujących się na dyskach przy pomocy technologii RAID. |  |

1. **Rozwiązanie NAS typ C - 1szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Pojemność użyteczna oferowanego rozwiązania pamięci dyskowej na dane użytkowników musi wynosić nie mniej niż 2300 TiB w obrębie jednego systemu plików przy zachowaniu dostępu do danych w przypadku awarii, co najmniej trzech dowolnych dysków jednocześnie, lub jednoczesnej awarii dysku i półki składającej się z nie mniej niż 35 dysków. |  |
| 2 | Pojemność ma być zbudowana na dyskach NLSAS oraz dyskach SSD nie mniejszych niż 1.6TB. |  |
| 3 | Rozwiązanie pamięci masowej musi zawierać, co najmniej 10 kontrolerów gdzie każdy realizuje dostęp plikowy do danych. |  |
| 4 | Rozwiązanie pamięci masowej musi umożliwiać rozbudowę, do co najmniej 140 kontrolerów w ramach tego samego systemu dyskowego. |  |
| 5 | W celu zapewnienia odpowiedniej wydajności oferowany system pamięci masowej musi posiadać nie mniej niż 7 CPU. |  |
| 6 | Dla maksymalizacji gęstości, tj. minimalizacji wykorzystania obszaru serwerowni do przechowywania danych, półka dyskowa lub węzeł stanowiący element rozwiązania pamięci dyskowej musi mieścić nie mniej, niż 15 dysków typu NL-SAS lub SAS w przeliczeniu na 1U (tj. np. nie mniej, niż 60 dysków w obudowie 4U). |  |
| 7 | Rozwiązanie pamięci dyskowej musi udostępniać całkowitą dostępną przestrzeń́ w ramach jednego ciągłego systemu plików. |  |
| 8 | Rozwiązanie pamięci masowej musi zapewniać dostępną̨, łączną̨ pojemność pamięci cache typu RAM nie mniejszą niż 336 GB. Ze względu na przewidywane obciążenie i wymaganą wydajność nie dopuszcza się realizacji pamięci w oparciu o dyski SSD. |  |
| 9 | Oferowane rozwiązanie musi zawierać nie mniej niż 7 dysków SSD o pojemności nie mniejszej niż 1.6TB każdy. Musi istnieć możliwość użycia tych dysków do przechowywania metadanych systemu plików. |  |
| 10 | Rozwiązanie pamięci masowej musi umożliwiać zwiększenie trzykrotne pojemności i wydajności bez wprowadzania zmian do zaproponowanych kontrolerów. |  |
| 11 | Oferowane rozwiązanie pamięci masowej musi umożliwiać dynamiczne rozszerzanie pojemności systemu plików w oparciu o całą pojemność fizyczną dodawaną do klastra bez konieczności:- modyfikacji już zainstalowanych kontrolerów - restartu systemu - ręcznej migracji/dystrybucji danych na nowe dyski systemu.  |  |
| 12 | Rozwiązanie pamięci masowej musi zapewniać dostęp z różnych systemów operacyjnych (UNIX, Mac, Linux, Windows) z wykorzystaniem wszystkich standardowych protokołów: NFS, SMB (CIFS), HTTP, FTP. Wszystkie protokoły muszą być włączone bez dodatkowych licencji i sprzętu. |  |
| 13 | Rozwiązanie pamięci masowej musi obsługiwać protokoły plikowe: NFS V3 i V4, CIFS 2.0 i 3.0, FTP, http. |  |
| 14 | Rozwiązanie musi zapewniać wsparcie dla SMB 3.0 multi-channel pozwalając na korzystanie z kilku kanałów komunikacji dla zwiększenia przepustowości, tolerancje awarii jednego z połączeń I automatycznego wychwycenia tego typu awarii. |  |
| 15 | Oferowane rozwiązanie pamięci dyskowej musi obsługiwać protokół NDMP w wersji 3 oraz 4 dla kopii zapasowych na taśmach, z dowolnego obszaru systemu plików. |  |
| 16 | Oferowane rozwiązanie pamięci dyskowej musi zapewnić gwarantowaną ochronę przed „cichym uszkodzeniem dysków” (silent data corruption) dla wszystkich technologii dyskowych (w tym SATA). |  |
| 17 | Oferowane rozwiązanie pamięci dyskowej musi umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia innych elementów urządzenia. Musi istnieć możliwość jasnego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej lub wyświetlenia numeru pojedynczej zatoki/kieszeni. |  |
| 18 | W przypadku awarii jednego dysku, czas od momentu jego wymiany do odzyskania pierwotnego poziomu ochrony danych nie może być dłuższy niż 12 godzin – w sytuacji braku obciążenia przez urządzenia klienckie. |  |
| 19 | Rozwiązanie pamięci dyskowej musi zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny dla zapewnienia niezawodności i dostępności danych. |  |
| 20 | Użytkownicy sieci muszą uzyskiwać dostęp do systemu pamięci masowej przy wykorzystaniu wewnętrznego load balancingu bez konieczności stosowania zewnętrznych urządzeń równoważących obciążenie. |  |
| 21 | Rozwiązanie pamięci dyskowej musi posiadać funkcjonalność replikacji asynchronicznej danych. |  |
| 22 | Rozwiązanie pamięci masowej musi realizować replikację asynchroniczną danych na poziomie pojedynczego katalogu celem dystrybucji treści i zapewnienia kopii danych z oferowanym "rozwiązaniem typu NAS typ B". |  |
| 23 | Rozwiązanie pamięci masowej musi zapewniać synchronizacje shareów SMB oraz NFS między oferowanym "rozwiązaniem typu NAS typ B" a "rozwiązaniem typu NAS typ C" |  |
| 24 | Rozwiązanie pamięci masowej musi zapewnić automatyczną detekcje zmian na określonych share’ach czy exportach (SMB,NFS) dotyczącą zabezpieczeń oraz synchronizacji. |  |
| 25 | Rozwiązanie pamięci dyskowej musi umożliwiać wykonanie, co najmniej 1000 kopii migawkowych (snapshot) danego katalogu oraz umożliwiać wykonanie nielimitowanej liczby kopii migawkowych w odniesieniu do całego systemu plików. |  |
| 26 | Komunikacja pomiędzy kontrolerami/półkami dyskowymi musi odbywać się za pośrednictwem osobnych (niewspółdzielonych z portami dostępowymi) interfejsów. Każdy kontroler musi posiadać interfejsy o łącznej przepustowości nie mniejszej, niż 20Gbitps/kontroler. Sumaryczna przepustowość interfejsów wszystkich kontrolerów musi być nie mniejsza, niż 140Gbitps. |  |
| 27 | Rozwiązanie pamięci masowej musi zapewnić zdalny monitoring w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta. |  |
| 28 | Administracja systemem musi odbywać się poprzez Web GUI oraz Command Line Interface. |  |
| 29 | Zapewniać dostęp do danych przy jednoczesnym wykorzystaniu portów/interfejsów typu 1 Gigabit Ethernet oraz 10 Gigabit Ethernet. |  |
| 30 | Rozwiązanie pamięci dyskowej posiadać nie mniej niż 14 portów 1 Gigabit Ethernet oraz nie mniej niż 14 portów typu 10 Gigabit Ethernet. Sumaryczna przepustowość portów zapewniających dostęp do danych (od strony serwerów i sieci LAN) musi być nie mniejsza niż 140 Gbps. |  |
| 31 | Urządzenie musi zapewniać przegląd statystyk historycznych jak i w czasie rzeczywistym w postaci graficznych raportów w zakresie:* Wydajności: klastra, dysków, kontrolerów, portów Ethernet oraz systemu plików rozbiciu na ścieżkę dostępu.
* Użycia systemu plików: użycie pojemności klastra oraz prognoza użycia, histogram wielkości składowanych plików, lista plików o największym rozmiarze, najstarszych w sensie utworzenia, dostępu, modyfikacji.

Należy dostarczyć licencję na cała pojemność systemu. |  |
| 32 | Rozwiązanie pamięci dyskowej pozwala na ochronę wybranych danych przed ich utratą z dynamiczną (na życzenie administratora) zmianą ich protekcji na poziomie plików i katalogów. |  |
| 33 | Rozwiązanie pamięci dyskowej oferuje zabezpieczenie chroniące je przed jednoczesną utratą minimalnie 4 dowolnych dysków lub czterech dowolnych półek dyskowych(węzłów) jednocześnie oferując mirroring określonych katalogów i plików od 1x do 8x. |  |
| 34 | Rozwiązanie pamięci masowej musi obsługiwać REST APIs (Restull Access to Namespace) dla aplikacji zewnętrznych. |  |
| 35 | Rozwiązanie pamięci masowej musi mieć możliwość rozbudowy o mechanizmy dotyczące szyfrowania danych oraz bezpieczeństwa takie jak HIPPA, PCI DSS, FIPS 140-2. |  |
| 36 | System pamięci masowej musi mieć możliwość skalowania pojemności zachowując pełny dostęp do danych i bez konieczności ich manualnej migracji na nowo przyłączane dyski/półki w celu ich redystrybucji. |  |
| 37 | "Rozwiązaniem typu NAS typ C" musi posiadać dedykowane oprogramowanie z portfolio produktu pamięci masowej służące do replikacji z oferowanym "rozwiązaniem typu NAS typ B". |  |
| 38 | System plików zaproponowanego rozwiązania zapewnia dostęp dla nieograniczonej liczby klientów bez względu na rodzaj użytego protokołu czy systemu operacyjnego. |  |
| 39 | System pamięci masowej nie opiera się na zabezpieczeniu danych znajdujących się na dyskach przy pomocy technologii RAID. |  |
| 40 | Należy dostarczyć switch LAN zapewniający komunikację wewnątrz całości rozwiązania oraz dodatkowo minimum 2 porty 10 Gigabit Ethernet i 2 porty 1 Gigabit Ethernet wraz z odpowiednimi wkładkami, do połączenia z posiadaną w lokalizacji infrastrukturą LAN. |  |
| 41 | Należy dostarczyć dobrany do całości rozwiązania zasilacz UPS, z podtrzymaniem zasilania na minimum 10 minut dla dostarczonego "rozwiązania typu NAS typ C". |  |
| 42 | Wraz z rozwiązaniem należy dostarczyć szafę RACK 42U, z odpowiednimi modułami zasilającymi PDU, do której należy zainstalować całość dostarczonego "rozwiązania typu NAS typ C". |  |

1. **Switch SAN – 2 szt.**

|  |  |  |
| --- | --- | --- |
| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. |  |
| 2 | W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8, 4 lub 2 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. |  |
| 3 | Przełącznik FC musi być wyposażony, w co najmniej 36 aktywnych portów FC obsadzonych wkładkami SFP 16Gb/s. |  |
| 4 | Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC. |  |
| 5 | Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 1536 Gb/s end-to-end full duplex. |  |
| 6 | Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 1,2µs. |  |
| 7 | Rodzaj obsługiwanych portów, co najmniej: E, D oraz F. |  |
| 8 | Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |  |
| 9 | Przełącznik FC posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika. |  |
| 10 | Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.  |  |
| 11 | Przełącznik FC musi wspierać mechanizm balansowania ruchu, pomiędzy co najmniej 6 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID. |  |
| 12 | Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Jednoczesne wykorzystanie obu mechanizmów powinno zapewnić dla dowolnej pary komunikujących się urządzeń końcowych uzyskanie kanału komunikacyjnego o zagregowanej przepustowości 768Gb/s half duplex.  |  |
| 13 | Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. |  |
| 14 | Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. |  |
| 15 | Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:* mechanizm szyfrowania i kompresji wybranych połączeń ISL wspierany, na co najmniej 2 portach przełącznika FC. Symetryczny klucz szyfrujący nie może być krótszy niż 256-bitów.
* mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric
* uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP
* uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP
* szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2.
* definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control)
* definiowane kont administratorów w środowisku RADIUS i LDAP
* szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS
* obsługa SNMP v1 oraz v3
* IP Filter dla portu administracyjnego przełącznika
* wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
* wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
 |  |
| 16 | Przełącznik FC musi mieć możliwość konfiguracji przez:* polecenia tekstowe w interfejsie znakowym konsoli terminala,
* przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.
 |  |
| 17 | Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:* logowanie zdarzeń poprzez mechanizm „syslog”,
* port diagnostyczny tzw. D\_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla wkładek SFP 16Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric.
* FC ping
* FC traceroute
* kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika.
 |  |
| 18 | Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 8Gb/s. |  |
| 19 | Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC. |  |
| 20 | Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. |  |
| 21 | W przełączniku FC musi istnieć możliwość wydzielenia logicznych, izolowanych od siebie przełączników. Każdy z logicznych przełączników musi mieć własny Domain ID, własne usługi fabric (tzw. fabric services), niezależną bazę zoningu oraz możliwość przypisanie dedykowanego administratora. |  |
| 22 | Musi istnieć możliwość połączenia wybranych logicznych przełączników wydzielonych w różnych fizycznych przełącznikach FC za pomocą dedykowanych połączeń ISL. Połączone w ten sposób przełączniki muszą tworzyć pojedynczą sieć fabric. |  |
| 23 | Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |  |
| 24 | Przełącznik FC musi obsługiwać protokół FCP na dowolnych portach przełącznika. |  |

1. **Przełączniki Data Center LAN typu SPINE – 2 szt.**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne sprzętu oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1.** | Wymagana architektura sieci LAN musi być oparta o architekturę typu SPINE-LEAF, z podziałem ról przełączników, tworzących tzw. IP Fabric. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19’’. |  |
| **2.** | Producent powinien oferować wsparcie dla modułów optycznych realizujących transmisję pochodzących od innych niż producent urządzeń dostawców. |  |
| **3.** | Przełącznik typu SPINE musi być wyposażony:- w co najmniej 32 porty 40GbE wraz z zainstalowanymi 32 wkładkami QSFP+ 40GBASE-LX4 40 Gigabit Optics for up to 150m transmission with OM4 over duplex MMF- z możliwością rozbudowy o dodatkowe 8 portów 40GbE.  |  |
| **4.** | Przedstawione rozwiązanie powinno zawierać:- 2 szt. przełącznik typu SPINEoferowane urządzenia muszą zapewnić rozbudowę do co najmniej:- 4 szt. przełącznik SPINE |  |
| **5.** | Przełącznik musi posiadać wymienny zasilacz AC. Przełącznik musi być wyposażony w dodatkowy redundantny zasilacz. Musi posiadać możliwość wymiany wszystkich modułów na gorąco (hot swap). Przełączniki musza wspierać funkcjonalność ISSU. |  |
| **6.** | Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band). |  |
| **7.** | Przełącznik musi być wyposażony w nie mniej niż 2 GB pamięci Flash oraz 2 GB pamięci DRAM. Ilość zainstalowanej pamięci RAM powinna zapewniać prawidłową pracę urządzenia oraz oprogramowania. |  |
| **8.** | Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, SSH, a także za pośrednictwem interfejsu WWW. |  |
| **9.** | Przełącznik musi posiadać architekturę non-blocking. |  |
| **10.** | Przełącznik musi obsługiwać ramki Jumbo (9KB). |  |
| **11.** | Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w liczbie nie mniejszej niż 4000 |  |
| **12.** | Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN.  |  |
| **13.** | Przełącznik musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grupy LAG, po nie mniej niż 16 portów.  |  |
| **14.** | Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003. |  |
| **15.** | Przełącznik musi obsługiwać protokół LLDP. |  |
| **16.** | Przełącznik musi obsługiwać routing między sieciami VLAN – routing statyczny, protokoły routingu dynamicznego: RIP, OSPF, IS-IS, BGP, MPLS oraz VXLAN, OVSDB. Jeżeli do realizacji tych wymagań jest wymagana licencja musi ona być dostarczona z urządzeniem |  |
| **17.** | Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD, oraz pozwalać na stworzenie klastra HA z protokołem VRRP. |  |
| **18.** | Przełącznik musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny. |  |
| **19.** | Przełącznik musi obsługiwać filtrowanie ruchu, na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo reguły filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów.  |  |
| **20.** | Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection.  |  |
| **21.** | Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS, (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC.. |  |
| **22.** | Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN. |  |
| **23.** | Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem. |  |
| **24.** | Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji. |  |

1. **Przełączniki Data Center LAN typu LEAF - 19 szt.**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne sprzętu oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1.** | Wymagana architektura sieci LAN musi być oparta o architekturze typu SPINE-LEAF, z podziałem ról przełączników, tworzących tzw. IP Fabric. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19’’. |  |
| **2.** | Producent powinien oferować wsparcie dla modułów optycznych realizujących transmisję pochodzących od innych niż producent urządzeń dostawców. |  |
| **3.** | Przełącznik typu LEAF musi być wyposażony:- w co najmniej 48 portów 1/10GbE oraz 6 portów 40Gbps wraz z 6 wkładkami QSFP+ 40GBase-SR4 40 Gigabit Optics, 850nm for up to 150m transmission on MMF, 12 wkładkami SFP 1000Base-T Copper Transceiver Module for up to 100m transmission on Cat5, 12 wkładkami SFP+ 10 Gigabit Ethernet Optics |  |
| **4.** | Przedstawione rozwiązanie powinno zawierać: - 19 szt. przełącznik typu LEAFoferowane urządzenia muszą zapewnić rozbudowę do co najmniej:- 24 szt. przełącznik typu LEAF |  |
| **5.** | Przełącznik musi posiadać wymienny zasilacz AC. Przełącznik musi być wyposażony w dodatkowy redundantny zasilacz. Musi posiadać możliwość wymiany wszystkich modułów na gorąco (hot swap). Przełączniki musza wspierać funkcjonalność ISSU. |  |
| **6.** | Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band). |  |
| **7.** | Przełącznik musi być wyposażony w nie mniej niż 2 GB pamięci Flash oraz 2 GB pamięci DRAM. Ilość zainstalowanej pamięci RAM powinna zapewniać prawidłową pracę urządzenia oraz oprogramowania. |  |
| **8.** | Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, SSH, a także za pośrednictwem interfejsu WWW. |  |
| **9.** | Przełącznik musi posiadać architekturę non-blocking. |  |
| **10.** | Przełącznik musi obsługiwać ramki Jumbo (9KB). |  |
| **11.** | Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w liczbie nie mniejszej niż 4000 |  |
| **12.** | Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN.  |  |
| **13.** | Przełącznik musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grupy LAG, po nie mniej niż 16 portów.  |  |
| **14.** | Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003. |  |
| **15.** | Przełącznik musi obsługiwać protokół LLDP. |  |
| **16.** | Przełącznik musi obsługiwać routing między sieciami VLAN – routing statyczny, protokoły routingu dynamicznego: RIP, OSPF, IS-IS, BGP, MPLS oraz VXLAN, OVSDB. Jeżeli do realizacji tych wymagań jest wymagana licencja musi ona być dostarczona z urządzeniem |  |
| **17.** | Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD, oraz pozwalać na stworzenie klastra HA z protokołem VRRP. |  |
| **18.** | Przełącznik musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny. |  |
| **19.** | Przełącznik musi obsługiwać filtrowanie ruchu, na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo reguły filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów.  |  |
| **20.** | Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection.  |  |
| **21.** | Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS, (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC.. |  |
| **22.** | Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN. |  |
| **23.** | Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem. |  |
| **24.** | Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji. |  |

1. **Router BGP - 2 szt.**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne sprzętu oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1.** | Router musi być dedykowanym urządzeniem sieciowym o wysokości max. 4 U przystosowanym do montowania w szafie rack, wyposażonym w wymienny zasilacz oraz wentylatory. Router musi być wyposażony w zasilacze dostosowane do napięcia 220-230V, w ilości umożliwiającej poprawną pracę rutera w pełnej konfiguracji przy obsadzeniu wszystkich dostępnych slotów modułami z interfejsami. |  |
| **2.** | Router musi posiadać możliwość wyposażenia w nadmiarowe zasilacze w celu uzyskania redundancji zasilania 1:1. |  |
| **3.** | Zarządzanie i konfiguracja rutera przez administratorów musi być realizowana przez moduł kontrolny. System operacyjny rutera musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi odpowiadać ze sterowanie i monitorowanie pracy komponentów urządzenia. Ruch tranzytowy użytkowników przechodzący przez ruter nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi być wyposażony w co najmniej 2 GB pamięci RAM, pamięć Flash, port konsoli oraz interfejs Ethernet służący do zarządzania out-of-band. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego rutera z nośnika danych podłączonego do slotu USB na module kontrolnym. |  |
| **4.** | System operacyjny routera musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo.  |  |
| **5.** | Router musi być wyposażony w 20 portów 1000Base wraz z modułami optycznymi (5\*1000Base-LX, 5\*1000Base-SX, 10\*1000Base-TX). Router musi zapewniać pełną przepustowość dla dostarczone liczby portów dla każdej dopuszczalnej długości pakietów. Router mieć możliwość rozbudowy przepustowości do nie mniej niż 55 Mpps full duplex bez konieczności wymiany obudowy, modułów zarządzających. |  |
| **6.** | Router musi obsługiwać interfejsy 10 Gigabit Ethernet zgodne z IEEE 802.3ae. Router musi obsługiwać interfejsy 1 Gigabit Ethernet SFP. Urządzenia musi obsługiwać moduły SFP o prędkościach 1 Gb/s i 100 Mb/s. Interfejsy GbE muszą współpracować z modułami SFP pochodzącymi od innych producentów. Router musi obsługiwać ramki Jumbo o wielkości 9 KB. |  |
| **7.** | Porty GbE i 10 GbE urządzenia muszą obsługiwać mechanizm Digital Optical Monitoring (DOM). |  |
| **8.** | Urządzenie musi obsługiwać w sprzęcie routing IPv4, IPv6 oraz MPLS. |  |
| **9.** | Urządzenie musi obsługiwać routing statyczny IPv4 oraz routing dynamiczny IPv4 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP. |  |
| **10.** | Urządzenie musi obsługiwać routing statyczny IPv6 oraz routing dynamiczny IPv6 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP. |  |
| **11.** | Router jednocześnie musi obsługiwać nie mniej niż 900 tysięcy wpisów w tablicy routingu IPv4, 900 tysięcy wpisów w tablicy VPN IPv4, 700 tysięcy wpisów w tablicy routingu IPv6 oraz 128 tysięcy adresów MAC. |  |
| **12.** | Router musi obsługiwać mechanizm tworzenia wirtualnych ruterów (kontekstów, ruterów logicznych) umożliwiający routing pakietów w oparciu o niezależne tablice routingu – musi m.in. umożliwiać uruchomienie nie mniej niż 5 instancji routingu BGP dla różnych numerów systemów autonomicznych. Ponadto ruter musi obsługiwać sprzętowo 3 pełne tablice BGP dla IPv4 dla 3 różnych numerów systemów autonomicznych (przy założeniu, że w pełnej tablicy BGP znajduje się 300 tysięcy prefiksów). Router musi obsługiwać nie mniej niż 500 sesji BGP. |  |
| **13.** | Router musi obsługiwać protokół redundancji VRRP. |  |
| **14.** | Mechanizm BFD musi być obsługiwany dla IPv4, IPv6 oraz MPLS LSP. |  |
| **15.** | Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów. Filtrowanie ruchu musi odbywać się co najmniej na podstawie adresów MAC, IPv4 i IPv6. Router musi obsługiwać nie mniej niż 10 000 reguł filtrowania ruchu. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza. |  |
| **16.** | Router musi obsługiwać protokół SNMP w wersjach 1, 2 i 3. Router musi udostępniać za pomocą protokołu SNMP co najmniej 64 bitowe liczniki ramek i bajtów wysłanych i odebranych na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą protokołu SNMP liczniki odebranych ramek zawierających błędy na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą CLI liczniki ramek wysłanych, odebranych oraz zawierających błędy na poszczególnych interfejsach tranzytowych. Ponadto po SNMP muszą być dostępne liczniki pakietów i bajtów przechwyconych przez poszczególne filtry ruchu (ACL). |  |
| **17.** | Router musi posiadać mechanizmy pozwalające na ograniczanie pasma dla ruchu wyjściowego i wejściowego na wszystkich interfejsach tranzytowych (z uwzględnieniem filtrów ruchu – ACL) oraz dla poszczególnych sieci VLAN. |  |
| **18.** | Router musi posiadać mechanizmy klasyfikowania ruchu, jego filtrowanie oraz znakowanie w oparciu co najmniej 802.1p, DSCP, ToS, MPLS EXP na wszystkich portach tranzytowych oraz dla poszczególnych sieci VLAN. Dodatkowo klasyfikacja pakietów musi się również odbywać o dane z protokołu BGP – nie mniej niż Community i AS Path. Znakowanie pakietów musi być wykonywane również przez tri-colored policer. |  |
| **19.** | Urządzenie musi wykonywać shaping lub policing ruchu per port. |  |
| **20.** | Router musi obsługiwać co najmniej 8 kolejek wyjściowych dla każdego portu tranzytowego. Urządzenie musi posiadać możliwość buforowania do 100 ms na wszystkich portach tranzytowych. Router musi obsługiwać mechanizm WRED. Router musi wspierać mechanizmy HQoS |  |
| **21.** | Router musi mieć zaimplementowane tunelowanie GRE oraz IP-IP bezpośrednio na karcie liniowej o wydajności przynajmniej 1Gbps. |  |
| **22.** | Router musi obsługiwać ruch IP multicast – w zakresie co najmniej protokołów IGMP (wersje 1, 2, 3) oraz PIM-SM. |  |
| **23.** | Na wszystkich interfejsach przeznaczonych do obsługi ruchu tranzytowego urządzenia musi obsługiwać usługi MPLS – nie mniej niż L2 VPN, VPLS (oparte o LDP i BGP) oraz BGP/MPLS VPN (L3 VPN). |  |
| **24.** | Router musi obsługiwać nie mniej niż 2000 sieci VPLS. |  |
| **25.** | Dla L2 VPN oraz VPLS musi być obsługiwany multihoming. |  |
| **26.** | Router musi obsługiwać protokół sygnalizacji RSVP-TE z mechanizmem Fast Reroute (node protection oraz link protection). |  |
| **27.** | Router musi posiadać możliwość uruchomienia mechanizmu DiffServ Traffic Engineering w celu przekierowania ruchu należącego do różnych klas obsługi ruchu na różne ścieżki MPLS. |  |
| **28.** | Router musi obsługiwać ruch multicast w IPVPN według draft-rosen-vpn-mcast-08.txt. |  |
| **29.** | W ramach IPVPN ruch multicast musi być obsługiwany wykorzystując sygnalizację BGP oraz w zakresie transportu MPLS point-to-multipoint według draft-ietf-l3vpn-2547bis-mcast-bgp-03.txt, draft draft-ietf-l3vpn-2547bis-mcast-02.txt, Requirements for Multicast in Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs) RFC4834 oraz draft-ietf-l3vpn-mvpn-considerations-01 |  |
| **30.** | Urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1q. Urządzenie musi pozwalać na skonfigurowanie i uruchomienie nie mniej niż 4094 sieci VLAN jednocześnie. |  |
| **31.** | Urządzenie musi obsługiwać mechanizm Q-in-Q włącznie z funkcją terminowania wewnętrznych sieci VLAN na interfejsach warstwy trzeciej. |  |
| **32.** | Urządzenie musi obsługiwać protokoły Spanning Tree – zgodnie z co najmniej IEEE 802.1d, 802.1w i 802.1s. |  |
| **33.** | Ramki BPDU pomiędzy sieciami VLAN muszą być przenoszone przez urządzenie również w trybie MPLS/VPLS. |  |
| **34.** | Urządzenie musi obsługiwać pracę w architekturze pierścienia z możliwością przerwania pierścienia w różnych miejscach dla różnych sieci wirtualnych (np. z wykorzystaniem Per VLAN Spanning Tree Protocol). Urządzenie musi umożliwiać szybkie przywrócenie (nie dłużej niż 1 sekunda) komunikacji w pierścieniu składającym się z co najmniej 100 urządzeń.  |  |
| **35.** | Router musi być zarządzany poprzez tekstowy interfejs linii komend (CLI) dostępny po porcie konsoli, oraz protokół Telnet i SSH dostępny przez interfejs do zarządzania out-of-band oraz dowolny interfejs tranzytowy. Router musi posiadać funkcję współpracy z zewnętrznymi serwerami AAA RADIUS (RFC 2138, RFC 2139) oraz TACACS+ (RFC 1492). |  |
| **36.** | Router musi posiadać funkcję limitowania pasma dla usług, których działania jest niezbędne do prawidłowego działania urządzenia, a które mogą stać się celem ataku Denial of Service. |  |
| **37.** | Urządzenia musi mieć domyślnie zaimplementowane zabezpieczenia przed atakami na poziomie protokołu ARP – minimalny wymagany poziom zabezpieczeń to limitowanie ruchu ARP. |  |

1. **Przełącznik LAN typu Top of the Rack - 13 szt.**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne sprzętu oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1.** | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19’’. |  |
| **2.** | Producent powinien oferować wsparcie dla modułów optycznych realizujących transmisję pochodzących od innych niż producent urządzeń dostawców. |  |
| **3.** | Przełącznik musi być wyposażony, w co najmniej 24 porty Ethernet 10/100/1000 Mb/s oraz minimum 4 porty typu SFP/SPF+ wraz z wkładkami 1/10G SFP/SFP+. Przełącznik musi umożliwiać stworzenie stosu w postaci pętli liczącego nie mniej niż 4 urządzenia. Stos musi być widoczny z punktu widzenia zarządzania, jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master. Wydajność połączenia stosu musi być nie mniejsza niż 80Gbps a pojedynczego urządzenia nie mniejsza niż 128Gbps i 95Mpps. |  |
| **4.** | Przełącznik musi posiadać zasilacz AC |  |
| **5.** | Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band). |  |
| **6.** | Przełącznik musi być wyposażony w nie mniej niż 2GB pamięci Flash oraz 2GB pamięci DRAM. Ilość zainstalowanej pamięci RAM powinna zapewniać prawidłową pracę urządzenia oraz oprogramowania. |  |
| **7.** | Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, SSH, a także za pośrednictwem interfejsu WWW. |  |
| **8.** | Przełącznik musi obsługiwać ramki Jumbo (9KB). |  |
| **9.** | Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w liczbie nie mniejszej niż 4000 |  |
| **10.** | Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN.  |  |
| **11.** | Przełącznik musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad  |  |
| **12.** | Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003. |  |
| **13.** | Przełącznik musi obsługiwać protokół LLDP. |  |
| **14.** | Przełącznik musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokoły routingu dynamicznego: RIP, OSPF. Jeżeli wymagana jest licencja na wsparcie dla tych mechanizmów wymaga się jej dostarczenia minimum dla protokołu RIP v1/v2. |  |
| **15.** | Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD (dopuszcza się jako opcję licencjonowaną). |  |
| **16.** | Przełącznik musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny. |  |
| **17.** | Przełącznik musi obsługiwać filtrowanie ruchu, na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo reguły filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów.  |  |
| **18.** | Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection. Pojemność tablicy forwarding musi być co najmniej rozmiaru 16000, VLAN min. 4000 a Tablica ARP min. 1024. |  |
| **19.** | Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS, (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC.. |  |
| **20.** | Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN. |  |
| **21.** | Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem. |  |
| **22.** | Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji. |  |

1. **Przełącznik Koncentrujący Top of the Rack - 1 szt.**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne sprzętu oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1.** | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie rack 19’’. |  |
| **2.** | Producent powinien oferować wsparcie dla modułów optycznych realizujących transmisję pochodzących od innych niż producent urządzeń dostawców. |  |
| **3.** | Przełącznik musi być wyposażony, w co najmniej 30 portów Ethernet typu SFP wraz z wkładkami 1 GbE SFP oraz musi umożliwiać rozbudowę o co najmniej 4 porty 10GbE lub 2 porty 40 GbE. Przełącznik musi umożliwiać stworzenie stosu nie mniej niż 9 urządzenia. Stos musi być widoczny z punktu widzenia zarządzania, jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master. Wydajność połączenia stosu musi być nie mniejsza niż 320Gbps a pojedynczego urządzenia nie mniejsza niż 450Gbps i 300Mpps. |  |
| **4.** | Przełącznik musi posiadać dwa zasilacz AC pracujące redundantnie |  |
| **5.** | Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band). |  |
| **6.** | Przełącznik musi być wyposażony w nie mniej niż 2GB pamięci Flash oraz 2GB pamięci DRAM. Ilość zainstalowanej pamięci RAM powinna zapewniać prawidłową pracę urządzenia oraz oprogramowania. |  |
| **7.** | Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, SSH, a także za pośrednictwem interfejsu WWW. |  |
| **8.** | Przełącznik musi obsługiwać ramki Jumbo (9KB). |  |
| **9.** | Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w liczbie nie mniejszej niż 4000 |  |
| **10.** | Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN.  |  |
| **11.** | Przełącznik musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad  |  |
| **12.** | Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spanning Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003. |  |
| **13.** | Przełącznik musi obsługiwać protokół LLDP. |  |
| **14.** | Przełącznik musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokoły routingu dynamicznego: RIP, OSPF, BGP, IS-IS. Jeżeli wymagana jest licencja na wsparcie dla tych mechanizmów wymaga się jej dostarczenia minimum dla protokołu RIP v1/v2. |  |
| **15.** | Przełącznik musi obsługiwać mechanizm wykrywania awarii BFD (dopuszcza się jako opcję licencjonowaną) ,  |  |
| **16.** | Przełącznik musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny. |  |
| **17.** | Przełącznik musi obsługiwać filtrowanie ruchu, na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo reguły filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów.  |  |
| **18.** | Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection. Pojemność tablicy forwarding musi być co najmniej rozmiaru 60000, VLAN min. 4000 a Tablica ARP min. 60000. |  |
| **19.** | Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS, (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. |  |
| **20.** | Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN. |  |
| **21.** | Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem. |  |
| **22.** | Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji. |  |

1. **Firewall do sieci Internet - 2 szt.**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne sprzętu oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1** | System zabezpieczeń firewall musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. |  |
| **2** | System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 10 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 5 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń. |  |
| **3** | System zabezpieczeń firewall musi być wyposażony w co najmniej 12 portów Ethernet 10/100/1000. Musi być możliwość zamontowania w urządzeniu minimum 8 interfejsów optycznych (SFP) oraz 4 interfejsów optycznych (SFP+). |  |
| **4** | System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. |  |
| **5** | Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.). |  |
| **6** | System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN. |  |
| **7** | System zabezpieczeń firewall musi obsługiwać nie mniej niż 125 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF. |  |
| **8** | System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji. |  |
| **9** | Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |  |
| **10** | System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. |  |
| **11** | System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. |  |
| **12** | Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 10 Gbit/s. |  |
| **13** | Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM). |  |
| **14** | Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. |  |
| **15** | Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS. |  |
| **16** | System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. |  |
| **17** | System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.  |  |
| **18** | System zabezpieczeń firewall musi posiadać możliwość definiowania i przydzielania różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi istnieć możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |  |
| **19** | System zabezpieczeń firewall musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. |  |
| **20** | System zabezpieczeń firewall musi umożliwiać analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji. |  |
| **21** | System zabezpieczeń firewall musi umożliwiać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików. |  |
| **22** | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |  |
| **23** | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |  |
| **24** | System zabezpieczeń firewall musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. |  |
|  | **Wymagania podstawowe identyfikacja użytkowników** |  |
| **25** | System zabezpieczeń firewall musi mieć możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) powinna precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. |  |
| **26** | System zabezpieczeń firewall musi mieć możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. |  |
| **27** | System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z nagłówka X-Forwarded-For i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. |  |
|  | **Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day** |  |
| **28** | System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |  |
| **29** | System zabezpieczeń firewall musi umożliwiać uruchomienie modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |  |
| **30** | System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |  |
| **31** | System zabezpieczeń firewall musi umożliwiać uruchomienie modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |  |
| **32** | System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |  |
| **33** | System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |  |
| **34** | System zabezpieczeń firewall musi umożliwiać uruchomienie modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |  |
| **35** | System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |  |
| **36** | System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. |  |
| **37** | System zabezpieczeń firewall musi posiadać funkcjonalność podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). |  |
| **38** | System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. |  |
|  | **Wymagania dodatkowe NAT, DoS, IPSEC VPN, SSL VPN, QoS** |  |
| **39** | System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. |  |
| **40** | System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |  |
| **41** | System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. |  |
| **42** | System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. |  |
| **43** | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników. |  |
| **44** | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego. |  |
|  | **Wymagania dodatkowe środowisko wirtualne VMware** |  |
| **45** | System zabezpieczeń firewall musi umożliwiać integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki mają skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla. |  |
|  | **Wymagania zarządzanie i raportowanie** |  |
| **46** | Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |  |
| **47** | System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. |  |
| **48** | System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. |  |
| **49** | System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). |  |
| **50** | Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. |  |
| **51** | System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos. |  |
| **52** | System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). |  |
| **53** | System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 120 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. |  |
| **54** | Nie jest dopuszczalne rozwiązanie, gdzie włączenie logowania na dysk może obniżyć wydajność urządzenia. |  |
| **55** | System zabezpieczeń firewall musi umożliwiać usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu. |  |
| **56** | System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa. |  |
| **57** | System zabezpieczeń firewall musi posiadać możliwość konfigurowania różnych serwerów Syslog per polityka bezpieczeństwa. |  |
| **58** | System zabezpieczeń firewall musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane mają zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www. |  |
| **59** | System zabezpieczeń firewall musi mieć możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. |  |
| **60** | System zabezpieczeń firewall musi mieć możliwość stworzenia raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni. |  |
| **61** | System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. |  |
| **62** | Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. |  |

1. **Urządzenia do nagrywania sesji zdalnego dostępu (appliance) - 1 szt.**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne sprzętu oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1** | Rozwiązanie typu „appliance”: sprzęt + oprogramowanie  |  |
| **2** | Rozwiązanie typu „solution in a box” - nie wymaga integracji z żadnym z istniejących elementów infrastruktury sieciowej |  |
| **3** | Rozwiązanie nie wymaga instalowania dodatkowego oprogramowania (agentów) na monitorowanych serwerach |  |
| **4** | Wspierane protokoły: |  |
| - protokoły tekstowe: SSH, Telnet, Telnet 3270, |  |
| - protokoły graficzne: RDP, VNC, X11, |  |
| - protokoły bazodanowe: Oracle, mysql, implementacja TDS dla MS SQL, |  |
| - pozostałe protokoły: HTTP, HTTPS, Modbus. |  |
| **5** | Rozwiązanie pozwala na kontrolę funkcjonalności w protokołach RDP, SSH, VNC  |  |
| **6** | Rozwiązanie posiada możliwość uwierzytelniania poprzez zewnętrzne serwery: Active Directory, LDAP, RADIUS |  |
| **7** | W rozwiązaniu analiza i rejestracja sesji dla ww. Protokołów odbywa się na urządzeniu, nie stosowane są „stacje przesiadkowe” |  |
| **8** | Rozwiązanie umożliwia synchronizację użytkowników z Active Directory, LDAP |  |
| **9** | W rozwiązaniu administrowanie, monitorowanie oraz podgląd sesji odbywa się poprzez przeglądarkę www |  |
| **10** | Rozwiązanie nagrywa cały ruch sieciowy związany z daną sesją |  |
| **11** | Rozwiązanie pozwala na selektywne wskazanie dla których połączeń lub grup połączeń ma być włączone nagrywanie sesji |  |
| **12** | Rozwiązanie umożliwia podmianę loginu i hasła wprowadzonego przez użytkownika na inny, znany na systemie docelowym |  |
| **13** | W rozwiązaniu podgląd monitorowanych sesji (zarówno “na żywo” jak i wcześniej nagranych) nie wymaga instalowania dodatkowego oprogramowania  |  |
| **14** | W rozwiązaniu obraz podglądu sesji jest dynamicznie budowany w dowolnej przeglądarce z zachowanych danych sesji (nie jest to odtwarzanie statycznego zapisu wideo) |  |
| **15** | W rozwiązaniu, dla zapisanych sesji terminalowych (np. Telnet, ssh) istnieje możliwość interakcji z tekstem (np. Copy & paste) |  |
| **16** | Rozwiązanie umożliwia przerwanie monitorowanej sesji |  |
| **17** | Rozwiązanie umożliwia chwilowe wstrzymanie i wznowienie sesji |  |
| **18** | Rozwiązanie umożliwia pro-aktywny monitoring, powodujący przerwanie sesji oraz alert administratora po wykryciu zadanych komend lub ciągu znaków |  |
| **19** | Rozwiązanie umożliwia dołączenie się administratora do sesji telnet, SSH, RDP, VNC z poziomu przeglądarki (np. Dla wprowadzenia hasła, wpisanie polecenia systemowego) |  |
| **20** | Rozwiązanie umożliwia udzielenie czasowego, „ad hoc”, dostępu do pojedynczej sesji za pośrednictwem www poprzez przesłanie adresu url |  |
| **21** | Rozwiązanie ma możliwość konfiguracji klastrowej w trybie multi-master |  |
| **22** | Rozwiązanie posiada bezpieczny mechanizm inicjacji systemu oraz generowania kluczy, które nie są znane producentowi |  |
| **23** | Rozwiązanie umożliwia znakowanie czasem zapisanych sesji, przez kwalifikowane podmioty (Trusted Timestamping) |  |
| **24** | Rozwiązanie zapewnia ochronę kryptograficzną wszystkich zapisanych danych (szyfrowanie oraz integralność zapewniona poprzez sumy kontrolne) |  |
| **25** | W rozwiązaniu klucze szyfrujące używane do ochrony kryptograficznej przechowywane na zewnętrznym nośniku USB |  |
| **26** | Rozwiązanie posiada min 24 TB przestrzeni na dane |  |
| **27** | Rozwiązanie posiada 2 interfejsy sieciowe, z możliwością rozszerzenia |  |
| **28** | Rozwiązanie obsługuje vlany |  |
| **29** | Rozwiązanie posiada dokumentację oraz interfejs użytkownika w języku polskim |  |
| **30** | Rozwiązanie posiada wsparcie techniczne w języku polskim |  |
| **31** | Zapewnia możliwość uwierzytelnienia użytkownika przed urządzeniem monitorującym |  |
| **32** | Rozwiązanie pozwala na podłączenie się administratora do nawiązanej sesji i interakcję w ramach tej sesji |  |
| **33** | Obsługa klawiatury polskiej, niemieckiej, rosyjskiej i angielskiej |  |
| **34** | Kontrola rozdzielczości i głębi kolorów w sesjach RDP |  |
| **35** | Rozwiązanie współpracuje z zewnętrznymi repozytoriami haseł: Lieberman ERPM, Thycotic Secret Server, Hitachi-ID, TPAM Dell oraz cyberark |  |
| **36** | Rozwiązanie umożliwia podanie powodu logowania na ekranie uwierzytelniającym |  |
| **37** | (Bastion) - dla protokołów RDP, VNC, SSH, TELNET, TELNET\_3270, rozwiązanie pozwala na uzyskanie dostępu do grupy monitorowanych serwerów poprzez jeden adres sieciowy (jedną parę IP i port) Nazwa docelowego serwera jest wskazywana w nazwie użytkownika przy użyciu separatora, np 'ssh -l user#mailserv nazwa-serwera’ |  |
| **38** | Rozwiązanie umożliwia tagowanie i komentowanie przeglądanych sesji |  |
| **39** | Rozwiązanie umożliwia kontekstowe przeszukiwanie sesji |  |
| **40** | (Business Intelligence) rozwiązanie ma możliwość monitorowania, raportowania oraz analizy aktywności użytkownika podczas sesji (np dla oceny produktywności i/lub kontroli stopnia zaangażowania i rozliczeń z firmą zewnętrzną) |  |
| **41** | Rozwiązanie pozwala na współpracę z rozwiązaniem Microsoft RD Connection Broker |  |
| **42** | Rozwiązanie posiada wsparcie dla klawiatury polskiej, niemieckiej, rosyjskiej i angielskiej w GUI i przy podłączaniu się do sesji z poziomu przeglądarki |  |
| **43** | (OCR) rozwiązanie umożliwia wyszukiwania tekstu w sesjach graficznych (np RDP) dla protokołu RDP, rozwiązanie współpracuje ze stacjami wyposażonymi w kilka monitorów |  |
| **44** | Szczegółowe raportowanie cykliczne na podstawie własnych definicji filtrowania, upraszcza pracę osób odpowiedzialnych za nadzór infrastruktury serwerów podlegających monitorowaniu  |  |
| **45** | Uproszczone zarządzanie czasowym dostępem do monitorowanych systemów dzięki możliwości zdefiniowania ram czasowych ważnych kont użytkowników  |  |
| **46** | Możliwość eksportowania I importowania konfiguracji (ustawienia sieciowe, adresy IP, definicje użytkowników, serwerów I połączeń) pozwalające na szybkie zainicjowanie maszyny zastępczej  |  |
| **47** | Usprawnienia w zarządzaniu dużą liczbą użytkowników, upraszczające pracę osoby odpowiedzialnej za konfiguracje system |  |
| **48** | Szybsza analiza zarejestrowanego materiału dzięki możliwości przeskakiwania pomiędzy wystąpieniami wyszukiwanej frazy  |  |
| **49** | Filtrowanie wpisów dziennika zdarzeń według obiektów, których dotyczą pozwala na sprawniejszy audyt  |  |
| **50** | Płynne współdzielenie sesji, wspólna praca na 2 pary oczu |  |
| **51** | Dostępne 4 tryby pracy: bastion, proxy, gateway, bridge |  |
| **52** | Ochrona przed wyłączeniem serwera zdalnego |  |
| **53** | Harmonogram generowania raportów i wysyłania mailem |  |
| **54** | Licencja na minimum 1500 hostów  |  |

1. **Firewall Data Center - 2 szt.**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymagania** | **Parametry techniczne sprzętu oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1.** | Firewall musi być dostarczony w postaci dwóch dedykowanych urządzeń typu appliance, przystosowanych do montażu w szafie rack, wyposażonych w pasywny midplane, wymienne wentylatory oraz 1 źródło zasilania AC. Ponadto urządzania muszą być wyposażone w nadmiarowe źródło zasilania w celu zapewnienia redundancji zasilania 1:1. |  |
| **2.** | Firewall musi posiadać wymienne karty z matrycą przełączającą, karty z interfejsami sieciowymi oraz karty usługowe realizujące sprzętowo funkcje bezpieczeństwa. |  |
| **3.** | Firewall musi posiadać 1 slot przeznaczony wyłącznie na kartę z matrycą przełączającą Karta z matrycą przełączającą musi posiadać wewnętrzne połączenie z wszystkimi kartami z interfejsami sieciowymi oraz wszystkimi kartami usługowymi.  |  |
| **4.** | Zarządzanie i konfiguracja firewalla przez administratorów musi być realizowana przez moduł kontrolny. System operacyjny firewalla musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi odpowiadać za sterowanie i monitorowanie pracy komponentów firewalla. Ruch tranzytowy użytkowników przechodzący przez firewall nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym.  |  |
| **5.** | System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł rutingu IP, odpowiedzialny za ustalenie tras rutingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo. System operacyjny firewalla musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. System operacyjny Firewall musi umożliwiać dostęp z zewnętrznych aplikacji poprzez mechanizmy API XML  |  |
| **6.** | Firewall musi obsługiwać co najmniej następujące rodzaje kart z interfejsami sieciowymi:  |  |
| Nie mniej niż 10 portów 10GE SFP+ |  |
| Możliwość rozbudowy o 10 portów 10GE |  |
| Możliwość rozbudowy o port 100GE |  |
| Możliwość rozbudowy o port 20 portów 1GE |  |
| **7.** | Firewall musi umożliwiać zainstalowanie nie mniej niż 3 kart z interfejsami sieciowymi (z możliwością rozbudowy do co najmniej 4 kart).  |  |
| Karty muszą posiadać przepustowość co najmniej 10 Gb/s full duplex.  |  |
| Każde z urządzeń musi być dostarczone z kartą wyposażoną w dwa interfejsy 10 GbE .  |  |
| **8.** | Mechanizmy QoS (policing, kolejkowaniem, shaping) oraz funkcje ochrony przed atakami DoS i DDoS muszą być realizowane sprzętowo.  |  |
| **9.** | Realizacja mechanizmów bezpieczeństwa musi się odbywać na wyspecjalizowanych kartach usługowych posiadających własny procesor. Karty usługowe muszą realizować sprzętowo co najmniej takie funkcje jak stateful firewall, translacja adresów IP, IPSec VPN, oraz po opcjonalnej rozbudowie: intrusion prevention (IPS), oraz cechy next generation firewall w zakresie identyfikacji i sterowania aplikacji sieciowych jak m.in. Skype, BitTorrent. Wszystkie karty usługowe muszą posiadać identyczną funkcjonalność i pracować pod kontrolą systemu operacyjnego firewalla – nie dopuszcza się możliwości realizacji całości lub części ww. funkcji bezpieczeństwa przez karty działające pod kontrolą innych systemów operacyjnych. Zwiększenie wydajności ww. funkcji bezpieczeństwa musi się odbywać przez zwiększanie ilości kart usługowych. Firewall musi posiadać minimum 6 slotów pozwalających na zainstalowanie i uruchomienie kart usługowych. Nie dopuszcza się również sytuacji, aby poszczególne moduły usługowe były traktowane przez system operacyjny firewalla jako niezależne urządzenia, z osobnymi regułami polityki firewall – z punktu widzenia systemu operacyjnego firewalla wszystkie moduły usługowe muszą być integralną częścią urządzenia i wszystkie muszą podlegać tej samej polityce bezpieczeństwa konfigurowanej na module kontrolnym.  |  |
| **10.** | Firewall (dla każdego urządzenia) : |  |
| * musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 256 strefami bezpieczeństwa z sumaryczną wydajnością nie mniejszą niż 200 Gb/s liczoną dla dużych pakietów.
 |  |
| * musi obsłużyć sumarycznie nie mniej niż 1mln równoległych sesji lub zestawić sumarycznie nie mniej niż 1000 tysięcy nowych połączeń/sekundę.
 |  |
| * jednocześnie musi istnieć możliwość rozbudowy by obsługiwało dla funkcji Stateful Firewall co najmniej przepustowość 400 Gb/s dla dużych pakietów i 2mln sesji równoległych.
 |  |
| **11.** | Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo przez karty usługowe. Firewall musi obsłużyć nie mniej niż 14 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 3 Gb/s dla pakietów typu IMIX. |  |
| **12.** | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 35 000 reguł polityki bezpieczeństwa. |  |
| **13.** | Firewall ma umożliwiać rozbudowę o funkcje wykrywania i blokowania ataków intruzów (IPS, intrusion prevention) oraz ochrony aplikacji (Application Security) realizowanej sprzętowo lub programowo na modułach usługowych. System zabezpieczeń musi wtedy identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z sumaryczną wydajnością nie mniejszą niż 8 Gb/s. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall, zawierać co najmniej 6000 sygnatur ataków. Baza sygnatur ataków musi być aktualizowana przez producenta co najmniej raz w tygodniu. Wymagane dostarczenie subskrypcji na okres 1 roku dla funkcjonalności Intrusion Prevention System (IPS) oraz ochrony aplikacyjnej od daty podpisania protokołu końcowego. |  |
| **14.** | Urządzenia muszą obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP. Urządzenie musi obsługiwać nie mniej niż 2 000 peer’ów BGP i nie mniej niż 1 000 000 prefiksów BGP (w RIB). Urządzenia muszą umożliwiać skonfigurowanie nie mniej niż 256 wirtualnych ruterów oraz 4000 sieci VLAN z tagowaniem 802.1Q i min. 20 wirtualnych systemów. |  |
| **15.** | Firewall musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenia muszą posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenia muszą posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach. |  |
| **16.** | Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive, Active/Active z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Klaster HA musi posiadać redundantne połączenia służące do synchronizacji konfiguracji i tablicy stanu sesji firewalli. |  |
| **17.** | Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta. Zarządzanie CLI obu węzłów klastra musi się odbywać z pojedynczego miejsca – konsoli jednego z węzłów (jeden plik konfiguracyjne na oba węzły klastra Firewall). |  |
| **18.** | Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji, w tym musi istnieć możliwość wskazania jednej z wersji konfiguracji jako bazowej, służącej odtworzeniu przy pomocy pojedynczej komendy konfiguracji tzw. minimalnej (nie fabrycznej). |  |
| **19.** | Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone są w języku polskim. |  |

1. **Oprogramowanie ITSM**

|  |  |  |
| --- | --- | --- |
| ID | Wymaganie | Parametry techniczne oprogramowania oferowanego przez Wykonawcę |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1. | Moduł procesów umożliwiający zarządzanie co najmniej wymienionymi procesami w rozumieniu biblioteki ITIL: 1. Zarządzanie incydentem,
2. Zarządzanie problemem,
3. Zarządzanie zmianą,
4. Zarządzanie konfiguracją,
5. Zarządzanie projektami,
6. Zarządzanie wnioskiem o usługę.
 |  |
| 2. | Centralną bazę konfiguracji CMDB wraz ze zintegrowanym wykrywaniem środowiska IT. |  |
| 3. | Moduł zarządzania umowami serwisowymi dla elementów konfiguracji (CI) przechowywanych w bazie konfiguracji CMDB. |  |
| 4. | Moduł zarządzania bazą wiedzy dla użytkowników. |  |
| 5. | Moduł raportowania. |  |
| 6. | Moduł procesów umożliwiający zarządzanie co najmniej wymienionymi procesami w rozumieniu biblioteki ITIL: 1. Zarządzanie incydentem,
2. Zarządzanie problemem,
3. Zarządzanie zmianą,
4. Zarządzanie konfiguracją,
5. Zarządzanie projektami,
6. Zarządzanie wnioskiem o usługę.
 |  |
| 7. | Centralną bazę konfiguracji CMDB wraz ze zintegrowanym wykrywaniem środowiska IT. |  |
| 8. | Moduł zarządzania umowami serwisowymi dla elementów konfiguracji (CI) przechowywanych w bazie konfiguracji CMDB. |  |
| 9. | Moduł zarządzania bazą wiedzy dla użytkowników. |  |
| 10. | Moduł raportowania. |  |
| I | **Moduł zarządzania procesami** |  |
| 1. | Moduł zarządzania procesami musi być w pełni konfigurowalny z poziomu interfejsu webowego oprogramowania, |  |
| 2. | Dostęp do modułu zarządzania procesami odbywa się z poziomu przeglądarki internetowej zarówno dla serwisanta jak i użytkownika systemu, |  |
| 3. | System musi posiadać możliwość dostosowania portalu w tym, rozmieszczenie poszczególnych elementów portalu metodą drag&drop, zagnieżdżanie stron html, |  |
| 4. | System musi posiadać mechanizm oznaczania pierwszej reakcji na zgłoszenie, jako rozwiązania zgłoszenia – first call resolution, |  |
| 5. | System musi posiadać możliwość oznaczenia pracy nad zgłoszeniem przez danego serwisanta, oznaczenie pracy uruchamia zegar naliczający czas pracy serwisanta nad zgłoszeniem. System w postaci graficznej prezentuje uruchomiony zegar w widoku zgłoszeń, jak i samym zgłoszeniu, |  |
| 6. | System pozwala określić typ czasu pracy poświęconego na rozwiązanie zgłoszenia, |  |
| 7. | System pozwala na dowolną rozbudowę pól wykorzystywanych do opisania czasu pracy poświęconego na rozwiązanie zgłoszenia, |  |
| 8. | Moduł zarządzania procesami umożliwia rejestrację zgłoszenia wieloma kanałami, w szczególności przez stronę WWW, telefon i email, |  |
| 9. | System posiada możliwość przekazywania wiadomości od serwisanta, bezpośrednio na skrzynkę pocztową zgłaszającego, |  |
| 10. | Moduł zarządzania procesami umożliwia w trakcie rejestracji zgłoszenia przez użytkownika na stronie www załączenia dowolnego formatu załączników, |  |
| 11. | Moduł zarządzania incydentami pozwala wstrzymać zegar SLA zgłoszenia wraz z ustawieniem automatycznego jego otwarcia i wysłania powiadomienia do serwisanta, |  |
| 12. | Moduł zarządzania procesami umożliwia użytkownikom przeglądanie na stronie www statusu własnych zgłoszeń, dodawania komentarzy, podgląd i edycję danych użytkownika, prowadzenie projektów oraz przeglądania bazy wiedzy znanych problemów i ich rozwiązań, |  |
| 13. | Moduł zarządzania procesami umożliwia definiowanie dodatkowych pól w formularzu incydentu, wniosku o usługę, problemu, zmiany, |  |
| 14. | Moduł zarządzania zgłoszeniami (0bsługa zgłoszeń incydentów i wniosków o usługę) zapewnia budowę dynamicznych szablonów zgłoszeń. Dynamiczność szablonu zgłoszeń polega na automatycznym i samodzielnym dostosowaniu się szablonu zgłoszenia, do wprowadzanych atrybutów przez użytkownika. System pozwala na:* Uruchamianie i wyłączanie z zgłoszenia wskazanych atrybutów,
* Chowanie i odsłanianie wybranych atrybutów,
* Oznaczanie i odznaczanie obligatoryjnych do wypełnienia atrybutów,
* Uruchamianie skryptów, pisanych w wbudowanym w aplikację edytorze skryptów,
* Uruchamianie powyższych automatyzacji na różnych etapach rejestrowania zgłoszenia, oraz od wprowadzanych bieżących atrybutów w zgłoszeniu;
 |  |
| 15. | Moduł zarządzania zgłoszeniami pozwala na konfigurację dedykowanych do wybranych typów zgłoszeń incydentów i wniosków o usługę przycisków, wyzwalających następujące akcje:* Uruchomienie dedykowanego pliku html, powiązanego z wykonywalnym skryptem lub klasą na systemie helpdeskowym,
* Uruchomienie dedykowanego pliku html, powiązanego z wykonywalnym skryptem lub klasą na systemie zintegrowanym z helpdeskowym,
* Uruchomienie wykonywalnego skryptu lub klasy na systemie helpdeskowym,
* Uruchomienie wykonywalnego skryptu lub klasy na systemie zintegrowanym z helpdeskowym,
 |  |
| 16. | Moduł zarządzania zgłoszeniami pozwala na konfigurację globalnych reguł biznesowych, wywołujących wykonywalny skrypt lub klasę na systemie helpdeskowym, lub na systemie zintegrowanym z systemem helpdeskowym, |  |
| 17. | Moduł zarządzania zgłoszeniami posiada możliwość wymuszenia podawania komentarzy przy zmianie statusów zgłoszenia, |  |
| 18. | Moduł zarządzania zgłoszeniami posiada możliwość budowania zależności miedzy zarejestrowanymi zgłoszeniami incydentów i wniosków o usługę. Zależności muszą pozwalać na uzależnienie zamykania zgłoszenia od zamknięcia zgłoszenia zależnego poprzedzającego dane zgłoszenie, |  |
| 19. | System pozwala na konfigurację funkcjonalności informującej zgłaszających o czasie na rozwiązanie zgłoszenia, dotyczy zarówno zgłoszeń incydentów jak i wniosków o usługę, |  |
| 20. | Moduł zarządzania procesami posiada centralne repozytorium incydentów, wniosków o usługę, problemów i zmian, umożliwiające filtrowanie i sortowania zapisanych zgłoszeń według co najmniej następujących kryteriów: status zgłoszenia, kategoria, użytkownik, czas rozwiązania, czas przyjęcia, przydzielona grupa wsparcia, |  |
| 21. | Moduł zarządzania procesami umożliwia centralne repozytorium incydentów, wniosków o usługę, problemów i zmian, umożliwiające definiowanie własnych filtrów umożliwiających sortowania zapisanych zgłoszeń, |  |
| 22. | Moduł zarządzania incydentami jest certyfikowany przez fundację Pink Elephant, |  |
| 23. | Moduł zarządzania procesami umożliwia dla każdego zgłoszenia określenie takich atrybutów, jak: dane osoby zgłaszającej, zasób, którego dotyczy zgłoszenie oraz priorytet, wpływ i pilność realizacji, |  |
| 24. | Moduł zarządzania procesami umożliwia przeszukiwanie zgłoszeń według co najmniej następujących atrybutów: nr zgłoszenia, użytkownik, tytuł, opis, data utworzenia, |  |
| 25. | Moduł zarządzania procesami umożliwia rejestrację zgłoszeń pochodzących z zewnętrznych narzędzi monitorujących, jednocześnie umożliwiając ich klasyfikację i na tej podstawie automatyczne przekazywanie do grup wsparcia, |  |
| 26. | Moduł zarządzani procesami umożliwia przesyłanie i prezentowanie na stronie www powiadomień dla użytkowników i/lub serwisantów, przesyłanie powiadomień do pojedynczych użytkowników lub grup użytkowników/serwisantów, |  |
| 27. | Moduł zarządzania procesami w ramach rozwiązywania zgłoszeń umożliwia komunikację z użytkownikiem poprzez pocztę elektroniczną i rejestrację wiadomości do właściwych wątków zgłoszeń, |  |
| 28. | Moduł zarządzania procesami umożliwia klasyfikację zgłoszeń, problemu lub zmiany, w co najmniej 3 poziomowej strukturze drzewiastej, przy czym struktura klasyfikacji powinna być dowolnie edytowalna przez uprawnionych administratorów z poziomu interfejsu webowego systemu, |  |
| 29. | Moduł zarządzania procesami umożliwia automatyczne wyliczenie i przydzielenie priorytetu do zgłoszenia na podstawie wprowadzonych do formularza zgłoszenia informacji o wpływie i pilności realizacji, |  |
| 30. | Moduł zarządzania procesami pozwala na automatyczną eskalację zgłoszeń do grup wsparcia, na podstawie co najmniej następujących atrybutów: użytkownik, priorytet, poziom, wpływ, pilność, tytuł zgłoszenia, słowo kluczowe w tytule i treści zgłoszenia, |  |
| 31. | Moduł zarządzania procesami umożliwia przekierowanie zgłoszeń do innych serwisantów lub grup wsparcia celem dalszej obsługi, |  |
| 32. | Moduł umożliwia zmianę typu zgłoszenia z incydentu na wniosek o usługę wraz ze zmianą parametrów zgłoszenia i trybu jego realizacji, zgodnie z procedurą określoną dla właściwego typu wniosku, |  |
| 33. | Moduł zarządzania procesami umożliwia tworzenie szablonów zgłoszeń z predefiniowanymi atrybutami i regułami przekazywania do odpowiednich zespołów wsparcia, |  |
| 34. | Moduł zarządzania procesami umożliwia tworzenie harmonogramów dla zgłoszeń okresowych, a w ramach realizacji takiego zgłoszenia automatyczne przydzielanie zadań do serwisantów, |  |
| 35. | Moduł zarządzania procesami umożliwia rejestrację historii incydentów, wniosków o usługę, problemów i zmian, zablokowaną do edycji dla użytkownika oprogramowania, |  |
| 36. | Moduł zarządzania procesami umożliwia rejestrowanie aktywności i zleceń pracy związanych z poszczególnymi incydentami, wnioskami o usługę, problemami i zmianami oraz śledzenie czasu pracy nad zgłoszeniem, |  |
| 37. | Moduł zarządzania procesami umożliwia rejestrowanie czasu pracy nad danym zgłoszeniem, problemem i zmianą przez poszczególnych serwisantów pracujących nad zgłoszeniem, |  |
| 38. | Moduł zarządzania procesami umożliwia wstawianie plików graficznych w treści rozwiązania zgłoszenia, |  |
| 39. | Moduł zarządzania procesami umożliwia globalne definiowanie szablonów wiadomości e-mail wykorzystywanych przez system do powiadamiania użytkowników o różnych zdarzeniach w systemie. Definiowanie szablonów odbywa się z poziomu interfejsu webowego aplikacji i umożliwiać zdefiniowanie treści powiadomienia, reguły wywołującej przesłanie powiadomienia oraz odbiorcy,  |  |
| 40. | Moduł zarządzania zgłoszeniami umożliwia definiowanie i filtrowanie szablonów zgłoszeń dedykowanych dla określonych grup użytkowników, |  |
| 41. | Moduł zarządzania procesami umożliwia przesyłanie do użytkowników powiadomień o następujących zdarzeniach zarejestrowanych przez system: przyjęcie zgłoszenia, aktualizacja zgłoszenia, rozwiązanie zgłoszenia, zamknięcie zgłoszenia, |  |
| 42. | Moduł zarządzania procesami ma wbudowaną funkcjonalność prezentowania w postaci graficznej istotnych wskaźników wydajności pozwalające na monitorowanie statusu poszczególnych procesów, moduł wskaźników pozwala ustalić okres odświeżania danych na tablicy wskaźników, |  |
| 43. | Moduł zarządzania procesami umożliwia automatyczne zamykanie rozwiązanych zgłoszeń po określonym czasie, |  |
| 44. | Moduł zarządzania procesami umożliwia przekazywanie do akceptacji osób trzecich działań podejmowanych w ramach rozwiązania zgłoszenia, np. akceptacja realizacji zlecenia na usługę serwisową, |  |
| 45. | Moduł zarządzania procesami umożliwia wielostopniowy poziom akceptacji wniosków o usługę wraz zdefiniowaniem procesu powiadomień kierowanych do osób akceptujących, |  |
| 46. | Moduł zarządzania procesami umożliwia przeglądanie bazy wiedzy z poziomu incydentu lub problemu i podłączanie rozwiązania z bazy rozwiązań do rozwiązania w zgłoszeniu, |  |
| 47. | Moduł zarządzania procesami umożliwia implementację warunków umów SLA i na tej podstawie obliczania czasu rozwiązania incydentu lub wniosku o usługę. Atrybuty umowy SLA, na postawie których system wylicza czas rozwiązania incydentu lub wniosku o usługę muszą zawierać co najmniej taki parametr jak nazwa użytkownika, oddział, komputer, priorytet, pilność, wpływ, poziom, |  |
| 48. | Moduł zarządzania wnioskami o usługi, musi posiadać możliwość zdefiniowania reguł biznesowych, z ich rozróżnieniem względem lokalizacji, |  |
| 49. | Moduł zarządzania wnioskami o usługi, posiada możliwość zdefiniowania umów SLA, z ich rozróżnieniem względem lokalizacji, |  |
| 50. | Moduł zarządzania procesami posiada wbudowaną funkcjonalność ankietowania użytkowników. Ankiety są rozsyłane przez aplikację automatycznie po zamknięciu incydentu, |  |
| 51. | Moduł zarządzania procesami umożliwia automatyczną konwersję incydentu na problem oraz przyłączania wielu incydentów do jednego problemu, |  |
| 52. | Moduł zarządzania problemami umożliwia zamknięcie powiązanych problemem incydentów w momencie zamykania problemu, |  |
| 53. | Moduł zarządzania procesami umożliwia zarejestrowanie znanego błędu oraz rozwiązania niezależnie i prezentacji rozwiązania tymczasowego użytkownikom, |  |
| 54. | Moduł zarządzania procesami umożliwia rejestrację i klasyfikację zmian, automatyczną konwersję problemu na zmianę oraz przyłączanie wielu incydentów i problemów do zmiany, |  |
| 55. |  Moduł zarządzania procesami umożliwia zarejestrowanie szczegółowych planów w zmianie, planu wdrożenia zmiany oraz planu wycofania zmiany, |  |
| 56. | Moduł zarządzania procesami umożliwia połączenie zmiany z zasobami i usługami, których ta zmiana dotyczy, |  |
| 57. | Moduł zarządzania procesami umożliwia przeprowadzenie procesu akceptacji dla zmiany przez komisję ds. zmiany (ang. Change Advisory Board), |  |
| 58. | Moduł zarządzania procesami musi umożliwiać zdefiniowanie na formularzach incydentu, wniosku o usługę, problemu i zmiany pól niezbędnych do wypełnienia w trakcie rejestracji i zamknięcia zgłoszenia, |  |
| 59. | Moduł zarządzania czasem pracy pozwala na rejestrację czasu pracy, przez uruchomienie zegara liczącego, czas spędzony nad zgłoszeniem przez technika, |  |
| 60. | Moduł zarządzania czasem pracy, pozwala na analizę czasów: przypisania zgłoszenia do danego technika, przypisania zgłoszenia do danej grupy suportu, przypisania zgłoszenia do danego statusu, |  |
| 61. | Moduł zarządzania czasem pracy pozwala na wprowadzanie dodatkowych atrybutów czasu pracy, możliwych do raportowania, |  |
| 62. | Moduł zarządzania czasem pracy pozwala na wprowadzenie dedykowanych typów czasu pracy, |  |
| 63. | Moduł zarządzania procesami umożliwia zdefiniowanie i zarządzanie projektami, |  |
| 64. | Moduł zarządzania procesami umożliwia w ramach zdefiniowanego projektu określenie tzw. kamieni milowych projektu, osób zaangażowanych w projekt oraz przydzielenie im zadań na każdym etapie realizacji projektu, |  |
| 65. | Moduł zarządzania procesami umożliwia definiowanie typów oraz statusów dla projektów wraz z możliwością filtrowania po tych parametrach, |  |
| 66. | Moduł zarządzania procesami umożliwia definiowanie ról w projekcie i przypisywanie ich zaangażowanym osobom, |  |
| 67. | Moduł zarządzania procesami pozwala na eksport widoku diagramu Gantta do pliku PDF, |  |
| 68. | Moduł zarządzania procesami umożliwia przedstawienie w sposób graficzny zaawansowania realizacji poszczególnych etapów w projekcie, |  |
| 69. | Moduł zarządzania zgłoszeniami jest udostępniony w aplikacjach mobilnych na systemach Android, zarówno dla kont serwisantów jak i zgłaszających. |  |
| II | **Centralna baza konfiguracji CMDB wraz ze zintegrowanym wykrywaniem środowiska** |  |
| 1. | CMDB umożliwia przechowywanie danych o wszystkich jednostki konfiguracji (CI) takich jak:* Komputery,
* Drukarki sieciowe,
* Urządzenia sieciowe,
* Pakiety oprogramowania,
* Komponenty komputerów i urządzeń sieciowych,
* Usługi biznesowe oraz IT,
* Zasoby ludzkie (np. użytkownicy, grupy użytkowników, serwisanci, grupy serwisowe);
 |  |
| 2. | CMDB zawiera gotowy schemat danych wraz z listą możliwych relacji pomiędzy jednostkami konfiguracji, jak również możliwość rozbudowanie go o własne, zdefiniowane relacje, |  |
| 3. | CMDB umożliwia dynamiczne rozszerzenie schematu danych o dodatkowe atrybuty, w tym atrybuty dedykowane dla konkretnego typu jednostki konfiguracji CI. Rozszerzenie odbywa się z poziomu interfejsu graficznego systemu, |  |
| 4. | CMDM umożliwia przedstawienie w sposób graficzny wzajemnych relacji pomiędzy jednostki konfiguracji CI, |  |
| 5. | CMDB umożliwia przechowywanie informacji pomiędzy incydentami, problemami oraz zmianami, a jednostkami konfiguracji, |  |
| 6. | CMDB umożliwia ręczne dodawanie jednostek konfiguracji oraz relacji pomiędzy nimi z poziomu interfejsu graficznego jak również importu danych o jednostkach konfiguracji z plików w formacie CSV lub XML, |  |
| 7. | CMDB posiada zintegrowany moduł wykrywania środowiska IT, pozwalający na wykrycie co najmniej konfiguracji komputerów, serwerów i oprogramowania. Wykrywanie opiera się na połączeniach protokołem SSH oraz protokołami SNMP lub WMI lub również przy wykorzystaniu skanowania agendowego. System zapewnia opcjonalność wykorzystywanej metody skanowania środowiska IT, |  |
| 8. | Moduł wykrywania środowiska umożliwia zbieranie danych o konfiguracji komputerów, co najmniej:* Ilości i rodzaju procesora,
* Wielkość dostępnej pamięci fizycznej i wirtualnej ,
* Nr seryjny komputera,
* Nazwa i wersja systemu operacyjnego,
* Zainstalowane oprogramowanie i poprawki;
 |  |
| 9. | Moduł wykrywania środowiska powinien posiadać mechanizm generowania kodów kreskowych dla zasobów. Moduł powinien pozwalać na zdefiniowanie formatu kodu kreskowego i jego wydruk według zdefiniowanego formatu wydruku, |  |
| 10. | Moduł wykrywania zasobów powinien posiadać możliwość wprowadzania zasobów skanowanych po kodzie kreskowym, |  |
| 11. | Moduł wykrywania środowiska umożliwia przeprowadzenie wykrywania zmian w konfiguracji i generowania raportów porównawczych zmian w elementach konfiguracji, |  |
| 12. | Moduł wykrywania środowiska umożliwia przeprowadzenie automatycznych, zdefiniowanych według cyklicznego harmonogramu audytów konfiguracji komputerów i serwerów, pod kątem zmian w konfiguracji i zainstalowanym oprogramowaniu, |  |
| 13. | Moduł wykrywania środowiska umożliwia przeprowadzenie skanowania komputerów i zasilenie danych do bazy dla komputerów niepodłączonych do sieci komputerowej. Możliwe jest zastosowanie specjalnych skryptów, których plik wynikowy następnie zostanie zaimportowany do bazy, |  |
| 14. | CMDB umożliwia przechowywanie informacji o poszczególnych elementach konfiguracji w taki sposób, by możliwe było rejestrowanie i śledzenie historii posiadania elementu konfiguracji przez użytkowników, powiązanie z nim informacji o koszcie zakupu, innych kosztach eksploatacyjnych, warunkach umowy serwisowej, dostawcy, |  |
| 15. | CMDB umożliwia wyszukiwanie elementów konfiguracji po dowolnych atrybutach, zarówno standardowych, jak i dodanych przez użytkownika, w tym po kodach kreskowych, |  |
| 16. | CMDB umożliwia zdefiniowanie wartości początkową elementu konfiguracji oraz mierzenie jego amortyzacji, |  |
| 17. | CMDB umożliwia powiązanie poszczególnych elementów konfiguracji z danymi użytkownika (jego imieniem i nazwiskiem, nr telefonu, departamentem), departamentu, innymi elementami konfiguracji i katalogiem usług, |  |
| 18. | CMDB umożliwia przechowywanie informacji o posiadanych przez użytkownika licencjach na oprogramowanie, powiązać posiadane licencje z zainstalowanym na komputerach oprogramowaniem, oraz rejestrować historię zmian posiadania danej licencji, |  |
| 19. | CMDB umożliwia zarządzanie licencjami na oprogramowanie posiadane przez użytkowników w tym zarządzanie umowami dotyczącymi zakupu licencji oraz zasilanie CMDB danymi dotyczącymi licencji pochodzącymi z innych źródeł danych, |  |
| 20. | CMDB umożliwia wygenerowanie raportu posiadanych licencji przez użytkownika oraz raportów zgodności licencji z zainstalowanym oprogramowaniem, |  |
| 21. | CMDB umożliwia z poziomu interfejsu oprogramowania nawiązanie sesji zdalnej w trybie przejęcia pulpitu użytkownika z komputerem przechowywanym w bazie, |  |
| 22. | CMDB posiada API, |  |
| III | **Moduł zarządzania umowami serwisowymi dla zasobów IT przechowywanych w bazie konfiguracji CMDB:** |  |
| 1. | Moduł zarządzania umowami serwisowymi umożliwia rejestrację warunków umów gwarancyjnych i serwisowych, w tym w szczególności dane teleadresowe gwaranta, czas obowiązywania umowy, jej koszt oraz powiązania ich z jednym lub wieloma elementami konfiguracji bazy CMDB, |  |
| 2. | Moduł zarządzania umowami serwisowymi posiada funkcjonalność pozwalającą przesyłać powiadomienia o wygaśnięciu okresu obowiązywania umowy serwisowej i gwarancyjnej; |  |
| IV | **Moduł zarządzania bazą wiedzy dla użytkowników** |  |
| 1. | Moduł zarządzania bazą wiedzy umożliwia rejestrację rozwiązań zawierających co najmniej następujące atrybuty: temat i opis rozwiązania, powiązane słowa kluczowe, klasyfikacja rozwiązania, |  |
| 2. | Moduł zarządzania bazą wiedzy umożliwia klasyfikację rozwiązań w strukturze drzewiastej katalogu, dowolnie definiowanego przez użytkownika, |  |
| 3. | Moduł zarządzania bazą wiedzy umożliwia przeszukiwanie danych po dowolnych atrybutach rozwiązania, |  |
| 4. | Moduł zarządzania bazą wiedzy umożliwia udostępnianie rozwiązań osobno dla użytkowników i osobno dla serwisantów, |  |
| 5. | Moduł zarządzania bazą wiedzy umożliwia rejestrację rozwiązań z poziomu incydentu i problemu, |  |
| 6. | Moduł zarządzania bazą wiedzy umożliwia przeglądanie rozwiązań bez konieczności logowania się użytkownika do systemu, |  |
| 7. | Moduł bazy wiedzy umożliwia dokonanie akceptacji dodawanego do bazy wiedzy rozwiązania przez administratora bazy wiedzy, |  |
| 8. | Moduł zarządzania bazą wiedzy umożliwia zamieszczanie i wyświetlanie w treści rozwiązania plików graficznych oraz dołączania dowolnej ilość załączników, |  |
| 9. | Moduł zarządzania bazą wiedzy umożliwia przesłanie rozwiązania do użytkownika za pomocą poczty elektronicznej bez konieczności powiązania tego działania z procesem zarządzania incydentem lub problemem, |  |
| 10. | Moduł Bazy wiedzy może być ukryty przed zgłaszającymi, |  |
| 11. | Moduł Bazy Wiedzy posiada API; |  |
| V | **Moduł zarządzania zakupami** |  |
| 1. | Moduł zarządzania zakupami umożliwia przeprowadzenie procesu zakupowego składającego się z co najmniej następujących kroków:* Utworzenie zamówienie – rejestracja numeru zamówienia, powiązanie z dostawcą, określenie terminu realizacji zamówienia,
* Dodanie pozycji do zamówienia – rejestracja produktów, ich ilości oraz ceny jednostkowej produktu,
* Przedstawienie zamówienia do akceptacji – moduł zarządzania zakupami umożliwia przeprowadzenie weryfikacji i akceptacji zamówienia przez osoby trzecie, z tymże użytkownik rejestrujący zamówienie nie może być jednocześnie osobą trzecią weryfikującą i akceptującą realizację zamówienia,
* Powiązanie zamówienia z elementami konfiguracji w bazie CMDB;
 |  |
| 2. | Moduł zarządzania zakupami umożliwia przesłanie powiadomienia do osób trzecich o przekroczonym terminie realizacji zamówienia, |  |
| 3. | Moduł zarządzania zakupami umożliwia przydzielenie zamówienia do wybranego centrum kosztów (Cost Center) oraz konta księgi głównej w księgowości. |  |
| VI | **Moduł raportowania** |  |
| 1. | Moduł raportowania umożliwia utworzenie raportów zarejestrowanych incydentów, problemów i zmian filtrowanych według kategorii, departamentu, statusu zgłoszenia, użytkownika, |  |
| 2. | Moduł raportowania umożliwia utworzenie raportów przedstawiających rozkład incydentów w czasie według dowolnego atrybutu, próbkowane co jeden dzień roboczy, |  |
| 3. | Moduł raportowania umożliwia utworzenie raportów czasu pracy użytkowników w ramach rozwiązywania zgłoszeń, |  |
| 4. | Moduł raportowania posiada wbudowaną funkcjonalność exportu utworzonych raportów do plików formatu PDF, XLS i HTML, |  |
| 5. | Moduł raportowania umożliwia automatyczne tworzenie raportów, zdefiniowanych według cyklicznego harmonogramu a następnie przesyłanie tychże raportów za pomocą poczty elektronicznej do dowolnego użytkownika, |  |
| 6. | Moduł raportowania umożliwia dostęp do modułu tylko wybranym użytkownikom, |  |
| 7. | Moduł raportowania jest wyposażony w funkcjonalność wykonywania zapytań SQL do bazy danych oprogramowania, funkcjonalność ta jest realizowana poprzez interfejs webowy oprogramowania, |  |
| 8. | Moduł raportowania pozwala na tworzenie dynamicznych wskaźników. Prezentowanych w tablicy wskaźników, |  |
| 9. | Moduł raportowania umożliwia przyłączenie do niego zewnętrznych systemów raportujących, takich jak Crystal Reports lub równoważnych. |  |

1. **Narzędzie do monitorowania**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne oprogramowania oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1.** | Oprogramowanie systemu monitorowania musi pracować w oparciu o system operacyjny Linux |  |
| **2.** | Oprogramowanie systemu monitorowania musi umożliwiać monitorowanie co najmniej: |  |
| 1500 elementów (urządzeń sieciowych, serwerów fizycznych, serwerów wirtualnych, aplikacji, baz danych (za jeden element uznaje się rozwiązanie posiadające adres IP) |  |
| W interfejsie GUI oprogramowanie systemu monitorowania musi wspierać przeglądarki WWW: Internet Explorer i Firefox. |  |
| Konfiguracja oprogramowania systemu monitorowania musi się odbywać poprzez stronę www oraz programistyczne, udokumentowane API. |  |
| Oprogramowanie musi umożliwiać monitorowanie podstawowych parametrów sprzętowych bez użycia dodatkowych agentów oraz pozostałe parametry działania systemu operacyjnego i usług za pomocą dedykowanych agentów (w zależności od konfiguracji monitorowanego hosta). |  |
| **3.** | Oferowane oprogramowanie systemu monitorowania musi śledzić parametry: |  |
| - Telnet na wybrany port - nasłuch na porcie |  |
| - Ping dostępność urządzenia |  |
| - Poprawne działanie serwera DHCP |  |
| - Poprawne działanie serwera czasu NTP |  |
| - Zajętość danych na poszczególnych partycjach |  |
| - Zajętość RAM |  |
| - Obciążenie systemu |  |
| - Obciążenie dysków |  |
| - Ilość zalogowanych użytkowników |  |
| - Ilość procesów |  |
| - Obecność procesów w systemie |  |
| - Synchronizacja dysków programowego RAID |  |
| - Synchronizacja dysków sprzętowego RAID |  |
| - Kontrola parametrów polecenia VMSTAT |  |
| - Obecność SSH |  |
| **4.** | Oferowane oprogramowanie systemu monitorowania musi śledzić parametry monitoringu systemu poczty:* Poprawne działanie serwera SMTP
* Poprawne działanie serwera POP3
* Poprawne działanie serwera IMAP
* Poprawne działanie serwera AMAVIS
* Ilość listów w kolejkach serwera Postfix
 |  |
| **5.** | Oferowane oprogramowanie systemu monitorowania musi śledzić parametry monitoringu DNS:* Poprawne działanie DNS
* Rozwiązywanie zadanych domen na adresy IP
* Parametry serwerów WWW
* Poprawne działanie serwera WWW
* Kontrola występowania oczekiwanych treści na stronie
* Czas odpowiedzi serwera WWW.
 |  |
| **6.** | Oferowane oprogramowanie systemu monitorowania musi śledzić parametry monitoringu bazy danych:* Poprawna praca bazy
* Kontrola stanu synchronizacji baz
* Zajętość przestrzeni danych
 |  |
| **7.** | Oferowane oprogramowanie systemu monitorowania musi śledzić parametry DRBD i HEARTBEAT :* Poprawne działanie klastra
 |  |
| * Poprawne działanie replikacji danych
 |  |
| **8.** | Oferowane oprogramowanie systemu monitorowania musi śledzić parametry macierzy dyskowych:* Analiza statusów ogólnych urządzenia,
* Analiza dysków urządzenia
 |  |
| **9.** | Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość tworzenia dokumentacji technicznych w systemie, możliwość zamieszczania zdjęć monitorowanych urządzeń w dokumentacji oraz opisów do nich.  |  |
| **10.** | Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość personalizacji podstawowego ekranu aplikacji w powiązaniu z użytkownikiem systemu, a także umożliwiać dowolną konfigurację składników wyświetlanych na podstawowym ekranie aplikacji poprzez wybór odpowiednich widget’ów.  |  |
| **11.** | Tworzenie i modyfikacja raportów musi być wykonywana za pośrednictwem interfejsu WWW i nie może wymagać instalacji dodatkowego oprogramowania (poza przeglądarką i ew. technologiami Java, Flash i podobnymi). Funkcjonalność tworzenia i modyfikacji raportów nie może wymagać zakupu dodatkowych licencji. |  |
| **12.** | Narzędzie raportujące musi umożliwiać automatyczną generację dowolnych raportów wg zdefiniowanego harmonogramu:* Możliwość generowania raportów dostępności (wg hostów lub usług)
* Możliwość generowania raportów SLA (wg hostów lub usług)
* Zapis raportów do plików PDF
* Okresowe wysyłanie raportów emailem do wskazanych użytkowników
* Zapis zdefiniowanych parametrów raportów celem późniejszego wywołania
 |  |
| **13.** | Oprogramowanie systemu monitorowania musi mieć możliwość grupowania monitorowanych elementów:* Możliwość grupowania hostów / usług w procesy biznesowe i monitorowania dostępności procesu jak pojedynczego elementu
* Wykonywanie operacji na grupach hostów / usług (komentarze, powiadomienia, potwierdzenia błędów, przerwy serwisowe).
 |  |
| **14.** | Oferowane oprogramowanie systemu monitorowania musi posiadać funkcje związane z bezpieczeństwem systemu:* Wbudowany mechanizm tworzenia kopii zapasowych ustawień systemu (monitorowane hosty i usługi),
* Wbudowany mechanizm zarządzania użytkownikami systemu,
 |  |
| * Możliwość tworzenia grup użytkowników,
* Mechanizm przydzielania uprawnień użytkowników (dostęp do danych nt. hostów lub usług, możliwość konfiguracji obiektów, powiadomienia).
 |  |
| **15.** | Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość globalnego wyłączania powiadomień w systemie. |  |
| **16.** | Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość rozbudowy o kolejne węzły. |  |
| **17.** | Oferowane oprogramowanie systemu monitorowania musi posiadać możliwość rozbudowy o elementy niezawodnościowe oraz elementy sond. Tak wykonana instalacja musi podlegać centralnemu zarządzaniu z poziomu interfejsu www i z poziomu jednego systemu. |  |
| **18.** | Oferowane oprogramowanie systemu monitorowania musi istnieć jako gotowy produkt komercyjny oraz być dostępne w oficjalnej dystrybucji na terenie Polski. |  |
| **19.** | Oferowane oprogramowanie systemu monitorowania musi posiadać oficjalne, nielimitowane wsparcie producenta. Nie jest akceptowalne wsparcie typu „community support”, oferowane przez społeczność jego użytkowników. |  |
| **20.** | Oferowane oprogramowanie systemu monitorowania  musi posiadać oficjalne  wsparcie na mocy współpracy z dostawcą oprogramowania, którego co najmniej pierwsza linia jest świadczona w języku polskim. |  |
| **21.** | Oprogramowanie musi być opatrzone licencją i ścieżką rozwoju producenta. |  |
| **22.** | Oprogramowanie musi umożliwiać konfigurację w zakresie pozyskiwania parametrów dotyczących aplikacji dedykowanych:1. Aktywność aplikacjiRozumiana jako bieżąca informacja która aplikacja działa a która nie. 2. Dostępność aplikacji Rozumiana jako stosunek ilości czasu w którym wybrana aplikacja jest dostępna w wybranym okresie do ilości czasu (total) w wybranym okresie. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie dostępności w ujęciu godzinowym, dziennym, tygodniowym, miesięcznym, rocznym3. Wydajność aplikacjiRozumiana jako czas odpowiedzi wybranej aplikacji, wyrażony w sekundach4. Przepustowość aplikacjiRozumiana jako ilość połączeń z aplikacją w jednostce czasu - na sekundę5. Lista użytkowników aplikacji bieżąca i historyczna w wybranym okresie czasu (miesięcznym, rocznym)6. Rozkład użytkowników aplikacji w kontekście dostępności do wybranych funkcjonalności aplikacji. Statystyka bieżąca i historyczna w wybranym okresie czasu (miesięcznym, rocznym)7. Rozkład użytkowników aplikacji w kontekście przynależności do jednostek administracyjnych8. Aktywność użytkowników aplikacji Rozumiana jako zestawienie użytkowników, aktywnie korzystających (logujących) z usługi w danym okresie. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie wartości parametru w ujęciu dziennym, tygodniowym, miesięcznym, rocznym.9. Godzinowe obciążenie aplikacjiRozumiane jako ilość połączeń z aplikacją w jednostce czasu – godzina.10. Podstawowe funkcjonalności i ich realizacja przez aplikacjeRozumiane jako zestawienie aplikacji i realizowanych przez nie funkcjonalności w kontekście biznesowym11. Zasoby sprzętowo – systemowe niezbędne do działania aplikacjiRozumiane jako zestawienie niezbędnych zasobów sprzętowo-systemowych do działania aplikacji.12. Niestandardowe zachowania aplikacjiRozumiany jako rejestr zdarzeń niestandardowego zachowania się aplikacji. Zbieranie i przechowywanie statystyk powinno pozwalać na prezentowanie wartości parametru w ujęciu dziennym, tygodniowym, miesięcznym, rocznym. 13. Incydenty i problemy zgłaszane do aplikacjiRealizacja po stronie narzędzi ITSM |  |

1. **System analizy ruchu sieciowego i wykrywania anomalii**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne oprogramowania oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1.** | System musi analizować dane statystyczne (czyli próbki ruchu, flow-y, sample) generowane przez urządzenia sieciowe różnych producentów. System musi obsługiwać co najmniej następujące formaty próbek ruchu: Netflow (wersje 5, 7, oraz 9), Sampled Netflow, IPFIX, J-Flow, sFlow, Netstream. |  |
| **2.** | System musi analizować kopię ruchu sieciowego udostępnianą przez sesje port mirroringu zdefiniowane na przełącznikach Ethernet, lub przy pomocy dedykowanych sprzętowych trapów sieciowych. |  |
| **3.** | System musi udostępniać funkcję aktywnego tworzenia próbek ruchu z analizowanej kopii ruchu sieciowego. Musi istnieć możliwość aktywnego tworzenia próbek ruchu w formatach co najmniej Netflow, J-Flow, sFlow. System musi posiadać funkcję wysyłania aktywnie tworzonych próbek ruchu do systemu NBAD tego samego producenta oraz do kolektorów innych producentów. |  |
| **4.** | System musi wykrywać nowe hosty pojawiające się w sieci teleinformatycznej. System musi zbierać i przechowywać informacje o MAC adresach komputerów oraz o przypisanych do nich adresów IPv4 i IPv6. |  |
| **5.** | System musi posiadać funkcję pobierania informacji o działających w sieci aktywnych urządzeniach przez protokół SNMP – co najmniej nazw urządzeń, listy interfejsów sieciowych z ich nazwami, opisami i prędkościami. |  |
| **6.** | System musi utrzymywać centralne repozytorium informacji o analizowanym ruchu sieciowym otrzymywanych z innych urządzeń sieciowych lub własnych komponentów. Dane muszą być przechowywane w bazie danych SQL. Musi istnieć możliwość wydawania zapytań bezpośrednio do bazy danych. |  |
| **7.** | System musi udostępniać graficzny interfejs użytkownika do przetwarzania zebranych danych, w tym wyliczania statystyk i generowania raportów. Statystyki i raporty muszą być dostępne na bieżąco w czasie rzeczywistym. |  |
| **8.** | System kolekcjonowania danych musi przechowywać informacje o czasie rozpoczęcia i zakończenia strumienia analizowanych danych z dokładnością do 1 milisekundy. |  |
| **9.** | System musi posiadać funkcje tworzenia profili i widoków analizowanych danych, aktualizowanych na bieżąco, na podstawie kryteriów zdefiniowanych przez administratora. |  |
| **10.** | System musi generować raporty pokazujące dane w formie graficznej (wykresy) jak i tabelarycznej, w oparciu o kryteria wprowadzane przez użytkowników w formie filtrów. Raporty muszą obejmować również informacje o wszystkich konwersacjach pomiędzy monitorowanymi hostami. |  |
| **11.** | System musi udostępniać statystyki obciążenia sieci przez: |  |
| ·         adresy i sieci IP (źródłowe i docelowe), |  |
| ·         aplikacje (protokoły, porty źródłowe, docelowe), |  |
| ·         klasy ruchu QoS (ToS/DSCP), |  |
| ·         systemy autonomiczne BGP (AS), |  |
| ·         kraje rozpoznawane na podstawie sieci IP (dla adresów źródłowych i docelowych) |  |
| ·         ruch z określonymi flagami TCP, |  |
| ·         protokoły IPv4 oraz IPv6. |  |
| **12.** | System musi generować raporty zgodnie z kryteriami ustalanymi przez administratorów oraz na podstawie predefiniowanych wzorców. Raport musza być tworzone w różnych formatach – minimum PDF i CSV. Użytkownik musi posiadać wpływa na układ raportu poprzez dobór ilości i rodzaju informacji, z których raport będzie się składał. |  |
| **13.** | System musi posiadać funkcję automatycznego rozwiązywania adresów IP do nazw domenowych. |  |
| **14.** | System musi posiadać funkcję nadawania nazw własnych następującym zaobserwowanym obiektom: |  |
| ·           podsieciom, |  |
| ·           aplikacjom (adresom IP i portom), |  |
| ·           systemom autonomicznym BGP (AS). |  |
| **15.** | System musi udostępniać zbiorcze dane statystyczne zawierające sumaryczną liczbę otrzymanych eksportów próbek ruchu określonego typu wysłanych przez każde z urządzeń, wraz z informacjami na temat średniej oraz szczytowej liczby otrzymywanych eksportów od każdego z urządzeń. |  |
| **16.** | System musi pozwalać na definiowania alarmów, które będą powiadamiać administratora o ruchu sieciowym (globalnym oraz z wybranych sieci, protokołów i aplikacji) przekraczającym zdefiniowane wartości progowe wyrażone w jednostkach ilości danych (pakietach oraz bajtach), a także w jednostkach prędkości transmisji (bitach/sekundę, pakietach/sekundę). |  |
| **17.** | Alarmy muszą być wysyłane przy wykorzystaniu co najmniej następujących metod: syslog, e-mail, SNMP trap, komunikaty SMS (w typ przypadku dopuszcza się możliwość integracji z zewnętrzną bramką SMS). |  |
| **18.** | System musi posiadać możliwość uruchomienia funkcji NBAD (Network Behavior Anomaly Detection). |  |
| **19.** | System musi posiadać możliwość analizy stanu i efektywności działania sieci teleinformatycznej, w tym również wykrywania sytuacji nieprawidłowych (tj. anomalii) związanych z kondycją sieci oraz stanem jej bezpieczeństwa. |  |
| **20.** | System musi posiadać możliwość wykrywania anomalii w działaniu sieci teleinformatycznej za pomocą analizy statystycznej i behawioralnej. W tym celu system musi na bieżąco budować profile normalnego stanu i zachowania sieci oraz identyfikować odchylenia od stanu normalnego – poprzez zaobserwowanie zwiększenia lub zmniejszenie natężenia ruchu sieciowego oraz przekraczanie zdefiniowanych wartości progowych. |  |
| **21.** | System musi posiadać możliwość wykrywania ataków Denial of Service i Distributed Denial of Service. |  |
| **22.** | System musi działać w architekturze standalone – kluczowe funkcje, czyli zbieranie danych, analiza zdarzeń oraz wykrywanie anomalii muszą być wykonywane na tym samym urządzeniu. |  |
| **23.** | W celu zwiększenia skalowalności systemu musi istnieć możliwość uruchomienia systemu w architekturze rozproszonej, poprzez uruchomienie funkcji zbierania danych, a także ich wstępnej analizy na dedykowanych kolektorach. |  |
| **24.** | System musi działać pod kontrolą dostrojonego przez producenta systemu operacyjnego klasy Unix. Nie jest dopuszczalne zastosowanie systemu operacyjnego klasy Microsoft Windows. |  |
| **25.** | System musi posiadać wydajność analizy nie mniej niż 100 flow próbek ruchu na sekundę. |  |
| **26.** | System musi zbierać dane z wydajnością nie mniejszą niż 75 000 próbek ruchu na sekundę (flow-ów/sekundę). System nie może posiadać ograniczeń co do liczby obsługiwanych urządzeń będących źródłami informacji. |  |
| **27.** | System musi być dostarczony jako rozwiązanie gotowe do użytku, pochodzące od jednego producenta. Nie jest dopuszczalna sytuacja, w której funkcje wymagane dla systemu realizowane są przez zestaw programów pochodzących od różnych producentów, działających na tej samej platformie sprzętowej ogólnego przeznaczenia. |  |
| **28.** | System musi być kompletny tzn. zawierać wszystkie licencje i zezwolenia, niezbędne do poprawnego funkcjonowania zgodnie z niniejszą specyfikacją, bez konieczności wnoszenia dodatkowych. |  |
| **29.** | Pełne zarządzanie systemem, analiza danych oraz raportowanie musi odbywać się poprzez graficzny interfejs użytkownika dostępny za pomocą standardowych przeglądarek WWW. Nie jest dopuszczalne zarządzanie przy pomocy dodatkowych aplikacji klienckich. |  |
| **30.** | System musi pozwalać na definiowanie kont administratorów o zróżnicowanym poziomie uprawnień w zakresie co najmniej: pełnej kontroli nad systemem, kontroli na poszczególnymi modułami funkcjonalnymi systemu, kont uprawnionych tylko do odczytu. Ponadto musi istnieć funkcja ograniczania uprawnień kont użytkowników do poszczególnych źródeł informacji (tj. urządzeń sieciowych generujących próbki ruchu) oraz do zbioru danych definiowanych na podstawie kryteriów z warstwy 3 i 4 modelu ISO. Tożsamość administratorów musi być weryfikowana w lokalnej bazie danych użytkowników, a także przy pomocy zewnętrznych serwerów uwierzytelniania – co najmniej LDAP. |  |
| **31.** | Musi być dostępna funkcja zapisywania i odtwarzania pełnej konfiguracji systemu oraz jedynie wybranych jego komponentów. Musi być dostępna funkcja wykonania kopii zapasowej systemu uwzględniającej konfigurację i ewentualne licencje. |  |
| **32.** | System musi posiadać narzędzia do: |  |
| ·           informowania o statusie systemu, zajętości pamięci, dostępności przestrzeni dyskowej, |  |
| ·           konfiguracji interfejsów sieciowych, |  |
| ·           zapisywania pełnego dziennika zdarzeń (logów) związanych z działaniem systemu i uruchomionym na nim usług. |  |

1. **Narzędzie do przechowywania, wizualizacji, wyszukiwania i analizy logów**

|  |  |  |
| --- | --- | --- |
| **ID** | **Wymaganie** | **Parametry techniczne oprogramowania oferowanego przez Wykonawcę** |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| **1** | ZBIERANIE DANYCH: |  |
| Oprogramowanie musi pozwalać na: |  |
| - zbieranie logów przesyłanych przez systemy operacyjne(Linux/Windows), urządzenia sieciowe oraz aplikacje  |  |
| - zbieranie danych przesyłanych po sieci (UDP/TCP), oprogramowanie musi rozpoznawać dane przesyłane przez syslog, ng-syslog, netflow. |  |
| - zbieranie danych ekstrahowanych z plików logów umieszczonych w wyszczególnionym katalogu na serwerze z oprogramowaniem  |  |
| - oprogramowanie musi być uzupełnione programami klienckimi przeznaczonymi na aktualne wersje systemów operacyjnych z rodziny Linux i z rodziny Windows, które można konfigurować na okoliczność zbierania danych o stanie i zdarzeniach występujących w danym systemie operacyjnym |  |
| - oprogramowanie musi być przygotowane na odbiór, indeksowanie i przetwarzanie nielimitowanej liczby zdarzeń w ramach wydajności pojedynczego serwera na którym pracuje |  |
| **2** | PRZECHOWYWANIE i PARSOWANIE DANYCH: |  |
| Oprogramowane musi : |  |
| - posiadać wbudowany mechanizm kompresji przechowywanych danych |  |
| - pozwalać na uniwersalne parsowanie przesyłanych danych |  |
| - pozwalać na pracę z logami zdarzeń jednolinijkowych oraz wielolinikowych  |  |
| - pozwalać na rozpoznanie formatów czasu i daty, i normalizowanie ich do jednego wspólnego formatu  |  |
| Oprogramowanie musi umożliwiać operatorowi oprogramowania samodzielne konfigurowanie parsowania nieznanych formatów logów w celu umożliwienia analizy zebranych w nich informacji przez opisywane oprogramowanie. |  |
| **3** | PRZESZUKIWANIE ZEBRANYCH DANYCH |  |
| Oprogramowanie musi być obsługiwane z poziomu przeglądarki. |  |
| Oprogramowanie musi pozwalać na wyszukiwanie w całym zgromadzonym przez nie zbiorze danych. |  |
| Oprogramowanie musi pozwalać na równoległe wyszukiwanie, z poziomu jednego interfejsu graficznego, w danych napływających w czasie rzeczywistym i danych historycznych. |  |
| Oprogramowanie musi pozwalać na użycie operatorów boolowskich, wzorców, wyrażeń regularnych (REGEX) do przeszukiwania danych. |  |
| Oprogramowanie musi pozwalać na przeszukiwania w ograniczonym zbiorze danych ( np. ze względu na zakres dat wystąpienia). |  |
| Oprogramowanie musi wraz z wyświetleniem wyszukiwanych wyników przedstawiać na tym samym ekranie związaną z tym wyszukiwaniem statystykę ilościową w dziedzinie czasu. |  |
| Oprogramowanie musi pozwalać na oznaczanie ( tag ) i korelacje danych ( pod kątem dowolnej z przechowywanych wartości ) bez względu na źródło tych danych. |  |
| Oprogramowanie wraz z prezentacją (wykres, tabela) zestawień zbiorczych, statystycznych itd. musi pozwalać na obejrzenie danych źródłowych w ich oryginalnym formacie (logi) na podstawie których powstała ta prezentacja. |  |
| Oprogramowanie musi pozwalać na geolokalizację zdarzeń na bazie adresów IP oraz umożliwiać jej wizualizacje na mapie. |  |
| Musi istnieć możliwość wyszukiwania na podstawie jednoczesnego wykorzystania więcej niż jednego zdefiniowanego wzorca wyszukiwania. |  |
| Musi istnieć możliwość zapisania wyników wyszukiwania i tworzenia z nich raportów. |  |
| Oprogramowanie musi oferować także udokumentowany interfejs programistyczny (API) służący do przeszukiwania danych gromadzonych w czasie rzeczywistym oraz danych historycznych. |  |
| Oprogramowanie musi oferować pełne sterowanie pracą dziennika zdarzeń poprzez API. |  |
| **4** | Eksport danych |  |
| Oprogramowanie musi pozwalać na eksport wyszukanych danych do formaty CSV. |  |
| **5** | RAPORTOWANIE |  |
| Oprogramowanie musi dawać : |  |
| - możliwość tworzenia raportów z predefiniowanych wyszukiwań w postaci tabelarycznej i graficznej ( minimum 3 typy wykresów (line, bar, pie).  |  |
| - możliwość równoległego użycia wielu predefiniowanych wyszukiwań w celu opracowania raportu. |  |
| **6** | GLOWNY INTERFEJS OPROGRAMOWANIA |  |
| Oferowana przez oprogramowanie strona www musi być zabezpieczona hasłem |  |
| Oprogramowanie musi wspierać pracę wielu użytkowników, posiadających własne loginy i hasła |  |
| Oprogramowanie musi posiadać dedykowany widok zarządzania użytkownikami. |  |
| Oprogramowanie musi udostępniać funkcjonalność podziału uprawnień pomiędzy użytkownikami, co pozwoli na ograniczenie dostępu użytkowników do poszczególnych zgromadzonych danych. W systemie musi być wprowadzony mechanizm bezpieczeństwa który kontroluje jaki użytkownik ma dostęp do jakiego fragmentu danych. Mechanizm konfiguracji uprawnień musi być dostępny w poziomu www aplikacji jak i z API. |  |
| **7** | INTEGRACJA Z IT TOOLS |  |
| Oprogramowanie musi udostępniać API pozwalające na integracje z innymi narzędziami służącymi do zarządzania i analizy danych |  |
| **8** | SKALOWALNOŚĆ  |  |
| Oprogramowanie musi być dostarczone wraz z wszystkimi komponentami koniecznymi do jego uruchomienia, działania i bezterminowego korzystania z wszystkich wymienionych |  |
| i opisanych w tym dokumencie funkcjonalności. |  |
| W przypadku istnienia ograniczenia licencyjnego na ilość agentów Zamawiający wymaga licencji umożliwiającej ciągłe zbieranie danych z minimum 20000 agentów. |  |
| Oprogramowanie musi posiadać funkcjonalność skalowania infrastruktury co w momencie zakupu dodatkowych licencji pozwoli na obsługę większej porcji ruchu. W systemie musi istnieć mechanizm dodawania nowych węzłów pozwalających na zwiększenie wydajności dziennika.  |  |
| Oprogramowanie musi posiadać opcję pracy klastrowej w celu zabezpieczenia danych przed utratą w momencie uszkodzenia jednego węzła. |  |
| **9** | ZABEZPIECZENIE DOSTĘPU  |  |
| Dostęp do oprogramowania musi być zabezpieczony hasłem.. |  |
| Oprogramowanie musi pozwalać na zabezpieczenie dostępu z poziomu operatora i użytkownika oprogramowania za pomocą protokołu HTTPS. |  |
| Oprogramowanie musi zapewniać kontrolę dostępu do gromadzonych danych bazującą na metodzie RBAC (Role Based Access Control). |  |

1. **Oprogramowanie komputerowe:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Typ oprogramowania** | **Liczba sztuk** | **Minimalne wymagane oprogramowanie** | **Oprogramowanie oferowane** |
|  | Oprogramowanie do wirtualizacji serwerów | licencje na 28 procesorów | VMware vSphere Enterprise plus lub równoważny |  |
|  | Oprogramowanie do wirtualizacji sieci | licencje na 112 procesorów | Wirtulizacja warstwy sieciowej dla VMware vSphere Enterprise plus |  |
|  | System operacyjny | licencje na 26 dostarczanych serwerów blade | MS Windows Server lub równoważny |  |
|  | Oprogramowanie do ochrony antywirusowej | licencje na 28 procesorów | Trend Micro Deep Security - Anti-malware lub równoważny |  |
|  | Oprogramowanie wykonywania kopii zapasowej środowiska wirtualizacji | licencje na oprogramowanie do wykonywania kopii bezpieczeństwa posiadanego przez Zamawiającego środowiska wirtualizacji VMware vSphere Enterprise plus na 40 procesorów fizycznych hostów ESX. | Oprogramowanie do wykonywania kopii bezpieczeństwa posiadanego przez Zamawiającego środowiska wirtualizacji VMware vSphere Enterprise plus na 40 procesorów fizycznych hostów ESX. |  |
|  | Oprogramowanie do centralnego zarządzania urządzeniami sieciowymi | Według wymagań określonych w OPZ | Oprogramowanie do centralnego zarządzania następującymi urządzeniami sieciowymi, wyspecyfikowanymi w OPZ: Przełącznik Data Center LAN typu SPINE, Przełącznik Data Center LAN typu LEAF, Router BGP, Przełącznik LAN typu Top of the Rack, Przełącznik Koncentrujący Top of the Rack, Firewall Data Center |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_2017 r.

..................................................................

(podpis i pieczęć Wykonawcy)