**ARCHITEKTURA REFERENCYJNA**

**ŚRODOWISKA IT CPD MF**

**Załącznik C – Standardy parametrów technicznych urządzeń teleinformatycznych**

# Standardy parametrów technicznych dla urządzeń teleinformatycznych

## Wartości progowe parametrów technicznych, funkcjonalnych i niefunkcjonalnych komponentów

Rozdział zawiera zestawienie parametrów technicznych funkcjonalnych i niefunkcjonalnych dla poszczególnych komponentów.

Każdy komponent opatrzono nagłówkiem zawierającym informacje o klasach systemów informatycznych oraz klasach bezpieczeństwa, w których ten komponent może być wykorzystany. Przypisanie komponentu do odpowiedniej klasy bezpieczeństwa nie oznacza w tym przypadku, iż komponent dostarcza mechanizmy właściwe dla tej klasy – oznacza jedynie, że może on być użyty w systemach tej klasy.

Poniższa tabela zawiera indeks wszystkich komponentów, wraz z ich identyfikatorami. Identyfikatory są równoznaczne z pojęciem „kod komponentu”, stosowanym zamiennie w innych produktach zadań architektonicznych SPKiCSCP.

| Identyfikator | Komponent |
| --- | --- |
| **C.PSR.R.X86** | **Serwery stelażowe x86–64** |
| C.PSR.R.X86.1 | [Serwer stelażowy x86-64, 36 cCPU.](#C_PSR_R_X86_4) |
| [C.PSR.R.X86.](#C_PSR_R_X86_6)2 | [Serwer stelażowy x86-64, 72 cCPU.](#C_PSR_R_X86_6) |
| [C.PSR.R.X86.](#C_PSR_R_X86_6)3 | [Serwer stelażowy x86-64, 24 cCPU.](#C_PSR_R_X86_6) |
|  |  |
| **C.PSR.B.X86** | **Serwery kasetowe x86–64** |
| [C.PSR.B.X86.](#C_PSR_B_X86_4)1 | [Serwer kasetowy x86-64, 36 cCPU.](#C_PSR_B_X86_4) |
|  |  |
| **C.PSR** | **Komponenty dodatkowe infrastruktury serwerowej** |
| [C.PSR.B.IA](#C_PSR_B_IA) | [Infrastruktura dla serwerów kasetowych](#C_PSR_B_IA) |
| [C.PSR.B.MGT](#C_PSR_B_MGT) | [Zarządzanie infrastrukturą serwerów kasetowych](#C_PSR_B_MGT) |
| [C.PSR.BR.RCK](#C_PSR_BR_RCK) | [Szafa stelażowa](#C_PSR_BR_RCK) |
| [C.PSR.BR.PDU](#C_PSR_BR_PDU) | [Listwa dystrybucyjna zasilania (PDU) w szafie stelażowej](#C_PSR_BR_PDU) |
| [C.PSR.BR.KVM](#C_PSR_BR_KVM) | [Konsola zarządzania serwerami w szafie stelażowej](#C_PSR_BR_KVM) |
|  |  |
| **C.STO** | **Macierze i biblioteki** |
| C.STO.UNI | [Macierz dyskowa typ 1](#_Macierz_dyskowa_typ) |
| C.STO.UNI2 | [Macierz dyskowa typ 2](#_Macierz_dyskowa_typ_1) |
| C.STO.FLS | [Macierz dyskowa flash](#_Macierz_dyskowa_) |
| C.STO.NAS | [Macierz dyskowa NAS](#_Macierz_dyskowa__1) |
| C.STO.VRT | [Wirtualizator macierzy dyskowych](#_Wirtualizator_macierzy_dyskowych.) |
| [C.STO.VLB](#C_STO_VLB) | [Biblioteka wirtualna.](#C_STO_VLB) |
| [C.STO.TLB](#C_STO_TLB) | [Biblioteka taśmowa.](#C_STO_TLB) |
|  |  |
| **C.SAN** | **Urządzenia SAN** |
| [C.SAN.SW.1](#C_SAN_SW_1) | [Przełączniki SAN w szkielecie komunikacyjnym](#C_SAN_SW_1) |
| [C.SAN.SW.2](#C_SAN_SW_2) | [Przełączniki SAN w lokalnym węźle rdzeniowym](#C_SAN_SW_2) |
|  |  |
| **C.LAN** | **Urządzenia LAN** |
| [C.LAN.SW.1](#C_LAN_SW_1) | [Przełączniki rdzeniowe LAN](#C_LAN_SW_1) |
| [C.LAN.SW.2](#C_LAN_SW_2) | [Przełączniki dystrybucyjne - LAN/WAN](#C_LAN_SW_2) |
| [C.LAN.SW.5](#C_LAN_SW_5) | [Przełączniki dystrybucyjne - bramka Internetowa](#C_LAN_SW_5) |
| [C.LAN.SW.3](#C_LAN_SW_3) | [Przełączniki dostępowe LAN - 48 portów](#C_LAN_SW_3) |
| [C.LAN.SW.4](#C_LAN_SW_4) | [Przełączniki dostępowe LAN - 24 porty](#C_LAN_SW_4) |
| C.LAN.SW.6 | Przełączniki dostępowy Top Of the Rack |
| [C.LAN.FW.1](#C_LAN_FW_1) | [Zapory sieciowe - typ 1](#C_LAN_FW_1) |
| [C.LAN.FW.2](#C_LAN_FW_2) | [Zapory sieciowe - typ 2](#C_LAN_FW_2) |
| C.LAN.FW.3 | Zapory sieciowe – typ 3 |
| [C.LAN.LB.1](#C_LAN_LB_1) | [Urządzenia równoważące ruch sieciowy - typ 1](#C_LAN_LB_1) |
| [C.LAN.LB.2](#C_LAN_LB_2) | [Urządzenia równoważące ruch sieciowy - typ 2](#C_LAN_LB_2) |
| [C.LAN.LB.3](#C_LAN_LB_3) | [Urządzenia równoważące ruch sieciowy - typ 3](#C_LAN_LB_3) |
| C.LAN.LB.4 | Urządzenia równoważące ruch sieciowy - typ 4 |
| [C.LAN.RT](#C_LAN_RT) | [Rutery](#C_LAN_RT) |
| [C.LAN.IPS](#C_LAN_IPS) | [System IPS](#C_LAN_IPS) |
| [C.LAN.SPM](#C_LAN_SPM) | [Badanie zawartości poczty elektronicznej](#C_LAN_SPM) |
| [C.LAN.VUL](#C_LAN_VUL) | [Badające podatności środowiska teleinformatycznego](#C_LAN_VUL) |
| [C.LAN.HSM.1](#C_LAN_HSM_1) | [Urządzenia do ochrony kluczy kryptograficznych - Ethernet](#C_LAN_HSM_1) |
| [C.LAN.HSM.2](#C_LAN_HSM_2) | [Urządzenia do ochrony kluczy kryptograficznych - PCI](#C_LAN_HSM_2) |
| [C.LAN.HSM.3](#C_LAN_HSM_3) | [Urządzenia do ochrony kluczy kryptograficznych – Root CA](#C_LAN_HSM_3) |
|  |  |
| **C.PRT** | **System wydruków** |
| [C.PRT.PDEV.1](#C_PRT_PDEV_1) | [Monochromatyczne urządzenie drukująco-kopiujące A4 typu Grupa Robocza](#C_PRT_PDEV_1) |
| [C.PRT.PDEV.2](#C_PRT_PDEV_2) | [Monochromatyczne urządzenie drukująco-kopiujące formatu A3 typu Departament](#C_PRT_PDEV_2) |
| [C.PRT.PDEV.3](#C_PRT_PDEV_3) | [Kolorowe urządzenie drukująco-kopiujące formatu A4 typu Grupa Robocza](#C_PRT_PDEV_3) |
| [C.PRT.PDEV.4](#C_PRT_PDEV_4) | [Kolorowe urządzenie drukująco-kopiujące formatu A3 typu Departament](#C_PRT_PDEV_4) |
| [C.PRT.PDEV.5](#C_PRT_PDEV_5) | [Drukarka monochromatyczna A4 typu Grupa Robocza](#C_PRT_PDEV_5) |
| [C.PRT.PDEV.6](#C_PRT_PDEV_6) | [Drukarka monochromatyczna A4 typu Departament](#C_PRT_PDEV_6) |
| [C.PRT.SW.MGMT](#C_PRT_SW_MGMT) | [Aplikacja zarządzająca urządzeniami drukującymi oraz drukująco-kopiującymi](#C_PRT_SW_MGMT) |
| [C.PRT.SW.ACNT](#C_PRT_SW_ACNT) | [Aplikacja do rozliczania kosztów wydruków](#C_PRT_SW_ACNT) |
|  |  |
| **C.CL** | **Oprogramowanie klastrowe** |
| C.CL.HA | Oprogramowanie klastrowe HA |
| [C.CL.HA.1](#C_CL_HA_1) | [Oprogramowanie klastrowe – typ 1](#C_CL_HA_1) |
| [C.CL.HA.5](#C_CL_HA_5) | [Oprogramowanie klastrowe – typ 2](#C_CL_HA_5) |
| [C.CL.HA.7](#C_CL_HA_7) | [Oprogramowanie klastrowe – typ 3](#C_CL_HA_7) |
| [C.CL.HA.8](#C_CL_HA_8) | [Oprogramowanie klastrowe – typ 4](#C_CL_HA_8) |
| [C.CL.HA.9](#C_CL_HA_9) | [Oprogramowanie klastrowe – typ 5](#C_CL_HA_9) |
| [C.CL.HA.11](#C_CL_HA_11) | [Oprogramowanie klastrowe – typ 6](#C_CL_HA_11) |
|  |  |
| C.CL.HEF | Oprogramowanie klastrowe wydajnościowe |
| [C.CL.HEF.RAC](#C_CL_HEF_RAC) | [Oprogramowanie klastrowe wydajnościowe – typ 1](#C_CL_HEF_RAC) |
| [C.CL.HEF.SYB](#C_CL_HEF_SYB) | [Oprogramowanie klastrowe wydajnościowe – typ 2](#C_CL_HEF_SYB) |
| [C.CL.HEF.DBX](#C_CL_HEF_DBX) | [Oprogramowanie klastrowe wydajnościowe – typ 3](#C_CL_HEF_DBX) |

### Serwery stelażowe i kasetowe

Dla wszystkich oferowanych serwerów stelażowych i kasetowych:

* Oferowany sprzęt musi; być nieużywany i fabrycznie nowy, pochodzić z seryjnej produkcji z uwzględnieniem opcji konfiguracyjnych przewidzianych przez Producenta dla oferowanego modelu sprzętu, pochodzić z oficjalnego kanału dystrybucji Producenta na rynek polski. Zamawiający nie dopuszcza oferowania sprzętu będącego prototypem.
* Wszystkie porty znajdujące się w kartach FC oraz LAN zainstalowanych w serwerach muszą być wyposażone we wkładki umożliwiające podłączenie do infrastruktury sieci LAN oraz SAN
* Wszystkie procesory jak i rdzenie procesorowe zainstalowane w serwerze muszą być aktywne i dostarczone z aktywnymi licencjami dla systemu operacyjnego oraz oprogramowania dodatkowego.
* Wymaga się, aby oferowana konfiguracja była zgodna, co do modelu serwera, modelu procesora, jego częstotliwości, wielkości pamięci L3 cache z konfiguracją serwera, dla której przeprowadzono test „SPECint\_rate2006 Baseline” potwierdzony przez organizację SPEC ([www.spec.org](http://www.spec.org/))..
* Liczba procesorów w serwerze, dla którego przeprowadzono test „SPECint\_rate2006 Baseline” musi być równa bądź większa niż ta, która jest wymagana przez Zamawiającego.
* W przypadku, gdy wynik przeprowadzonego testu „SPECint\_rate2006 Baseline” dotyczy większej liczby procesorów fizycznych niż w oferowanej konfiguracji, Oferent musi przeliczyć i podać wydajność zgodnie ze wzorem:

*N*

*N*

W

W

*proc*

*test*

*proc*

*ofer*

*ofic*

*sz*

\_

\_



gdzie:

Wsz - jest wynikiem przeliczenia wydajności oferowanej konfiguracji,

Wofic - jest oficjalnym wynikiem testu potwierdzonym przez organizację SPEC ([www.spec.org](http://www.spec.org/))

Nofer\_proc - jest liczbą procesorów w oferowanej konfiguracji,

Ntest\_proc - jest liczbą procesorów użytych w oficjalnym teście, na podstawie którego dokonywane jest przeliczenie,

* Zarządzanie i obsługa techniczna:

- Serwer musi być wyposażony w dedykowaną kartę zdalnego zarządzania (konsoli) niezależną od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port RJ-45 1 Gb/s pozwalającej na:

- włączenie, wyłączenie i restart serwera,

- podgląd logów sprzętowych serwera i karty,

- przejęcie zdalnej konsoli graficznej i podłączanie wirtualnych napędów CD/DVD/ISO i FDD bez konieczności dokładania elementów sprzętowych,

- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera, ),

- szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika,

- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer,

- integracja z usługą katalogową MS Active Directory,

- możliwość obsługi przez dwóch administratorów jednocześnie,

- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej

- Oferowany serwer musi być dostarczony i zapewniać pełną integrację z oprogramowaniem do centralnego zarządzania serwerami rack umożliwiające:

- monitoring stanu serwera i jego komponentów – procesory, dyski, pamięć, karty sieciowe itp.,

- wykrywanie i komunikacji z kartą zdalnego zarządzania,

- inwentaryzację serwera – informacja o konfiguracji serwera, numerze seryjnym, numerze produktu (komponentu),

- zarządzanie wieloma serwerami z jednej konsoli z podziałem na grupy bez udziału dedykowanego agenta , funkcjonalne wg. minimum kategorii lokalizacji maszyny oraz grupy funkcyjnej,

- równoczesne zarządzanie wieloma alarmami na serwerach,

- zarządzanie i aktualizację oprogramowania firmware centralne dla wielu serwerów,

- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram

- Możliwość eksportu raportu co najmniej do CSV lub HTML lub XLS

- Szybki podgląd stanu środowiska

- Podsumowanie stanu dla każdego urządzenia

- Szczegółowy status urządzenia/elementu/komponentu,

- Generowanie alertów przy zmianie stanu urządzenia,

- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń,

- Możliwość przejęcia zdalnego pulpitu,

- Możliwość podmontowania wirtualnego napędu CD/DVD/ISO i FDD bez konieczności dokładania elementów sprzętowych

- Możliwość definiowania ról administratorów

- Możliwość zdalnej aktualizacji sterowników i oprogramowania wewnętrznego serwerów,

- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów,

- automatyczne przywracanie ustawień serwera,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) zapisanych na karcie zarządzającej

### Serwery stelażowe x86-64

#### Serwer stelażowy x86-64, 36 cCPU

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.R.X86.1 |
| **Nazwa** | Serwer stelażowy x86-64, 36 cCPU |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

|  |  |  |
| --- | --- | --- |
| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| Obudowa | Wysokość maksymalnie 2U, przystosowana do montażu w szafie stelażowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie stelażowej) |  |
| Procesor | Minimum dwa procesory osiemnastordzeniowe, osiągające w testach „SPECint\_rate2006 Baseline” wynik nie gorszy niż określony przez atrybuty „WYNIK\_SPECINT\_RATE\_BASELINE” (dla konfiguracji serwera z dwoma procesorami osiemnastordzeniowymi). Wynik testu musi być potwierdzony przez organizację SPEC (www.spec.org). | WYNIK\_SPECINT\_RATE\_BASELINE – [pkt] = **1330** |
| Pamięć operacyjna | Minimum określone przez atrybut „MINIMUM\_RAM\_SIZE” z ochrona pamięci ECC. Pamięci w oferowanej konfiguracji muszą pracować z prędkością taktowania nie niższą niż określona przez atrybut „MINIMUM\_FREQ\_RATE”. Serwer musi umożliwiać rozbudowę pamięci. Serwer musi posiadać co najmniej ilość gniazd pamięci określonych atrybutem MINIMUM\_RAM\_SLOT. | MINIMUM\_RAM\_SIZE – [GB] = **768 GB** MINIMUM\_FREQ\_RATE – [MHZ] = **1866 MHz**  MINIMUM\_RAM\_SLOT – [szt.] = **24** |
| Gniazda rozszerzeń | Co najmniej 7 gniazd PCI Express generacji 3 w tym minimum jedno gniazdo PCI Express generacji 3 o prędkości x16 pełnej długości i wysokości. Dla jednego z powyższych gniazd dopuszczalne jest zastosowanie dedykowanego złącza umożliwiającego instalację karty pracującej w technologii PCI Express generacji 3. |  |
| Dysk twardy | Możliwość instalacji minimum 8 dysków SAS 2.5" Hot Plug, w wewnętrznych kieszeniach serwera. Zainstalowane minimum 2 dyski minimum 300 GB 6 Gb SAS 10K RPM SFF HDD oraz 2 klucze USB lub zamiast kluczy USB 2 karty SD działające w trybie mirror w obudowie serwera. |  |
| Kontroler | Kontroler macierzowy SAS w wersji min. 3.0 wyposażony w pamięć cache minimum 2048 MB oraz mechanizm podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy RAID 0/1/1+0 (10)/5/6/50/60. |  |
| Napęd optyczny | Wewnętrzny lub zewnętrznyDVD-ROM. |  |
| Karty sieciowe | Minimum określone przez atrybut „MINIMUM\_ONBOARD\_ETH\_PORT” porty pracujące z prędkością określoną przez atrybut „MINIMUM\_ONBOARD\_ETH\_SPEED” zintegrowane z płytą główną oraz określone przez atrybut „MINIMUM\_EXT\_ETH\_PORT” porty pracujące z prędkością określoną przez atrybut „MINIMUM\_EXT\_ETH\_SPEED” typu SFP+ obsługiwane przez co najmniej określone przez atrybut „MINIMUM\_EXT\_ETH\_CARD” niezależne wymienne kontrolery PCI.  Wsparcie dla technologii VMQ (obsługa głębokości kolejki min. 100) oraz NetQueue. | MINIMUM\_ONBOARD\_ETH\_PORT – [szt.] = **2** MINIMUM\_ONBOARD\_ETH\_SPEED – [Gb/s] = **1 Gb/s** MINIMUM\_EXT\_ETH\_CARD – [szt.] = **2**  MINIMUM\_EXT\_ETH\_PORT – [szt.] = **4**  MINIMUM\_EXT\_ETH\_SPEED – [Gb/s] = **10 Gb/s** |
| Karty FC | Zainstalowane minimum określone przez atrybut „MINIMUM\_EXT\_FC\_CARD” wymienne karty FC z określonymi przez atrybut „MINIMUM\_EXT\_FC\_PORT” portami pracującymi z prędkością minimum określoną przez atrybut „MINIMUM\_EXT\_FC\_SPEED “, możliwość dołożenia trzeciej dwuportowej karty FC minimum 16 Gb/s w serwerze. | MINIMUM\_EXT\_FC\_CARD – [szt.] = 2  MINIMUM\_EXT\_FC\_PORT – [szt.] = 4  MINIMUM\_EXT\_FC\_SPEED - Gb/s = **16 Gb/s** |
| Karta graficzna | Zintegrowana karta graficzna. |  |
| Porty | Minimum 1 dodatkowy port RJ-45 dedykowany dla interfejsu zdalnego zarządzania, minimum 4 x USB 2.0, minimum 1 x VGA. |  |
| Zasilacz | Minimum dwa zasilacze hot-plug, zapewniające redundancję zasilania na poziomie N+N. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego serwera, przy zachowaniu jego pełnych możliwości operacyjnych. |  |
| Chłodzenie | Zestaw wentylatorów zapewniających redundantne chłodzenie serwera, typu hot-plug. |  |
| Wspierane systemy operacyjne | MS Windows 2012 R2, Red Hat Enterprise Linux 7.1, SUSE Linux Enterprise Server 12, VMware ESX 6.0 |  |

#### Serwer stelażowy x86-64, 72 cCPU

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.R.X86.2 |
| **Nazwa** | Serwer stelażowy x86-64, 72 cCPU |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

|  |  |  |
| --- | --- | --- |
| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| Obudowa | Wysokość maksymalnie 4U, przystosowana do montażu w szafie stelażowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie stelażowej) |  |
| Procesor | Minimum cztery procesory osiemnastordzeniowe, osiągające w testach „SPECint\_rate2006 Baseline” wynik wynik nie gorszy niż określony przez atrybuty „WYNIK\_SPECINT\_RATE\_BASELINE” (dla konfiguracji serwera z czteroma procesorami osiemnastordzeniowymi). Wynik testu musi być potwierdzony przez organizację SPEC (www.spec.org). | WYNIK\_SPECINT\_RATE\_BASELINE – [pkt] = **2740** |
| Pamięć operacyjna | Minimum określone przez atrybut „MINIMUM\_RAM\_SIZE” z ochrona pamięci ECC. Pamięci w oferowanej konfiguracji muszą pracować z prędkością taktowania nie niższą niż określona przez atrybut „MINIMUM\_FREQ\_RATE”. Serwer musi umożliwiać rozbudowę pamięci. Serwer musi posiadać co najmniej ilość gniazd pamięci określonych atrybutem MINIMUM\_RAM\_SLOT. | MINIMUM\_RAM\_SIZE – [GB] = **3072** MINIMUM\_FREQ\_RATE – [MHZ] = **1866 MHz**  MINIMUM\_RAM\_SLOT – [szt.] = **96** |
| Gniazda rozszerzeń | Łącznie minimum 8 gniazd PCI Express trzeciej generacji z możliwością rozbudowania do 10 gniazd PCI Express trzeciej generacji w tym minimum dwa gniazda o prędkości x8 oraz minimum 4 gniazda o prędkości x16. Dla jednego z powyższych gniazd dopuszczalne jest zastosowanie dedykowanego złącza umożliwiającego instalację karty pracującej w technologii PCI Express generacji 3. |  |
| Dysk twardy | Możliwość instalacji minimum ~~20~~ 10 dysków SAS 2.5" Hot Plug, w wewnętrznych kieszeniach serwera. Zainstalowane minimum 2 dyski minimum 300 GB 6 Gb SAS 10K RPM SFF HDD oraz 2 klucze USB lub zamiast kluczy USB 2 karty SD działające w trybie mirror w obudowie serwera. |  |
| Kontroler | Kontroler macierzowy SAS w wersji min. 3.0 wyposażony w pamięć cache minimum 2048 MB oraz mechanizm podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy RAID 0/1/1+0 (10)/5/6/50/60. |  |
| Napęd optyczny | Wewnętrzny lub zewnętrznyDVD-ROM. |  |
| Karty sieciowe | Minimum określone przez atrybut „MINIMUM\_ONBOARD\_ETH\_PORT” porty pracujące z prędkością określoną przez atrybut „MINIMUM\_ONBOARD\_ETH\_SPEED” zintegrowane z płytą główną oraz określone przez atrybut „MINIMUM\_EXT\_ETH\_PORT” porty pracujące z prędkością określoną przez atrybut „MINIMUM\_EXT\_ETH\_SPEED” typu SFP+ obsługiwane przez co najmniej określone przez atrybut „MINIMUM\_EXT\_ETH\_CARD” niezależne wymienne kontrolery PCI.  Wsparcie dla technologii VMQ (obsługa głębokości kolejki min. 100) oraz NetQueue. | MINIMUM\_ONBOARD\_ETH\_PORT – [szt.] = **2** MINIMUM\_ONBOARD\_ETH\_SPEED – [Gb/s] = **1 Gb/s** MINIMUM\_EXT\_ETH\_CARD – [szt.] = **2**  MINIMUM\_EXT\_ETH\_PORT – [szt.] = **8**  MINIMUM\_EXT\_ETH\_SPEED – [Gb/s] = **10 Gb/s** |
| Karty FC | Zainstalowane minimum określone przez atrybut „MINIMUM\_EXT\_FC\_CARD” wymienne karty FC z określonymi przez atrybut „MINIMUM\_EXT\_FC\_PORT” portami pracującymi z prędkością minimum określoną przez atrybut „MINIMUM\_EXT\_FC\_SPEED “, możliwość dołożenia trzeciej dwuportowej karty FC minimum 16 Gb/s w serwerze. | MINIMUM\_EXT\_FC\_CARD – [szt.] = 2  MINIMUM\_EXT\_FC\_PORT – [szt.] = 8  MINIMUM\_EXT\_FC\_SPEED - Gb/s = **16 Gb/s** |
| Karta graficzna | Zintegrowana karta graficzna. |  |
| Porty | Minimum 1 dodatkowy port RJ-45 dedykowany dla interfejsu zdalnego zarządzania, minimum 4 x USB 2.0, minimum 1 x VGA. |  |
| Zasilacz | Minimum cztery zasilacze hot-plug, zapewniające redundancję zasilania na poziomie N+N. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego serwera, przy zachowaniu jego pełnych możliwości operacyjnych. |  |
| Chłodzenie | Zestaw wentylatorów zapewniających redundantne chłodzenie serwera, typu hot-plug. |  |
| Wspierane systemy operacyjne | MS Windows 2012 R2, Red Hat Enterprise Linux 7.1, SUSE Linux Enterprise Server 12, VMware ESX 6.0 |  |

#### Serwer stelażowy x86-64, 24 cCPU

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.R.X86.3 |
| **Nazwa** | Serwer stelażowy x86-64, 24 cCPU |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

|  |  |  |
| --- | --- | --- |
| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| Obudowa | Wysokość maksymalnie 2U, przystosowana do montażu w szafie stelażowej 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w oferowanej szafie stelażowej) |  |
| Procesor | Minimum dwa procesory dwunastordzeniowe, osiągające w testach „SPECint\_rate2006 Baseline” wynik nie gorszy niż określony przez atrybuty „WYNIK\_SPECINT\_RATE\_BASELINE” (dla konfiguracji serwera z dwoma procesorami osiemnastordzeniowymi). Wynik testu musi być potwierdzony przez organizację SPEC (www.spec.org). | WYNIK\_SPECINT\_RATE\_BASELINE – [pkt] = **1060** |
| Pamięć operacyjna | Minimum określone przez atrybut „MINIMUM\_RAM\_SIZE” z ochrona pamięci ECC. Pamięci w oferowanej konfiguracji muszą pracować z prędkością taktowania nie niższą niż określona przez atrybut „MINIMUM\_FREQ\_RATE”. Serwer musi umożliwiać rozbudowę pamięci. Serwer musi posiadać co najmniej ilość gniazd pamięci określonych atrybutem MINIMUM\_RAM\_SLOT. | MINIMUM\_RAM\_SIZE – [GB] = **768** MINIMUM\_FREQ\_RATE – [MHZ] = **1866**  MINIMUM\_RAM\_SLOT – [szt.] = **24** |
| Gniazda rozszerzeń | Co najmniej 7 gniazd PCI Express generacji 3 w tym minimum jedno gniazdo PCI Express generacji 3 o prędkości x16 pełnej długości i wysokości. Dla jednego z powyższych gniazd dopuszczalne jest zastosowanie dedykowanego złącza umożliwiającego instalację karty pracującej w technologii PCI Express generacji 3. |  |
| Dysk twardy | Możliwość instalacji minimum 8 dysków SAS 2.5" Hot Plug, w wewnętrznych kieszeniach serwera. Zainstalowane minimum 2 dyski minimum 300 GB 6 Gb SAS 10K RPM SFF HDD oraz 2 klucze USB lub zamiast kluczy USB 2 karty SD działające w trybie mirror w obudowie serwera. |  |
| Kontroler | Kontroler macierzowy SAS w wersji min. 3.0 wyposażony w pamięć cache minimum 2048 MB oraz mechanizm podtrzymywania zawartości pamięci cache w razie braku zasilania, obsługujący poziomy RAID 0/1/1+0 (10)/5/6/50/60. |  |
| Napęd optyczny | Wewnętrzny lub zewnętrznyDVD-ROM. |  |
| Karty sieciowe | Minimum określone przez atrybut „MINIMUM\_ONBOARD\_ETH\_PORT” porty pracujące z prędkością określoną przez atrybut „MINIMUM\_ONBOARD\_ETH\_SPEED” zintegrowane z płytą główną oraz określone przez atrybut „MINIMUM\_EXT\_ETH\_PORT” porty pracujące z prędkością określoną przez atrybut „MINIMUM\_EXT\_ETH\_SPEED” typu SFP+ obsługiwane przez co najmniej określone przez atrybut „MINIMUM\_EXT\_ETH\_CARD” niezależne wymienne kontrolery PCI.  Wsparcie dla technologii VMQ (obsługa głębokości kolejki min. 100) oraz NetQueue. | MINIMUM\_ONBOARD\_ETH\_PORT – [szt.] = **2** MINIMUM\_ONBOARD\_ETH\_SPEED – [Gb/s] = **1 Gb/s** MINIMUM\_EXT\_ETH\_CARD – [szt.] = **2**  MINIMUM\_EXT\_ETH\_PORT – [szt.] = **4**  MINIMUM\_EXT\_ETH\_SPEED – [Gb/s] = **10 Gb/s** |
| Karty FC | Zainstalowane minimum określone przez atrybut „MINIMUM\_EXT\_FC\_CARD” wymienne karty FC z określonymi przez atrybut „MINIMUM\_EXT\_FC\_PORT” portami pracującymi z prędkością minimum określoną przez atrybut „MINIMUM\_EXT\_FC\_SPEED “, możliwość dołożenia trzeciej dwuportowej karty FC minimum 16 Gb/s w serwerze. | MINIMUM\_EXT\_FC\_CARD – [szt.] = 2  MINIMUM\_EXT\_FC\_PORT – [szt.] = 4  MINIMUM\_EXT\_FC\_SPEED - Gb/s = **16 Gb/s** |
| Karta graficzna | Zintegrowana karta graficzna. |  |
| Porty | Minimum 1 dodatkowy port RJ-45 dedykowany dla interfejsu zdalnego zarządzania, minimum 4 x USB 2.0, minimum port 1 x VGA. |  |
| Zasilacz | Minimum dwa zasilacze hot-plug, zapewniające redundancję zasilania na poziomie N+N. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego serwera, przy zachowaniu jego pełnych możliwości operacyjnych. |  |
| Chłodzenie | Zestaw wentylatorów zapewniających redundantne chłodzenie serwera, typu hot-plug. |  |
| Wspierane systemy operacyjne | MS Windows 2012 R2, Red Hat Enterprise Linux 7.1, SUSE Linux Enterprise Server 12, VMware ESX 6.0 |  |

### Serwery kasetowe x86-64

#### Serwer kasetowy x86-64, 36 cCPU.

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.B.X86.1 |
| **Nazwa** | Serwer kasetowy x86-64, 36 cCPU |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

|  |  |  |
| --- | --- | --- |
| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| Procesory (liczba i typ) | Minimum dwa procesory osiemnastordzeniowe, osiągające w testach „SPECint\_rate2006 Baseline” wynik nie gorszy niż określony przez atrybuty „WYNIK\_SPECINT\_RATE\_BASELINE” (dla konfiguracji serwera z dwoma procesorami osiemnastordzeniowymi). Wynik testu musi być potwierdzony przez organizację SPEC (www.spec.org). | WYNIK\_SPECINT\_RATE\_BASELINE – [pkt] = **1330** |
| Pamięć RAM | Minimum określone przez atrybut „MINIMUM\_RAM\_SIZE” z ochrona pamięci ECC. Pamięci w oferowanej konfiguracji muszą pracować z prędkością taktowania nie niższą niż określona przez atrybut „MINIMUM\_FREQ\_RATE”. Serwer musi umożliwiać rozbudowę pamięci. Serwer musi posiadać co najmniej ilość gniazd pamięci określonych atrybutem MINIMUM\_RAM\_SLOT. | MINIMUM\_RAM\_SIZE – [GB] = **768** MINIMUM\_FREQ\_RATE – [MHZ] = **1866**  MINIMUM\_RAM\_SLOT – [szt.] = **24** |
| Dyski twarde | Możliwość instalacji minimum 2 dysków SAS 2.5" Hot Plug, w wewnętrznych kieszeniach serwera. Minimum 2 dyski 300 GB 6 Gb SAS 10K RPM SFF HDD oraz dwa klucze USB lub dwie karty SD działające w trybie mirror w obudowie serwera. |  |
| Interfejsy sieciowe (LAN) | Minimum 2 interfejsy sieciowe o łącznej przepustowości minimum 40 Gigabit Ethernet (GbE), na 2 fizycznie oddzielnych kartach sieciowych, z możliwością zdefiniowania minimum 40 kart sieciowych poprzez mechanizm wirtualizacji (posiadające własne adresy MAC oraz widoczne z poziomu systemu operacyjnego, jako fizyczne karty sieciowe). Powyższa funkcjonalność musi być niezależna od zainstalowanego na serwerze systemu operacyjnego/platformy wirtualizacyjnej.  Dopuszczalne jest zastosowanie standardu Fibre Channel over Ethernet (FCoE).  Wsparcie dla technologii VMQ (obsługa głębokości kolejki min. 100) oraz NetQueue. |  |
| Interfejsy FC (SAN) | Minimum 4 interfejsy Fibre Channel 16 Gb/s. Wymaga się, aby interfejsy te były widziane przez system operacyjny działający bezpośrednio na serwerze, jako interfejsy fizyczne - posiadające swój adres WWN. Dopuszczalna jest wirtualizacja interfejsów Fibre Channel (FC) poprzez interfejsy 40 Gigabit Ethernet (GbE) i zastosowanie standardu Fibre Channel over Ethernet (FCoE). |  |
| Wspierane systemy operacyjne | MS Windows 2012 R2, Red Hat Enterprise Linux 7.1, SUSE Linux Enterprise Server 12, VMware ESX 6. |  |

## Komponenty dodatkowe infrastruktury serwerowej

### Infrastruktura dla serwerów kasetowych

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.B.IA |
| **Nazwa** | Infrastruktura dla serwerów kasetowych. |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Rodzaj obsługiwanych serwerów kasetowych | Infrastruktura musi obsługiwać serwery z procesorami x86-64 |
| Obudowa serwerów kasetowych | Dostosowana do zamontowania w szafie stelażowej 19”.  Umożliwiająca zainstalowanie w niej minimum 8 serwerów kasetowych dwuprocesorowych bez konieczności rozbudowy o kolejne elementy sprzętowe. |
| Sposób wyprowadzenia połączeń LAN | Obsługiwane minimum 4 urządzenia typu 10 Gb/s Ethernet w ramach jednej obudowy serwerów kasetowych, agregujące i wyprowadzające sygnały z portów sieciowych na serwerach z zachowaniem redundancji połączeń.  Możliwość dodania dodatkowych modułów w ramach obudowy, wyprowadzających interfejsy Ethernet z kart rozbudowy dla serwerów kasetowych.  Moduły muszą wyprowadzać wszystkie porty Ethernet znajdujące się w serwerach kasetowych.  Dopuszcza się zastosowanie rozwiązania opartego o centralny kontroler/przełącznik (w konfiguracji redundantnej) z wyniesionymi modułami I/O w obudowach blade.  W przypadku architektury opartej o centralny kontroler każda obudowa blade musi posiadać minimum 2 wyniesione moduły typu 4x10 Gigabit Ethernet (GbE). Urządzenia te muszą umożliwiać agregację połączeń LAN i SAN Fibre Channel over Ethernet (FCoE) oraz ich wyprowadzenie do centralnego kontrolera/przełącznika z zachowaniem redundancji połączeń. Wymagane jest zapewnienie interfejsów oferujących pasmo łącznie 40 GigabitEthernet, rozłożone na 2 wyniesione moduły. Centralne kontrolery należy dołączyć do sieci LAN za pomocą pasma 40GE każdy. |
| Sposób wyprowadzenia połączeń SAN | Obsługiwane minimum cztery moduły typu 16 Gb/s FC agregujące i wyprowadzające sygnały ze wszystkich portów FC w serwerach.  Dopuszczalne jest stosowanie modułów wspólnych z modułami sieci LAN (FCoE).  Urządzenia te muszą umożliwiać wyprowadzenie sygnałów SAN z infrastruktury z zachowaniem redundancji połączeń.  Wszystkie porty muszą być aktywne i wyposażone w moduły SFP minimum 16 Gb/s SFP+ SW.  Moduły muszą wyprowadzać wszystkie porty FC znajdujące się w serwerach kasetowych.  Dopuszcza się zastosowanie technologii Fiber Chanel over Ethernet (FCoE). Wówczas wymagane jest zapewnienie dedykowanych interfejsów oferujących pasmo łącznie 40 Gigabit Ethernet (FCoE). Wymaga się, aby były one rozłożone, na co najmniej dwóch fizycznych modułach. Interfejsy muszą zapewniać komunikację zewnętrzną wszystkim wewnętrznym interfejsom Fiber Chanel serwerów.  Dopuszcza się zastosowanie rozwiązania opartego o centralny kontroler/przełącznik (w konfiguracji redundantnej) z wyniesionymi modułami I/O w obudowach blade.  W przypadku architektury opartej o centralny kontroler/przełącznik każda obudowa blade musi posiadać minimum 2 wyniesione moduły typu 40 Gigabit Ethernet. Urządzenia te muszą umożliwiać agregację połączeń LAN i SAN (FCoE) oraz ich wyprowadzenie do centralnego kontrolera/przełącznika z zachowaniem redundancji połączeń. Centralne kontrolery należy dołączyć do sieci SAN za pomocą pasma 4x8G FC każdy. |
| Zarządzanie połączeniami LAN i SAN z serwerów kasetowych | W ramach obudowy lub modułów LAN/SAN wymagana jest możliwość przydzielania predefiniowanych adresów MAC i WWN odpowiednio na karty Ethernet i FC.  Dodatkowo w ramach modułów Ethernet 40 Gb/s i kart 10 Gb/s, na serwerach musi istnieć możliwość podzielenia kart na minimum 40 interfejs-ów sieciowych, widzianych jako interfejsy fizyczne przez system operacyjny (posiadające predefiniowany adres MAC).  Rozwiązanie musi być niezależne od systemu operacyjnego, dostarczane w infrastruktury |
| Chłodzenie | Zestaw redundantnych wiatraków zapewniających chłodzenie dla serwerów i urządzeń I/O zainstalowanych w infrastrukturze serwerów kasetowych. |
| Zasilanie | Zasilanie napięciem zmiennym: 230 V, 50 Hz.  Dwa niezależne, redundantne źródła zasilania na obudowę – zdolne do obsługi awarii modułów zasilaczy oraz awarii jednego źródła zasilania przy ciągłym dostarczeniu mocy niezbędnej do zasilenia obudowy w pełni obsadzonej serwerami.  W każdym przypadku procesory serwerów winny pracować z nominalną, maksymalną częstotliwością. Możliwość wymiany zasilaczy bez potrzeby odłączania kabla doprowadzającego zasilanie do obudowy. |
| Sygnalizacja/monitoring | Redundantne moduły zarządzania w każdej obudowie. |

### Zarządzanie infrastrukturą serwerów kasetowych

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.B.MGT |
| **Nazwa** | Zarządzanie infrastrukturą serwerów kasetowych |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

| Element/cecha | Charakterystyka |
| --- | --- |
| Podstawowe operacje | Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera. |
| Napędy wirtualne | Zdalne udostępnianie napędów, w tym CD-ROM na potrzeby każdego serwera z możliwością bootowania z w/w napędów. |
| Sposób zarządzania | Zdalny z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.  System odporny na awarie pojedynczych komponentów, dostarczony na dedykowanych komponentach |
| Liczba jednoczesnych sesji zarządzania | W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów w ramach infrastruktury. |
| Zdalna identyfikacja | Możliwość zdalnego włączenia i wyłączenia identyfikatora (sygnalizatora) optycznego w serwerze kasetowym, umożliwiająca zidentyfikowanie serwera fizycznego w obudowie. |
| Konfiguracja sprzętowa serwera | Możliwość zautomatyzowania procesu konfiguracji sprzętowej pojedynczego serwera lub grupy serwerów za pomocą skryptów. |
| Dodatkowe cechy oprogramowania do zarządzania | - zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci)  - System musi mieć możliwość zarządzania serwerami kasetowymi dostarczanymi w ramach postępowania oraz zarządzania zewnętrznymi serwerami stelażowymi  - 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  - zdalna dystrybucja oprogramowania,  - automatyczne wykrywanie i identyfikacja urządzeń zainstalowanych w ramach infrastruktury (serwery, obudowy serwerów kasetowych, karty zarządzające) i prezentacja infrastruktury w postaci graficznej  - monitorowanie wykorzystania (obciążenia) następujących podzespołów serwera: procesor, pamięć, dyski twarde, interfejsy sieciowe  - infrastruktura musi umożliwiać zastosowanie technologii Distributed Power Management  (DPM) lub równoważnej tj. umożliwiającej skonfigurowanie automatycznego usypiania serwerów w klastrach wirtualizacyjnych w przypadku niskiego ich obciążenia i automatycznego wzbudzania gdy obciążenie klastrów wzrasta.  - definicja oraz konfiguracja serwera przy pomocy logicznego profilu obejmującego adres MAC, adresy WWNN/WWPN, sekwencję bootowania systemu, ustawienia BIOS.  - możliwość przeniesienia logicznego profilu serwera między dowolną parą serwerów kasetowych  - Jedna konsola do zarządzania serwerami fizycznymi rack oraz blade, oprogramowaniem wirtualizacyjnym, przełącznikami LAN i SAN oraz fizycznymi macierzami  - automatyzacja konfiguracji serwerów, macierzy, przełączników oraz wirtualizacji dostarczonych w postępowaniu za pomocą skryptów z obsługą błędów.  - musi pozwalać na tworzenie własnych scenariuszy dostarczania fizycznej i wirtualnej infrastruktury na wymienionej infrastrukturze  - musi pozwalać na równoległą konfigurację środowiska z interfejsów zarządzających dedykowanych dla macierzy, przełączników oraz serwerów |
| Licencje | Licencje na powyższą funkcjonalność dla wszystkich serwerów kasetowych możliwych do zainstalowania w oferowanej infrastrukturze. |

#### Szafa stelażowa

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.BR.RCK |
| **Nazwa** | Szafa stelażowa |

|  |  |
| --- | --- |
| **Element/cecha** | **Charakterystyka** |
| Standard szafy | EIA-310D 19 cali |
| Wysokość (podana w jednostkach EIA) | - Szafy dedykowane przez producenta dla macierzy - minimum 42U.  - Pozostałe szafy – 47 U. |
| Szerokość x głębokość | (od 60 do 100 cm) x (od 120 do 130 cm) |
| Wyposażenie | Szafa wyposażona w zdejmowane drzwi przednie i tylne zamykane na klucz, zdejmowane panele boczne oraz elementy stabilizujące, zabezpieczające szafę przed wywróceniem.  Zawiasy drzwiowe muszą być umieszczone w obrębie obudowy.  Zestaw „zaślepek” wypełniających puste miejsce w szafie – każde miejsce w szafie nie wypełnione sprzętem musi być wyposażone w zaślepkę.  Szafa musi zostać zintegrowana z istniejącym w ośrodku przetwarzania danych systemem kontroli dostępu. Dopuszcza się stosowanie innych czytników przy zachowaniu kompatybilności z elementami ww. systemu w przypadku gdy nie została przewidziana możliwość instalacji w szafie RACK 19”. Przednie oraz tylne drzwi szafy muszą być wyposażone w zamki elektryczne otwierane kluczem oraz przy pomocy kart zbliżeniowych z wykorzystaniem istniejącego systemu kontroli dostępu, a także zdalnie przez administratora. Osłony boczne szaf również muszą umożliwiać zabezpieczenie przed nieuprawnionym dostępem, np. poprzez zastosowanie zestawu mikrowyłączników, połączonych z systemem kontroli dostępu. Wymagane jest wykonanie wszystkich prac i dostarczenie wszystkich niezbędnych elementów instalacyjnych w celu zintegrowania z istniejącym systemem kontroli dostępu obiektu przy zachowaniu standardów nie gorszych niż zastosowane w istniejącej w instalacji. W szczególności wymagane jest dostarczenie i zainstalowanie czytników kart, mikrowyłączników, sterowników, okablowania oraz zasilaczy do istniejącego systemu kontroli dostępu, jeśli zachodzi taka konieczność. |
| Chłodzenie | Zamontowane w szafie drzwi przednie i tylne muszą być perforowane, zapewniające chłodzenie urządzeń zimnym powietrzem wchodzącym od przodu szafy. Perforacja, za wyjątkiem szaf dedykowanych przez producenta dla macierzy, musi posiadać prześwit min. 75%, poziom prześwitu dla perforacji min. 75%. Ciepłe powietrze (po schłodzeniu urządzeń) musi być wypuszczane poprzez tył szafy. |
| Nośność | Co najmniej 1100 kg/m2. |
| Zasilanie | Szafa stelażowa musi być wyposażona w odpowiednią liczbę dystrybutorów zasilania (PDU), pozwalającą na zabezpieczenie zasilania wszystkich zainstalowanych w niej urządzeń. |

#### Listwa dystrybucyjna zasilania (PDU) w szafie stelażowej

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.BR.PDU |
| **Nazwa** | Listwa dystrybucyjna zasilania (PDU) w szafie stelażowej |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Prąd i moc | Minimum 32 A / 7,3 kVA. |
| Podłączenie wejściowe |  |
| Podłączenie wyjściowe | Minimum 6 gniazd IEC 320 C-19.  Minimum 18 gniazd IEC 320 C-13  Wszystkie złącza muszą posiadać zabezpieczenie przed wysuwaniem się z nich wtyków kabli zasilających. |
| Wymagania montażowe | Listwa dystrybucyjna (PDU) nie może zajmować pozycji montażowych w szafie stelażowej przeznaczonych dla urządzeń IT. |
| Elementy dodatkowe | Listwa dystrybucyjna (PDU) musi umożliwiać (bez zastosowania urządzeń dodatkowych) monitorowanie i wprowadzić do systemu BMS następujące informacje: obecność napięcia na każdej z faz listwy PDU [V], prąd na każdej z faz listwy PDU [A], moc pobierana z każdej faz listwy PDU [W], całkowita moc pobierana przez listwę PDU [W], całkowita moc pobrana(zużycie energii) [kWh]. moc bierna [var], współczynnik mocy, częstotliwość [Hz], Temperatura [stopnie C]. Listwa PDU musi umożliwiać komunikację za pośrednictwem protokołu komunikacyjnego SNMP oraz Modbus TCP.  Listwa dystrybucyjna (PDU) musi umożliwiać (bez zastosowania urządzeń dodatkowych) skonfigurowanie alarmów wyzwalanych parametrami pracy. Alarmy muszą mieć możliwość rejestrowania zdarzeń w bazie danych. Minimalny zakres alarmów wymaganych to: alarm braku obecności napięcia na listwie PDU, alarm o przekroczeniu dopuszczalnej mocy dla każdej z faz listwy PDU, alarm przekroczenia całkowitej mocy listwy PDU. |

#### Konsola zarządzania serwerami w szafie stelażowej

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.PSR.BR.KVM |
| **Nazwa** | Konsola zarządzania serwerami w szafie stelażowej |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Konsola zarządzająca | Konsola składająca się z monitora (minimum 17’’), klawiatury i urządzenia wskazującego (trackball, touchpad, itp.), zajmująca w szafie stelażowej nie więcej niż 1U (wysokość). |  |
| Przełącznik KVM | Porty RJ45 w ilości określonej atrybutem MIN\_LICZBA\_PORTÓW [szt.] do podłączenia z serwerami.  Obsługa mapowania do serwerów zdalnych napędów (w tym obrazów ISO) – tzw. Virtual Media.  Jednoczesna obsługa minimum 2 zdalnych użytkowników (poprzez sieć TCP/IP)  Możliwość instalacji za oferowaną konsolą zarządzającą, tak, aby całość rozwiązania zajmowała w szafie stelażowej wysokość maksymalnie 1U.  Możliwość łączenia wielu oferowanych przełączników KVM w celu podłączenia do minimum 256 serwerów.  Obsługa przewodów o minimalnej długość 30m ( między serwerem a przełącznikiem KVM) | MIN\_LICZBA\_PORTÓW - [szt.] |
| Adaptery do przełącznika KVM | Adapterów RJ45 do USB lub PS2/VGA w ilości określonej atrybutem MIN\_ADAPTERÓW z możliwością obsługi Virtual Media. | MIN\_ADAPTERÓW - [szt.] |

#### Macierz dyskowa typ 1.

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.STO.UNI |
| **Nazwa** | Macierz dyskowa. |

| **Lp.** | | **Element/cecha** | **Minimalne parametry techniczne** | **Atrybuty** |
| --- | --- | --- | --- | --- |
| 1 | | Kompatybilność | Dostarczany model macierzy dyskowych musi znajdować się na liście sprzętu kompatybilnego z posiadanym przez zamawiającego wirtualizatorem macierzy dyskowych SVC |  |
| 2 | | Pojemność użytkowa | Macierz musi dostarczać całkowitą pojemność NETTO (przestrzeni użytkowej, widzianej przez HOSTA) określoną przez atrybut: NETTO CAŁKOWITA.  Dostarczana przestrzeń NETTO macierzy dyskowej musi rozkładać się na następujące grupy, określone parametrami:  NETTO SSD – Minimalna pojemność przestrzeni w oparciu o dyski SSD (pojemność pojedynczego dysku max. 400 GB w technologii eMLC lub SLC).  Niedopuszczalne są w szczególności dyski cMLC (Consumer MLC).   1. NETTO SAS – Minimalna pojemność netto przestrzeni w oparciu o dyski SAS (pojemność pojedynczego dysku max. 300GB, prędkość obrotowa min. 15k obr/min.) lub o dyski SSD (pojemność pojedynczego dysku max. 800 GB w technologii eMLC lub SLC), 2. NETTO NL-SAS – minimalna pojemność przestrzeni w oparciu o dyski NL-SAS (pojemność pojedynczego dysku max. 4TB, prędkość obrotowa min. 7.2k obr/min.) | - NETTO CAŁKOWITA [TiB]  - NETTO SAS [TiB]  - NETTO NL-SAS [TiB]  - NETTO SSD [TiB] |
| 3 | | Bezpieczeństwo danych | Dostarcza pojemność musi zostać zabezpieczona przed awarią co najmniej pojedynczego dysku (RAID 5 o ilości dysków maksymalnie 8+1 dla dysków SSD i SAS oraz maksymalnie 6+2 dla dysków NL-SAS) oraz poprzez obszary Hot Spare zgodnie z rekomendacjami producenta macierzy. |  |
| 4 | | Wydajność | Wynik jaki musi zostać osiągnięty przez dostarczoną macierz dyskową określony atrybutem MIN WYDAJNOŚĆ MACIERZY IOPS (operacji wejścia/wyjścia na sekundę) przy maksymalnym średnim czasie odpowiedzi określonym atrybutem MAX ŚREDNI CZAS ODPOWIEDZI osiągnięty w teście Vdbench zgodnym z wewnętrzną procedurą testową. | MIN WYDAJNOŚĆ MACIERZY [IOPS] = **150 000**  MAX ŚREDNI CZAS ODPOWIEDZI [ms] = **5 ms** |
| 5 | | Kompresja i deduplikacja | Macierz dyskowa musi posiadać możliwość kompresji i deduplikacji danych.  W przypadku gdy macierz nie posiada funkcjonalności kompresji niezbędne jest dostarczenie dodatkowej przestrzeni NETTO w ilości 1,5 razy większej niż określona atrybutem „NETTO CAŁKOWITA” (wymaganie dotyczy każdej grupy dyskowej) wskazanym w lp. 2 niniejszej tabeli.  W przypadku gdy macierz nie posiada funkcjonalności deduplikacji niezbędne jest dostarczenie dodatkowej przestrzeni NETTO w ilości 2 razy większej niż określona atrybutem „NETTO CAŁKOWITA” (wymaganie dotyczy każdej grupy dyskowej) wskazanym w lp. 2 niniejszej tabeli.  W przypadku gdy macierz nie posiada zarówno funkcjonalności kompresji jak i deduplikacji niezbędne jest dostarczenie dodatkowej przestrzeni NETTO w ilości 3 razy większej niż określona atrybutem „NETTO CAŁKOWITA” (wymaganie dotyczy każdej grupy dyskowej) wskazanym w lp. 2 niniejszej tabeli. |  |
| 6 | | Pamięć podręczna | Minimalna wielkość zainstalowanej pamięci określona cechą PAMIĘĆ CACHE [GB]  (Zamawiający nie dopuszcza możliwości zastosowania dysków SSD lub kart pamięci FLASH jako pamięci cache). Mirrorowanie pamięci Cache kontrolerów macierzowych. Podtrzymanie bateryjne pamięci Cache kontrolerów macierzowych przez minimum 48 h lub czas niezbędny na przeniesienie pamięci Cache na dyski wewnętrzne lub do pamięci flash. | - PAMIĘĆ CACHE [GB]= **256** |
| 7 | | Liczba portów zewnętrznych | Minimalna liczba sztuk portów FC typu frontend określona atrybutem LICZBA PORTÓW FC, o prędkości minimalnej określonej parametrem PRĘDKOŚĆ PORTÓW FC. Dopuszczalne wartości atrybutu PRĘDKOŚĆ PORTÓW FC:  - 8 [Gbps]  - 16 [Gbps],  Minimalna liczba sztuk portów iSCSCI określona atrybutem LICZBA PORTÓW iSCSI, o prędności minimalnej określonej parametrem PRĘDKOŚĆ PORTÓW iSCSI. Dopuszczalne wartości atrybutu PRĘDKOŚĆ PORTÓW iSCSI:  - 1 [Gbps]  - 10 [Gbps], | LICZBA PORTÓW FC [szt.] = **32**  PRĘDKOŚĆ PORTÓW FC [Gbps] = **16**  LICZBA PORTÓW iSCSI – [szt] - **brak**  PRĘDKOŚĆ PORTÓW iSCSI – [Gbps] - **brak** |
| 8 | | Obudowa | Macierz dyskowa musi zostać dostarczona w szafie stelażowej RACK 19” lub w dedykowanej szafie producenta macierzy. |  |
| 9 | | Architektura macierzy | Architektura macierzy w pełni oparta o technologię min. SAS 6 Gb/s.  Zainstalowane minimum dwa kontrolery do obsługi danych pracujące nadmiarowo w trybie Active/Active. Oferowane rozwiązanie musi być pojedynczą macierzą dyskową. Niedopuszczalna jest dostarczenie rozwiązania składającego się z wielu macierzy dyskowych. |  |
| 10 | | Tryby ochrony danych | Macierz musi mieć możliwość definiowania grup dyskowych jednego z dwóch poniższych typów:  Typ 1:   * RAID 1+0 (RAID 10); * RAID 5; * RAID 6.   Typ 2:   * RAID 4; * RAID 6 (RAID-DP).   Możliwość definiowania globalnych przestrzeni lub dysków SPARE.  Podwójne niezależne przyłącza min. SAS 6 Gb/s wewnętrznych napędów dyskowych. |  |
| 11 | | Skalowalność | Możliwość rozbudowy, co najmniej do wartości określonej atrybutem ROZBUDOWA DO MIN. LICZBY DYSKÓW bez konieczności wymiany kontrolerów macierzowych. Możliwość rozbudowy pamięci Cache do wartości określonej atrybutem ROZBUDOWA CACHE DO MIN. POJEMNOŚCI [TB] (Zamawiający dopuszcza możliwość zastosowania dysków SSD lub kart pamięci FLASH jako rozbudowę podstawowej pamięci cache) bez konieczności wymiany kontrolerów macierzowych. Pamięć cache musi być dostępna dla operacji zapisu i odczytu. Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD. W celu zapewnienia wysokiej wydajności komunikacji serwer-macierz, macierz musi posiadać możliwość rozbudowy interfejsów FC do wartości określonej atrybutem ROZBUDOWA DO MIN. LICZBY PORTÓW FC FRONTEND [szt.] (bez stosowania dodatkowych przełączników lub koncentratorów FC chyba że jest to klastrowanie kontrolerów macierzy umożliwiające zarządzanie z poziomu jednego interfejsu GUI). Porty FC typu frontend mogą być wykorzystane również do replikacji międzymacierzowej, natomiast niedopuszczalne jest wykorzystanie tych portów do klastrowania kontrolerów. Wymagane jest aby pojedynczy port FC miał możliwość obsługi min. 250 host’ów inicjatorów a cała macierz obsługiwała min. 1024 host’ów inicjatorów. | ROZBUDOWA DO MIN. LICZBY DYSKÓW [szt.] = **1400**  ROZBUDOWA CACHE DO MIN. POJEMNOŚCI [TB] = **2**  ROZBUDOWA DO MIN. LICZBY PORTÓW FC FRONTEND [szt.] = **64** |
| 12 | | Zarządzanie | Oprogramowanie do zarządzania macierzą musi:  Posiadać graficzny interfejs do monitorowania stanu oraz wydajności wszystkich komponentów macierzy oraz pozwalać na tej podstawie optymalizować konfigurację macierzy. Realizować: konfigurację, diagnostykę i analizę wydajności macierzy. Umożliwiać mapowanie zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking). Umożliwiać odczyt danych historycznych (część z wymienionych funkcjonalności może być realizowana poprzez oprogramowanie dodatkowe pod warunkiem, że zostanie dostarczone wraz z niezbędnymi licencjami na całą pojemność dostarczonej macierzy).  Umożliwiać konfigurowanie wolumenów logicznych LUN o pojemności użytkowej przekraczającej 2 TB.  Oprogramowanie macierzy musi zapewniać funkcjonalność automatycznego przemieszczania się danych pomiędzy różnymi warstwami i technologiami składowania ([Tiering](http://www.f5.com/it-management/solutions/storage-tiering/overview/)) działającą na poziomie bloku danych. Funkcjonalność [Tiering](http://www.f5.com/it-management/solutions/storage-tiering/overview/)’u musi być możliwa pomiędzy wszystkimi typami stosowanych dysków tj. SSD, SAS oraz NL-SAS.  Macierz musi umożliwiać przenoszenie całych dysków logicznych (LUN) udostępnionych do hostów pomiędzy poszczególnymi obszarami macierzy dyskowej bez przerywania dostępu do danych i pracy aplikacji korzystających z tych dysków.  Dostarczenie funkcjonalności typu thin provisioning umożliwiającej alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.  Macierz musi posiadać funkcjonalność space reclamation tzn. musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin.  Macierz musi posiadać funkcjonalność tworzenia lokalnych kopii migawkowych dysków logicznych wewnętrznymi mechanizmami macierzy. Należy dostarczyć licencje na całą pojemność macierzy.  Macierz musi posiadać funkcjonalność zarządzania poziomem dostępności QOS polegającą na możliwości skonfigurowania maksymalnej ilości operacji IO oraz przepustowości MB/s dla poszczególnych wolumenów logicznych.  Wymagane jest dostarczenie wszystkich niezbędnych licencji potrzebnych do zrealizowania powyższych funkcjonalności. |  |
| 13 | | Wspierane systemy operacyjne | Wsparcie, dla co najmniej MS Windows 2012 R2, VMware 5.X oraz Linux RedHat 6.x oraz SUSE 11.x.  Wsparcie dla systemów klastrowych, co najmniej, RedHat Cluster, Suse Cluster, MSCS.  Wsparcie musi być dostępne w ramach oferowanych licencji oprogramowania. |  |
| 14 | | Obsługa kanałów wejścia/wyjścia | Obsługa wielu kanałów I/O (Multipathing) - wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Automatyczne przełączanie kanału I/O w wypadku awarii ścieżki dostępu serwerów do macierzy z utrzymaniem ciągłości dostępu do danych. Przełączanie kanałów I/O oparte o natywne mechanizmy systemów operacyjnych wspieranych przez macierz, tj. Windows, Linux RedHat, Linux SuSE, VMware. |  |
| 15 | | Obsługiwane protokoły | FC |  |
| 16 | | Wysoka dostępność macierzy | Zdublowanie następujących elementów macierzy:   1. kontrolery macierzowe, 2. wentylatory, 3. zasilacze (odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy).   Dostęp do urządzenia oraz do składowanych na nim danych musi być realizowany bez przerywania pracy korzystającej z niego aplikacji/systemu, nawet w przypadku awarii lub wymiany pojedynczego elementu urządzenia z ww. grup urządzeń.  Macierz musi umożliwiać aktualizację mikrokodu w trybie online bez przerywania dostępu do zasobów dyskowych. |  |
| 17 | Zasilanie | Napięcie jednofazowe zmienne 230 V, 50 Hz. lub napięcie trójfazowe zmienne 400 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| 18 | Monitoring | Oprogramowanie macierzy musi umożliwiać monitorowanie i raportowanie zasobów blokowych. Wymagana jest funkcjonalność raportowania (generacji raportów), co najmniej w zakresie:  1) Przestrzeni macierzy - całościowa, wolna, wykorzystywana, skonfigurowana-nieprzydzielona dla aplikacji2) Przestrzeni macierzy jw. z podziałem na poszczególne grupy RAID/storage pool'e/wolumeny logiczne/,  3) Wydajności - mierzonej w IOPS oraz MB/s dla zasobów blokowych, ,  4) Utylizacji kontrolerów części blokowej macierzy  5) Raportów capacity planning - prezentujących trendy czasowe w zakresie przestrzeni oraz wydajności macierzy (dla obszarów parametrów podanych powyżej - w punktach 1 i 2),  6) Raporty inwentarzowe, prezentujące skonsolidowane zestawienia zasobów fizycznych macierzy, wolumenów logicznych, pul dyskowych, podłączonych hostów, wraz z odpowiednimi szczegółami dla poszczególnych kategorii,  7) Raporty dla zasobów korzystających z mechanizmu "Thin Provisioningu", zawierające szczegóły dotyczące wykorzystania zasobów, over-subskrypcji oraz trendów/prognoz konsumpcji zasobów.  8) Oprogramowanie musi posiadać funkcjonalność rozliczania wykorzystywanych zasobów storage, tzw. chargeback.  9) Dostarczone oprogramowanie musi umożliwiać tworzenie i generowanie własnych raportów (tzw. custom reports) - w zakresie raportowania wydajności i capacity.  10) Oprogramowanie musi umożliwiać eksportowanie generowanych raportów (mechanizmami wbudowanymi) do zewnętrznych, ogólnie stosowanych formatów plikowych - wymagane co najmniej formaty PDF oraz CSV, oraz możliwość automatycznego wysyłania wygenerowanych raportów pocztą elektroniczną. |  | |

#### Macierz dyskowa typ 2.

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.STO.UNI.2 |
| **Nazwa** | Macierz dyskowa. |

| **Lp.** | | **Element/cecha** | **Minimalne parametry techniczne** | **Atrybuty** |
| --- | --- | --- | --- | --- |
| 2 | | Pojemność użytkowa | Macierz musi dostarczać całkowitą minimalną pojemność NETTO (przestrzeni użytkowej, widzianej przez HOSTA) określoną przez atrybut: POJEMNOŚĆ CAŁKOWITA, zwymiarowaną w jednostkach TiB.  Dostarczana przestrzeń NETTO CAŁKOWITA na każdej macierzy dyskowej musi rozkładać się na następujące grupy, określane cechami:   1. NETTO RAID5 NL SAS - Minimalna pojemność netto przestrzeni w TiB w oparciu o dyski NL-SAS (pojemność pojedynczego dysku max. 2TB, prędkość obrotowa min. 7.2k obr/min.), 2. NETTO RAID1 NL SAS – Minimalna pojemność netto przestrzeni w TiB w oparciu o dyski NL-SAS (pojemność pojedynczego dysku max. 2TB, prędkość obrotowa min. 7.2k obr/min.) 3. NETTO RAID6 NL SAS – Minimalna pojemność netto przestrzeni w TiB w oparciu o dyski NL-SAS (pojemność pojedynczego dysku max. 2TB, prędkość obrotowa min. 7.2k obr/min.) | - NETTO CAŁKOWITA [TiB]  - NETTO RAID5 NL SAS [TiB]  - NETTO RAID1 NL SAS [TiB]  - NETTO RAID6 NL SAS [TiB] |
| 3 | | Bezpieczeństwo danych | Dostarczana pojemność musi zostać zabezpieczona przed awarią co najmniej dwóch dysków (RAID 6 o ilości dysków maksymalnie 6+2 dla dysków NL-SAS), a także przez typ zabezpieczenia RAID1/10 oraz poprzez obszary Hot Spare zgodnie z rekomendacjami producenta macierzy. |  |
| 4 | | Wydajność | Wynik jaki musi zostać osiągnięty przez dostarczoną macierz dyskową określony atrybutem MIN WYDAJNOŚĆ MACIERZY IOPS (operacji wejścia/wyjścia na sekundę) przy maksymalnym średnim czasie odpowiedzi określonym atrybutem MAX ŚREDNI CZAS ODPOWIEDZI osiągnięty w teście Vdbench zgodnym z wewnętrzną procedurą testową. | MIN WYDAJNOŚĆ MACIERZY [IOPS]  MAX ŚREDNI CZAS ODPOWIEDZI [ms] |
| 5 | | Pamięć podręczna | Minimalna wielkość zainstalowanej pamięci Cache określona jest cechą PAMIĘĆ CACHE  (Zamawiający nie dopuszcza możliwości zastosowania dysków SSD lub kart pamięci FLASH jako pamięci cache). Mirrorowanie pamięci Cache kontrolerów macierzowych. Podtrzymanie bateryjne pamięci Cache kontrolerów macierzowych przez minimum 48 h lub czas niezbędny na przeniesienie pamięci Cache na dyski wewnętrzne lub do pamięci flash. | PAMIĘĆ CACHE [GB] |
| 6 | | Liczba portów zewnętrznych | Minimalna liczba sztuk portów FC typu frontend określona atrybutem LICZBA PORTÓW FC, nie mniej niż 8 oraz PRĘDKOŚĆ PORTÓW, nie mniej niż 8Gbps | LICZBA PORTÓW FC [szt.]  PRĘDKOŚĆ PORTÓW [Gbps] |
| 7 | | Obudowa | Macierz dyskowa musi zostać dostarczona w szafie stelażowej RACK 19” lub w dedykowanej szafie producenta macierzy. |  |
| 8 | | Architektura macierzy | Architektura macierzy w pełni oparta o technologię SAS minimum 6 Gb/s.  Zainstalowane minimum dwa kontrolery do obsługi danych pracujące nadmiarowo w trybie Active/Active. Oferowane rozwiązanie musi być pojedynczą macierzą dyskową. Niedopuszczalna jest dostarczenie rozwiązania składającego się z wielu macierzy dyskowych. |  |
| 9 | | Tryby ochrony danych | Macierz musi mieć możliwość definiowania grup dyskowych jednego z dwóch poniższych typów:  Typ 1:   * RRAID 1+0 (RAID 10); * RRAID 5; * RRAID 6.   Możliwość definiowania globalnych przestrzeni lub dysków SPARE.  Podwójne niezależne przyłącza min. SAS 6 Gb/s wewnętrznych napędów dyskowych. |  |
| 10 | | Skalowalność | Możliwość rozbudowy, do co najmniej 1000 dysków bez konieczności wymiany/dodawania kontrolerów macierzowych. Możliwość rozbudowy pamięci Cache do co najmniej 2,5 TB (Zamawiający dopuszcza możliwość zastosowania dysków SSD lub kart pamięci FLASH jako rozbudowę podstawowej pamięci cache) bez konieczności wymiany kontrolerów macierzowych. Pamięć cache musi być dostępna dla operacji zapisu i odczytu. Możliwość rozbudowy macierzy za pomocą nowych dysków o większych pojemnościach oraz dysków typu SSD. W celu zapewnienia wysokiej wydajności komunikacji serwer-macierz, macierz musi posiadać możliwość rozbudowy, do co najmniej 16 interfejsów FC typu frontend (bez stosowania dodatkowych przełączników lub koncentratorów FC chyba że jest to klastrowanie kontrolerów macierzy umożliwiające zarządzanie z poziomu jednego interfejsu GUI). Wymagane jest aby pojedynczy port FC miał możliwość obsługi min. 250 host’ów inicjatorów a cała macierz obsługiwała min. 1024 host’ów inicjatorów. |  |
| 11 | | Zarządzanie | Oprogramowanie do zarządzania macierzą musi:  Posiadać graficzny interfejs do monitorowania stanu oraz wydajności wszystkich komponentów macierzy oraz pozwalać na tej podstawie optymalizować konfigurację macierzy. Realizować: konfigurację, diagnostykę i analizę wydajności macierzy. Umożliwiać mapowanie zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking). Umożliwiać odczyt danych historycznych (część z wymienionych funkcjonalności może być realizowana poprzez oprogramowanie dodatkowe pod warunkiem, że zostanie dostarczone wraz z niezbędnymi licencjami na całą pojemność dostarczonej macierzy).  Umożliwiać konfigurowanie wolumenów logicznych LUN o pojemności użytkowej przekraczającej 2 TB.  Oprogramowanie macierzy musi zapewniać funkcjonalność automatycznego przemieszczania się danych pomiędzy różnymi warstwami i technologiami składowania ([Tiering](http://www.f5.com/it-management/solutions/storage-tiering/overview/)) działającą na poziomie bloku danych i zapewniać możliwość buforowania danych (Cache) na pamięciach Flash, w tym na pulach dyskowych Flash SSD bądź na pamięciach Flash umieszczonych na kartach PCIe. Funkcjonalność [Tiering](http://www.f5.com/it-management/solutions/storage-tiering/overview/)’u może być możliwa pomiędzy wszystkimi typami stosowanych dysków tj. SSD, SAS oraz NL-SAS.  Macierz musi umożliwiać przenoszenie całych dysków logicznych (LUN) udostępnionych do hostów pomiędzy poszczególnymi obszarami macierzy dyskowej bez przerywania dostępu do danych i pracy aplikacji korzystających z tych dysków.  Dostarczenie funkcjonalności typu thin provisioning umożliwiającej alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.  Macierz musi posiadać funkcjonalność space reclamation tzn. musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin.  Macierz musi posiadać funkcjonalność tworzenia lokalnych kopii migawkowych dysków logicznych wewnętrznymi mechanizmami macierzy. Należy dostarczyć licencje na całą pojemność macierzy.  Macierz musi posiadać funkcjonalność zarządzania poziomem dostępności QOS polegającą na możliwości skonfigurowania maksymalnej ilości operacji IO oraz przepustowości MB/s dla poszczególnych wolumenów logicznych.  Wymagane jest dostarczenie wszystkich niezbędnych licencji potrzebnych do zrealizowania powyższych funkcjonalności. |  |
| 12 | | Wspierane systemy operacyjne | Wsparcie, dla co najmniej MS Windows 2012 R2, VMware 5.X oraz Linux RedHat 6.x oraz SUSE 11.x.  Wsparcie dla systemów klastrowych, co najmniej, RedHat Cluster, Suse Cluster, MSCS.  Wsparcie musi być dostępne w ramach oferowanych licencji oprogramowania. |  |
| 13 | | Obsługa kanałów wejścia/wyjścia | Obsługa wielu kanałów I/O (Multipathing) - wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Automatyczne przełączanie kanału I/O w wypadku awarii ścieżki dostępu serwerów do macierzy z utrzymaniem ciągłości dostępu do danych. Przełączanie kanałów I/O oparte o natywne mechanizmy systemów operacyjnych wspieranych przez macierz, tj. Windows, Linux RedHat, Linux SuSE, VMware. |  |
| 14 | | Obsługiwane protokoły | FC |  |
| 16 | | Wysoka dostępność macierzy | Zdublowanie następujących elementów macierzy:   1. kontrolery macierzowe, 2. wentylatory, 3. zasilacze (odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy).   Dostęp do urządzenia oraz do składowanych na nim danych musi być realizowany bez przerywania pracy korzystającej z niego aplikacji/systemu, nawet w przypadku awarii lub wymiany pojedynczego elementu urządzenia z ww. grup urządzeń.  Macierz musi umożliwiać aktualizację mikrokodu w trybie online bez przerywania dostępu do zasobów dyskowych. |  |
| 17 | Zasilanie | Napięcie jednofazowe zmienne 230 V, 50 Hz. lub napięcie trójfazowe zmienne 400 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| 18 | Monitoring | Oprogramowanie macierzy musi umożliwiać monitorowanie i raportowanie zasobów blokowych. Wymagana jest funkcjonalność raportowania (generacji raportów), co najmniej w zakresie:  1) Przestrzeni macierzy - całościowa, wolna, wykorzystywana, skonfigurowana-nieprzydzielona dla aplikacji, z podziałem na zasoby blokowe i plikowe,  2) Przestrzeni macierzy jw. z podziałem na poszczególne grupy RAID/storage pool'e/wolumeny logiczne/systemy plików skonfigurowane w części NAS,  3) Wydajności - mierzonej w IOPS oraz MB/s dla zasobów blokowych, oraz File Ops/s dla zasobów NAS,  4) Utylizacji kontrolerów części blokowej oraz plikowej macierzy  5) Raportów capacity planning - prezentujących trendy czasowe w zakresie przestrzeni oraz wydajności macierzy (dla obszarów parametrów podanych powyżej - w punktach 1 i 2),  6) Raporty inwentarzowe, prezentujące skonsolidowane zestawienia zasobów fizycznych macierzy, wolumenów logicznych, pul dyskowych, podłączonych hostów, wraz z odpowiednimi szczegółami dla poszczególnych kategorii,  7) Raporty dla zasobów korzystających z mechanizmu "Thin Provisioningu", zawierające szczegóły dotyczące wykorzystania zasobów, over-subskrypcji oraz trendów/prognoz konsumpcji zasobów.  8) Oprogramowanie musi posiadać funkcjonalność rozliczania wykorzystywanych zasobów storage, tzw. chargeback.  9) Dostarczone oprogramowanie musi umożliwiać tworzenie i generowanie własnych raportów (tzw. custom reports) - w zakresie raportowania wydajności i capacity.  10) Oprogramowanie musi umożliwiać eksportowanie generowanych raportów (mechanizmami wbudowanymi) do zewnętrznych, ogólnie stosowanych formatów plikowych - wymagane co najmniej formaty PDF, XLS oraz CSV, oraz możliwość automatycznego wysyłania wygenerowanych raportów pocztą elektroniczną. |  | |

#### Macierz dyskowa flash.

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.STO.FLS |
| **Nazwa** | Macierz dyskowa flash |

| **Lp.** | **Element/cecha** | **Minimalne parametry techniczne** | | **Atrybut** |
| --- | --- | --- | --- | --- |
| 1 | Pojemność użytkowa | Macierz musi dostarczać całkowitą pojemność NETTO (przestrzeni użytkowej, widzianej przez HOSTA) określoną atrybutem NETTO CAŁKOWITA.  Dostarczana przestrzeń NETTO musi być zbudowana w oparciu o dyski SSD (MLC lub SLC – maksymalna pojemność dysku 800 GB) lub karty pamięci flash. Macierz, ani żaden z jej komponentów nie może wykorzystywać dysków mechanicznych do przechowywania danych. | | NETTO CAŁKOWITA [TiB] = **30** |
| 2 | Bezpieczeństwo danych | Macierz musi posiadać nadmiarową pojemność przeznaczoną na odbudowę uszkodzonych dysków. Urządzenie musi rezerwować nadmiarową pojemność wymaganą do odbudowy co najmniej jednego dysku/nośnika flash w ramach każdej półki, a pojemność ta nie może być składową deklarowanej pojemności użytkowej macierzy.  Macierz musi zapewniać w razie utraty zasilania zabezpieczenie przed utratą danych. | |  |
| 3 | Deduplikacja i kompresja inline (w locie) | | Deduplikacja:  Macierz musi umożliwiać globalną deduplikację (realizowaną w ramach całej pojemności macierzy niezależnie od logicznej i fizycznej konfiguracji) na poziomie blokowym. Wymaga się dostarczenia licencji deduplikacji na całą oferowaną pojemność macierzy.  Deduplikacja musi być wykonywana zawsze jako część operacji zapisu danych (w trybie inline). Niedopuszczalne są rozwiązania, które zapisują dane na dyski bez wykonania procesu deduplikacji.  Deduplikacja nie może wpływać negatywnie na wydajność macierzy tj. na ilość operacji IO oraz na czas odpowiedzi.  Deduplikacja musi być realizowana globalnie we wszystkich udziałach i dla wszystkich rodzajów danych bez względu na udział.  Deduplikacja nie może być realizowana za pomocą zewnętrznego urządzenia lub oprogramowania.  Kompresja:  Macierz musi umożliwiać kompresję na poziomie blokowym. Wymaga się dostarczenia licencji na oferowaną pojemność macierzy. Kompresja musi być wykonywana zawsze jako część operacji zapisu danych (w trybie inline). Niedopuszczalne są rozwiązania, które zapisują dane na dyski bez wykonania procesu kompresji.  Kompresja nie może wpływać negatywnie na wydajność macierzy tj. na ilość operacji IO oraz na czas odpowiedzi. Dozwolone jest zastosowanie dedykowanej karty kompresującej. |  |
| 4 | Wydajność | | Wynik jaki musi zostać osiągnięty przez dostarczoną macierz dyskową określony atrybutem MIN WYDAJNOŚĆ MACIERZY IOPS (operacji wejścia/wyjścia na sekundę) przy maksymalnym średnim czasie odpowiedzi określonym atrybutem MAX ŚREDNI CZAS ODPOWIEDZI osiągnięty w teście Vdbench zgodnym z wewnętrzną procedurą testową.  Wymagane jest, aby dostarczone urządzenie w okresie objętym gwarancją zachowało parametry wydajnościowe uzyskane w testach.  W przypadku stwierdzenia w trakcie eksploatacji macierzy drastycznego spadku jej wydajności  (25% spadek wydajności odczytu lub zapisu względem wyników uzyskanych w testach, nie bądący skutkiem awarii urządzenia) Wykonawca w ramach gwaracji zobowiązany jest do przywrócenia  stanu pierwotnego (+- 5% wartości uzyskanych w testach). | MIN WYDAJNOŚĆ MACIERZY [IOPS] = **400 000**  MAX ŚREDNI CZAS ODPOWIEDZI [ms] = **poniżej 1 ms** |
| 5 | Pamięć podręczna | Macierz obsługująca przestrzeń dyskową musi być wyposażona w pamięć RAM o sumarycznej pojemności, nie mniejszej niż wartość określona atrybutem PAMIĘĆ RAM | | PAMIĘĆ RAM [GB] = **512** |
| 6 | Liczba portów zewnętrznych | Minimalna liczba sztuk portów FC typu frontend określona atrybutem LICZBA PORTÓW FC, o prędkości minimalnej określonej parametrem PRĘDKOŚĆ PORTÓW FC. Dopuszczalne wartości atrybutu PRĘDKOŚĆ PORTÓW FC:  - 8 [Gbps]  - 16 [Gbps], | | LICZBA PORTÓW FC [szt.] = **8**  PRĘDKOŚĆ PORTÓW FC [Gbps] = **8** |
| 7 | Obudowa | Macierz dyskowa musi zostać zainstalowana w szafie stelażowej RACK 19” dostarczonej w ramach dostawy nowej macierzy dyskowej z funkcjonalnością NAS lub w dostarczonej dedykowanej szafie stelażowej RACK 19”. | |  |
| 8 | Architektura macierzy | Zainstalowane minimum cztery kontrolery do obsługi danych pracujące nadmiarowo w trybie Active/Active. Oferowane rozwiązanie musi być pojedynczą macierzą dyskową. Niedopuszczalna jest dostarczenie rozwiązania składającego się z wielu macierzy dyskowych. | |  |
| 9 | Skalowalność | Macierz musi umożliwiać rozbudowę pojemności oraz wydajności poprzez dołożenie kontrolerów bez konieczności migracji danych.  Macierz musi umożliwiać wyposażenie w co najmniej 16 kontrolerów pracujących w trybie Active/Active zajmujących się obsługą dostępu do dysków i danych od strony hosta  Możliwość rozbudowy, do co najmniej 200 dysków lub kart flash. Możliwość rozbudowy pamięci RAM do min. 4096 GB.  W celu zapewnienia wysokiej wydajności komunikacji serwer-macierz, macierz musi posiadać możliwość rozbudowy, do co najmniej 32 interfejsów FC typu frontend o prędkości max 8 Gbps, lub 16 interfejsów FC typu frontend o prędkości max 16 Gbps(bez stosowania dodatkowych przełączników lub koncentratorów FC). Wymagane jest aby macierz obsługiwała min. 512 host’ów inicjatorów. | |  |
| 10 | Zarządzanie | Oprogramowanie do zarządzania macierzą musi:  Posiadać graficzny interfejs do monitorowania stanu oraz wydajności wszystkich komponentów macierzy oraz pozwalać na tej podstawie optymalizować konfigurację macierzy. Realizować: konfigurację, diagnostykę, i analizę wydajności macierzy. Umożliwiać mapowanie zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking). Umożliwiać odczyt danych historycznych (część z wymienionych funkcjonalności może być realizowana poprzez oporgramowanie dodatkowe pod warunkiem, że zostanie dostarczone wraz z niezbędnymi licencjami na całą pojemność dostarczonej macierzy).  Umożliwiać konfigurowanie wolumenów logicznych LUN o pojemności użytkowej przekraczającej 2 TB.  Wymagane jest dostarczenie funkcjonalności typu thin provisioning umożliwiającej alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości.  Macierz musi posiadać funkcjonalność space reclamation tzn. musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin.  Macierz musi posiadać funkcjonalność tworzenia lokalnych kopii migawkowych dysków logicznych wewnętrznymi mechanizmami macierzy.  Macierz musi obsługiwać 64 kopie migawkowe pojedynczego wolumenu dyskowego. Należy dostarczyć licencje na całą pojemność macierzy.  Wymagane jest dostarczenie wszystkich niezbędnych licencji potrzebnych do zrealizowania powyższych funkcjonalności. | |  |
| 11 | Wspierane systemy operacyjne | Wsparcie, dla co najmniej MS Windows 2012 R2, VMware 5.X oraz Linux RedHat 6.x oraz SUSE 11.x.  Wsparcie dla systemów klastrowych, co najmniej, RedHat Cluster, Suse Cluster, MSCS.  Wsparcie musi być dostępne w ramach oferowanych licencji oprogramowania. | |  |
| 12 | Obsługa kanałów wejścia/wyjścia | Obsługa wielu kanałów I/O (Multipathing) - wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Automatyczne przełączanie kanału I/O w wypadku awarii ścieżki dostępu serwerów do macierzy z utrzymaniem ciągłości dostępu do danych. Przełączanie kanałów I/O oparte o natywne mechanizmy systemów operacyjnych wspieranych przez macierz, tj. Windows, Linux RedHat, Linux SuSE, VMware. | |  |
| 13 | Obsługiwane protokoły | FC, IP SAN (iSCSI), | |  |
| 14 | Wysoka dostępność macierzy | Zdublowanie następujących elementów macierzy:  • Kontrolery macierzowe,  • wentylatory,  • zasilacze (odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy).  Dostęp do urządzenia oraz do składowanych na nim danych musi być realizowany bez przerywania pracy korzystającej z niego aplikacji/systemu, nawet w przypadku awarii lub wymiany pojedynczego elementu urządzenia z ww. grup urządzeń.  Macierz musi umożliwiać aktualizację mikrokodu w trybie online bez przerywania dostępu do zasobów dyskowych. | |  |
| 15 | Zasilanie | Napięcie jednofazowe zmienne 230 V, 50 Hz. lub napięcie trójfazowe zmienne 400 V, 50 Hz. Minimum dwa zasilacze zapewniające redundancję zasilania N+N, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. | |  |

#### Macierz dyskowa NAS.

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.STO.NAS |
| **Nazwa** | Macierz dyskowa NAS |

| **Lp.** | **Element/cecha** | **Minimalne parametry techniczne** | **Atrybuty** |
| --- | --- | --- | --- |
| 1 | Pojemność użytkowa | Macierz musi dostarczać całkowitą minimalną pojemność NETTO (przestrzeni użytkowej, widzianej przez HOSTA) określoną przez atrybut: POJEMNOŚĆ CAŁKOWITA, zwymiarowaną w jednostkach TiB.  Dostarczana przestrzeń NETTO CAŁKOWITA na macierzy dyskowej musi :  - zbudowana być z dysków NLSAS nie większych niż 4TB,  - udostępniać całkowitą dostępną przestrzeń́ w ramach jednego ciągłego systemu plików, | * NETTO CAŁKOWITA [TiB] |
| 2 | Bezpieczeństwo danych | Dostarczana pojemność musi zostać zabezpieczona przed awarią co najmniej dwóch dowolnych dysków jednocześnie, albo jednego kontrolera. |  |
| 3 | Pamięć podręczna | Minimalna wielkość zainstalowanej pamięci Cache określona jest cechą PAMIĘĆ CACHE  (Zamawiający nie dopuszcza możliwości zastosowania dysków SSD lub kart pamięci FLASH jako pamięci cache). Mirrorowanie pamięci Cache kontrolerów macierzowych. Podtrzymanie bateryjne pamięci Cache kontrolerów macierzowych przez minimum 48 h lub czas niezbędny na przeniesienie pamięci Cache na dyski wewnętrzne lub do pamięci flash. | * PAMIĘĆ CACHE [GB] |
| 4 | Liczba portów zewnętrznych | Minimalna liczba sztuk portów LAN określona atrybutami:  LICZBA PORTÓW LAN 1Gbps  LICZBA PORTÓW LAN 10Gbps  Wszystkie porty muszą być wyposażone w niezbędne wkładki umożliwiające natychmiastowe włączenie ich do infrastruktury. | * LICZBA PORTÓW LAN 1Gbps * LICZBA PORTÓW LAN 10Gbps |
| 5 | Obudowa | Macierz dyskowa musi zbudowana być z półki dyskowej lub węzła stanowiącego element rozwiązania pamięci dyskowej mieszczącej nie mniej, niż 8 dysków typu NL-SAS lub SAS w przeliczeniu na 1U (tj. np. nie mniej, niż 32 dyski w obudowie 4U), |  |
| 6 | Architektura macierzy | Macierz musi  -    być zbudowana być w oparciu o liczbę kontrolerów określoną parametrem LICZBA KONTROLERÓW, gdzie każdy realizuje dostęp do danych plikowy  - zapewniać pracę jednocześnie wszystkich kontrolerów w trybie aktywny/aktywny  Oferowane rozwiązanie musi być pojedynczą macierzą dyskową. Niedopuszczalna jest dostarczenie rozwiązania składającego się z wielu macierzy dyskowych.  Oferowane rozwiązanie musi posiadać funkcjonalność umożliwiającą replikację zgromadzonych danych pomiędzy dostarczonymi macierzami przez warstwę sieci LAN. | * LICZBA KONTROLERÓW [szt.] |
| 7 | Tryby ochrony danych | Macierz musi  - zapewniać gwarantowaną ochronę przed „cichym uszkodzeniem dysków” (silent data corruption) dla wszystkich technologii dyskowych (w tym SATA),  - umożliwiać wymianę uszkodzonego dysku przy zachowaniu nieprzerwanej dostępności wszystkich zasobów, tj. bez czasowego wyłączania z użycia innych elementów urządzenia,  - mieć możliwość jasnego określenia lokalizacji uszkodzonego dysku, np. za pomocą lampki kontrolnej lub wyświetlenia numeru pojedynczej zatoki/kieszeni,  - umożliwić, w przypadku awarii jednego dysku, odzyskanie pierwotnego poziomu ochrony danych w czasie dłuższy niż 12 godzin od momentu jego wymiany – w sytuacji braku obciążenia przez urządzenia klienckie. |  |
| 8 | Skalowalność | Macierz musi  -     umożliwiać rozbudowę co najmniej do ilości kontrolerów określonej atrybutem ROZBUDOWA DO MININMALNEJ LICZBA KONTROLERÓW w ramach tego samego systemu dyskowego,  -      umożliwiać rozbudowę do co najmniej wielkości powierzchni netto określonej atrybutem ROZBUDOWA DO MINIMALNEJ POWIERZCHNI NETTO zwymiarowanej w jednostkach TiB,  -    pozwalać na rozbudowę o funkcjonalność replikacji asynchronicznej danych  -  zapewniać możliwość rozbudowy o funkcjonalność deduplikacji na poziomie bloków o wielkości nie większej, niż 8KiB dla wyznaczonych katalogów. Zamawiający nie dopuszcza wykorzystania oprogramowania firm zewnętrznych czy OEM. | * ROZBUDOWA DO MINIMALNEJ LICZBY KONTROLERÓW [szt.] * ROZBUDOWA DO MINIMALNEJ POWIERZCHNI  NETTO [TiB] |
| 9 | Zarządzanie | Oprogramowanie do zarządzania macierzą musi odbywać się poprzez Web GUI oraz Command Line Interface  Oprogramowania macierzy musi  - zapewniać funkcjonalność zautomatyzowanego wykonywania kopii migawkowych (snapshotów) dla wybranych folderów. Interwały czasowe i czasy retencji muszą być definiowalne przez administratora systemu,  - umożliwiać wykonanie co najmniej 100 kopii migawkowych (snapshotów) danego katalogu oraz umożliwiać wykonanie co najmniej 20 000 snapshotów w odniesieniu do całego filesystemu,  - obsługiwać integrację mechanizmu kopii migawkowych z usługą VSS (Volume Shadow Copy Service) firmy Microsoft,  - zawierać wbudowaną funkcjonalność określania limitów ilości przechowywanych danych dla wybranych użytkowników lub grup użytkowników (tzw. filesystem quota). Zamawiający nie dopuszcza wykorzystania oprogramowania firm zewnętrznych czy OEM (Original Equipment Manufacturer),  - obsługiwać monitorowanie SNMP,  - umożliwiać uruchomienie automatycznego monitoringu zdarzeń w celu diagnozy i usuwania usterek oraz w zakresie konserwacji – musi mieć możliwość automatycznej diagnozy i samodzielnego zgłaszania usterek w centrum serwisowym producenta.  Wymagane jest dostarczenie wszystkich niezbędnych licencji potrzebnych do zrealizowania powyższych funkcjonalności. |  |
| 10 | Wspierane systemy operacyjne | Wsparcie, dla co najmniej MS Windows 2012 R2, VMware 5.X oraz Linux RedHat 6.x oraz SUSE 11.x.  Wsparcie dla systemów klastrowych, co najmniej, RedHat Cluster, Suse Cluster, MSCS.  Wsparcie musi być dostępne w ramach oferowanych licencji oprogramowania. |  |
| 11 | Obsługiwane protokoły | System musi obsługiwać protokoły plikowe: NFS V3 i V4, CIFS 2.0 i 3.0, FTP, HTTP.  Oferowane rozwiązanie pamięci dyskowej musi obsługiwać protokół NDMP w wersji 3 oraz 4 dla kopii zapasowych na taśmach, z dowolnego obszaru systemu plików. |  |
| 16 | Wysoka dostępność macierzy | Zdublowanie następujących elementów macierzy:   1. kontrolery macierzowe, 2. wentylatory, 3. zasilacze (odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy).   Dostęp do urządzenia oraz do składowanych na nim danych musi być realizowany bez przerywania pracy korzystającej z niego aplikacji/systemu, nawet w przypadku awarii lub wymiany pojedynczego elementu urządzenia z ww. grup urządzeń.  Macierz musi umożliwiać aktualizację mikrokodu w trybie online bez przerywania dostępu do zasobów dyskowych. |  |
| 17 | Zasilanie | Napięcie jednofazowe zmienne 230 V, 50 Hz. lub napięcie trójfazowe zmienne 400 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  |

#### Wirtualizacja macierzy dyskowych.

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.STO.VRT |
| **Nazwa** | Wirtualizacja macierzy dyskowych |

| **Lp.** | **Element/cecha** | **Minimalne parametry techniczne** | **Atrybuty** |
| --- | --- | --- | --- |
| 1 | Wirtualizacja zasobów dyskowych pamięci masowych | Rozwiązanie musi umożliwiać wirtualizację zasobów dyskowych pamięci masowych (macierzy) dyskowych pochodzących od różnych dostawców, m. in. HP, IBM, EMC, HDS na poziomie sieci SAN.  Wirtualizacja rozumiana jest jako możliwość podłączenia LUNów z macierzy dyskowych do oferowanego rozwiązania, a następnie udostępnienie tych zasobów do hostów poprzez wymagane protokoły dostępu w sposób nienaruszający zawartości tych wolumenów (prezentacja 1 do 1).  Rozwiązanie musi umożliwiać prezentacje zwirtualizowanych zasobów dyskowych do aplikacji pracujących na różnych platformach OS, mi. in Linux, MS Windows, Solaris, VMware.  Rozwiązanie musi posiadać możliwość dynamicznej zmiany wielkości prezentowanych jednostek LUN oraz wolumenów w trakcie pracy.  Wirtualizator musi umożliwiać prezentowanie do aplikacji wolumenów wirtualnych będących złożeniem wielu fizycznych wolumenów logicznych wystawionych z macierzy dyskowych. Wymagana jest możliwość łączenia ze sobą fizycznych wolumenów logicznych prezentowanych z różnych macierzy dyskowych. Wymagana jest możliwość łączenia ze sobą wolumenów logicznych za pomocą konkatenacji oraz stripingu.  Wirtualizator musi umożliwiać prezentowanie do aplikacji wolumenów wirtualnych składających się z dwóch fizycznych wolumenów logicznych połączonych relacją kopii lustrzanej. Wymagane jest, aby w wypadku niedostępności jednego z fizycznych wolumenów logicznych nie nastąpiła przerwa w dostępie do wirtualnego wolumenu logicznego.  Wirtualizator musi umożliwiać przenoszenie danych należących do wirtualnego wolumenu logicznego pomiędzy fizycznymi wolumenami logicznymi (także należącymi do różnych macierzy dyskowych) bez przerywania dostępu do tego wirtualnego wolumenu logicznego.  Wirtualizator musi umożliwiać podzielenie fizycznego wolumenu logicznego prezentowanego z macierzy dyskowej i zaprezentowanie go jako kilku niezależnych wirtualnych wolumenów logicznych.  Wsparcie dla technologii VMware VAAI oraz VASA.  Wymagane jest dostarczenie pary wirtualizatorów umożliwiających wirtualizację zasobów macierzowych w ilości określonej atrybutem MIN WIRTUALIZACJA ZASOBÓW [TiB] użytkowej powierzchni dyskowej, zarówno lokalnie jak i pomiędzy lokalizacjami.  Rozwiązanie wirtualizujące musi posiadać wbudowany mechanizm pozwalający na realizację lokalnej lub zdalnej (trzeci ośrodek) kopii danych w trybie umożliwiającym jej odtworzenie na dowolny moment w czasie. Licencja realizująca powyższa funkcjonalność nie musi być oferowana w ramach postępowania. | MIN WIRTUALIZACJA ZASOBÓW [TiB] |
| 2 | Kontrolery i porty | Oferowane rozwiązanie musi umożliwiać podłączenie zasobów dyskowych służących mu później do składowania danych za pomocą protokołu Fibre Channel (FC).  Wirtualizator (w ramach pojedynczej lokalizacji) musi być wyposażony w min.:  - odpowiednią ilość kontrolerów wskazaną atrybutem ILOŚĆ KONTROLERÓW [szt.] gdzie każdy kontroler posiada min.:  - odpowiednią ilość portów Fibre Channel (FC) służących do komunikacji z serwerami określoną atrybutem ILOŚĆ PORTÓW FC FRONTEND [szt.] o prędkości określonej atrybutem MIN PRĘDKOŚĆ FC FRONTEND [Gb/s];  - odpowiednią ilość portów Fibre Channel (FC) służących do komunikacji z macierzami dyskowymi określoną atrybutem ILOŚĆ PORTÓW FC BACKEND [szt.] o prędkości określonej atrybutem MIN PRĘDKOŚĆ FC BACKEND [Gb/s];  - odpowiednią ilość portów Fibre Channel (FC) służących do komunikacji pomiędzy lokalizacjami określoną atrybutem MIN ILOŚĆ PORTÓW CLUSTER [szt.] o prędkości określonej atrybutem MIN PRĘDKOŚĆ FC WAN CLUSTER [Gb/s].  - odpowiednią ilość portów Fibre Channel (FC) służących do komunikacji pomiędzy lokalizacjami określoną atrybutem MIN ILOŚĆ PORTÓW INTERLINK [szt.] o prędkości określonej atrybutem MIN PRĘDKOŚĆ FC INTERLINK [Gb/s]. | ILOŚĆ KONTROLERÓW [szt.] = **8**  ILOŚĆ PORTÓW FC FRONTEND [szt,] = **4**  MIN PRĘDKOŚĆ FC FRONTEND [Gb/s] = **8**  ILOŚĆ PORTÓW FC BACKEND [szt.] = **4**  MIN PRĘDKOŚĆ FC BACKEND [Gb/s] = **8**  MIN ILOŚĆ PORTÓW CLUSTER [szt.] = **4**  MIN PRĘDKOŚĆ FC CLUSTER [Gb/s]. = **8**  MIN ILOŚĆ PORTÓW INTERLINK [szt.] = **2**  MIN PRĘDKOŚĆ FC INTERLINK [Gb/s]. = **8** |
| 3 | Wysoka dostępność | Rozwiązanie musi być wykonane w architekturze w pełni nadmiarowej, nie posiadającej pojedynczych punktów awarii.  Rozwiązanie musi zapewniać ciągłość pracy (dostęp do danych) w przypadku awarii kontrolera.  Rozwiązanie musi zapewniać mechanizmy LUN masking i obsługę wielościeżkowości. |  |
| 4 | Replikacja danych | Rozwiązanie musi umożliwiać replikację synchroniczną danych na odległość określona atrybutem OD - DO ODLEGŁOŚĆ DC [km] przy wykorzystaniu łącz światłowodowych (DWDM). | OD - DO ODLEGŁOŚĆ DC [km] = **od 1 km do 150 km** |
| 5 | Kopie migawkowe | Wirtualizator musi zapewniać możliwość tworzenia kopii migawkowych (tzw. Snapshot) dla udostępnianych przez niego przestrzeni dyskowych. Wymagane jest dostarczenie wszystkich niezbędnych licencji w celu realizacji powyższych wymagań.  Dopuszcza się realizację funkcjonalności przy pomocy urządzeń zewnętrznych przy czym nie może to mieć wpływu na wydajność wirtualizatora |  |
| 6 | Pamięć RAM | Rozwiązanie musi oferować możliwość wykorzystania pamięci typu cache dla operacji odczytu. Ilość pamięci cache określona atrybutem MIN PAMIĘĆ RAM [GB] dla każdego kontrolera (noda) wirtualizatora. | MIN PAMIĘĆ CACHE [GB] = **36 GB** |
| 7 | Zarządzanie | Rozwiązanie musi umożliwiać zarządzanie za pomocą interfejsu graficznego oraz linii komend bez potrzeby instalowania dodatkowego serwera zarządzającego.  Oprogramowanie do zarządzania musi umożliwiać prezentację bieżących jak i historycznych danych dotyczących jego funkcjonowania (np. zajętość dysków, obciążenie, opóźnienia)  Wymagane jest dostarczenie wszystkich niezbędnych licencji w celu realizacji powyższych wymagań. |  |
| 8 | Migracja danych | Rozwiązanie musi umożliwić migracje danych pomiędzy macierzami różnych producentów w sposób zapewniający ciągły dostęp do danych podczas całego procesu.  Wymagane jest dostarczenie wszystkich niezbędnych licencji w celu realizacji powyższych wymagań.  Rozwiązanie musi zapewnić możliwość mirroringu tj. udostępnienia pojedynczej przestrzeni dyskowej do host’ów składjącej się z dwóch dysków logicznych udostępnionych z dwóch różnych macierzy dyskowych. |  |
| 9 | Thin provisioning | Rozwiązanie musi umożliwić maksymalizację wykorzystanie przestrzeni dyskowej poprzez wirtualne wolumeny, które alokują fizycznie tylko aktualnie niezbędne miejsce, a logicznie prezentując się systemowi z docelową wielkością.  Wymagane jest dostarczenie wszystkich niezbędnych licencji w celu realizacji powyższych wymagań. |  |
| 10 | Wsparcie dla środowisk oddalonych geograficznie (DR) | Rozwiązanie musi umożliwić dostępność aplikacji poprzez zapewnienie jednoczesnego dostępu do pamięci masowych w dwóch odległych ośrodkach przetwarzania danych w trybie active/active.  Rozwiązanie musi umożliwiać instalację pary wirtualizatorów w dwóch oddalonych od siebie centrach przetwarzania danych (ośrodkach) i połączenie ich ze sobą w celu umożliwienia wirtualizacji zasobów dyskowych pomiędzy tymi centrami – rozwiązanie separowane geograficznie.  Wymagane jest, aby rozwiązanie umożliwiało transmisję danych pomiędzy ośrodkami w trybie synchronicznym oraz asynchronicznym. Nie jest wymagane zapewnienie obu trybów transmisji jednocześnie.  Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało oddalenie pary wirtualizatorów na odległość, dla której maksymalne opóźnienie transmisji danych RTT określone jest atrybutem MAX RTT SYNC [ms] dla transmisji synchronicznej oraz określone jest atrybutem MAX RTT ASYNC [ms] dla transmisji asynchronicznej.  Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało prezentację tego samego wirtualnego wolumenu logicznego w obu ośrodkach jednocześnie. W obu ośrodkach wirtualny wolumen logiczny musi być prezentowany jednocześnie w trybie zapis/odczyt – tzw. – tzw. urządzenie dystrybuowane przez wszystkie kontrolery wirtualizatora.  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 oraz asynchronicznego trybu replikacji.  Wymagane jest, aby rozwiązanie separowane geograficznie umożliwiało zastosowanie arbitra, znajdującego się w trzeciej lokalizacji, w celu uniknięcia zjawiska split-brain w przypadku awarii komunikacji DWDM (SAN) pomiędzy centrami przetwarzania danych. Komunikacja z arbitrem musi odbywać się za pośrednictwem sieci WAN (Ethernet).  Rozwiązanie separowane geograficznie musi posiadać mechanizmy umożliwiające pracę, przy zachowaniu pełnej funkcjonalności oraz bezpieczeństwa i spójności danych także bez stosowania arbitra.  Zamawiający wymaga dostarczenia rozwiązania separowanego geograficznie wykorzystującego synchroniczny tryb transmisji danych. | MAX RTT SYNC [ms] = **5**  MAX RTT ASYNC [ms] = **50** |

#### Biblioteka wirtualna

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.STO.VLB |
| **Nazwa** | Biblioteka wirtualna. |

|  |  |  |
| --- | --- | --- |
| **Element/cecha** | **Minimalne parametry techniczne** | **Atrybut** |
| Pojemność | Urządzenie musi posiadać pojemność określoną atrybutem POJEMNOŚĆ NETTO [TiB] (po odjęciu przestrzeni wykorzystywanej na zabezpieczenie RAID) przeznaczonej na przechowywanie unikalnych segmentów danych (backupów). | POJEMNOŚĆ NETTO [TiB] |
| Pojemność - skalowanlość | Urządzenie musi posiadać możliwość rozbudowy do pojemności określonej atrybutem ROZBUDOWA POJEMNOŚCI NETTO [TiB] (po odjęciu przestrzeni wykorzystywanej na zabezpieczenie RAID) przeznaczonej na przechowywanie unikalnych segmentów danych (backupów). | ROZBUDOWA POJEMNOŚCI NETTO [TiB] |
| Interfejsy | Urządzenie musi posiadać minimum :   * 1. porty Ethernet 1 Gb określone atrybutem PORTY ETHERNET 1 Gb [szt.] (wymagane w urządzeniu) i możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle,   2. porty Ethernet 10 Gb określone atrybutem PORTY ETHERNET 10 Gb [szt.] (wymagane w urządzeniu) i możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle   3. porty FC 8Gb określone atrybutem PORTY FC 8Gb [szt.] i możliwość obsługi każdym portem FC protokołów VTL, de-duplikacja na źródle | PORTY ETHERNET 1 Gb [szt.] = **4**  PORTY ETHERNET 10Gb [szt.] = **2**  PORTY FC 8Gb [szt.] = **2** |
| Interfejsy - skalowalność | Urządzenie musi mieć możliwość (przyszła rozbudowa) rozszerzenia o dodatkowe porty. Zamawiający musi mieć możliwość rozszerzenia o dowolną z możliwości:   1. porty Ethernet 1 Gb określone atrybutem PORTY ETHERNET 1 Gb ROZBUDOWA [szt.] i możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle 2. porty FC 8Gb określone atrybutem PORTY FC ROZBUDOWA 8Gb [szt.] i możliwość obsługi każdym portem FC protokołów VTL, de-duplikacja na źródle 3. porty Ethernet 10 Gb określone atrybutem PORTY ETHERNET ROZBUDOWA 10 Gb [szt.] i możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, de-duplikacja na źródle | PORTY ETHERNET 1 Gb ROZBUDOWA [szt.] = **12**  PORTY FC ROZBUDOWA 8Gb [szt.] = **6**  PORTY ETHERNET ROZBUDOWA 10 Gb [szt.] = **2** |
| Protokoły | Urządzenie musi zapewniać jednoczesny dostęp wszystkimi poniższymi protokołami czyli dla Ethernet:   * CIFS, NFS de-duplikacja na źródle   oraz jednocześnie dla FC   * VTL, de-duplikacja na źródle |  |
| Licencje | Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, de-duplikacja na źródle do pełnej pojemności urządzenia. |  |
| Wydajność | Pojedyncze urządzenie musi osiągać zagregowaną wydajność protokołami CIFS, NFS, VTL określoną atrybutem WYDAJNOŚĆ [TB/h] (dane podawane przez producenta) oraz określoną atrybutem WYDAJNOŚĆ DEDUPLIKACJA NA ŹRÓDLE [TB/h] z wykorzystaniem de-duplikacji na źródle OST/BOOST (dane podawane przez producenta). | WYDAJNOŚĆ [TB/h] = **12**  WYDAJNOŚĆ DEDUPLIKACJA NA ŹRÓDLE [TB/h] = **28** |
| Strumienie | Urządzenie musi pozwalać na jednoczesną obsługę strumieni określonych atrybutem MIN. LICZBA STRUMIENI JEDNOCZESNYCH [szt.] w tym:   * określonego atrybutem MIN. LICZBA STRUMIENI DLA ZAPISU DANYCH [szt.] * określonego atrybutem MIN. LICZBA STRUMIENI DLA ODCZYTU DANYCH [szt.] * określonego atrybutem MIN. LICZBA STRUMIENI DLA REPLIKACJI [szt.]   pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, de-duplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie wszystkich dla zapisu i jednocześnie wszystkich strumieni dla odczytu i jednocześnie wszytstkich strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej de-duplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. | MIN. LICZBA STRUMIENI JEDNOCZESNYCH [szt.] = **540**  MIN. LICZBA STRUMIENI DLA ZAPISU DANYCH [szt.] = **340**  MIN. LICZBA STRUMIENI DLA ODCZYTU DANYCH [szt.] = **150**  MIN. LICZBA STRUMIENI DLA REPLIKACJI [szt.] = **50** |
| Emulacja VTL | Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:   * StorageTek L180 * Adic Scalar i2000 * Adic Scalar i6000 * IBM 3500 |  |
| Emulacja LTO | Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO1, LTO2, LTO3, LTO4. LTO-5 |  |
| VTL | Urządzenie musi eksportować i importować definicje bibliotek taśmowych. Musi być możliwość eksportu / importu definicji bibliotek taśmowych między różnymi modelami urządzeń producenta. |  |
| Deduplikacja | Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia. |  |
| Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi automatycznie dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. |
| De-duplikacja zmiennym, dynamicznym blokiem musi oznaczać, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) jest inna niż poprzedniego i jest indywidualnie ustalana przez algorytm urządzenia. |
| Urządzenie musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, de-duplikacja na źródle) przechowywanych w obrębie całego urządzenia.  Raz otrzymany i zapisany w urządzeniu fragment danych nie może nigdy więcej zostać zapisany niezależnie od fizycznej i logicznej konfiguracji urządzenia oraz bez względu na to, jakim protokołem zostanie ponownie otrzymany. |
| Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej de-duplikacji pomiędzy wirtualnymi bibliotekami (rozszerzenie w przyszłości). Blok danych otrzymany i zapisany w wirtualnej bibliotece A, nie powinien nigdy więcej zostać zapisany bez względu do jakiej wirtualnej biblioteki trafi. |
| Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych. |
| Proces de-duplikacji powinien odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. |
| Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej). |
| Kompatybilność z systemami backupu | Urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie: HP Data Protector, IBM TSM, Symantec NetBackup, EMC Networker, EMC, Avamar, Oracle RMAN, IBM BRMS, IBM DB2, VMware VDP, SAP, SAP HANA, MSSQL, Veeam. |  |
| W przypadku współpracy z każdą z poniższych aplikacji:   * Oracle RMAN (bez dodatkowego oprogramowania backupowego) * Microsoft MSSQL (bez dodatkowego oprogramowania backupowego) * IBM DB2 (bez dodatkowego oprogramowania backupowego) * SAP/Oracle (bez dodatkowego oprogramowania backupowego) * SAP HANA (bez dodatkowego oprogramowania backupowego) * VMware VDP (vShpehre Data Protection) * Symantec NetBackup * Symantec BackupExec * HP Data Protector * EMC NetWorker * EMC Avamar * Veeam   urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  De-duplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność Media Servera NetBackup’a / Agenta Avamara / serwera RMAN / serwera SQL / serwera SAP / serwera DB2, maszyny VDP / klienta systemu NetWorker nie posiadającego licencji Storage Node.  De-duplikacja w wyżej wymienionych przypadkach musi zapewniać by z serwerów do urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.  Ewentualna licencja na de-duplikację na źródle musi być dostarczona w ramach postępowania. |  |
| Deduplikacja | W przypadku przyjmowania backupów od aplikacji Symantec NetBackup, EMC NetWorker, Oracle RMAN, Microsoft MSSQL, IBM DB2, SAP/Oracle, SAP HANA, Veeam urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  De-duplikacja w wyżej wymienionych przypadkach musi zapewniać by z serwerów do urządzenia były transmitowane poprzez sieć FC tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. |  |
| W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WA), musi być możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |  |
| Backup Syntetyczny | Dla aplikacji Symantec NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z urządzenia. Zarządzanie łączeniem backupów pełnych i inkrementalnych musi być wykonywane z poziomu aplikacji Symantec NetBackup, EMC NetWorker |  |
| Replikacja | Urządzenie musi umożliwiać bezpośrednią replikację danych do obecnego urządzenia Data Domain DD4500. Konfiguracja replikacji musi być możliwa dwukierunkowo.  Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania. |  |
| Urządzenie musi również umożliwiać wydzielenie określonych portów Ethernet do replikacji. |
| W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
| W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy VMware VDP / Symantec NetBackup / Symantec BackupExec / HP Data Protector / EMC Avamar / EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:   * replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących * replikacji podlegają tylko te fragmenty danych, które nie znajdują się w docelowym urządzeniu * replikacja zarządzana tylko jest z poziomu aplikacji backupowej * aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach |
| Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami. |
|  |
| RAID | Każda grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych. Dyski hot-spare muszą być globalne, możliwe do wykorzystania w innych półkach, w przypadku wyczerpania w nich dysków hot-spare.  Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6. |  |
| HotSpare | Łącznie urządzenie musi posiadać zapasowe dyski typu hot-spare stanowiące minimum 7% powierzchni roboczej urządzenia. |  |
| Urządzenie musi umożliwiać wykonywanie SnapShot’ów, czyli możliwość zamrożenia obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania backupów / odtwarzania). |
| Kopie Migawkowe | Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie. |  |
| Podział Logiczny | Urządzenie musi pozwalać na podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia). |  |
| Urządzenie musi mieć możliwość podziału na minimum 25 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 25 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
| Dla każdej z logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkowników zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
|  | Musi być możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia:   * CIFS * NFS * VTL * BOOST/OST |  |
| Dla każdej z logicznych części oferowanego urządzenia musi być możliwe zdefiniowanie blokady skasowania danych. Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):   1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (compliance)   Ewentualne licencje na blokadę usunięcia / zmiany przechowywanych plików nie musza dostarczone. Są elementem przyszłego rozszerzenia. |
| WORM | Urządzenie musi mieć możliwość trzymania danych niezmienialnych:   * Video * Grafika * Nagrania dźwiękowe * Pliki pdf   na udziałach CIFS/NFS.  Wymagane jest formalne wsparcie producenta dla trzymania powyższych danych na urządzeniu.  Wymagana jest formalne wsparcie producenta dla:   * przechowywania na urządzeniu minimum 500 milionów plików * dziennego zasilenia urządzenia na poziomie minimum 500 tysięcy plików |  |
| OS | Urządzenie musi mieć dedykowany, oddzielny system plików dla przechowywanych danych (backupy, archiwa).  System operacyjny urządzenia oraz logi urządzenia nie mogą być przechowywane na systemie plików dedykowanym dla przechowywanych danych. |  |
| Czas niedostępności | Po niespodziewanym wyłączeniu prądu urządzenia i ponownym uruchomieniu, urządzenie musi być gotowe do przyjmowania danych (backupy, archiwa) w czasie nie dłuższym niż 60 minut od włączenia. |  |
| Weryfikacja danych | Urządzenie musi weryfikować ewentualne przekłamanie (zmianę danych) w wyniku działań:   * systemu plików * RAID   zaimplementowanych w urządzeniu.  Wymaga się by urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych po przejściu danych przez system plików / RAID. |  |
| Urządzenie musi weryfikować dane po zapisie. Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Wymagane potwierdzenie faktu weryfikacji danych po zapisie w dokumencie producenta. |
| Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych da dysk oraz rozpoznawać i naprawiać błędy w locie.  Każde zapisane na fizycznych dyskach dane muszą być odczytane i porównane z danymi otrzymanymi. Proces ten musi dziać się w locie – musi być elementem procesu zapisu danych przez urządzenie. |
| Reklamacja | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |  |
| Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracę procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
| Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora) |
| Musi istnieć możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia). |
| Musi być możliwość by usuwanie przeterminowanych danych (czyszczenie) odbywało się raz na tydzień minimalizując czas w którym backupy / odtworzenia narażone są na spowolnienie. |
| Zarządzanie | Urządzenie musi mieć możliwość zarządzania poprzez   * Interfejs graficzny dostępny z przeglądarki internetowej * Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |  |
| Oprogramowanie do zarządzania musi rezydować oferowanym na urządzeniu de-duplikacyjnym. |
| Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy spradzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. |
| Szyfrowanie danych | Oferowany produkt musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych przed zapisaniem na dysk realizowany na poziomie urządzenia – długość klucza minimum 256-bit. Ewentualna licencja szyfrowania nie jest przedmiotem niniejszego zamówienia. |  |
| Dodatkowe | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway z uwagi na brak miarodajnych danych dotyczących ich wydajności oraz dostępności. |  |

#### Biblioteka taśmowa

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.STO.TLB |
| **Nazwa** | Biblioteka taśmowa. |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Liczba napędów | Oferowana biblioteka taśmowa musi być wyposażona w sześć napędów LTO Ultrium-5 o wydajności, co najmniej 140 MB/s oraz pojemności pojedynczej taśmy, co najmniej 1.5 TB – parametry podane bez kompresji danych. Napędy muszą wspierać sprzętowe szyfrowanie danych w standardzie AES-256. |
| Typy napędów | Biblioteka musi posiadać możliwość pracy z napędami taśm LTO-5 oraz LTO-4.  Musi istnieć możliwość wymiany napędu bez wyłączania biblioteki.  Oferowany napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie, co najmniej 47-140 MB/s. |
| Liczba slotów | Oferowana biblioteka musi być wyposażona, w co najmniej 200 slotów na taśmy magnetyczne. |
| Interfejs | Oferowane napędy LTO-5 muszą posiadać interfejs FC. |
| Rozbudowa | Oferowana biblioteka taśmowa musi posiadać możliwość rozbudowy do minimum 16 napędów LTO z kwantem 4 napędy na jeden moduł obsługujący napędy. |
| Obudowa | Oferowana biblioteka taśmowa musi być przystosowana do montażu w szafie stelażowej 19”. |
| Zarządzanie | Oferowana biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej.  Biblioteka musi być wyposażona w panel LCD przeznaczony do jej obsługi. |
| Inne | Oferowana biblioteka musi być wyposażona w czytnik kodów kreskowych etykiet taśm.  Oferowana biblioteka taśmowa musi posiadać możliwość wykorzystania, co najmniej pięciu i mieć możliwość rozbudowy do piętnastu, interfejsów (ang. *mail slots)*, umożliwiających wymianę pojedynczej taśmy bez konieczności wyjmowania z biblioteki całego magazynka z taśmami. |
| Nośniki danych | Oferowana konfiguracja biblioteki taśmowej musi zawierać minimum 70 taśm o pojemności minimum 1.5 TB bez kompresji danych oraz minimum 2 taśmy czyszczące.  Oferowane nośniki taśmowe muszą mieć spersonalizowane kody paskowe (ang. customized barcode). |
| Niezawodność | Dla oferowanej biblioteki taśmowej parametr MTBF musi wynosić, co najmniej 100 000 godzin.  Dla oferowanej biblioteki taśmowej parametr MSBF musi wynosić, co najmniej 2 000 000 pełnych cykli „załaduj/wyładuj”. |
| Wsparcie systemów | Oferowana biblioteka taśmowa musi posiadać wsparcie dla następującego oprogramowania służącego do tworzenia kopii bezpieczeństwa:   * HP Storage Data Protector, * EMC NetWorker, * IBM Tivoli Storage Manager, * Symantec Backup Exec, * Symantec NetBackup. |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Redundantne zasilacze i wentylatory typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. | |

#### Przełączniki SAN – Szkielet komunikacyjny

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.SAN.SW.1 |
| **Nazwa** | Przełączniki SAN w szkielecie komunikacyjnym |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Architektura | Możliwość dostępu do zasobów macierzy realizowana jest poprzez redundantną sieć Storage Area Network (SAN) opartą o technologię FC o prędkości określanej przez atrybut: MAX PRĘDKOŚĆ PORTÓW PRZEŁĄCZNIKÓW | -MAX PRĘDKOŚĆ PORTÓW PRZEŁĄCZNIKÓW [Gbps] | |
| Interfejsy FC | Wymagane dostarczenie dla każdego przełącznika minimum 3 kart rozszerzeń z dostępną liczbą portów określanych przez parametr LICZBA PORTÓW KARTY każda karta wraz z wkładkami FC oraz licencjami na dostarczane porty | - LICZBA PORTÓW KARTY | |
| Możliwości rozbudowy | Przełącznik musi nieć możliwość rozbudowy do liczby portów określanej przez atrybut: -MAX MOŻLIWA LICZBA PORTÓW  Możliwość połączenia z drugim przełącznikiem tej samej klasy za pomocą dedykowanych interfejsów o przepustowości minimum 512 Gb/s w celu zwiększenia liczby portów do minimum 1000.  Możliwość instalacji w obrębie obudowy, portów do obsługi protokołu FCoIP oraz FCoE..  Możliwość uruchomienia funkcjonalności szyfrowania ruchu w sieci SAN za pomocą szyfratora sprzętowego montowanego w obudowie przełącznika.  Możliwość łączenia przełączników za pomocą dedykowanych szybkich połączeń zgodnie ze standardem IST (InterSwitch Trunk), | -MAX MOŻLIWA LICZBA PORTÓW | |
| Zagregowana przepustowość wewnętrzna | Minimum o prędkości określanej przez atrybut: -PRZEPUSTOWOŚĆ WEWNĘTRZNA | -PRZEPUSTOWOŚĆ WEWNĘTRZNA [Tbps] | |
| Agregacja połączeń | Możliwość agregacji kilku połączeń fizycznych w jedno połączenie logiczne dwóch przełączników. Wymagane dostarczenie funkcjonalności agregacji dla minimum 8 połączeń fizycznych. |  | |
| Dodatkowe oprogramowanie | Możliwość zarządzanie pasmem (Quality of Service) w połączeniach pomiędzy przełącznikami. Wymagane dostarczenie funkcjonalności zarządzania pasmem.  Możliwość agregowania kilku połączeń fizycznych w jedno połączenie logiczne o maksymalnej przepustowości na jednym połączeniu 64 Gb/s (ISL).  Możliwość ograniczania przepustowości łącza bez względu na wynegocjowaną prędkość połączenia (Adaptive Networking).  Możliwość proaktywnej detekcji awarii (Fabric Vision).  Możliwość realizacji połączeń ISL na odległość większą niż 10 km. (Extended Fabric). |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |

#### Przełączniki SAN – lokalny węzeł rdzeniowy

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.SAN.SW.2 |
| **Nazwa** | Przełączniki SAN w lokalnym węźle rdzeniowym |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Architektura | Możliwość dostępu do zasobów macierzy realizowana jest poprzez redundantną sieć Storage Area Network (SAN) opartą o technologię FC 8 Gb/s. | |
| Interfejsy FC | 24 porty w jednym przełączniku z wkładkami FC 8 Gb/s typu ShortWave dla każdego portu. | |
| Możliwości rozbudowy | Przełącznik musi mieć możliwość rozbudowy do minimum 40 portów. | |
| Dodatkowe oprogramowanie | Możliwość zarządzanie pasmem (Quality of Service) w połączeniach pomiędzy przełącznikami.  Wymagane dostarczenie funkcjonalności zarządzania pasmem.  Możliwość agregowania kilku połączeń fizycznych w jedno połączenie logiczne o maksymalnej przepustowości na jednym połączeniu 64 Gb/s (ISL).  Możliwość ograniczania przepustowości łącza bez względu na wynegocjowaną prędkość połączenia (Adaptive Networking).  Możliwość proaktywnej detekcji awarii (Fabric Watch).  Możliwość realizacji połączeń ISL na odległość większą niż 10 km. (Extended Fabric).  Możliwość routingu portów (Integrated Routing). | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. | |

#### Przełączniki rdzeniowe

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.1 |
| **Nazwa** | Przełączniki rdzeniowe LAN/WAN |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Pojemność przełączania backplane | Możliwość komunikacji sieciowej pomiędzy środowiskiem serwerowym a infrastruktura sieciową realizowane jest poprzez redundantną sieć LAN opartą na przełącznikach dystrybucyjnych o pojemności przełączania backplane określanej przez atrybut: MIN POJEMNOŚĆ PRZEŁĄCZANIA | - MIN POJEMNOŚĆ PRZEŁĄCZANIA [Tb/s] | |
| Prędkość przełączania pakietów | Przełącznik musi charakteryzować się minimalną pojemnością przełączania pakietów okteślane atrybutem – MIN prędkość przełączania pakietów | - MIN prędkość przełączania pakietów [Mb/s] | |
| Interfejsy sieciowe 40Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 40Gb QSFP+ określanej atrybutem MIN liczba portów 40Gb | - MIN liczba portów 40Gb [szt.] | |
| Interfejsy sieciowe 10Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 10Gb Ethernet określonej atrybutem MIN liczba portów 10Gb | -MIN liczba portów 10Gb [szt.] | |
| Interfejsy sieciowe 1Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 1Gb Ethernet zależnie od wykorzystanej wkładki MIN liczba portów 1Gb | -MIN liczba portów 1Gb [szt.] | |
| Liczba gniazd kart liniowych | Przełącznik musi mieć możliwość rozbudowy o dodatkowe karty liniowe w liczbie minimum określanej przez atrybut MIN liczba kart liniowych | - MIN liczba kart liniowych [szt.] | |
| Redundancja zarządzania | Przełącznik musi posiadać liczbę interfejsów przeznaczonych do zarządzania w liczbie nie mniejszej jak atrybut określany mianem MIN liczba interfejsów MGMT przy założeniu, że moduł zarządzający posiada jeden interfejs MGMT | - MIN liczba interfejsów MGMT [szt.] | |
| Wirtualizacja | Przełącznik musi posiadać możliwość tworzenia logicznych wirtualnych kontekstów (wykorzystując zasoby fizycznego urządzenia) które z punku widzenia zarządzania oraz działania zachowywać się będą jak odrębne przełączniki o funkcjonalnościach macierzystego urządzenia |  | |
| Obsługa funkcjonalności STP | Przełącznik musi mieć możliwość obsługi protokołów: RSTP i MSTP. |  | |
| Obsługa funkcjonalności QoS | Priorytetyzacja zgodna z IEEE 802.1p, priorytetyzacja na bazie warstwy 4 modelu OSI, kontrola pakietów rozgłoszeniowych, klasyfikacja ruchu na bazie wielu kryteriów protokołów warstwy 2, 3 i 4 modelu OSI, regulacja pasma za pomocą algorytmów bazujących na portach i/lub klasyfikatorach pakietów. |  | |
| Obsługa funkcjonalności VLAN | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. |  | |
| Obsługiwane protokoły i funkcje | Obsługa protokołów: RIP, OSPF, BGP, IS-IS, VRRP, możliwość uruchomienia MPLS, DLDP lub UDLD.  Obsługa funkcji: Non Stop Forwarding/Graceful Restart (NSF/GR).  Wsparcie dla IPv6. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| System zarządzania | Kompatybilność z systemami zarządzania posiadanymi przez Zamawiającego lub równoważnym systemem zarządzania dostarczonym przez Wykonawcę\* (patrz 1.2.2.15.4) |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  | |
| Redundancja dla modułów liniowych | Zamawiający wymaga dostarczenia redundancji dla modułów liniowych 10GB (N+N) |  | |

#### Przełączniki dystrybucyjne – LAN/WAN

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.2 |
| **Nazwa** | Przełączniki dystrybucyjne – LAN/WAN |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Pojemność przełączania backplane | Możliwość komunikacji sieciowej pomiędzy środowiskiem serwerowym a infrastruktura sieciową realizowane jest poprzez redundantną sieć LAN opartą na przełącznikach dystrybucyjnych o pojemności przełączania backplane określanej przez atrybut: MIN POJEMNOŚĆ PRZEŁĄCZANIA | - MIN POJEMNOŚĆ PRZEŁĄCZANIA [Tb/s] | |
| Prędkość przełączania pakietów | Przełącznik musi charakteryzować się minimalną pojemnością przełączania pakietów okteślane atrybutem – MIN prędkość przełączania pakietów | - MIN prędkość przełączania pakietów [Mb/s] | |
| Interfejsy sieciowe 40Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 40Gb QSFP+ określanej atrybutem MIN liczba portów 40Gb | - MIN liczba portów 40Gb [szt.] | |
| Interfejsy sieciowe 10Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 10Gb Ethernet określonej atrybutem MIN liczba portów 10Gb | -MIN liczba portów 10Gb [szt.] | |
| Interfejsy sieciowe 1Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 1Gb Ethernet (1000BASE-T) zależnie od wykorzystanej wkładki MIN liczba portów 1Gb | -MIN liczba portów 1Gb [szt.] | |
| Liczba gniazd kart liniowych | Przełącznik musi mieć możliwość rozbudowy o dodatkowe karty liniowe w liczbie minimum określanej przez atrybut MIN liczba kart liniowych | - MIN liczba kart liniowych [szt.] | |
| Redundancja zarządzania | Przełącznik musi posiadać liczbę interfejsów przeznaczonych do zarządzania w liczbie nie mniejszej jak atrybut określany mianem MIN liczba interfejsów MGMT przy założeniu, że moduł zarządzający posiada jeden interfejs MGMT | - MIN liczba interfejsów MGMT [szt.] | |
| Wirtualizacja | Przełącznik musi posiadać możliwość tworzenia logicznych wirtualnych kontekstów (wykorzystując zasoby fizycznego urządzenia) które z punku widzenia zarządzania oraz działania zachowywać się będą jak odrębne przełączniki o funkcjonalnościach macierzystego urządzenia |  | |
| Obsługa funkcjonalności STP | Przełącznik musi mieć możliwość obsługi protokołów: RSTP i MSTP. |  | |
| Obsługa funkcjonalności QoS | Klasyfikacja ważności ruchu na bazie list kontroli dostępu, techniką IEEE 802.1p CoS, IP, DSCP lub Type of Service (ToS); filtrowanie, przekierowanie, powielanie lub znacznikowanie; kolejkowanie zgodnie z algorytmami: strict priority (SP), weighted fair queuing (WFQ), weighted random early discard (WRED) lub Shaped Round Robin (SRR) oraz Weighted Tail Drop (WTD). |  | |
| Obsługa funkcjonalności VLAN | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| System zarządzania | Kompatybilność z systemami zarządzania posiadanymi przez Zamawiającego lub równoważnym system zarządzania dostarczonym przez Wykonawcę\* (patrz 1.2.2.15.4) |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  | |
| Redundancja dla modułów liniowych | Zamawiający wymaga dostarczenia redundancji dla modułów liniowych 10GB (N+N) |  | |

#### Przełączniki dystrybucyjne – bramka Internetowa

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.5 |
| **Nazwa** | Przełączniki dystrybucyjne – bramka Internetowa |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Pojemność przełączania backplane | Możliwość komunikacji sieciowej pomiędzy środowiskiem serwerowym a infrastruktura sieciową realizowane jest poprzez redundantną sieć LAN opartą na przełącznikach dystrybucyjnych o pojemności przełączania backplane określanej przez atrybut: MIN POJEMNOŚĆ PRZEŁĄCZANIA | - MIN POJEMNOŚĆ PRZEŁĄCZANIA [Tb/s] | |
| Prędkość przełączania pakietów | Przełącznik musi charakteryzować się minimalną pojemnością przełączania pakietów okteślane atrybutem – MIN prędkość przełączania pakietów | - MIN prędkość przełączania pakietów [Mb/s] | |
| Interfejsy sieciowe 40Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 40Gb QSFP+ określanej atrybutem MIN liczba portów 40Gb | - MIN liczba portów 40Gb [szt.] | |
| Interfejsy sieciowe 10Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 10Gb Ethernet określonej atrybutem MIN liczba portów 10Gb | -MIN liczba portów 10Gb [szt.] | |
| Interfejsy sieciowe 1Gb | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 1Gb Ethernet (1000BASE-T) zależnie od wykorzystanej wkładki MIN liczba portów 1Gb | -MIN liczba portów 1Gb [szt.] | |
| Port konsoli | Przełącznik musi posiadać port konsoli do zarządzania lokalnego |  | |
| Port USB | Przełącznik musi posiadać port USB |  | |
| Liczba gniazd kart liniowych | Przełącznik musi mieć możliwość rozbudowy o dodatkowe karty liniowe w liczbie minimum określanej przez atrybut MIN liczba kart liniowych | - MIN liczba kart liniowych [szt.] | |
| Redundancja zarządzania | Przełącznik musi posiadać liczbę interfejsów przeznaczonych do zarządzania w liczbie nie mniejszej jak atrybut określany mianem MIN liczba interfejsów MGMT przy założeniu, że moduł zarządzający posiada jeden interfejs MGMT | - MIN liczba interfejsów MGMT [szt.] | |
| Obsługa funkcjonalności STP | Przełącznik musi mieć możliwość obsługi protokołów: RSTP i MSTP. |  | |
| Obsługa funkcjonalności QoS | Klasyfikacja ważności ruchu na bazie list kontroli dostępu, techniką IEEE 802.1p CoS, IP, DSCP lub Type of Service (ToS); filtrowanie, przekierowanie, powielanie lub znacznikowanie; kolejkowanie zgodnie z algorytmami: strict priority (SP), weighted fair queuing (WFQ), weighted random early discard (WRED) lub Shaped Round Robin (SRR) oraz Weighted Tail Drop (WTD). |  | |
| Obsługa funkcjonalności VLAN | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| System zarządzania | Kompatybilność z systemami zarządzania posiadanymi przez Zamawiającego lub równoważnym system zarządzania dostarczonym przez Wykonawcę\* (patrz 1.2.2.15.4) |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  | |
| Redundancja dla modułów liniowych | Zamawiający wymaga dostarczenia redundancji dla modułów liniowych 10GB (N+N) |  | |

##### Przełączniki dostępowe – 48 portów

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.3 |
| **Nazwa** | Przełączniki dostępowe LAN – 48 portów |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Pojemność przełączania | Możliwość komunikacji sieciowej w warstwie zarządzającej dostarczaną infrastrukturą serwerową oraz w warstwie DMZ poprzez redundantną sieć LAN opartą na przełącznikach o pojemności przełączania określanej przez atrybut: MIN POJEMNOŚĆ PRZEŁĄCZANIA | -MIN pojemność przełączania [Gb/s] | |
| Interfejsy sieciowe 1/10Gb SFP+ | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 1/10Gb (zależnie od wykorzystanej wkładki SFP) określonej przez atrybut MIN liczba portów 10Gb | -MIN liczba portów 10Gb [szt.] | |
| Porty 10/100/1000  IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 10/100/1000Mb określane atrybutem MIN liczba portów 1Gb | -MIN liczba portów 1Gb [szt.] | |
| Obsługa funkcjonalności STP | Przełącznik musi mieć możliwość obsługi protokołów: RSTP i MSTP. |  | |
| Obsługa funkcjonalności QoS | Klasyfikacja ważności ruchu na bazie list kontroli dostępu, techniką IEEE 802.1p CoS, IP, DSCP lub Type of Service (ToS); filtrowanie, przekierowanie, powielanie lub znacznikowanie; kolejkowanie zgodnie z algorytmami: strict priority (SP), weighted fair queuing (WFQ), weighted random early discard (WRED) lub Shaped Round Robin (SRR) oraz Weighted Tail Drop (WTD).. |  | |
| Obsługa funkcjonalności VLAN | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. |  | |
| Obsługa funkcjonalności agregacji portów | Obsługa protokołu 802.3ad Link Aggregation. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| Obsługa funkcjonalności STACK | Możliwość łączenia kilku przełączników w jeden logiczny (stack) |  | |
| Zarządzanie | Kompatybilność z systemami zarządzania posiadanymi przez Zamawiającego lub równoważnym system zarządzania dostarczonym przez Wykonawcę\* (patrz 1.2.2.15.4) |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  | |

##### Przełączniki dostępowe – 24 porty

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.4 |
| **Nazwa** | Przełączniki dostępowe LAN – 24 porty |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Pojemność przełączania backplane | Możliwość komunikacji sieciowej w warstwie zarządzającej dostarczaną infrastrukturą serwerową poprzez redundantną sieć LAN opartą na przełącznikach o pojemności przełączania backplane określanej przez atrybut: MIN POJEMNOŚĆ PRZEŁĄCZANIA | -MIN pojemność przełączania [Gb/s] | |
| Interfejsy sieciowe 1/10Gb SFP+ | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 1/10Gb zależnie od wykorzystanej wkładki SFP określane atrybutem MIN liczba portów 10Gb | -MIN liczba portów 10Gb [szt.] | |
| Porty 10/100/1000  IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 10/100/1000Mb określane atrybutem MIN liczba portów 1Gb | -MIN liczba portów 1Gb [szt.] | |
| Obsługa funkcjonalności STP | Przełącznik musi mieć możliwość obsługi protokołów: RSTP i MSTP. |  | |
| Obsługa funkcjonalności QoS | Klasyfikacja ważności ruchu na bazie list kontroli dostępu, techniką IEEE 802.1p CoS, IP, DSCP lub Type of Service (ToS); filtrowanie, przekierowanie, powielanie lub znacznikowanie; kolejkowanie zgodnie z algorytmami: strict priority (SP), weighted fair queuing (WFQ), weighted random early discard (WRED) lub Shaped Round Robin (SRR) oraz Weighted Tail Drop (WTD).. |  | |
| Obsługa funkcjonalności VLAN | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. |  | |
| Obsługa funkcjonalności agregacji portów | Obsługa protokołu 802.3ad Link Aggregation. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| Obsługa funkcjonalności STACK | Możliwość łączenia kilku przełączników w jeden logiczny (stack) |  | |
| Zarządzanie | Kompatybilność z systemami zarządzania posiadanymi przez Zamawiającego lub równoważnym system zarządzania dostarczonym przez Wykonawcę\* (patrz 1.2.2.15.4) |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  | |

##### Przełączniki dostępowy Top Of the Rack

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.6 |
| **Nazwa** | Przełączniki dostępowe LAN |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Pojemność przełączania backplane | Możliwość komunikacji sieciowej pomiędzy dostarczanym środowiskiem serwerowym a infrastruktura sieciową realizowane jest poprzez redundantną sieć LAN opartą na przełącznikach Top OF the Rack o pojemności przełączania backplane określanej przez atrybut: MIN POJEMNOŚĆ PRZEŁĄCZANIA | -MIN pojemność przełączania [Gb/s] | |
| Interfejsy sieciowe 1/10Gb SFP+ | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 1/10Gb zależnie od wykorzystanej wkładki SFP określane atrybutem MIN liczba portów SFP+ | -MIN liczba portów SFP+ [szt] | |
| Interfejsy sieciowe 40 Gb/s QSFP+ | Przełącznik musi mieć możliwość rozbudowy do liczby portów o prędkości 40Gb określonej atrybutem MIN liczba portów QSFP+ | -MIN liczba portów QSFP+ [szt] | |
| STP | Obsługa protokołów: RSTP i MSTP |  | |
| QoS | -Klasyfikacja ruchu w oparciu o: 802.1p CoS,  -Przynajmniej 8 kolejek sprzętowych per każdy port  -Konfiguracja QoS per port  -Weighted Round Robin (WRR) |  | |
| Obsługa VLAN’ów | -Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych)  -Grupowanie EtherChannel  -Ramki Jumbo dla wszystkich portów (min. 9216 bajtów)  -Private VLAN |  | |
| Agregacja portów | Możliwość obsługi protokołu 802.3ad Link Aggregation. |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |
| Zarządzanie | Kompatybilność z systemami zarządzania posiadanymi przez Zamawiającego lub równoważnym system zarządzania dostarczonym przez Wykonawcę\* (patrz 1.2.2.15.4) |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  | |

##### \* Równoważność dla dostarczanego przez Wykonawcę systemu zarządzania

* licencja na obsługę min. 200 urządzeń;
* możliwość zarządzania min 200 urządzeniami (grupowe wykonywanie poleceń z poziomu konsoli pojedynczego urządzenia);
* automatyczne wykonywanie poleceń na urządzeniach według ustalonego harmonogramu zadań;
* monitorowanie parametrów urządzeń w trybie LIVE takich jak: obciążenie procesora, utylizacja interfejsów, użycie pamięci, liczba połączeń;
* raportowanie i powiadamianie o błędach, awariach, incydentach polegających na przekroczeniu zdefiniowanych limitów za pomocą poczty elektronicznej;
* raportowanie stanu urządzeń oraz zarządzanie zdarzeniami syslog;
* raportowanie obciążenia urządzeń polegające na generowaniu dla grupy wybranych urządzeń historycznego obciążenia: procesora, utylizacji interfejsów, przepustowość interfejsów, zajętości pamięci, liczby połączeń i prezentowanie wyników w postaci wykresów graficznych i zestawień tabelarycznych;
* zarządzanie konfiguracjami(możliwość automatycznego archiwizowania konfiguracji z urządzeń, możliwość porównywania wersji konfiguracji między sobą, możliwość grupowego wprowadzania konfiguracji na urządzenia);
* zdalne i zautomatyzowane zarządzanie konfiguracją, poprawkami oraz obrazami systemów operacyjnych urządzeń sieciowych;
* kontrolę konfiguracji urządzeń pod kątem polityk zgodności i standardów;
* audyt konfiguracji;
* ewidencjonowanie urządzeń;
* system zarządzania musi pracować w trybie HA, klaster min. 2 urządzeń, zapewniając w ten sposób wysoką dostępność, przy czym awaria jednego z urządzeń nie może powodować niedostępności żadnej z funkcjonalności opisanych powyżej;
* wsparcie w/w funkcjonalności dla urządzeń sieciowych posiadanych przez Zamawiającego

Wykonawca zapewni wsparcie i gwarancję dla dostarczanego systemu oraz konto serwisowe umożliwiające dostęp do materiałów i najnowszych wersji oprogramowania producenta.

#### Zapory sieciowe – typ 1

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.FW.1 |
| **Nazwa** | Zapory sieciowe – typ 1 |

| **Element/cecha** | **Charakterystyka** |  |
| --- | --- | --- |
| Przepustowość zapory sieciowej | Określone atrybutem MIN PRZEPUSTOWOŚĆ | - MIN PRZEPUSTOWOŚĆ [Gb/s] | |
| Przepustowość dla funkcjonalności VPN IPSec | Określone atrybutem MIN PRZEPUSTOWOŚĆ VPN IPSec | - MIN PRZEPUSTOWOŚĆ VPN IPSec [Gb/s] | |
| Przepustowość funkcjonalności IPS | Określone atrybutem MIN PRZEPUSTOWOŚĆ IPS. | - MIN PRZEPUSTOWOŚĆ IPS [Gb/s] | |
| Liczba połączeń na sekundę | Określone atrybutem LICZBA POŁĄCZEŃ NA SEKUNDĘ | - LICZBA POŁĄCZEŃ NA SEKUNDĘ [SZT/s] | |
| Liczba jednoczesnych sesji | Określone atrybutem LICZBA JEDNOCZESNYCH SESJI | - LICZBA JEDNOCZESNYCH SESJI [SZT] | |
| Mechanizm przechowywania i śledzenia sesji TCP/UDP | Statefull inspection - dynamiczne tworzenie list dostępu na podstawie rzeczywistego stanu sesji. |  | |
| Funkcjonalność zapory | Obsługa VPN, NAT, obsługa protokołów IPv6. |  | |
| Liczba dostępnych interfejsów | Określone atrybutem MIN LICZBA INTERFEJSÓW 10/100/1000 Mb/s oraz MIN LICZBA INTERFEJSÓW SFP+ 10  Gb/s. | MIN LICZBA INTERFEJSÓW 10/100/1000 Mb/s [SZT]  MIN LICZBA INTERFEJSÓW SFP+ 10  Gb/s [SZT] | |
| Dedykowana konsola zarządzająca | System zarządzania musi zapewniać możliwość współpracy z co najmniej sześcioma sondami, bez konieczności wykupywania dodatkowych licencji w przyszłości  Logowanie zdarzeń:  - Ilość obsługiwanych zdarzeń – 10Gb na dzień.  - Korelacja zdarzeń ze wszystkich zarządzanych urządzeń.  Integracja z zewnętrznymi systemami typu SIEM  Integracja z zewnętrzną bazą LDAP, RADIUS  Wbudowane mechanizmy HA |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. |  | |
| Redundancja | Możliwość łączenia urządzeń w klastry wysokiej dostępności. |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |

#### Zapory sieciowe – typ 2

|  |  |  |  |
| --- | --- | --- | --- |
| [Identyfikator](#A_Identyfikator) | | C.LAN.FW.2 | |
| **Nazwa** | | Zapory sieciowe – typ 2 | |
| **Element/cecha** | **Charakterystyka** | | **Atrybuty** |
| Przepustowość zapory sieciowej | Określone atrybutem MIN PRZEPUSTOWOŚĆ | | - MIN PRZEPUSTOWOŚĆ [Gb/s] | |
| Przepustowość dla funkcjonalności IPS+AV | Określone atrybutem MIN PRZEPUSTOWOŚĆ IPS+AV | | - MIN PRZEPUSTOWOŚĆ IPS+AV [Gb/s] | |
| Minimalna Liczba nowych połączeń na sekundę | Określone atrybutem MIN. LICZBA NOWYCH POŁĄCZEŃ NA SEKUNDĘ | | - MIN. LICZBA NOWYCH POŁĄCZEŃ NA SEKUNDĘ [SZT/s] | |
| Minimalna Liczba jednoczesnych sesji | Określone atrybutem MIN. LICZBA JEDNOCZESNYCH SESJI | | - MIN.LICZBA JEDNOCZESNYCH SESJI [SZT] | |
| Minimalna Liczba jednoczesnych sesji przy uruchomionym IPS+AV | Określone atrybutem MIN. LICZBA JEDNOCZESNYCH SESJI przy uruchomionym IPS+AV | | - MIN.LICZBA JEDNOCZESNYCH SESJI przy uruchomionym IPS+AV [SZT] | |
| Mechanizm przechowywania i śledzenia sesji TCP/UDP | Statefull inspection - dynamiczne tworzenie list dostępu na podstawie rzeczywistego stanu sesji. | |  | |
| Funkcjonalność zapory | Obsługa VPN, NAT. | |  | |
| Liczba dostępnych interfejsów | Określone atrybutem MIN LICZBA INTERFEJSÓW 10/100/1000 Mb/s oraz MIN LICZBA INTERFEJSÓW SFP+ 10  Gb/s. | | MIN LICZBA INTERFEJSÓW 10/100/1000 Mb/s [SZT]  MIN LICZBA INTERFEJSÓW SFP+ 10  Gb/s [SZT] | |
| AntyWirus | Ochrona antywirusowa w oparciu o wewnętrzny silnik producenta urządzenia | |  | |
| IPS | Funkcjonalność IPS w oparciu  o wewnętrzny silnik producenta | |  | |
| URL Filtering  Wraz z dostawa licencji/subskrypcji niezbędnych dla realizacji tej funkcjonalności. | Filtrowanie ruchu po adresie URL w oparciu o wewnętrzny silnik producenta urządzenia. | |  | |
| Wspierane funkcjonalności | * 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. * 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. * System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali. * System zabezpieczeń firewall musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. | |  | |
| Dedykowana konsola zarządzająca | Zarządzanie w oparciu o HTTP, HTTPS, SSH, dedykowane oprogramowanie.  System zarządzania musi zapewniać możliwość współpracy z co najmniej sześcioma sondami, bez konieczności wykupywania dodatkowych licencji w przyszłości  Logowanie zdarzeń:  - Ilość obsługiwanych zdarzeń – 5Gb na dzień.  - Korelacja zdarzeń ze wszystkich zarządzanych urządzeń.  Integracja z zewnętrznymi systemami typu SIEM  Integracja z zewnętrzną bazą LDAP, RADIUS  Wbudowane mechanizmy HA | |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. | |  | |
| Redundancja | Możliwość łączenia urządzeń w klastry wysokiej dostępności. | |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków | |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |  | |

#### Zapory sieciowe – typ 3

|  |  |  |  |
| --- | --- | --- | --- |
| [Identyfikator](#A_Identyfikator) | | C.LAN.FW.3 | |
| **Nazwa** | | Zapory sieciowe – typ 3 | |
| **Element/cecha** | **Charakterystyka** | | **Atrybuty** |
| Przepustowość zapory sieciowej | Określone atrybutem MIN PRZEPUSTOWOŚĆ | | - MIN PRZEPUSTOWOŚĆ [Gb/s] | |
| Liczba połączeń na sekundę | Określone atrybutem LICZBA POŁĄCZEŃ NA SEKUNDĘ | | - LICZBA POŁĄCZEŃ NA SEKUNDĘ [SZT/s] | |
| Liczba jednoczesnych sesji | Określone atrybutem LICZBA JEDNOCZESNYCH SESJI | | - LICZBA JEDNOCZESNYCH SESJI [SZT] | |
| Mechanizm przechowywania i śledzenia sesji TCP/UDP | Statefull inspection - dynamiczne tworzenie list dostępu na podstawie rzeczywistego stanu sesji. | |  | |
| Funkcjonalność zapory | Obsługa VPN, NAT. | |  | |
| Liczba dostępnych interfejsów | Określone atrybutem MIN LICZBA INTERFEJSÓW 10/100/1000 Mb/s oraz MIN LICZBA INTERFEJSÓW SFP+ 10  Gb/s. | | MIN LICZBA INTERFEJSÓW 10/100/1000 Mb/s [SZT]  MIN LICZBA INTERFEJSÓW SFP+ 10  Gb/s [SZT] | |
| URL filtering | Filtrowanie adresów URL w oparciu o wewnętrzny silnik producenta urządzenia | |  | |
| Dedykowana konsola zarządzająca | Zarządzanie w oparciu o HTTP, HTTPS, SSH, dedykowane oprogramowanie.  System zarządzania musi zapewniać możliwość współpracy z co najmniej sześcioma sondami, bez konieczności wykupywania dodatkowych licencji w przyszłości  Logowanie zdarzeń:  - Ilość obsługiwanych zdarzeń – 5Gb na dzień.  - Korelacja zdarzeń ze wszystkich zarządzanych urządzeń.  Integracja z zewnętrznymi systemami typu SIEM  Integracja z zewnętrzną bazą LDAP, RADIUS  Wbudowane mechanizmy HA | |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. | |  | |
| Redundancja | Możliwość łączenia urządzeń w klastry wysokiej dostępności. | |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków | |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |  | |

#### Urządzenia równoważące ruch sieciowy – typ 1

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.LB.1 |
| **Nazwa** | Urządzenie równoważące ruch – SDN |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Przepływność dla warstwy 4 | Urządzenie musi charakteryzować się przepływnością dla warstwy 4 określone jako atrybut MIN przepływność warstwa 4 | - MIN przepływność L4 [Gb/s] | |
| Przepływność dla warstwy 7 | Urządzenie musi charakteryzować się przepływnością dla warstwy 7 określone jako atrybut MIN przepływność warstwa 7 | - MIN przepływność L7 [Gb/s] | |
| Ilość obsługiwanych jednoczesnych połączeń | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń określoną atrybutem MIN jednoczesnych połączeń | - MIN jednoczesnych połączeń [mln] | |
| Ilość jednocześnie obsługiwanych połączeń SSL | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń SSL określoną atrybutem MIN jednoczesnych połączeń SSL | - MIN jednoczesnych połączeń SSL [tyś] | |
| Ilość obsługiwanych połączeń w warstwie 4 | Urządzenie musi obsłużyć liczbę połączeń w warstwie 4 określone przez MIN liczba połączeń L4 | - MIN liczba połączeń L4 [tyś/s] | |
| Funkcjonalności LAN | Obsługa sieci VLAN w standardzie 802.1q  Obsługa agregacji linków w standardzie 802.3ad (LACP) |  | |
| Monitorowanie serwerów | Obsługiwane mechanizmy monitorowania stanu serwerów: TCP , SSL, http/https |  | |
| Funkcjonalność utrzymywania sesji | Obsługiwane mechanizmy przywiązywania sesji:  -cookie, JSESSIONID  -adres źródłowy;  -SSL ID,  -MSRDP |  | |
| Wsparcie dla usług warstw 4-7 | inspekcja warstwy 7:  -blokowanie URL;  - rewrite URL;  - content rewrite; |  | |
| Tryby pracy | - OneArm (SNAT, obsługa wstrzykiwania do nagłówka X-Forwarded-For);  - routed |  | |
| Funkcjonalności dostępne w obrębie jednego urządzenia | * Terminowanie sesji SSL * DNAT * SNAT |  | |
| Metody równoważenia ruchu | * Cykliczna * Ważona * Najmniejsza liczba połączeń |  | |
| Zarządzanie i monitorowanie | * Z użyciem interfejsu webowego. |  | |
| Wirtualizacja | Urządzenie występuje w postaci wirtualnej |  | |
| Redundancja | * Urządzenie musi mieć możliwość pracy w klastrze wysokiej dostępności. Awaria jednego z urządzeń nie może wpływać na działanie usług. |  | |

#### Urządzenia równoważące ruch sieciowy – typ 2

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.LB.2 |
| **Nazwa** | Urządzenie równoważące ruch |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Przepływność dla warstwy 4 | Urządzenie musi charakteryzować się przepływnością dla warstwy 4 określone jako atrybut MIN przepływność warstwa 4 | - MIN przepływność L4 [Gb/s] |
| Przepływność dla warstwy 7 | Urządzenie musi charakteryzować się przepływnością dla warstwy 7 określone jako atrybut MIN przepływność warstwa 7 | - MIN przepływność L7 [Gb/s] |
| Ilość obsługiwanych jednoczesnych połączeń | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń określoną atrybutem MIN jednoczesnych połączeń | - MIN jednoczesnych połączeń [mln] |
| Ilość jednocześnie obsługiwanych połączeń http | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń http określoną atrybutem MIN jednoczesnych połączeń http | - MIN jednoczesnych połączeń http [mln] |
| Ilość obsługiwanych połączeń w warstwie 4 | Urządzenie musi obsłużyć liczbę połączeń w warstwie 4 określone przez MIN liczba połączeń L4 | - MIN liczba połączeń L4 [mln/s] |
| Ilość odpowiedzi DNS | Urządzenie musi obsłużyć liczbę zapytań DNS określoną przez MIN odpowiedzi DNS | - MIN odpowiedzi DNS [mln/s] |
| Wydajność DDoS | Urządzenie musi obsłużyć liczbę pakietów SYN cookies określoną atrybutem MIN liczba SYN cookies | - MIN liczba SYN cookies [mln/s] |
| Interfejsy sieciowe 1/10Gb SFP+ | Urządzenie musi mieć możliwość rozbudowy do liczby portów o prędkości 1/10Gb zależnie od wykorzystanej wkładki SFP określane atrybutem MIN liczba portów SFP+ | -MIN liczba portów SFP+ [szt] |
| Funkcjonalności LAN | Obsługa sieci VLAN w standardzie 802.1q  Obsługa agregacji linków w standardzie 802.3ad (LACP) |  |
| Monitorowanie serwerów | Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, Radius, SIP, POP3, IMAP, SMTP, SNMP, SOAP, skryptowy, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne |  |
| Funkcjonalność utrzymywania sesji (persistance oraz stickiness) | Obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert,passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID |  |
| Wsparcie dla usług warstw  4-7 | inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, multipleksacja zapytań HTTP, kompresja i cache’owanie HTTP, |  |
| Źródłowy NAT dla adresów VIP i dla farm serwerów | Możliwość zawarcia adresu wirtualnego VIP w puli translacji NAT dla translacji dynamicznych i PAT.  Możliwość źródłowej translacji w kierunku zapasowej farmy serwerów przypadku awarii farmy podstawowej |  |
| Funkcjonalności wspierane przez blok~~\*~~ | * Rozkład ruchu pomiędzy serwerami aplikacji Web * Selektywny http caching * Selektywna kompresja danych * Terminowanie sesji SSL * Kopiowanie informacji o sesji SSL pomiędzy urządzeniami pracującymi w klastrze wysokiej dostępności (HA) * Filtrowanie pakietów * Obsługiwany tryb full proxy * Globalne równoważenie obciążenia za pomocą protokołu DNS * Funkcje zabezpieczenia aplikacji web poprzez moduł WAF (ang. Web Application Firewall) * Anty DoS/DDoS |  |
| Metody równoważenia ruchu | * Cykliczna * Ważona * Najmniejsza liczba połączeń * Najszybsza odpowiedź serwera * Najmniejsza liczba połączeń i najszybsza odpowiedź serwera * Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie * Dynamicznie ważona oparta na SNMP/WMI * Definiowana na podstawie grupy priorytetów dla serwerów |  |
| Bezpieczeństwo | * Szyfrowanie kluczy prywatnych zapisywanych na dysku urządzenia * Wsparcie przy użyciu następujących metod uwierzytelniania: certyfikatów cyfrowych, SecurID, Kerberos SSO, tokenów RSA, Radius; |  |
| Zarządzanie i monitorowanie | * Z użyciem linii komend oraz aplikacji graficznej lub interfejsu webowego. * Wielopoziomowe zarządzanie dostępem (poziomem uprzywilejowania) dla administratorów * Obsługa protokołu SNMP v1/v2c/v3 * Zewnętrzny syslog * Zbieranie danych i ich wyświetlanie zgodnie z ustawieniami administratora * Osobna brama domyślna dla interfejsu zarządzającego * Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot) * Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy) * Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu |  |
| Funkcjonalności globalnego równoważenia ruchu | Rozwiązanie musi zapewniać globalne, inteligentne sterowanie ruchem wykorzystując usługę DNS, jako mechanizm rozdziału ruchu (Global Solution Load Balancing), w ramach, którego zapewni:  a. Monitorowanie stanu pracy usług korzystając z monitorów działających w warstwie sieci, transportowej oraz aplikacji modelu ISO/OSI  b. Rozdzielanie ruchu korzystając, co najmniej z metod:   * Cykliczna * Ważona * Na podstawie adresów IP klienta usługi (topologii) * Obciążenia serwera * Najmniejszej liczby połączeń   c. Mechanizmy utrzymywania sesji polegające na kierowaniu zapytań z lokalnego serwera DNS klienta aplikacji zawsze do tego samego centrum danych i serwera aplikacji  d. Wbudowany w system operacyjny język skryptowy, umożliwiający analizę i zmianę parametrów w protokole DNS  e. Ochronę serwerów DNS z wykorzystanie DNSSEC a także na zastosowaniu list kontroli dostępu umożliwiających filtrowanie ruchu DNS bazując na typie rekordu  f. Możliwość pracy, jako serwer DNS obsługujący następujące rekordy: A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV,  g. Konwersja rekordów między IPv4 i IPv6  h. Wsparcie dla usług geolokacji, możliwość przekierowania ruchu do najbliższej geograficznie lokalizacji  i. Wybór lokalizacji na podstawie ilości urządzeń pośredniczących oraz ilości przetwarzanych danych  j. Możliwość wysyłania zapytań dotyczących obciążenia do urządzeń firm trzecich  k. Możliwość bezpośredniego odpytywania serwerów o obciążenie  l. Możliwość przekierowania ruchu do innej lokalizacji po przekroczeniu zdefiniowanego progu ilości sesji |  |
| Wirtualizacja | Urządzenie musi wspierać wirtualizację na logiczne konteksty obsługujące wymienione funkcjonalności  W takim przypadku wydajność odnosi się do fizycznego urządzenia. |  |
| Funkcjonalność anty DoS/DDoS | * sprzętowa ochrona przed atakami DoS/DDoS i SYN Flood, * ochrona DoS/DDoS dla protokołu DNS * funkcjonalność stanowej zapory sieciowej zapewniająca kontrolę ruchu sieciowego oraz ochronę przed atakami typu DoS w warstwie  3 i 4 ISO/OSI. * Rozwiązanie musi chronić przed atakami typu flood, sweep, teardrop oraz smurf. |  |
| Funkcjonalność WAF | * Weryfikacja zarówno zapytań jak i odpowiedzi http pod kątem naruszeń, w przypadku wykrycia incydentu musi istnieć możliwość aktywnego blokowania ruchu * Filtrowanie odpowiedzi serwera i kodów błędu, ukrycie zasobów serwera * WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web (URLi, metod dostępu, cookie, oczekiwanych typów znaków oraz długości zapytań). * Profil aplikacji web tworzony musi być na podstawie analizy ruchu sieciowego. Musi istnieć możliwość ograniczania zaufanych adresów źródłowych, z których komunikacja z aplikacją tworzyć będzie oczekiwany profil zachowań użytkowników. * Możliwość definiowania przepływu ruchu w obrębie aplikacji z uwzględnieniem jej logiki biznesowej * Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń) * Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr * Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki dostępu * Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów * WAF musi posiadać funkcje analizy i odczytu CSS/XSS * WAF musi posiadać możliwość walidacji XML poprzez: walidację Schema/WSDL, wybór dozwolonych metod SOAP, opis ataków na XML, rejestrację zapytań XML. * WAF musi posiadać mechanizmy ochrony przed atakami: SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, Session hijacking, Command Injection, Cookie/Session Poisoning, Parameter/Form Tampering, Forceful Browsing, Brute Force Login * WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http) * Powinna istnieć możliwość doboru odpowiedzi w zależności do rodzaju naruszenia * WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania dużej ilości incydentów wykonywanych w zdefiniowanym czasie przez jednego użytkownika. * W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP, SMTP oraz FTP. * Musi istnieć możliwość rozszerzenia funkcji WAF o dodatkowy serwis, sprawdzający reputację adresów IP dostających się do chronionej aplikacji. Serwis reputacyjny powinien być dostępny poprzez dokupienie licencji, bez konieczności wprowadzania zmian w architekturze sprzętowej oraz programowej proponowanego rozwiązania. * WAF musi umożliwiać automatyczne budowanie polityk w oparciu o skanowanie przez zewnętrznych dostawców np. Cenzic, HP WebInspect, IBM AppScan, Qualys Guard, WhiteHat Sentinel. * WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. |  |
| Redundancja | Musi być dostarczony w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1  Klaster wysokiej dostępności musi zapewnić synchronizację:   * Konfiguracji * Stanu połączeń * Przywiązywania sesji (Session persistence) |  |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  |

#### Urządzenia równoważące ruch sieciowy – typ 3

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.LB.3 |
| **Nazwa** | Urządzenie równoważące ruch –VM |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Przepływność dla warstwy 4 | Urządzenie musi charakteryzować się przepływnością dla warstwy 4 określone jako atrybut MIN przepływność warstwa 4 | - MIN przepływność L4 [Gb/s] |
| Przepływność dla warstwy 7 | Urządzenie musi charakteryzować się przepływnością dla warstwy 7 określone jako atrybut MIN przepływność warstwa 7 | - MIN przepływność L7 [Gb/s] |
| Ilość obsługiwanych jednoczesnych połączeń | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń określoną atrybutem MIN jednoczesnych połączeń | - MIN jednoczesnych połącze [mln] |
| Ilość jednocześnie obsługiwanych połączeń SSL | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń http określoną atrybutem MIN jednoczesnych połączeń https dla kluczy o długości – 2k | - MIN jednoczesnych połączeń SSL [tyś] |
| Ilość obsługiwanych połączeń w warstwie 4 | Urządzenie musi obsłużyć liczbę połączeń w warstwie 4 określone przez MIN liczba połączeń L4 | - MIN liczba połączeń L4 [tyś/s] |
| Ilość obsługiwanych połączeń w warstwie 7 | Urządzenie musi obsłużyć liczbę połączeń w warstwie 7 określone przez MIN liczba połączeń L7 | - MIN liczba połączeń L7 [tyś/s] |
| Funkcjonalności LAN | Obsługa sieci VLAN w standardzie 802.1q  Obsługa agregacji linków w standardzie 802.3ad (LACP) |  |
| Monitorowanie serwerów | Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, Radius, SIP, POP3, IMAP, SMTP, SNMP, SOAP, skryptowy, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne |  |
| Funkcjonalność utrzymywania sesji (persistance oraz stickiness) | Obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert,passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID |  |
| Wsparcie dla usług warstw  4-7 | inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, multipleksacja zapytań HTTP, kompresja i cache’owanie HTTP, |  |
|  |  |  |
| Źródłowy NAT dla adresów VIP i dla farm serwerów | Możliwość zawarcia adresu wirtualnego VIP w puli translacji NAT dla translacji dynamicznych i PAT.  Możliwość źródłowej translacji w kierunku zapasowej farmy serwerów przypadku awarii farmy podstawowej |  |
| Funkcjonalności wspierane przez blok~~\*~~ | * Rozkład ruchu pomiędzy serwerami aplikacji Web * Selektywny http caching * Selektywna kompresja danych * Terminowanie sesji SSL * Kopiowanie informacji o sesji SSL pomiędzy urządzeniami pracującymi w klastrze wysokiej dostępności (HA) * Filtrowanie pakietów * Obsługiwany tryb full proxy * Globalne równoważenie obciążenia za pomocą protokołu DNS |  |
| Metody równoważenia ruchu | * Cykliczna * Ważona * Najmniejsza liczba połączeń * Najszybsza odpowiedź serwera * Najmniejsza liczba połączeń i najszybsza odpowiedź serwera * Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie * Dynamicznie ważona oparta na SNMP/WMI * Definiowana na podstawie grupy priorytetów dla serwerów |  |
| Bezpieczeństwo | * Szyfrowanie kluczy prywatnych zapisywanych na dysku urządzenia * Wsparcie przy użyciu następujących metod uwierzytelniania: certyfikatów cyfrowych, SecurID, Kerberos SSO, tokenów RSA, Radius; |  |
| Zarządzanie i monitorowanie | * Z użyciem linii komend oraz aplikacji graficznej lub interfejsu webowego. * Wielopoziomowe zarządzanie dostępem (poziomem uprzywilejowania) dla administratorów * Obsługa protokołu SNMP v1/v2c/v3 * Zewnętrzny syslog * Zbieranie danych i ich wyświetlanie zgodnie z ustawieniami administratora * Osobna brama domyślna dla interfejsu zarządzającego * Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot) * Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy) * Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu |  |
| Funkcjonalności globalnego równoważenia ruchu | Rozwiązanie musi zapewniać globalne, inteligentne sterowanie ruchem wykorzystując usługę DNS, jako mechanizm rozdziału ruchu (Global Solution Load Balancing), w ramach, którego zapewni:  a. Monitorowanie stanu pracy usług korzystając z monitorów działających w warstwie sieci, transportowej oraz aplikacji modelu ISO/OSI  b. Rozdzielanie ruchu korzystając, co najmniej z metod:   * Cykliczna * Ważona * Na podstawie adresów IP klienta usługi (topologii) * Obciążenia serwera * Najmniejszej liczby połączeń   c. Mechanizmy utrzymywania sesji polegające na kierowaniu zapytań z lokalnego serwera DNS klienta aplikacji zawsze do tego samego centrum danych i serwera aplikacji  d. Wbudowany w system operacyjny język skryptowy, umożliwiający analizę i zmianę parametrów w protokole DNS  e. Ochronę serwerów DNS z wykorzystanie DNSSEC a także na zastosowaniu list kontroli dostępu umożliwiających filtrowanie ruchu DNS bazując na typie rekordu  f. Możliwość pracy, jako serwer DNS obsługujący następujące rekordy: A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV,  g. Konwersja rekordów między IPv4 i IPv6  h. Wsparcie dla usług geolokacji, możliwość przekierowania ruchu do najbliższej geograficznie lokalizacji  i. Wybór lokalizacji na podstawie ilości urządzeń pośredniczących oraz ilości przetwarzanych danych  j. Możliwość wysyłania zapytań dotyczących obciążenia do urządzeń firm trzecich  k. Możliwość bezpośredniego odpytywania serwerów o obciążenie  l. Możliwość przekierowania ruchu do innej lokalizacji po przekroczeniu zdefiniowanego progu ilości sesji |  |
| Wirtualizacja | * Urządzenie musi być dostarczone w postaci Virtualnej Maszyny. * Dodatkowo rozwiązanie musi posiadać możliwość wirtualizacji na logiczne konteksty, w takim przypadku specyfikowana wydajność rozwiązania odnosi się do całości urządzenia. |  |
| Redundancja | Musi być dostarczony w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1  Klaster wysokiej dostępności musi zapewnić synchronizację:   * Konfiguracji * Stanu połączeń * Przywiązywania sesji (Session persistence) |  |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  |

#### Urządzenia równoważące ruch sieciowy – typ 4

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.LB.4 |
| **Nazwa** | Urządzenie równoważące ruch |

| **Element/cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Przepływność dla warstwy 4 | Urządzenie musi charakteryzować się przepływnością dla warstwy 4 określone jako atrybut MIN przepływność warstwa 4 | - MIN przepływność L4 [Gb/s] |
| Przepływność dla warstwy 7 | Urządzenie musi charakteryzować się przepływnością dla warstwy 7 określone jako atrybut MIN przepływność warstwa 7 | - MIN przepływność L7 [Gb/s] |
| Ilość obsługiwanych jednoczesnych połączeń | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń określoną atrybutem MIN jednoczesnych połączeń | - MIN jednoczesnych połączeń [mln] |
| Ilość obsługiwanych jednoczesnych połączeń HTTP | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń określoną atrybutem MIN jednoczesnych połączeń HTTP | - MIN jednoczesnych połączeń http [mln/s] |
| Ilość obsługiwanych połączeń w warstwie 4 | Urządzenie musi obsłużyć liczbę połączeń w warstwie 4 określone przez MIN liczba połączeń L4 | - MIN liczba połączeń L4 [tyś./s] |
| Ilość jednocześnie obsługiwanych połączeń SSL | Urządzenie musi obsłużyć liczbę jednoczesnych połączeń http określoną atrybutem MIN jednoczesnych połączeń http | - MIN jednoczesnych połączeń SSL [tyś] |
| Interfejsy sieciowe 1/10Gb SFP+ | Urządzenie musi mieć możliwość rozbudowy do liczby portów o prędkości 1/10Gb zależnie od wykorzystanej wkładki SFP określane atrybutem MIN liczba portów SFP+ | -MIN liczba portów SFP+ [szt] |
| Funkcjonalności LAN | Obsługa sieci VLAN w standardzie 802.1q  Obsługa agregacji linków w standardzie 802.3ad (LACP) |  |
| Monitorowanie serwerów | Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, Radius, SIP, POP3, IMAP, SMTP, SNMP, SOAP, skryptowy, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne |  |
| Funkcjonalność utrzymywania sesji (persistance oraz stickiness) | Obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert,passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID |  |
| Wsparcie dla usług warstw  4-7 | inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, multipleksacja zapytań HTTP, kompresja i cache’owanie HTTP, |  |
|  |  |  |
| Źródłowy NAT dla adresów VIP i dla farm serwerów | Możliwość zawarcia adresu wirtualnego VIP w puli translacji NAT dla translacji dynamicznych i PAT.  Możliwość źródłowej translacji w kierunku zapasowej farmy serwerów przypadku awarii farmy podstawowej |  |
| Funkcjonalności wspierane przez blok~~\*~~ | * Rozkład ruchu pomiędzy serwerami aplikacji Web * Selektywny http caching * Selektywna kompresja danych * Terminowanie sesji SSL * Kopiowanie informacji o sesji SSL pomiędzy urządzeniami pracującymi w klastrze wysokiej dostępności (HA) * Filtrowanie pakietów * Obsługiwany tryb full proxy * Globalne równoważenie obciążenia za pomocą protokołu DNS * Funkcje zabezpieczenia aplikacji web poprzez moduł WAF (ang. Web Application Firewall) * Anty DoS/DDoS |  |
| Metody równoważenia ruchu | * Cykliczna * Ważona * Najmniejsza liczba połączeń * Najszybsza odpowiedź serwera * Najmniejsza liczba połączeń i najszybsza odpowiedź serwera * Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie * Dynamicznie ważona oparta na SNMP/WMI * Definiowana na podstawie grupy priorytetów dla serwerów |  |
| Bezpieczeństwo | * Szyfrowanie kluczy prywatnych zapisywanych na dysku urządzenia * Wsparcie przy użyciu następujących metod uwierzytelniania: certyfikatów cyfrowych, SecurID, Kerberos SSO, tokenów RSA, Radius; |  |
| Zarządzanie i monitorowanie | * Z użyciem linii komend oraz aplikacji graficznej lub interfejsu webowego. * Wielopoziomowe zarządzanie dostępem (poziomem uprzywilejowania) dla administratorów * Obsługa protokołu SNMP v1/v2c/v3 * Zewnętrzny syslog * Zbieranie danych i ich wyświetlanie zgodnie z ustawieniami administratora * Osobna brama domyślna dla interfejsu zarządzającego * Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot) * Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy) * Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu |  |
| Wirtualizacja | Urządzenie musi wspierać wirtualizację na logiczne konteksty obsługujące wymienione funkcjonalności  W takim przypadku wydajność odnosi się do fizycznego urządzenia. |  |
| Redundancja | Musi być dostarczony w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1  Klaster wysokiej dostępności musi zapewnić synchronizację:   * Konfiguracji * Stanu połączeń * Przywiązywania sesji (Session persistence) |  |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  |

### Rutery

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.RT |
| **Nazwa** | Rutery |

| **Element/cecha** | **Charakterystyka** | **Atrybut** |
| --- | --- | --- |
| Wydajność | Zdolność urządzenia do przesyłania wymaganej liczby pakietów na sekundę określone jako atrybut – MIN wydajność | - MIN wydajność [Mp/s] | |
| Interfejsy 10Gb | Ruter musi posiadać lub umożliwiać rozbudowę o liczbę interfejsów Ethernet pracujących z prędkością 10Gb/s w liczbie określonej atrybutem MIN liczba portów 10Gb | - MIN liczba portów 10Gb | |
| Interfejsy 1Gb SFP | Ruter musi umożliwiać rozbudowę o liczbę interfejsów Ethernet pracujących z prędkością 1Gb/s w zależności od wkładki (miedź/światło) w liczbie okresonej atrybutem MIN liczba portów 1Gb | - MIN liczba portów 1Gb | |
| Port konsoli | Ruter musi posiadać port konsoli do zarządzania lokalnego |  | |
| Port AUX | Ruter musi posiadać port AUX do zarządzania zdalnego |  | |
| Port USB | Ruter musi posiadać port USB |  | |
| Wsparcie protokołu warstwy L2 | Ruter musi umożliwiać obsługę protokołów warstwy L2:  -ARP: Dynamic/static ARP, proxy ARP -Ethernet, sub-interface VLAN -PPPoE server -PPP, -FR, FRF12 fragment, FR -HDLC |  | |
| Wsparcie protokołów rutingu IP | Rutowanie statyczne IP. Rutowanie dynamiczne za pomocą protokołów: RIPv1/v2, OSPFv2, BGP, IS-IS. |  | |
| Wsparcie protokołów IPv4 multicast | Obsługa protokołów multikastowych: IGMP (Internet Group Management Protocol) v1/v2/v3;  PIM (Protocol Independent Multicast) DM/SM;  MSDP (Multicast Source Discovery Protocol);  MBGP:  Multicast static routing; |  | |
| Wsparcie protokołów sieciowych | Obsługa protokołów:  DHCP Server/Relay/Client;  DNS Client; NTP Server/Client; Telnet Server/Client; TFTP Client; FTP Client; UDP Helper; |  | |
| Wsparcie IPv6 | Obsługa: IPv6 ND, IPv6 PMTU, dual-stack forwarding, IPv6 ACL; tunel IPv6: IPv6 tunelowane w IPv4; automatyczne tunelowanie IPv6 w IPv4; tunel Intra-Site Automatic Tunnel Addressing Protocol. Rutowanie statyczne. Rutowanie dynamiczne za pomocą protokołów: RIPng, OSPFv3, IS-ISv6, BGP dla IPv6. Obsługi transmisji multikastowej IPv6: MLDv1/v2,PIM-DM,PIM-SM,PIM-SSM |  | |
| Wsparcie QoS | Klasyfikacja ważności ruchu na bazie: numeru portu adresu IP, techniką IEEE 802.1p CoS, DSCP lub numeru portu TCP lub UDP i typu protokołu; znacznikowanie ważności; kolejkowanie zgodnie z algorytmami: FIFO, PQ, CQ, WFQ, CBWFQ. Unikanie zakleszczeń zgodnie z algorytmem: Tail-Drop, WRED. Obsługa MPLS QoS, IPv6 QoS. |  | |
| Bezpieczeństwo | Obsługa list kontroli dostępu, Obsługa protokołów: AAA, RADIUS, SSH, RSA, IPSec, IKE, Funkcje: Packet filter firewall, stateful firewall.  Regulacja pasma. Obsługa mechanizmu URPF, Virtual fragment reassembly.  Hierarchizacja ról zarządzania. |  | |
| Usługi | Obsługa funkcji: NAT, logowanie sesji NAT; Tunelowanie GRE i L2TP. |  | |
| MPLS | Obsługa protokołów i funkcji L3 VPN: MPLS VPN, CE dual homing tunelowanie GRE. Obsluga protokołów i funkcji L2 VPN: MPLS TE, RSVP TE, Multicast VPN. |  | |
| Redundancja | Obsługa protokołów: VRRP, MPLS TE FRR,  IGP fast routing convergence, BFD z obsługa rutowania statycznego i dynamicznego za pomocą protokołów RIP/OSPF/ISIS/ BGP.  Obsługa wymiany kart z interfejsami sieciowymi bez konieczności wyłączania całego urządzenia. |  | |
| Zarządzanie | Konfiguracja za pomocą zestawu poleceń CLI. Konfiguracja poprzez port konsoli zarządzania. Konfiguracja zdalna za pomocą Telnet. Zdalna konfiguracja poprzez portAUX. Obsluga protokołów i funkcji SNMP (v1, v2c, v3). Możliwość składowania logów systemowych. Alarmy hierarchiczne. Obsługa poleceń typu Ping i Trace. Wsparcie dla protokołów i funkcji: PBR i rutowania statycznego. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnych możliwości operacyjnych. |  | |
| Zarządzanie | Kompatybilność z systemami zarządzania posiadanymi przez Zamawiającego lub równoważnym systemem zarządzania dostarczonym przez Wykonawcę\* (patrz 1.2.2.15.4) |  | |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania posiadanym przez Zamawiającego HP NNM w zakresie:  - dostępności urządzenia  - aktywności interfejsów sieciowych  - zdarzeń związanych z awariami: interfejsów sieciowych, zasilaczy  - incydentów związanych z zajętością/wysyceniem zasobów urządzenia: CPU, pamięci, dysków |  | |

### System IPS

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.IPS |
| **Nazwa** | System IPS |

| **Element/cecha** | **Charakterystyka** |  |
| --- | --- | --- |
| Przepustowość IPS | Określone atrybutem MIN PRZEPUSTOWOŚĆ | MIN PRZEPUSTOWOŚĆ [Gb/s] | |
| Wydajność deszyfrowania sesji SSL | Określone atrybutem MIN WYDAJNOŚĆ DESZYFROWANIA SESJI SSL przy 10% zawartości sesji SSL w całkowitym strumieniu danych. | MIN WYDAJNOŚĆ DESZYFROWANIA SESJI SSL | |
| Opóźnienie wprowadzane przez IPS | Określone atrybutem MAKS. OPÓŹNIENIE | MAKS. OPÓŹNIENIE [s] | |
| Liczba jednoczesnych sesji | Określone atrybutem LICZBA JEDNOCZESNYCH SESJI | LICZBA JEDNOCZESNYCH SESJI [SZT] | |
| Liczba dostępnych portów | Określone atrybutem MIN LICZBA INTERFEJSÓW 1Gb /s oraz MIN LICZBA INTERFEJSÓW SFP+ 10  Gb/s.  dla 8 portów 1GE oraz 2 portów 10GE zapewniona możliwość pracy w topologii inline w trybie fail-open | 8 x 1Gb/s  8 x 10Gb/s SFP+  1 x 10/100/1000 – dedykowany port zarządzający Ethernet RJ45 | |
| Wymagane zaimplementowane technologie | * + - 1. IPS (Instrusion Prevention System) - oparty na sygnaturach       2. Bezsygnaturowa (signature-less) analiza malware’u       3. Analiza behawiorystyczna ataków       4. Korzystanie z zewnętrznych systemów reputacyjnych . |  | |
| Wymagane typy ochrony przed zagrożeniami | * + - 1. Sieciowymi  1. DoS/DDoS zero-day flood, 2. TCP Floods, 3. UDP floods, 4. ICMP floods, 5. IGMP floods 6. Skanowaniem    1. TCP,    2. UDP,    3. PING, 7. SYN (dowolne typy ataków SYN flood) 8. Limitowaniem połączeń w ramach protokołów 9. TCP, 10. UDP, 11. ICMP 12. IP, 13. Mechanizm selektywnego blokowania ataków pochodzących z jednego źródła (adresu IP) z rozróżnianiem sesji legalnego ruchu od ataku typu DoS/DDoS 14. Mechanizm selektywnego blokowania ataków pochodzących z wielu źródeł (adresów IP) z rozróżnianiem sesji legalnego ruchu od ataku typu DoS/DDoS 15. HTTP flood (np. HTTP GET flood) i pochodne 16. Malware (worm, trojan, spyware, backdoor) 17. Nieuprawniony dostęp 18. Black list, 19. White list, 20. Access Control List, 21. IP Reputation, 22. Zaimplementowane mechanizmy zarządzanie pasmem 23. Zaimplementowane mechanizmy ograniczania ilości połączeń 24. Wszystkie funkcje muszą być dostępne w wersji IPv4 oraz IPv6 |  | |
| Wykrywanie anomalii w pakietach | 1. Invalid TCP Header Length 2. Invalid UDP Header Length 3. Invalid TCP Flags 4. Unsupported L4 Protocol 5. Invalid IPv4 Header or Total Length 6. Incorrect IPv4 Checksum   Unrecognized L2 Format   1. TTL Less Than or Equal to 1 2. Inconsistent IPv6 Headers 3. IPv6 Hop Limit Reached 4. Source or Destination Address same as Local Host 5. Source Address same as Dest. Address (i.e.:Land Attack) 6. L4 Source or Destination Port Zero |  | |
| Typy akcji podjęte w przypadku wykrycia ataku | 1. odrzucenie pakietu (drop), 2. tylko raportowanie, 3. reset połączenia (dla źródła i celu oraz obu kierunkach), 4. zawieszenie połączenia (dowolna kombinacja parametrów: adres źródłowy, port źródłowy, adres docelowy, port docelowy) w kwarantannie, 5. Challenge-Response dla ataków używających protokołów HTTP (co najmniej 302 redirection) |  | |
| Funkcja awaryjnego omijania urządzenia IPS na trasie sieciowej (ang. *bypass*) | fail open/close; w przypadku awarii możliwość ominięcia (bypass) inspekcji IPS dla każdego segmentu chronionej sieci i/lub całego urządzenia |  | |
| Dedykowana konsola zarządzająca | 1. Zarządzanie w oparciu o HTTP, HTTPS, dedykowane oprogramowanie. 2. System zarządzania musi zapewniać możliwość współpracy z co najmniej sześcioma sondami skanującymi (sensorami), bez konieczności wykupywania dodatkowych licencji w przyszłości. 3. Korelacja zdarzeń ze wszystkich zarządzanych urządzeń 4. Integracja z zewnętrznymi systemami typu SIEM 5. Integracja z zewnętrzną baza LDAP 6. Szczegóły ataku muszą zawierać następujące informacje (jeśli są dostępne dla danego typu ataku): 7. Source L4 Port 8. Protocol 9. Packet Count 10. Flow Label (tylko IPv6) 11. ToS 12. Packet Size 13. ICMP Message Type— tylko dla protokołu ICMP. 14. L4 Checksum 15. TCP Sequence Number 16. IP ID Number 17. Fragmentation Offset 18. Fragmentation Flag 19. Physical Port 20. Bandwidth [Kbits] 21. VLAN 22. MPLS RD 23. Device IP 24. TTL 25. Source IP 26. Destination IP 27. Source Ports 28. Destination Ports 29. DNS Query 30. DNS ID 31. DNS Query Count |  | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania, typu hot-plug. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |

### Badanie zawartości poczty elektronicznej

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SPM |
| **Nazwa** | Urządzenia badające zawartość poczty elektronicznej |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Liczba dostępnych interfejsów | Co najmniej 4 interfejsy Ethernet 1 Gb/s | |
| Filtr antyspamowy | Tak | |
| Filtr antywirusowy | Tak | |
| Obsługa protokołów | SMTP oraz SMTP/S+SSL lub SMTP/S+TLS | |
| Auktualizacje reguł filtrowania | Możliwość automatycznej aktualizacji reguł filtrowania poczty. | |
| Zasilanie | Napięcie zmienne 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania, typu hot-plug. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |

### Badanie podatności środowiska teleinformatycznego

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.VUL |
| **Nazwa** | Urządzenia badające podatność środowiska teleinformatycznego |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Badanie podatności | Wsparcie dla branżowych standardów, OWASP, OSSTMM .  Możliwość badania podatności/audytu:   * usług i urządzeń sieciowych, * aplikacji webowych, * baz danych * systemów operacyjnych, * środowisk wirtualnych,   Możliwość wykrycia ujawnienia danych wrażliwych.  Możliwość cyklicznego uruchamiania automatycznego badania podatności określonych obiektów w sieci, wg zadanego harmonogramu.  Możliwość testowania aplikacji backendowych nie posiadających interfejsu użytkownika lub warstwy prezentacji.  Wsparcie minimum dla protokołów:  HTML4, HTML5, IPv4.  Udostępnienie API.  Operacja badania podatności nie wymaga instalacji dodatkowych komponentów w badanym obiekcie.  Możliwość integracji z systemem SIIEM Zamawiającego. (l HP ArcSight | |
| Auktualizacje bazy (definicji) podatności i zagrożeń | Możliwość automatycznej aktualizacji danych o nowych potencjalnych podatnościach i zagrożeniach sieciowych. | |
| Patchowanie podatności | Możliwość patchowania z wykorzystaniem własnych reguł. | |
| Ocena stopnia zagrożenia | Możliwość oceny stopnia zagrożenia z wykorzystaniem standardu Common Vulnerability Scoring System (CVSS). | |
| Raportowanie | Możliwość definiowania i dostosowywania zawartości raportów do potrzeb użytkownika wraz z możliwością zapisywania konfiguracji zdefiniowanych raportów, w celu ich późniejszego użycia.  Możliwość zapisywania raportów z badań, minimum w formatach:   * czysty tekst * HTML, * XML, * CSV (rozdzielanych przecinkiem lub innym znakiem).   Możliwość analizy trendów zmian w zakresie wykrytych podatności i zagrożeń. | |
| Zasilanie | Napięcie zmienne 230 V, 50 Hz. | |
| Obudowa | W przypadku rozwiązania opartego na sprzęcie fizycznym muszą to być urządzenia przemysłowe dedykowane do pracy ciągłej, dostosowane do montażu w szafie stelażowej 19”. | |

### Ochrona kluczy kryptograficznych

#### Urządzenia do ochrony kluczy kryptograficznych – Ethernet

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.HSM.1 |
| **Nazwa** | Urządzenia do ochrony kluczy kryptograficznych – Ethernet |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Realizowane operacje | Urządzenie musi mieć możliwość wykonania przynajmniej następujących operacji:  - generowanie par kluczy kryptograficznych,  - fizyczna i logiczna ochrona kluczy kryptograficznym,  - kontrola dostępu do kluczy kryptograficznych,  - wykonywanie operacji z użyciem kluczy kryptograficznych,  - archiwizacja kluczy,  - odtwarzanie kluczy po awarii urządzenia. |
| Klucze | Musi istnieć możliwość generowania kluczy dla algorytmu RSA o następującej sile: klucze 1024 bity, 2048 bitów oraz 4096 bitów.  Urządzenie musi pozwalać na archiwizację kluczy i ich odtwarzanie w przypadku uszkodzenia urządzenia.  Wymagana jest możliwość wykonywania operacji kryptograficznych z użyciem algorytmu RSA z kluczem o długości 1024 bity z prędkością 1400 operacji na sekundę lub większą. |
| Obsługa serwerów w sieci | Możliwość obsługi wielu serwerów oraz aplikacji z wielu lokalizacji przez pojedynczy moduł HSM. |
| Redundancja | Urządzenie powinno być wyposażone w podwójne zasilanie typu hot-swap (redundancja N+N) oraz redundantne wymienne wentylatory (N+N lub N+M). |
| Obudowa | Obudowa o wysokości nie większej niż 2U, dostosowana do montażu w szafie stelażowej 19”. |
| Interfejsy | Możliwość podłączenia do modułu przez co najmniej 2 interfejsy Ehternet 1 Gb/s. |
| Oprogramowanie | Urządzenie musi zostać dostarczone ze sterownikami i niezbędnym do prawidłowej pracy oprogramowaniem. |
| Obsługiwane API i protokoły | API: PKCS#11, CSP for Microsoft CryptoAPI/CNG, Java JCA/JCE CSP, OpenSSL |
| Algorytmy kryptograficzne | Kryptografia symetryczna: AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, Triple DES  Kryptografia asymetryczna: RSA, Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH  Funkcje skrótu: SHA-2, SHA-1 |
| Certyfikaty | - FIPS 140-2 Level3 lub wyższy,  - Common Criteria EAL4 lub wyższy. |
| Wspierane systemy operacyjne | Windows Server 2012, Linux. |

#### Urządzenia do ochrony kluczy kryptograficznych – PCI

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.HSM.2 |
| **Nazwa** | Urządzenia do ochrony kluczy kryptograficznych – PCI |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Realizowane operacje | Urządzenie musi mieć możliwość wykonania przynajmniej następujących operacji:  - generowanie par kluczy kryptograficznych,  - fizyczna i logiczna ochrona kluczy kryptograficznym,  - kontrola dostępu do kluczy kryptograficznych,  - wykonywanie operacji z użyciem kluczy kryptograficznych,  - archiwizacja kluczy,  - odtwarzanie kluczy po awarii urządzenia. |
| Klucze | Możliwość generowania kluczy dla algorytmu RSA o następującej sile: klucze 1024 bity, 2048 bitów oraz 4096 bitów.  Urządzenie musi pozwalać na archiwizację kluczy i ich odtwarzanie w przypadku uszkodzenia urządzenia.  Wymagana jest możliwość wykonywania operacji kryptograficznych z użyciem algorytmu RSA z kluczem o długości 1024 bity z prędkością 1400 operacji na sekundę lub większą. |
| Format urządzenia | Urządzenie musi być dostarczone w postaci karty formatu PCI, PCI-X lub PCI Express, zależnie od rodzaju portu dostępnego w komputerze, w którym będzie ono zainstalowane. |
| Oprogramowanie | Urządzenie musi zostać dostarczone ze sterownikami i niezbędnym do prawidłowej pracy oprogramowaniem. |
| Obsługiwane API | PKCS#11, MSCAPI/CNG, Java JCA/JCE API, OpenSSL. |
| Algorytmy kryptograficzne | Kryptografia symetryczna: AES, DES, Triple-DES.  Kryptografia asymetryczna: DSA, RSA, Diffie-Hellman.  Funkcje skrótu: MD5, SHA-2, SHA-1. |
| Certyfikaty | - FIPS 140-2 Level3  - Common Criteria EAL4+ |
| Wspierane systemy operacyjne | Windows Server 2012, Linux. |

#### Urządzenia do ochrony kluczy kryptograficznych – Root CA

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.HSM.3 |
| **Nazwa** | Urządzenia do ochrony kluczy kryptograficznych |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Realizowane operacje | Urządzenie musi mieć możliwość wykonania przynajmniej następujących operacji:  - generowanie par kluczy kryptograficznych,  - fizyczna i logiczna ochrona kluczy kryptograficznym,  - kontrola dostępu do kluczy kryptograficznych,  - wykonywanie operacji z użyciem kluczy kryptograficznych,  - archiwizacja kluczy,  - odtwarzanie kluczy po awarii urządzenia. |
| Klucze | Możliwość generowania kluczy dla algorytmu RSA o następującej sile: klucze 1024 bity, 2048 bitów oraz 4096 bitów.  Urządzenie musi pozwalać na archiwizację kluczy i ich odtwarzanie w przypadku uszkodzenia urządzenia.  Wymagana jest możliwość wykonywania operacji kryptograficznych z użyciem algorytmu RSA z kluczem o długości 1024 bity z prędkością 25 operacji na sekundę lub większą. |
| Oprogramowanie | Urządzenie musi zostać dostarczone ze sterownikami i niezbędnym do prawidłowej pracy oprogramowaniem. |
| Obsługiwane API | PKCS#11, MSCAPI/CNG, Java JCA/JCE API, OpenSSL. |
| Algorytmy kryptograficzne | Kryptografia symetryczna: AES, DES, Triple-DES.  Kryptografia asymetryczna: DSA, RSA, Diffie-Hellman.  Funkcje skrótu: MD5, SHA-2, SHA-1. |
| Certyfikaty | - FIPS 140-2 Level3  - Common Criteria EAL4+ |
| Wspierane systemy operacyjne | Windows Server 2012, Linux. |

### Badanie zawartości poczty elektronicznej

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SPM |
| **Nazwa** | Urządzenia badające zawartość poczty elektronicznej |

| **Element/ cecha** | **Charakterystyka** | **Atrybuty** |
| --- | --- | --- |
| Architektura systemu ochrony | System ochrony musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową z wsparciem dla wielu domen pocztowych, polityk filtrowania tworzonych w oparciu o adresy mailowe, nazwy domenowe, adresy IP (w szczególności reguła all-all), Email routing (m.in w oparciu o atrybuty LDAP) oraz zarządzanie kolejkami bazujące na politykach.  Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). |  | |
| Funkcjonalności | System musi posiadać funkcjonalności:   * Kwarantanna poczty z dziennym podsumowaniem (możliwość samodzielnego zwalniania plików z kwarantanny przez użytkownika) * Dostęp do kwarantanny poprzez WebMail lub POP3 * Archiwizacja poczty przychodzącej i wychodzącej, backup poczty do różnych miejsc przeznaczenia * Whitelist’y definiowane dla użytkownika |  | |
| System operacyjny | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia. |  | |
| Liczba dostępnych interfejsów | Minimalna liczba interfejsów Ethernet 1Gbps określona atrybutem LICZBA INTERFEJSÓW 1Gbps  i minimalna liczba interfejsów Ethernet 10Gbps określona atrybutem LICZBA INTERFEJSÓW 10Gbps. Wszystkie interfejsy muszą być gotowe do podłączenia okablowania. | LICZBA INTERFEJSÓW 1Gbps [szt.]  LICZBA INTERFEJSÓW 10Gbps [szt.] | |
| Dysk Lokalny | Liczba lokalnych dysków określona atrybutem LICZBA DYSKÓW  Pojemność lokalnych dysków określona atrybutem POJEMNOŚĆ DYSKÓW (sumaryczna pojemność dysków) | LICZBA DYSKÓW [szt. ]  POJEMNOŚĆ DYSKÓW [TB] | |
| Wysoka dostępność | System musi pracować w trybie klastra wysokiej dostępności zbudowanego z min dwóch urządzeń.  System musi zapewniać:   * Konfigurację HA [Active-Passive] w każdym z trybów: gateway, transparent, serwer * Tryb A-P z synchronizacją polityk i wiadomości, gdzie cluster występuje pod jednym adresem IP * Tryb synchronizacji konfiguracji dla scenariuszy rozległych (osobne adresy IP) * Wykrywanie awarii i powiadamianie administratora * Monitorowanie stanu połączeń |  | |
| Filtr antywirusowy /antyspyware | System musi realizować:   * Skanowanie antywirusowe wiadomości SMTP * Kwarantannę dla zainfekowanych plików * Skanowanie załączników skompresowanych * Definiowanie komunikatów powiadomień w języku polskim * Blokowanie załączników ze względu na typ pliku * Obsługę nie mniej niż liczbę profili antywirusowych z możliwością definiowania na użytkownika w oparciu o atrybuty LDAP określoną atrybutem LICZBA PROFILI AV | LICZBA PROFILI AV [szt.] | |
| Filtr antyspam | System musi zapewniać poniższe metody filtrowania spamu:  Heurystyczna analiza spamu  Filtrowanie treści załączników  Szczegółowa kontrola nagłówka wiadomości  Filtrowanie w oparciu o filtry Bayes’a, z możliwością dostrajania dla poszczególnych użytkowników  Filtrowanie poczty w oparciu o sumy kontrolne spamu  Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF  Analiza poczty w oparciu o dynamiczną bazę spamu dostarczaną przez tego samego producenta  Współpraca z zewnętrznymi serwerami RBL  Kontrola w oparciu o Greylist’y  Białe i czarne listy definiowane globalnie oraz per użytkownik  Kwarantanna oraz oznaczanie spamu   * Weryfikacja źródłowego adresu IP oraz Kontrola Reverse DNS (Anty-Spoofing)   Możliwość zdefiniowania profili antyspamowych z możliwością definiowania na użytkownika w oparciu o atrybuty LDAP w liczbie nie mniej niż atrybut LICZBA PROFILI AS | LICZBA PROFILI AS [szt.] | |
| Ochrona przed atakami DoS | System musi mieć możliwość ochrony przed:   * Denial of Service (Mail Bombing) * Ochrona przed atakami na adres odbiorcy * Definiowanie maksymalnych ilości wiadomości pocztowych * Weryfikacja poprawności adresu e-mail nadawcy |  | |
| Obsługa protokołów | SMTP oraz SMTP/S+SSL lub SMTP/S+TLS |  | |
| Zarządzanie | Możliwość zarządzania przez:  Konsolę szeregową RS-232, interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH |  | |
| Logowanie i raportowanie | Możliwość logowania i powiadamiania administratora zdarzeniach systemowych, zmianach konfiguracji, krytycznych zdarzeniach systemowych, działalności wirusów, informacji na temat spamu i niedozwolonych załączników,  Możliwość planowania czasu generowania raportów, predefiniowanie szablonów raportów.  System musi mieć możliwość przesyłania wszystkich zdarzeń do zewnętrznego serwera SYSLOG.  System musi mieć możliwość podglądu logów w czasie rzeczywistym. |  | |
| Uwierzytelnianie SMTP i administracyjne | System musi mieć możliwość uwierzytelniania po LDAP, RADIUS, oraz POP3 i IMAP.  System musi mieć możliwość uwierzytelniania w celach administracyjnych po LDAP, RADIUS |  | |
| Aktualizacje reguł filtrowania | Możliwość automatycznej aktualizacji reguł filtrowania poczty w czasie rzeczywistym,  Aktualizacje planowane (scheduler),  Wymuszona aktualizacja reguł (tryb push) |  | |
| Zasilanie | Napięcie zmienne 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania, typu hot-plug. |  | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. |  | |