**Zapytanie o informację**

**(RFI)**

**Rozeznanie Rynku**

**na Rozbudowę infrastruktury systemowo-sprzętowej środowisk Access Point (AP) i RINA w Centrali ZUS**

Warszawa, sierpień 2018 r.

# Przedmiot i cel Zapytania o informację

1. Zakład Ubezpieczeń Społecznych planuje dokonanie zakupu polegającego na ***Rozbudowie infrastruktury systemowo-sprzętowej środowisk Access Point (AP) i RINA w Centrali ZUS w Centrali ZUS.***
2. Szczegółowy opis przedmiotu zapytania stanowi **Załącznik nr 2** do Zapytania o informację.
3. Celem niniejszego Zapytania o informację jest pozyskanie przez Zakład Ubezpieczeń Społecznych od podmiotów zajmujących się profesjonalnie określonym zakresem, danych dotyczących szacunkowego kosztu realizacji.

# Ogólne informacje o charakterze formalnym

1. Niniejsze Zapytanie o informację **nie stanowi oferty zawarcia umowy w rozumieniu przepisów *ustawy z dnia 23 kwietnia 1964 r.- Kodeks cywilny*.** Udzielenie odpowiedzi na niniejsze Zapytanie o informację nie będzie uprawniało do występowania z jakimikolwiek roszczeniami w stosunku do Zakładu Ubezpieczeń Społecznych.
2. Niniejsze Zapytanie o informację **nie jest elementem jakiegokolwiek postępowania o udzielenie zamówienia, w rozumieniu *ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych***, jak również nie jest elementem jakiegokolwiek procesu zakupowego prowadzonego w oparciu o wewnętrzne regulacje Zakładu Ubezpieczeń Społecznych.
3. Złożenie odpowiedzi na niniejsze Zapytanie o informację jest jednoznaczne z wyrażeniem zgody przez podmiot składający taką odpowiedź na nieodpłatne wykorzystanie przez Zakład Ubezpieczeń Społecznych wszystkich lub części przekazanych informacji.
4. Przedmiot niniejszego Zapytania o informację jest współfinansowany ze środków europejskich w ramach programu „Łącząc Europę” (Connecting Europe Facility - CEF) UE na lata 2014-2020 (umowa nr INEA/CEF/ICT/A2016/119324o dofinansowanie Projektu zawartej w dniu 1 marca 2017 r. pomiędzy Agencją Wykonawczą ds. Innowacyjności i Sieci (The Innovation and Networks Executive Agency – INEA) z siedzibą w Brukseli na mocy uprawnień przekazanych przez Komisję Europejską a Centralą Zakładu Ubezpieczeń Społecznych (Nr zarejestrowania umowy w C/ZUS 1060088).

# Termin i sposób złożenia odpowiedzi na Zapytanie o informację

1. Odpowiedź na Zapytanie o informację należy przygotować w oparciu o formularz stanowiący **Załącznik nr 1** do Zapytania o informację.
2. W przypadku, gdy informacje zawarte w odpowiedzi na Zapytanie o informację stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, podmiot składający taką odpowiedź winien to wyraźnie zastrzec w odpowiedzi. Brak przedmiotowego zastrzeżenia, Zakład Ubezpieczeń Społecznych będzie traktował przekazane informacje jako informacje, które nie stanowią tajemnicy przedsiębiorstwa.
3. Odpowiedź na Zapytanie o informację należy przesłać w terminie do **7 września 2018 r.** na adres e-mail: [rfi-rina@zus.pl](mailto:rfi-rina@zus.pl)

# Opis przedmiotu Zapytania o informację

Przedmiotem wyceny jest zakup Infrastruktury Techniczno-Systemowej o minimalnych wymaganiach zgodnych z podaną przez Zamawiającego docelową specyfikacją   
w Załączniku nr 2 do Zapytania o informację. Zamawiający dopuszcza doposażenie obecnie posiadanej ITS w taki sposób aby spełnione zostały minimalne wymagania podane w Załączniku 2.

W przypadku rozbudowy istniejącej ITS należy przyjąć zasadę, iż Wykonawca obejmie serwisem gwarancyjnym całe rozbudowywane urządzenie (nie tylko dostarczoną część). W wycenie należy uwzględnić koszty związane z dostawą na terenie Warszawy zakupywanego ITS, jego zainstalowanie i objęcie serwisem gwarancyjnym oraz wykonanie podstawowego przeszkolenia przystanowiskowego oraz konsultacji związanych z zaproponowanym sprzętem i oprogramowaniem.

Czas wdrożenia (dostawa, instalacja i przeszkolenie przystanowiskowe) ma zostać wykonane w ciągu 6 tygodni od daty podpisania umowy, a serwis gwarancyjny   
i konsultacje mają obowiązywać w ciągu 36 miesięcy od daty podpisania protokołu odbioru. Serwis gwarancyjny ma być świadczony w trybie 366/365dni/24h z 24h godzinnym czasem naprawy i czasem reakcji 30 min.

**Aktualnie posiadana przez Zamawiającego infrastruktura techniczno-systemowa:**

**Urządzenia:**

1 **Szafa Serwerowa RACK**

Szafa Rack Universal 42U -sztuk 1,

PDU 40A -sztuk 2,

PDU Extension Bar: 7X C-13 -sztuk 4,

KVM Server Console Switch 0x2x8 -sztuk 1,

KVM Console and Monitor -sztuk 1.

2 **Infrastruktura serwerów**

1 x obudowa serwera HP typu blade BLc7000

wyposażona w następujące moduły rozszerzeń:

- 2 x przełącznik SAN HP B-series 8/24c BladeSystem ,

- 2 x Virtual Connect Flex-10 Enet Module,

- 1 x zasilacz 6X 2400W,

- 1 x konsola zarządzająca HP BLc7000 DDR2,

- 1 x wentylator 6X Active Cool 200.

3 **Serwery BLADE**

12 x serwer kasetowy HP BL460c G7 wyposażone w:

- 4 x RAM HP 8GB 2Rx4 PC3-10600R-9,

- 2 x HDD 146GB 6G SAS 10K 2.5in DP,

- 1 x karta HP BLc QLogic QMH2562 8Gb FC,

4 **Macierz Dyskowa**

2 x obudowy macierzy HP M6612 3.5-inch SAS Drive Enclosure

wyposażone w:

* 16 x HDD HP M6612 300GB 6G SAS 15K 3.5in,
* 1 x kontroler HP P6500 EVA Dual Controller FC Array.

5 **Firewall**

ASA5520-AIP40-K9 ASA 5520 Appliance sztuk 2

6 **Router brzegowy**

CISCO2911/K9 Cisco 2911 sztuk 1

7 **Przełącznik Ethernet**

WS-C2960S-24TS-L Cisco Catalyst 2960S 24 GigE, 4 x SFP LAN Base

sztuk 1

8 **Sprzętowy moduł kryptograficzny HSM**

NH2033 nShield Connect 500; F3; SEE Ready sztuk 1

**Oprogramowanie:**

1 VMware vSphere 5 Ent 1P E-LTU licencja na 1 CPU

TD418AAE VMw vSphere Ent 1P 1yr9x5 E-LTU sztuk 8

2 HP Red Hat Enterprise Linux Server Version 6 , licencja 2 socket,

1 Guest BC321AAE RHEL 2Skt 1 Guest 24x7 3yr Lic E-LTU sztuk 8

3 HP Red Hat Enterprise Linux Server Version 6 , licencja 2 socket,

4 Guest BC322AAE RHEL 2Skt 4 Guest 24x7 3yr Lic E-LTU sztuk 4

**Załącznik nr 2 – Formularz odpowiedzi na Zapytanie**

|  |  |
| --- | --- |
| Dane podmiotu | **…………………..\*** |
| Adres Wykonawcy: kod, miejscowość, ulica, nr lokalu | **…………………..\*** |
| Nr telefonu | **…………………..\*** |
| E-mail | **…………………..\*** |

**Zakład Ubezpieczeń Społecznych**

**ul. Szamocka 3, 5**

**01-748 Warszawa**

**FORMULARZ ODPOWIEDZI NA ZAPYTANIE O INFORMACJĘ**

W odpowiedzi na Zapytanie o informację dotyczące **rozbudowy infrastruktury systemowo-sprzętowej środowisk Access Point (AP) i RINA w Centrali ZUS** przedstawiam poniższe informacje:

1. Poniższe informacje (\**wybrać właściwe\**):
   1. \*zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i nie mogą być ujawniane innym podmiotom.
   2. \*nie zawierają informacji stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i mogą być ujawniane innym podmiotom.

**UWAGA**: w przypadku gdy Wykonawca nie zaznaczy żadnej z ww. opcji, ZUS przyjmie, że Wykonawca nie zastrzega przekazanych informacji jako stanowiących tajemnicę przedsiębiorstwa, co w konsekwencji oznaczać będzie, że takie informacje będą udostępnianie przez ZUS w trybie dostępu do informacji publicznej, na stosowny wniosek innych podmiotów.

1. Przedstawione informacje dotyczące szacunkowych kosztów (\**wybrać właściwe*):

* \*zawierają upusty na poziome ….% od „cen katalogowych”,
* \*nie zawierają upustów od „cen katalogowych” i ZUS może uzyskać upust na poziome ….% od poniżej przedstawionych kosztów;

1. Wszelką korespondencję dotyczącą przedmiotowej odpowiedzi na Zapytanie o informację należy kierować na:

|  |  |
| --- | --- |
| Imię i Nazwisko | **…………………..\*** |
| Nazwa podmiotu | **…………………..\*** |
| Adres | **…………………..\*** |
| Nr telefonu | **…………………..\*** |
| Nr faksu | **…………………..\*** |
| Adres e-mail | **…………………..\*** |

**FORMULARZ CENOWY**

Tabela 1.1.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| **Lp.** | **Opis** | **Producent, model, typ** | **Jednostka** | **Cena jednostkowa w PLN**  **(bez VAT)** | **Stawka podatku VAT w %** | **Cena jednostkowa w PLN**  **(z VAT)** | **Całkowita**  **Liczba** | **Razem**  **w PLN**  **(bez VAT)**  (kol. 4 x kol. 7) | **Razem**  **w PLN**  **(z VAT)**  (kol. 6 x kol. 7) |
| **SPRZĘT** | | | | | | | | | |
| **1** | Serwer typ1 | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 11 | **\*………** | **\*………** |
| **2** | Serwer typ2 | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 4 | **\*………** | **\*………** |
| **3** | Serwer typ3 | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 2 | **\*………** | **\*………** |
| **4** | Macierz dyskowa | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 2 | **\*………** | **\*………** |
| **5** | Wirtualizator taśm | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 2 | **\*………** | **\*………** |
| **6** | Biblioteka taśmowa | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 2 | **\*………** | **\*………** |
| **7** | Przełącznik LAN | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 4 | **\*………** | **\*………** |
| **8** | Firewall | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 8 | **\*………** | **\*………** |
| **9** | LoadBalancer | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 4 | **\*………** | **\*………** |
| **10** | Przełącznik SAN | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 4 | **\*………** | **\*………** |
| **11** | HSM – moduł sprzętowy | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 4 | **\*………** | **\*………** |
| **12** | KMS - Urządzenie do zarządzania kluczami kryptograficznymi | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 4 | **\*………** | **\*………** |
| **13** | Szafa RACK | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | \*………..min. 2 | **\*………** | **\*………** |
| **14** | Obudowa blade (opcjonalnie) | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 2 | **\*………** | **\*………** |
| **15** | Konsola KVM | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 2 | **\*………** | **\*………** |
| **16** | Wkładki SFP+ 10G SR -światłowodowe | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 68 | **\*………** | **\*………** |
| **17** | Wkładki SFP 10G - miedziane | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 8 | **\*………** | **\*………** |
| **18** | Wkładki SFP 1G - miedziane | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 53 | **\*………** | **\*………** |
| **OPROGRAMOWANIE** | | | | | | | | | |
| **17** | VMWare | **\*………** | sztuk | **\*………** | **\*………** | **\*………** | 22 |  |  |
| **18** | Ubuntu | **\*………** | Sztuk | **\*………** | **\*………** | **\*………** | 24 |  |  |
| **19** | Oprogramowanie backupu | **\*………** | Sztuk | **\*………** | **\*………** | **\*………** | 1 |  |  |
| **20** | Oprogramowanie do zarządzania HSM | **\*………** | Sztuk | **\*………** | **\*………** | **\*………** | 1 |  |  |
| **Razem** | | | | | | | | |  |

Prosimy o uzupełnienie danych w tabeli dotyczących zaproponowanych urządzeń tj. nazwy producenta /producentów typu, modelu itp. dla jakich wycena została skalkulowana.

Tabela nr 1.2:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| **Lp.** | **Opis** | **Jednostka** | **Cena jednostkowa w PLN**  **(bez VAT)** | **Stawka podatku VAT w %** | **Cena jednostkowa w PLN**  **(z VAT)** | **Całkowita**  **Liczba** | **Razem**  **w PLN**  **(bez VAT)**  (kol. 3 x kol. 6) | **Razem**  **w PLN**  **(z VAT)**  (kol. 5 x kol. 6) |
| **1** | Usługa wdrożenia | Sztuka | **\*………** | **\*………** | **\*………** | 1 | **\*………** | **\*………** |
| **2** | Usługa serwisowa | Miesiąc | **\*………** | **\*………** | **\*………** | 36 | **\*………** | **\*………** |
| **3** | Konsultacje | Godziny | **\*………** | **\*………** | **\*………** | 75 | **\*………** | **\*………** |
| **4** | Usługi szkoleniowe | Dzień | **\*………** | **\*………** | **\*………** | 2grupyx7osób | **\*………** | **\*………** |
| **Razem** | | | | | | | |  |

Wycena powinna być podana w PLN, kwota netto i z podatkiem VAT. Okres ważności wyceny nie krótszy niż 3 miesiące. Wycena powinna zawierać wszystkie koszty własne Wykonawcy związane z realizacją Zamówienia np. ubezpieczenie, transport itp. oraz uwzględniać koszty osprzętu niezbędnego do uruchomienia sprzętu u Zamawiającego.

\* wypełnia Oferent

|  |  |  |
| --- | --- | --- |
| Nazwisko i imię osoby (osób) uprawnionej(-ych) | Podpis(-y) osoby(osób) uprawnionej(-ych) | Miejscowość i data |
|  |  |  |

Załącznik nr 2 do Zapytania o informację

**SZCZEGÓŁOWA SPECYFIKACJA URZADZEŃ**

**dla architektury docelowej Zamawiającego**

1. **Opis wymagań technicznych Infrastruktury Techniczno-Systemowej**
   1. **Urządzenia serwerowe**

**SERWER typ 1 - sztuk 11**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 2. Specyfikacja konfiguracji serwerów TYP 1

|  |  |  |
| --- | --- | --- |
| Lp. | Wymaganie | Opis wymagania |
| 1 | Procesory | Procesor szesnastordzeniowy x86 - 64 bity, osiągający w testach SPECint\_rate\_base\_2006 dla konfiguracji 2 procesorowej wynik nie gorszy niż 1280 punktów. Wynik testu musi być publikowany na stronie [www.spec.org](http://www.spec.org) |
| 2 | Liczba procesorów w każdym serwerze | Minimum 2 procesory |
| 3 | Pamięć RAM | 512 GB RAM DDR4. Możliwość instalacji w serwerze minimum 1TB pamięci RAM. |
| 4 | Dyski twarde, nośniki danych | Zainstalowane wewnątrz serwera 2 karty SD/microSD/dyski SSD, pracujące w RAID 1, o pojemności umożliwiającej instalację hypervisora, zapewniające odporność na awarię jednej z kart SD/microSD/dysku SSD. |
| 5 | Interfejsy sieciowe (LAN) | Minimum 2 Interfejsy sieciowe 10G SR |
| 6 | Interfejsy FibreChannel SAN | Minimum jedna karta FC zapewniająca minimum dwa interfejsy Fibre Channel, każdy interfejs o szybkości 16Gb/sek. |
| 7 | Karta zdalnego zarządzania | Serwer wyposażony w kartę zdalnego zarządzania wraz z licencją zapewniającą:  - Monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe  - Wbudowane narzędzia diagnostyczne  - Zdalną konfigurację serwera(BIOS) i instalację systemu operacyjnego  - Zdalne włączanie/wyłączanie/restart serwera  - Wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji.  - Zdalny dostęp z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.  - Zdalną identyfikację fizycznego serwera za pomocą sygnalizatora optycznego.  - Wirtualną zdalną konsolę, tekstową i graficzną, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD, USB i wirtualnych folderów, obrazów ISO  - Podgląd logów sprzętowych serwera i karty  - Przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS)  - Zdalną aktualizację oprogramowania (firmware)  - Minimum jeden interfejs sieciowy 1GbE na potrzeby zdalnego zarządzania |
| 8 | Wspierane systemy operacyjne | - Microsoft Windows Server 2016 i nowsze  - VMware vSphere 6.5 i nowsze  - RHEL 7.x  - Ubuntu 16.04 lub nowszy |
| 9 | Zasilanie | Redundantne zasilacze Hot-Plug (jeśli dostarczone zostaną serwery inne niż typu BLADE) |

**SERWER typ 2 - sztuk 4**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 3. Specyfikacja konfiguracji serwerów TYP 2

|  |  |  |
| --- | --- | --- |
| Lp. | Wymaganie | Opis wymagania |
| 1 | Procesory | Procesor szesnastordzeniowy x86 - 64 bity, osiągający w testach SPECint\_rate\_base\_2006 dla konfiguracji 2 procesorowej wynik nie gorszy niż 1450 punktów. Wynik testu musi być publikowany na stronie www.spec.org |
| 2 | Liczba procesorów w każdym serwerze | Minimum 2 procesory |
| 3 | Pamięć RAM | Zainstalowane minimum 512 GB RAM DDR4. Możliwość instalacji w serwerze minimum 1TB pamięci RAM. |
| 4 | Dyski twarde, nośniki danych | Zainstalowane wewnątrz serwera min. 2 dyski SSD 1TB pracujące w RAID 1 |
| 5 | Interfejsy sieciowe (LAN) | Minimum 2 Interfejsy sieciowe 10G SR |
| 6 | Interfejsy FibreChannel SAN | Minimum jedna karta FC zapewniająca minimum dwa interfejsy Fibre Channel, każdy interfejs o szybkości 16Gb/sek. |
| 7 | Karta zdalnego zarządzania | Serwer wyposażony w kartę zdalnego zarządzania wraz z licencją zapewniającą:  - Monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe  - Wbudowane narzędzia diagnostyczne  - Zdalną konfigurację serwera(BIOS) i instalację systemu operacyjnego  - Zdalne włączanie/wyłączanie/restart serwera  - Wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji.  - Zdalny dostęp z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.  - Zdalną identyfikację fizycznego serwera za pomocą sygnalizatora optycznego.  - Wirtualną zdalną konsolę, tekstową i graficzną, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD, USB i wirtualnych folderów, obrazów ISO,  - Podgląd logów sprzętowych serwera i karty  - Przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS)  - Zdalną aktualizację oprogramowania (firmware)  - Minimum jeden interfejs sieciowy 1GbE na potrzeby zdalnego zarządzania |
| 8 | Wspierane systemy operacyjne | - Microsoft Windows Server 2016 i nowszy  - VMware vSphere 6.5 i nowszy  - Ubuntu 16.04 i nowsze |
| 9 | Zasilanie | Redundantne zasilacze Hot-Plug (jeśli dostarczone zostaną serwery inne niż typu BLADE) |

**SERWER typ 3 - sztuk 2**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 4. Specyfikacja konfiguracji serwerów TYP3

|  |  |  |
| --- | --- | --- |
| Lp. | Wymaganie | Opis wymagania |
| 1 | Procesory | Procesor ośmiordzeniowy x86 - 64 bity, osiągający w testach SPECint\_rate\_base\_2006 dla konfiguracji 1 procesorowej wynik nie gorszy niż 885 punktów. Wynik testu musi być publikowany na stronie www.spec.org |
| 2 | Liczba procesorów w każdym serwerze | Minimum 1 procesor |
| 3 | Pamięć RAM | Zainstalowane minimum 64 GB RAM DDR4. Możliwość instalacji w serwerze minimum 1TB pamięci RAM. |
| 4 | Dyski twarde, nośniki danych | Zainstalowane wewnątrz serwera min. 2 dyski SSD 512GB pracujące w RAID 1 |
| 5 | Interfejsy sieciowe (LAN) | Minimum 2 Interfejsy sieciowe 10G SR |
| 6 | Interfejsy FibreChannel SAN | Minimum jedna karta FC zapewniająca minimum dwa interfejsy Fibre Channel, każdy interfejs o szybkości 16Gb/sek. |
| 7 | Karta zdalnego zarządzania | Serwer wyposażony w kartę zdalnego zarządzania wraz z licencją zapewniającą:  - Monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe  - Wbudowane narzędzia diagnostyczne  - Zdalną konfigurację serwera(BIOS) i instalację systemu operacyjnego  - Zdalne włączanie/wyłączanie/restart serwera  - Wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji.  - Zdalny dostęp z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.  - Zdalną identyfikację fizycznego serwera za pomocą sygnalizatora optycznego.  - Wirtualną zdalną konsolę, tekstową i graficzną, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD, USB i wirtualnych folderów, obrazów ISO,  - Podgląd logów sprzętowych serwera i karty  - Przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS)  - Zdalną aktualizację oprogramowania (firmware)  - Minimum jeden interfejs sieciowy 1GbE na potrzeby zdalnego zarządzania |
| 8 | Wspierane systemy operacyjne | System operacyjny serwera zgodny z dostarczanym rozwiązaniem backupu. |
| 9 | Licencje | System operacyjny serwera zapewniający pełne wykorzystanie zasobów sprzętowych serwera oraz gwarantujący pełną, wymaganą funkcjonalność dostarczanego rozwiązania backupu. |
| 10 | Zasilanie | Redundantne zasilacze Hot-Plug (jeśli dostarczone zostaną serwery inne niż typu BLADE) |

**MACIERZ DYSKOWA - sztuk 2 \***

Podane niżej wymagania dotyczą jednej sztuki

\*Wszystkie wymagane pojemności macierzy użyte w specyfikacji odpowiadają założeniu: 1TB = 1024GB, 1GB = 1024MB,

1MB = 1024kB, 1kB = 1024B.

Tabela 5. Specyfikacja wymagań dla macierzy dyskowej

| **Lp** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| 1 | Zasoby dyskowe | 1. Macierz dyskowa musi być dostarczona z minimum:    1. dyskami SSD prezentującymi pojemność użytkową minimum 36 TB w konfiguracji RAID6 (8+2)    2. dyskami SAS prezentującymi pojemność użytkową minimum 30 TB w konfiguracji RAID6 (8+2) 2. Macierz musi mieć możliwość utworzenia grupy RAID w której dwa dyski będą przechowywać dane parzystości. Awaria dwóch dowolnych dysków w obrębie takiej pojedynczej grupy RAID nie może spowodować utraty danych. 3. Należy dodatkowo dostarczyć dyski zapasowe w ilości zgodnej z zaleceniami producenta, 4. Podczas awarii dysku kontroler macierzy dyskowej musi automatycznie rozpoczynać odtwarzanie danych na fizycznym dysku zapasowym lub na odpowiedniej przestrzeni zapasowej. |
| 2 | Kontrolery macierzy dyskowej | 1. Macierz dyskowa musi być złożona z minimum jednej pary identycznych kontrolerów tworzących klaster wysokiej dostępności (high availability cluster). Każdy kontroler musi posiadać identyczną konfigurację, tzn. liczbę i parametry CPU, parametry i pojemność pamięci cache, parametry i liczbę portów we/wy. Te same kontrolery muszą udostępniać dane poprzez FCP. 2. Obszar pamięci cache przeznaczony do zapisów danych, musi posiadać lustrzaną kopię (ang. mirror). 3. W przypadku awarii zasilania dane nie zapisane na dyskach muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez minimum 72 godziny lub zachowane w pamięci nieulotnej kontrolera do momentu przywrócenia zasilania. 4. Kontrolery w klastrze wysokiej dostępności muszą oferować funkcjonalność automatycznego przejmowania funkcjonalności i zadań w przypadku awarii drugiego kontrolera w tej samej parze 5. Macierz musi mieć minimum 128 GB pamięci cache obsługującej zapis i odczyt dostępnej dla wszystkich wolumenów macierzy. Włączenie lub wyłączenie pamięci cache nie może wymagać operacji usunięcia i utworzenia na nowo wolumenów lub grup dyskowych. 6. Każdy kontroler musi pracować pod kontrolą jednego systemu operacyjnego stworzonego przez producenta urządzenia. Nie dopuszcza się zastosowania systemu, w którym udostępnianiem danych zarządzają różne systemy operacyjne w jednym zintegrowanym urządzeniu. 7. Awaria dowolnego pojedynczego aktywnego elementu macierzy dyskowej nie może powodować przerwy w dostępie do danych. |
| 3 | Interfejsy | Macierz musi być wyposażona w następujące działające porty:   1. Minimum 4 porty 10GbE SFP+, porty muszą być obsadzone odpowiednimi wkładkami SFP+ 10GbBaseSR. 2. Minimum 12 portów FC 16Gbps, porty muszą być obsadzone odpowiednimi wkładkami SFP+ 16Gb SW. |
| 4 | Kopie migawkowe | 1. Macierz dyskowa musi natywnie obsługiwać mechanizm kopii migawkowych, który będzie dostępny dla wszystkich rodzajów danych udostępnianych. Licencja na mechanizm kopii migawkowych musi obejmować całą powierzchnię użytkową macierzy. Jeśli do uruchomienia tej funkcjonalności potrzebna jest licencja to zamawiający wymaga jej dostarczenia. 2. Macierz dyskowa musi umożliwiać i wykonywanie kopii migawkowych wolumenów plikowych, w trybie on-line, bez zatrzymywania operacji odczytu i zapisu. 3. Mechanizm kopii migawkowych musi być zgodny z dostarczonym systemem backupu. |
| 5 | Obsługiwane protokoły | 1) Macierz dyskowa musi udostępniać dane za pomocą protokołu CIFS i FCP - jeśli do uruchomienia potrzebna jest licencja to zamawiający wymaga jej dostarczenia.  2)Macierz dyskowa musi mieć możliwość uruchomienia udostępniania danych za pomocą protokołów MIN. NFS V.4 I SMB V.3 oraz iSCSI wraz z licencjami na protokoły CIFS, MIN. NFS V.4 I SMB V.3, FCP oraz iSCSI.  3)Jednoczesna obsługa różnych protokołów dostępu do danych nie może być zrealizowana za pomocą dodatkowego oprogramowania, ani dodatkowych urządzeń pośredniczących typu wirtualizator, gateway, switch, etc. |
| 6 | Pozostałe wymagania | 1. Macierz dyskowa musi umożliwiać dynamiczną zmianę rozmiaru plikowych wolumenów danych: (zwiększanie) bez przerywania pracy i bez przerywania użytkownikom zewnętrznym dostępu do danych. 2. Musi istnieć możliwość konfiguracji macierzy dyskowej za pomocą GUI, zbieranie i wyświetlanie informacji o stanie zasobów macierzy dyskowej, prezentowanie i gromadzenie zdarzeń zachodzących w macierzy dyskowej oraz prezentowanie bieżących statystyk wydajnościowych macierzy dyskowej, podgląd parametrów wydajnościowych macierzy dyskowej w czasie rzeczywistym. 3. Dostęp do linii poleceń systemu operacyjnego kontrolerów musi odbywać się przy użyciu połączenia szyfrowanego. 4. Zamawiający wymaga dostarczenia licencji na zdalne zarządzanie. |
| 7 | Wspierane systemy operacyjne | Macierz musi wspierać pracę z systemami   1. Microsoft Windows Server 2016 lub nowszy 2. VMware vSphere 6.5 lub nowszy 3. Ubuntu 16.04 lub nowszy 4. Red Hat linux 6.0 lub nowszy 5. Microsoft SQL Server 2016 i nowsze 6. AIX 6 lub nowszy |
| 9 | Zasilanie | Redundantne zasilacze Hot-Plug |

**WIRTUALIZATOR TAŚM - sztuk 2**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 7. Specyfikacja konfiguracji wirtualizatora taśm

|  |  |
| --- | --- |
| Lp. | Opis wymagania |
| 1 | Wymagane porty:  - 4x10Gb/s Eth SFP, wszystkie porty wyposażone we wkładki SFP+ 10Gb SR  - 4x16Gb/s FC SFP, wszystkie porty wyposażone we wkładki SFP+ 16Gb SW |
| 2 | Wymagana pojemność: 210 TB netto  Wymagana możliwość zwiększenia pojemności do co najmniej 250 TB |
| 3 | Zaoferowany model urządzenia deduplikacyjnego musi umożliwiać rozbudowę do konfiguracji wysoko dostępnej (HA) – co oznacza możliwość rozbudowy do konfiguracji minimum dwu-kontrolerowej w obrębie pojedynczego urządzenia, współdzielącej zasoby dyskowe urządzenia. Zamawiający do realizacji powyższej funkcjonalności nie dopuszcza zastosowania wielokontrolerowych macierzy dyskowych będących częścią składową przestrzeni dyskowej deduplikatora. Konfiguracja wysoko dostępna musi umożliwiać automatyczny fail-over oraz kontynuację pracy urządzenia z uszkodzonym kontrolerem, przy zapewnieniu nominalnych parametrów wydajnościowych. Wymóg konfiguracji HA nie będzie spełniony jeżeli producent oferowanego urządzenia nie oferuje oficjalnie takiej funkcjonalności w ramach zaoferowanego modelu, potwierdzenie funkcjonalności HA musi znaleźć potwierdzenie w ogólnie dostępnej dokumentacji dla oferowanego urządzenia. |
| 4 | Wymagana wydajność: min. 30TB/h w przypadku deduplikacji na źródle, 14TB/h bez deduplikacji na źródle – parametry wydajnościowe muszą być dostępne w ogólnie dostępnych dokumentach |
| 5 | Wymagana możliwość jednoczesnej obsługi min. 400 strumieni. |
| 6 | Urządzenie musi być przeznaczone do de-duplikacji i przechowywania kopii zapasowych. |
| 7 | Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:   1. CIFS, 2. MIN. NFS V.4 I SMB V.3 3. zapewniającymi deduplikację na źródle – BOOST/CATALYST 4. VTL |
| 8 | Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, MIN. NFS V.4 I SMB V.3, VTL, BOOST/CATALYST dla oferowanej pojemności urządzenia |
| 9 | Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych: LTO4, LTO5, LTO6 |
| 10 | 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. |
| 11 | Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. De-duplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. |
| 12 | Oferowany produkt musi posiadać obsługę mechanizmów de-duplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, MIN. NFS V.4 I SMB V.3, VTL, BOOST/CATALYST) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały MIN. NFS V.4 I SMB V.3/CIFS również muszą podlegać deduplikacji. W przypadku braku wymaganej funkcjonalności tzn. jeżeli oferowane urządzenie deduplikuje dane, jednak w obrębie jednocześnie wykorzystywanego każdego z wymaganych interfejsów/udziałów deduplikacja jest rozdzielna (co powoduje składowanie powielonych danych w obrębie oferowanego urządzenia), oferowane urządzenie musi mieć dwukrotnie większą pojemność netto w stosunku do pojemności wymaganych dla deduplikatora oraz zapewniać dwukrotnie większe skalowanie w stosunku do wymaganego. |
| 13 | Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) |
| 14 | Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane |
| 15 | Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia) co najmniej następujące aplikacje backupujące bezpośrednio na oferowane urządzenie:   1. Micro Focus Data Protector, 2. IBM TSM,EMC Networker, 3. Veeam Backup. |
| 16 | W przypadku współpracy z Microsoft SQL Server  urządzenie musi umożliwiać de-duplikację na źródle (de-duplikację na zabezpieczanej maszynie) i przesyłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków. |
| 17 | W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
| 18 | Urządzenie musi umożliwiać zaszyfrowanie przechowywanych danych. Należy dostarczyć licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. |
| 19 | Urządzenie musi wspierać de-duplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych wpieranych przez producenta:   1. Windows 2. Linux (RedHat, Ubuntu) |
| 20 | Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu. Licencja na replikację musi być dostarczona w ramach postępowania. |
| 21 | W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
| 22 | W przypadku replikacji danych między dwoma urządzeniami, kontrolowanej przez dostarczane Oprogramowanie Backupu, muszą być możliwe do uzyskania następujące funkcjonalności:   1. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących 2. replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu 3. replikacja zarządzana jest z poziomu aplikacji backupowej, aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |
| 23 | Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6. |
| 24 | 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. |
| 25 | Łącznie oferowane urządzenie musi posiadać zapasowe dyski typu hot-spare zgodnie z zaleceniami producenta urządzenia. |
| 26 | Urządzenie musi mieć możliwość podziału na logiczne części pracujące równolegle. |
| 27 | Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:   1. CIFS 2. MIN. NFS V.4 I SMB V.3 3. VTL 4. BOOST/CATALYST |
| 28 | Urządzenie musi weryfikować ewentualne przekłamania (zmianę danych) na poziomie:   1. systemu plików   oraz   1. grup RAID   Wymaga się aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezależnie od używanego interfejsu. |
| 29 | Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność. Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. |
| 30 | Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych na 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 odbywać się „w locie” – musi być elementem procesu zapisu danych przez urządzenie. |
| 31 | Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |
| 32 | Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu i odtwarzania danych. |
| 33 | Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. |
| 34 | Urządzenie musi mieć możliwość zarządzania poprzez   1. Interfejs graficzny dostępny z przeglądarki internetowej 2. Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
| 35 | Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania. |
| 36 | Redundantne zasilacze Hot-Plug |

**BIBLIOTEKA TAŚMOWA - sztuk 2**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 8. Specyfikacja konfiguracji biblioteki taśmowej

|  |  |  |
| --- | --- | --- |
| Lp. | Wymaganie | Opis wymagania |
| 1 | Interfejsy | Wymagane porty:  - 2x1Gb/s E  - 2x16Gb/s FC SFP, wszystkie porty wyposażone we wkładki SFP+ 16Gb SW |
| 2 | Czytnik | Wbudowany czytnik kodów kreskowych |
| 3 | Napęd | Minimum 4 napędów LTO-8 z możliwością rozbudowy |
| 4 | Ilość slotów | Minimum 48 z możliwością rozbudowy (biblioteka modułowa) |
| 5 | Pojemność | Minimum 500TB bez kompresji do 1.2 PB z kompresją |
| 9 | Zarzadzanie | 1. Możliwość zarządzania biblioteką, poprzez WWW i SNMP 2. Możliwość zdalnego monitorowania. 3. Możliwość zarządzania poprzez protokół SMI-S 4. Wbudowany dotykowy wyświetlacz umożliwiający konfiguracje i diagnostykę urządzenia. 5. Biblioteka powinna być wykonana w technologii umożliwiającej sprzętowy podział biblioteki na mniejsze „biblioteki logiczne”, a następnie podłączenie ich do różnych serwerów wykorzystujących różne oprogramowanie do wykonywania kopii zapasowych i archiwizacji, |
| 10 | Bezpieczeństwo | Obsługa taśm WORM uniemożliwiających zmianę zapisanych danych.  Urządzenie musi bez ograniczeń umożliwiać szyfrowanie danych zapisywanych na taśmach. Jeśli to tego celu wymagana jest odpowiednia licencja i/lub oprogramowanie bądź klucz sprzętowy, to należy je dostarczyć razem z urządzeniem. |
| 11 | MTBF | Nie mniej niż 100 000 cykli |
| 13 | Wspierane systemy | Wspierane systemy operacyjne wspierane przez producenta   1. Microsoft Windows Server, 2. Red Hat Enterprise Linux 3. Ubuntu 16,04 lub nowszym |
| 14 | Dodatkowe akcesoria | Minimum 96 taśm LTO-8 z naklejkami z kodem kreskowym oraz 5 taśm czyszczących. |
| 15 | Obudowa | Do instalacji w standardowej szafie RACK 19” |
| 16 | Zasilanie | Redundantne zasilacze Hot-Plug |
|  | Inne wymagania | Biblioteka musi umożliwiać pełną współpracę z centralnym systemem backupu  Napęd z mechanizmem automatycznie dostosowującym prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie przynajmniej 40-80 MB/s,  Minimum 10 slotów wejścia/wyjścia,  Biblioteka musi wykorzystywać pamięć chip-memory w nośnikach taśmowych do przechowywania informacji statystycznych, aby przewidywać wystąpienie awarii napędu czy uszkodzenie nośnika,  Biblioteka musi mieć możliwość automatycznej inwentaryzacji taśm,  Biblioteka musi wspierać kilka niezależnych dróg sterowania automatyką (multipathing) w obrębie połączeń FC biblioteki i serwera (serwerów) backupu. Dopuszcza się manualne przełączanie ścieżki, |

* 1. **Urządzenie sieciowe**

**PRZEŁĄCZNIK LAN - sztuk: 4**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 11. Specyfikacja wymagań na przełączniki LAN

|  |  |
| --- | --- |
| L.p. | Opis wymagania |
| 1 | przepustowość minimum 4Tbps |
| 2 | Interfejsy:   * minimum 2 porty 40G SR * Minimum 48 portów typu 1/10 Gigabit SFP+ * możliwość rozbudowy o minimum, 2 porty 40G, |
| 3 | obsługa Virtual Extensible LAN (VXLAN) i Ethernet Virtual Private Network (EVPN) |
| 4 | interfejsy muszą mieć możliwość grupowania w logiczne połączenia |
| 5 | minimum 10000 instancji wirtualnego routingu (oddzielne tablice routingu) |
| 6 | obsługa minimum 3000 sieci VLAN |
| 7 | obsługa routing IPv4 (statyczny, BGP, OSPF) |
| 8 | obsługa szyfrowania w warstwie drugiej (L2) |
| 9 | Urządzenie musi mieć możliwość pobrania konfiguracji w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. |
| 10 | urządzenie musi posiadać redundantne zasilacze |
| 11 | urządzenie musi być przystosowane do montażu w 19” szafie rack (zestaw montażowy dostarczony z urządzeniem) |

**WKŁADKI:**

Wkładki SFP+ 10G SR – szt. 68

Wkładki SFP 10G – miedziane – szt. 8

Wkładki SFP 1G – miedziane – szt. 53

**FIREWALL - sztuk: 8**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 12. Specyfikacja wymagań na zapory ogniowe

|  |  |
| --- | --- |
| L.p. | Opis wymagania |
| 1 | Minimum trzy interfejsy 10G SR i 8 portów 10/100/1000 (RJ-45) |
| 2 | System zabezpieczeń firewall musi obsługiwać nie mniej niż 8 wirtualnych firewalli/systemów/domen/kontekstów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych tablic routingu, polityk bezpieczeństwa oraz koncentratorów VPN. |
| 3 | System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 4 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 2 Gbps dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 800 000 jednoczesnych połączeń. |
| 4 | Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, OSPF. |
| 5 | System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). |
| 6 | System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN. |
| 7 | System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). |
| 8 | 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. |
| 9 | System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |
| 10 | System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. |
| 11 | System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. |
| 12 | Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |
| 13 | System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ |
| 14 | System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. |
| 15 | Urządzenie musi mieć możliwość pobrania konfiguracji w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. |
| 16 | Urządzenie musi posiadać redundantne zasilacze |
| 17 | Urządzenie musi być przystosowane do montażu w 19” szafie rack (zestaw montażowy dostarczony z urządzeniem). |

**LOADBALANCER - sztuk: 4**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 13. Specyfikacja wymagań na urządzenia równoważenia obciążenia sieciowego

|  |  |
| --- | --- |
| L.p. | Opis wymagania |
| 1 | przepustowość szyfrowania (sprzętowa) 12Gbps , 10000 TPS |
| 2 | przepustowość minimum 15Gbps L4/L7 |
| 3 | obsługa minimum 750000 żądań na sekundę L7 |
| 4 | obsługa minimum 350000 połączeń na sekundę L4 |
| 5 | posiadać wbudowany język skryptowy pozwalający na zaawansowaną modyfikację ruchu http |
| 6 | rozwiązanie na dedykowanej platformie sprzętowej (appliance) |
| 7 | pamięć operacyjna RAM minimum 32GB |
| 8 | architektura oprogramowania 64-bitowa |
| 9 | 2 porty 10GBASE-SR |
| 10 | musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management (Ethernet RJ-45) |
| 11 | Możliwość kreowania minimum 5 partycji wirtualnych (osobne tablice routingu) |
| 12 | Urządzenie musi mieć możliwość pobrania konfiguracji w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. |
| 13 | Urządzenie musi posiadać redundantne zasilacze |
| 14 | Przystosowane do montażu w 19” szafie rack (zestaw montażowy dostarczony z urządzeniem) |

**PRZEŁĄCZNIK SAN - sztuk 4**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 15. Wykaz wymagań dla przełączników FC.

|  |  |
| --- | --- |
| **Lp.** | **Opis wymagań minimalnych** |
| 1 | Przełącznik FC musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. |
| 2 | W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. |
| 3 | Przełącznik FC musi być wyposażony, w co najmniej 48 aktywne porty FC obsadzone wkładkami SFP 16Gb/s. |
| 4 | Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC |
| 5 | Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 384 Gb/s end-to-end. |
| 6 | Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 800ns. |
| 7 | Rodzaj obsługiwanych portów, co najmniej: E oraz F. |
| 8 | Przełącznik FC musi mieć wysokość maksymalnie 2U (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. |
| 9 | Przełącznik FC musi posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika. |
| 10 | Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN. |
| 11 | Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC. |
| 12 | Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:   1. mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric 2. uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP 3. uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP 4. szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2. 5. definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control) 6. definiowane kont administratorów w środowiskach RADIUS, TACACS+, LDAP w MS Active Directory, TACACS+ 7. szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS 8. obsługa SNMP v1 oraz v3 9. IP Filter dla portu administracyjnego przełącznika 10. wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP 11. wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP |
| 13 | Przełącznik FC musi mieć możliwość konfiguracji przez:   1. polecenia tekstowe w interfejsie znakowym konsoli terminala 2. przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie |
| 14 | Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC. |
| 15 | Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. |
| 16 | Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu. |
| 17 | Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS\_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie. |
| 18 | Przełącznik FC musi posiadać funkcjonalność wprowadzenia ograniczenia prędkości dla danych wchodzących dla dowolnego portu lub portów. Musi być możliwość określenia wartości limitu przepustowości danych wchodzących niższej niż wynegocjowana prędkość portu. |
| 19 | Przełącznik FC musi posiadać funkcjonalność N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. |
| 20 | Przełącznik FC musi posiadać funkcjonalność agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. |
| 21 | Przełącznik FC musi posiadać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. |
| 22 | Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:   1. ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administrator musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu. 2. Przełącznik musi być wyposażony w mechanizm sprzętowego monitorowania przepływów danych dla wskazanych jak i automatycznie wykrywanych par urządzeń komunikujących się przez dany port przełącznika. Dla każdego monitorowanego przepływu muszą być gromadzone statystyki dotyczące, co najmniej liczby wysłanych i odebranych ramek, przepustowości, liczby zapisów i odczytów SCSI, przy czym musi istnieć możliwość zawężenia zakresu monitorowania do następujących typów ramek: SCSI Reserve, SCSI Aborts, SCSI Read, SCSI Write, rejected frames. 3. Przełącznik musi być wyposażony w mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe. 4. Przełącznik musi być wyposażony w mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy. |
| 23 | Przełącznik FC musi posiadać funkcjonalność przydzielenia, co najmniej 7900 tzw. buffer credits do pojedynczego portu FC przełącznika. |
| 24 | Jeżeli wykorzystanie któregokolwiek z wymienionych funkcjonalności wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć wraz z rozwiązaniem. |
| 25 | Zasilacze redundante Hot-Plug |

* 1. **Bezpieczeństwo**

**System do zarządzania kluczami kryptograficznymi KMS - sztuk 4**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 16. Wymagania na system zarządzania kluczami (KMS)

|  |  |
| --- | --- |
| **Lp** | **Opis wymagania** |
| 1. | Moduł centralnego zarządzania kluczami musi być dostępny w postaci rozwiązania sprzętowego, jak i wirtualnego (ang. virtual appliance) gotowego do uruchomienia w środowisku wirtualnym |
| 2. | Muszą być wspierane m.in. następujące platformy wirtualizacyjne: VMware, AWS, Microsoft Azure, Oracle VM VirtualBox, OpenStack, Microsoft Hyper-V |
| 3. | Rozwiązanie sprzętowe musi zapewniać:   * Dwa redundantne zasilacze typu hot-swap. * Nie mniej niż 2 porty Ethernet minimum 1 Gbps. * Interfejs sieciowy musi wspierać standard minimum IPv4 * Być przeznaczony do zamontowania w szafie 19”. * Wysokość rozwiązania nie większa niż 1U. |
| 4. | Rozwiązanie musi posiadać możliwość implementowania architektury wysokiej dostępności w oparciu o co najmniej klastry typu active-active |
| 5. | W przypadku rozwiązania opartego na maszynach wirtualnych system musi posiadać możliwość zaszyfrowania maszyny wirtualnej |
| 6. | Konfiguracja wstępna realizowana poprzez terminal szeregowy i linię komend przy wykorzystaniu protokołu SSH |
| 7. | Zarządzanie systemem musi być realizowane poprzez interfejs przeglądarki internetowej w połączeniu szyfrowanym |
| 8. | System musi mieć możliwość wykorzystania zewnętrznego repozytorium użytkowników poprzez interfejs LDAP |
| 9. | System musi prowadzić niezaprzeczalny rejestr operacji administracyjnych wykonanych w systemie oraz działań na kluczach szyfrujących i zmian polityk |
| 10. | System musi wysyłać zdarzenia za pomocą syslog lub SNMP v3 do zewnętrznych systemów np. klasy SIEM |
| 11. | System musi automatyczne wykonywać zabezpieczoną kopię zapasową swojej konfiguracji |
| 12. | System musi umożliwiać separację zadań poprzez granularne przydzielanie uprawnień użytkowników lub ich grup do kluczy szyfrujących |
| 13. | System musi posiadać interfejs tzw. REST API dla czynności administracyjnych |
| 14. | System musi mieć możliwość integracji z rozwiązaniami klasy HSM, w celu przechowywania jego głównych kluczy tzw. master keys |
| 15. | System musi obsługiwać połączenia dla co najmniej 1 000 modułów wykonawczych – systemów usługowych wykorzystujących klucze |
| 16. | System musi umożliwiać szyfrowaną komunikację z modułami wykonawczymi systemów szyfrowania danych za pomocą protokołu SSL/TLS NAE |
| 17. | System musi posiadać możliwość wykonywania ręcznego, na żądanie jak i zautomatyzowanego backupu |
| 18. | Monitorowanie musi być realizowane poprzez statystyki:   * Główne systemu m.in. obciążenie CPU, długość pracy systemu, połączeń z systemem (ilość zaakceptowanych, ilość odrzuconych, ilość szyfrowanych SSL itp), obciążenia interfejsów ETH * Kryptograficzne m.in. ilość, typ i jakość operacji kryptograficznych |
| 19. | Celem system jest zapewnienie platformy do zarządzania kluczami kryptograficznymi dla systemów IT realizujących co najmniej funkcje:   * szyfrowania aplikacji * szyfrowania baz danych w szczególności natywnych rozwiązań dostępnych w bazach danych * szyfrowanie plików i folderów |
| 20. | Zarządzanie kluczami ma być realizowane poprzez:   * Generację kluczy * Import i eksport kluczy * Rotację kluczy * Usuwanie kluczy |
| 21. | Przechowywanie i obsługę do jednego miliona kluczy szyfrujących w przypadku rozwiązania sprzętowego i co najmniej 25 tysięcy w przypadku rozwiązania wirtualnego z możliwością skalowania wertykalnego. |
| 22. | System musi obsługiwać protokoły i interfejsy dostępu do usług systemu:   * KMIP v1.0 i 1.1 - wszystkie systemy zgodne z tą specyfikacją * Network-Attached Encryption(NAE)-XML – dla potrzeb budowy własnych autorskich rozwiązań |
| 23. | System musi obsługiwać co najmniej następujące algorytmy szyfrowania:   * AES o długości: 128, 192, 256 * TDES o długości: 128, 192 * RSA o długości: 512, 1024, 2048, 3072, 4096 * HMAC-SHA1 o długości co najmniej: 128, 160 * HMAC-SHA256 o długości: 128, 192, 256 * HMAC-SHA385 o długości: 192, 288, 384 * HMAC-SHA512 o długości: 256, 384, 512 * Krzywe eliptyczne EC: brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, prime256v1, secp224k1, secp224r1,secp256k1, secp384r1, secp521r1 |
| 24. | System musi umożliwiać pełną synchronizację czasu, niezbędnego do operacji na kluczach, przy wykorzystaniu protokołu NTP |

**Sprzętowy moduł bezpieczeństwa HSM – sztuk 4**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 17. Wymagania na sprzętowe moduły bezpieczeństwa

|  |  |
| --- | --- |
| **Lp** | **Opis wymagania** |
| 1. | Sprzętowy moduł kryptograficzny (HSM) musi umożliwiać wykonanie przynajmniej następujących operacji:   * generowanie kluczy kryptograficznych symetrycznych i asymetrycznych, * fizyczną i logiczną ochronę kluczy kryptograficznych, * kontrolę dostępu do kluczy kryptograficznych, * wykonywanie operacji z użyciem kluczy kryptograficznych, * archiwizację kluczy, * odtwarzanie kluczy z kopii bezpieczeństwa. |
| 2. | Moduł musi posiadać certyfikat FIPS 140-2 Level3 lub wyższy lub równoważny, |
| 3. | Dopuszcza się aby certyfikacja dotyczyła właściwego modułu HSM wykorzystanego w urządzeniu sieciowym, |
| 4. | Klucze kryptograficzne muszą być przechowywane wewnątrz urządzenia HSM, urządzenie powinno pozwalać na przechowanie, co najmniej 500 kluczy. |
| 5. | Urządzenie powinno posiadać wydajność, co najmniej:   * 1 000 podpisów na sekundę kluczem RSA o długości 2048 bity. * 2 000 podpisów na sekundę kluczem ECDSA o długości 256 bitów. |
| 6. | Urządzanie musi mieć możliwość obsługi wielu serwerów oraz aplikacji z wielu lokalizacji poprzez sieć. Urządzenie powinno pozwalać na jednoczesną obsługę do 100 serwerów i aplikacji. |
| 7. | System musi pozwalać na tymczasowe podłączenie, w razie konieczności, dodatkowych np: testowych bądź awaryjnie aplikacji/systemów bez konieczności rozbudowywania jego licencji |
| 8. | Urządzenie musi pozwalać na tworzenie logicznych partycji do przechowywania materiału kryptograficznego. Partycje muszą być niezależnie zarządzane (wymagane jest oddzielne uwierzytelnienie do każdej partycji). Partycje muszą pozwalać na całkowitą separację materiału kryptograficznego i zarządzanie nim. Wymagane jest, aby urządzenie pozwalało na rozbudowę, do co najmniej 100 takich partycji. |
| 9. | Uwierzytelnienie do administracji modułem HSM, jak i do każdej partycji, powinno odbywać się z użyciem mechanizmu silnego uwierzytelniania (np. z użyciem kart inteligentnych lub tokenów) i wspierać mechanizm kworum M z N (do poprawnego uwierzytelnienia wymagane jest przedłożenie N poświadczeń z zestawu M poświadczeń, gdzie N=<M) |
| 10. | Urządzenie powinno umożliwiać zdalną administrację za pomocą REST API. Z urządzeniem powinna być dostarczona licencja, umożliwiającą wykorzystanie tej funkcji. |
| 11. | Urządzenie musi pozwalać na całkowitą zdalną administrację bez konieczności asysty operatorów przy urządzeniu (np. w celu przedkładania kart lub tokenów do slotu w urządzeniu). |
| 12. | Wraz z urządzeniem musi być dostarczony moduł uwierzytelniania wraz z kartami lub tokenami mikroprocesorowymi. Dopuszcza się dostarczenie jednego urządzenia na klaster dwóch modułów kryptograficznych oraz co najmniej 20 kart lub tokenów |
| 13. | Urządzenie powinno być fabrycznie nowe i dostarczone do Zamawiającego w sposób, który gwarantuje (w oparciu o mechanizmy kryptograficzne) brak ingerencji w jego zawartości i integralność (zainstalowane oprogramowanie, firmware, itp) na drodze dostawy od producenta do Zamawiającego |
| 14. | Urządzenie wraz z dostarczonym oprogramowaniem musi pozwalać na wykorzystanie następujących interfejsów programistycznych (API): PKCS#11, Microsoft CAPI i CNG, Java(JCA/JCE), OpenSSL. |
| 15. | Z urządzeniem powinny zostać dostarczony pakiet dla twórców oprogramowania (SDK) dla platform Windows i Linux, |
| 16. | Oprogramowanie klienckie dostarczone wraz urządzeniem powinno wspierać następujące platformy: Windows Server 2008 R2, 2012, 2012 R2, 2016; Windows 10; Red Hat Enterprise Linux Server minimum 6, Ubuntu minimum 16. |
| 17. | Urządzenie wraz z dostarczonym oprogramowaniem musi umożliwiać pracę w trybie wysokiej dostępności w klastrze typu active-pasive i active-active. |
| 18. | Urządzenie wraz z dostarczonym oprogramowaniem pracując w trybie active-active samo musi dokonywać równoważenie obciążenia pomiędzy węzłami klastra. |
| 19. | Komunikacja – urządzenie wraz z dostarczonym oprogramowaniem musi pozwalać na zestawienie bezpiecznego kanału komunikacyjnego pomiędzy urządzeniem a serwerem uruchomionym w środowisku wirtualnym (np. VMware, Hyper-V). |
| 20. | Komunikacja - urządzenie musi zapewniać bezpieczny kanał komunikacyjny pomiędzy aplikacją wykorzystująca interfejs PKCS#11 a partycją w module HSM, klucze do zabezpieczenia tej komunikacji muszą być przechowywane w postaci pliku na kliencie lub w dedykowanym urządzeniu sprzętowym (karta, token). |
| 21. | Urządzenie musi obsługiwać min. następujące algorytmy:   * Kryptografia symetryczna: AES, * Kryptografia asymetryczna: RSA, Diffie-Hellman, Krzywe eliptyczne m. in. ECDSA, ECDH * Funkcje skrótu: SHA2 (SHA-224, SHA-256, SHA-384, SHA-512) * Techniki: Key Wrapping, Key Derivation |
| 22. | System musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jego odtwarzanie, |
| 23. | Kopia bezpieczeństwa musi być wykonywana na dedykowane urządzenie zewnętrzne |
| 24. | Urządzenie zewnętrzne musi mieć możliwość składowania w dowolnym, niezależnym od pracującego systemu, miejscu. |
| 25. | Zestaw dwóch modułów pracujących w klastrze wysokiej dostępności musi być wyposażony w co najmniej jedno urządzenie do wykonywania kopii zapasowej i archiwizacji, posiadające wszystkie niezbędne licencje do wykonania kopii wszystkich pracujących w klastrze partycji. |
| 26. | Urządzenie do wykonywania kopii bezpieczeństwa musi posiadać certyfikat FIPS 140-2 Level3 lub wyższy lub równoważny |
| 27. | Dedykowane urządzenie zewnętrzne do wykonywania kopii bezpieczeństwa musi posiadać taki sam poziom certyfikacji jak urządzenie główne, oraz zapewniać retencję danych przez okres 10 lat. |
| 28. | Rozwiązanie musi pozwalać na wykonywanie kopii bezpieczeństwa w sposób zdalny – tj. bez konieczności asysty operatorów bezpośrednio przy urządzeniu i bez konieczności podłączania urządzenia do wykonywania kopii bezpośrednio do HSM. |
| 29. | Moduł kryptograficzny HSM musi pozwalać na rejestrowanie w sposób weryfikowalny i niezaprzeczalny:   * Wszystkich operacji związanych z administracją modułem HSM (logowanie, wylogowanie, zmiana polityk dostępu, zerowanie, itp.), * Wszystkich operacji wykonywanych na kluczach kryptograficznych (tworzenie, niszczenie, użycie) |
| 30. | Monitorowanie - moduł HSM musi pozwalać na obserwowanie stanu za pomocą protokołu SNMP następujących elementów urządzenia:   * zasilaczy sieciowych * wentylatorów * stanu baterii urządzenia * dysków twardych * wykrycie stanu naruszenia zabezpieczeń (tamper). |
| 31. | HSM musi posiadać obudowę o wysokości nie większej niż 1U, dostosowana do montażu w szafie stelażowej 19”. Dostarczone urządzenie musi posiadać wszystkie niezbędne elementy (szyny, uchwyty, śruby, itp.) do zamontowania urządzenia w szafie, |
| 32. | Urządzenie powinno być wyposażone w dwa zasilacze z możliwością wymiany w trakcie działania (hot-swap), |
| 33. | Moduł HSM musi posiadać co najmniej dwa interfejsy Ethernet o szybkości minimum 1 Gbps |
| 34. | Interfejs sieciowy musi wspierać standard minimum IPv4 |
| 35. | Porty Ethernet urządzenia muszą wspierać agregację łącza (port bonding), |

* 1. **Inne**

**Szafa RACK, minimum 2 szt.**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 19. Wymagania na szafę RACK

|  |  |
| --- | --- |
| L.p. | Opis wymagania |
| 1 | Do montażu urządzeń o rozmiarze 19’’ |
| 2 | Szafa musi umożliwiać zamontowanie urządzeń, które będą dostarczone w ramach zamówienia. Wyjątkiem są urządzenia dostarczane razem z własnymi szafami. |
| 3 | Minimum dwie listwy zasilające zapewniające możliwość podłączenia dostarczonej infrastruktury. |
| 4 | System wentylacyjny zapewniający wentylację zlokalizowanej w szafie infrastruktury tak, aby zapewnić pracę poszczególnych urządzeń w warunkach zgodnych z zaleceniami ich producentów. |
| 5 | W przypadku, kiedy urządzenie montowane w szafie nie jest wyposażone w kabel zasilający, lub kabel zasilający ma inną wtyczkę niż gniazda w oferowanej szafie, muszą zostać dostarczone odpowiednie kable zasilające. |
| 6 | Szafa wyposażona w zdejmowane drzwi przednie i tylne zamykane na klucz, zdejmowane panele boczne oraz elementy stabilizujące, zabezpieczające szafę przed wywróceniem. Drzwi tylne dzielone. Dodatkowo wymagane jest uziemienie szafy, panele chroniące przed mieszaniem powietrza gorącego z zimnym oraz elementy ułatwiające organizację kabli w szafie. W komplecie zestaw z niezbędną ilością elementów do organizacji kabli: mocowań typu D (D-rings), przednich paneli szczotkowych 1U, przednich paneli szczotkowych 2U. |
| 7 | Zgodność z normami EIA-310  Zgodność z normami RoHS |

**Obudowa BLADE - sztuk 2**

(opcjonalnie, gdy zostaną dostarczone serwery typu BLADE)

Obudowa ma być kompatybilna z zaoferowanymi serwerami kasetowymi

Tabela 20. Wymagania na obudowę blade

|  |  |
| --- | --- |
| L.p. | Opis wymagania |
| 1 | Obudowa, o wysokości maksymalnie 10U, musi być przystosowana do montażu w szafie typu rack 19”, umożliwiająca obsadzenie minimum 10 serwerów dwuprocesorowych bez konieczności rozbudowy o kolejne elementy sprzętowe. |
| 2 | Sposób agregacji/wyprowadzeń sygnałów LAN dla pojedynczej obudowy.  Minimum dwa przełączniki LAN. Urządzenia te muszą umożliwiać agregację połączeń LAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów LAN z infrastruktury z zachowaniem redundancji połączeń.  Każdy z modułów musi posiadać porty zewnętrzne:  • Minimum 4 porty 40Gb  • Minimum 4 porty 10Gb  Sumaryczna przepustowość portów zewnętrznych (porty 40Gb oraz porty 10Gb; nie dopuszcza się samych portów 40Gb) musi wynosić minimum 200Gb dla pojedynczego modułu LAN.  Dostarczone moduły należy obsadzić odpowiednimi do prędkości portów wkładkami.  Wszystkie dostępne, fizyczne porty (wewnętrzne oraz zewnętrzne) każdego modułu LAN (niezależnie od minimalnej wymaganej ilości portów) muszą być aktywne i gotowe do obsługi ruchu sieciowego bez konieczności dokupowania elementów sprzętowych lub dodatkowych licencji. Należy dostarczyć wszystkie niezbędne licencje do aktywacji wszystkich portów urządzeń. |
| 3 | Obudowa musi posiadać minimum dwa moduły typu switch 16Gb Fibre-Channel wyprowadzające sygnały z minimum 2 portów FC każdego serwera. Urządzenia te muszą umożliwiać agregację połączeń SAN w infrastrukturze blade i muszą umożliwiać wyprowadzenie sygnałów SAN z infrastruktury z zachowaniem redundancji połączeń. Każdy moduł musi posiadać minimum 8 zewnętrznych portów obsadzonych modułami 16Gb SFP+ SW.  Wszystkie dostępne, fizyczne porty każdego modułu Fibre-Channel muszą być aktywne i gotowe do obsługi ruchu sieciowego SAN bez konieczności dokupowania elementów sprzętowych lub dodatkowych licencji.  Każdy moduł powinien umożliwiać (posiadać licencje):  • ISL Trunking  • Fabric Watch  • Extended Fabric  • Zaawansowane zarządzanie wydajnością |
| 4 | Obudowa na serwery wyposażona w zestaw redundantnych wentylatorów (typ hot plug, czyli możliwość wymiany podczas pracy urządzenia) zapewniających chłodzenie dla maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie blade. Wentylatory niezależne od zasilaczy, wymiana wentylatora (wentylatorów) nie może powodować konieczności wyjęcia zasilacza (zasilaczy). |
| 5 | Obudowa wyposażona w zestaw zasilaczy redundantnych typu Hot Plug. System zasilania zdolny do obsługi awarii połowy z zainstalowanych zasilaczy (dowolne N zasilaczy przy założeniu konfiguracji N + N), wymagane ciągłe dostarczenie mocy niezbędnej do zasilenia maksymalnej liczby serwerów i urządzeń I/O zainstalowanych w obudowie. Procesory serwerów winny pracować z nominalną, maksymalną częstotliwością.  Wymiana zasilacza nie może powodować konieczności odłączenia zewnętrznej infrastruktury zasilania (kabla zasilającego), jak również nie może powodować konieczności wyjęcia lub odłączenia wentylatorów (pojedynczego wentylatora lub modułu wentylatorów). |
| 6 | Możliwość instalacji switchy w standardzie InfiniBand. |
| 7 | 2 Moduły KVM, umożliwiający podłączenie klawiatury, myszy i monitora. |
| 8 | Wraz z infrastrukturą blade, należy dostarczyć odpowiednią ilość modułów PDU do prawidłowego, redundantnego podłączenia infrastruktury blade do zasilania w szafach Zamawiającego. PDU muszą spełniać minimalne wymagania:  - minimum 32A  - minimum dwa redundantne moduły (należy uwzględnić odpowiednią ilość modułów dla redundantnego podłączenia całej infrastruktury blade)  - ilość gniazd zapewniająca podłączenie dostarczonej infrastruktury blade |
| 9 | Dwa redundantne, sprzętowe moduły zarządzające typu Hot Plug. |
| 10 | Wymagania dot. zarządzania:  - Podstawowe funkcje: Zdalne włączanie/wyłączanie/restart niezależnie dla każdego serwera.  - Zdalne udostępnianie napędu CD-ROM/DVD/ISO na potrzeby każdego serwera z możliwością bootowania z w/w napędów.  - Zdalny sposób zarządzania z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.  - W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów w ramach infrastruktury  - Zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego.  - Automatyzowana konfiguracja sprzętowa każdego serwera niezależnie oraz wielu serwerów równocześnie za pomocą skryptów.  - Zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci)  - Zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego.  - Zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu.  - Zdalna dystrybucja oprogramowania.  - Automatyczne wykrywanie i identyfikacja urządzeń zainstalowanych w ramach infrastruktury (serwery, obudowy blade, karty zarządzające) i prezentacja infrastruktury w postaci graficznej.  - Monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć.  - Licencje na powyższą funkcjonalność na wszystkie serwery blade możliwe do obsadzenia w oferowanej infrastrukturze blade. |

**Konsola KVM - 2 szt.**

Podane niżej wymagania dotyczą jednej sztuki

Tabela 2.21 Wymagania na konsolę KVM

| **L.p.** | **Opis wymagania** |
| --- | --- |
| **1** | Konsola musi być wysuwana ze składanym panelem LCD/LED, przystosowana do montażu w szafie stelażowej 19”, o wysokości max. 1U wraz z szynami montażowymi. |
| **2** | Konsola musi posiadać matrycę aktywną co najmniej 18,5 cala i wspierać rozdzielczość natywną co najmniej SXGA (1280x1024). |
| **3** | Konsola musi zawierać klawiaturą typu International ze zintegrowanym w obudowie urządzeniem wskazującym. |
| **4** | *Wymagane w przypadku, gdy dostarczone będą serwery typu innego niż BLADE.*  Konsola musi posiadać min. 10 portów do podłączania serwerów, porty standardu RJ45, wykorzystujące kable CAT 5 lub wyższej.  Konsola musi posiadać min. 10 przejściówek (interface adapterów) RJ-45 na USB i VGA, pozwalających podłączyć serwery do przełącznika KVM. |
| **5** | Konsola musi posiadać porty dodatkowe:  - port cyfrowy/analogowy do podłączenia monitora  - minimum 2 porty USB do podłączenia klawiatury i urządzenia wskazującego  - port do łączenia (stakowania) przełączników KVM |
| **6** | Konsola musi posiadać zarządzanie z poziomu interfejsu graficznego (wbudowany interfejs webowy), zarządzanie zdalne (jednoczesne sesje) minimum dla 2 użytkowników zdalnych, dostępne menu ekranowe przy dostępie lokalnym. |

* 1. **Oprogramowanie**

**OPROGRAMOWANIE BACKUPU - sztuk 1**

Tabela 10. Specyfikacja wymagań oprogramowania backupu

| **Lp.** | **Opis wymaganej funkcjonalności** |
| --- | --- |
| 1 | Wymagane jest dostarczenie licencji oprogramowania backupowego dla trzech niezależnych od siebie środowisk obejmujących zarówno serwery niezwirtualizowane oraz zwirtualizowane, charakteryzujących się sumaryczną ilością CPU jak i rozmiarem danych źródłowych określonych w niniejszym projekcie dla każdego z w/w środowisk. |
| 2 | Wymagane jest, aby wszystkie dostępne funkcjonalności oferowanego rozwiązania były odblokowane w ramach oferowanych licencji. |
| 3 | Wymagane jest dostarczenie wszystkich modułów oprogramowania backupowego tak, aby zapewnić backup wyspecyfikowanych środowisk oraz spełnić wszystkie wymienione w niniejszej tabeli funkcjonalności. |
| 4 | Oprogramowanie backupowe musi być w pełni zintegrowane z oferowanymi deduplikatorami oraz umożliwiać backup zabezpieczanych maszyn na oferowane deduplikatory zarówno poprzez sieć LAN jak również SAN. |
| 5 | Wymagana jest możliwość wyboru miejsca de-duplikacji   1. na źródle 2. na medium backupowym |
| 6 | Backup z de-deduplikacją na źródle musi być dostępny dla wszystkich typów danych w ramach oferowanego rozwiązania: pliki, bazy danych, obrazy maszyn wirtualnych. |
| 7 | Oprogramowanie backupowe musi zapewniać bezpośredni backup z każdej zabezpieczanej maszyny bezpośrednio na oferowany deduplikator bez pośrednictwa jakichkolwiek innych serwerów w trybie z deduplikacją na źródle oraz bez deduplikacji na źródle - wymagane obie opcje z możliwością dowolnego użycia oraz możliwością przełączania. Funkcjonalność musi dostępna dla minimum następujących platform: Windows, RedHat, Ubuntu. |
| 8 | Wymagana jest możliwość automatycznego łączenia backupu blokowego pełnego i inkrementalnego po wykonaniu blokowego backupu inkrementalnego w celu uzyskania aktualnego backupu pełnego. |
| 9 | Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności. |
| 10 | Oprogramowanie backupowe musi mieć możliwość backupu własnej bazy danych na następujące nośniki:   1. urządzenie dyskowe 2. deduplikatory będące przedmiotem zamówienia 3. nośniki taśmowe będące przedmiotem zamówienia |
| 11 | W przypadku backupu na nośniki taśmowe wymagana jest możliwość zdefiniowania puli taśm (zawierającej jedną lub więcej taśm), na którą będą zapisywane tylko i wyłącznie backupy wewnętrznej bazy danych systemu backupowego. |
| 12 | Oprogramowanie backupowe musi mieć możliwość automatycznego wykonywania backupu własnej bazy danych. |
| 13 | Oprogramowanie backupowe po każdorazowym backupie wewnętrznej bazy danych musi raportować poprzez e-mail miejsce, w którym znajduje się ostatni backup wewnętrznej bazy danych oprogramowania backupowego. |
| 14 | Backup własnej bazy danych musi pozwalać na odtworzenie wszystkich ustawień systemu backupowego na zupełnie nowej, świeżo zainstalowanej instancji oprogramowania backupowego. |
| 15 | Oprogramowanie backupowe musi mieć możliwość (wymagane formalne wsparcie producenta oprogramowania backupowego) działania jako wirtualna maszyna systemu VMware. |
| 16 | W przypadku backupu systemów produkcyjnych (klientów systemu backupu) na nośniki taśmowe, oferowane oprogramowanie backupowe musi umożliwiać zapisywanie backupów o tym samym terminie ważności na jednej, tej samej, z góry zdefiniowanej puli taśm (zawierającej jedną lub więcej taśm). |
| 17 | W przypadku gdy w puli taśmowej zabraknie taśm na których można zapisywać nowe backupy, oprogramowanie backupowe musi mieć możliwość automatycznego przyporządkowania:   1. wolnych, nieprzyporządkowanych taśm znajdujących się w bibliotece 2. nieużywanych lub przeterminowanych taśm z innych pul taśmowych |
| 18 | W przypadku użycia biblioteki taśmowej, oferowany system musi generować samoopisujące się taśmy dla całości zapisywanych taśm, co oznacza to, że wyjęcie jakiejkolwiek taśmy z biblioteki i włożenie jej do zupełnie innej biblioteki zarządzanej przez zupełnie inną instancję oferowanego oprogramowania backupowego (w tym również działającą na innym systemie operacyjnym) musi pozwolić na odtworzenie danych znajdujących się na w/w taśmie. |
| 19 | Oprogramowanie backupowe musi umożliwiać łączenie strumieni backupowych z wielu zabezpieczanych serwerów w sieci LAN i bezpośredni zapis na napędzie taśmowym (multiplexing). |
| 20 | Oprogramowanie backupowe musi umożliwiać zarządzanie bezpośrednią replikacją backupów między oferowanymi urządzeniami de-duplikacyjnymi (replikacja realizowana na poziomie urządzeń de-duplikacyjnych) - bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań   1. replikacji podlegają tylko te bloki które nie znajdują się na docelowym oferowanym urządzeniu de-duplikacyjnym 2. replikacja między urządzeniami de-duplikacyjnymi może nastąpić zarówno bezpośrednio po zakończeniu backupu jak również zgodnie z kalendarzem 3. oferowane oprogramowanie backupowe przechowuje informacje o wszystkich kopiach danych znajdujących się oferowanych urządzeniach de-duplikacyjnych m.in. źródłowych jak i po replikacji   GUI oferowanego oprogramowania backupowego musi umożliwiać wybór urządzenia de-duplikacyjnego z którego zostanie wykonane odtwarzanie - w efekcie umożliwiając odtworzenie z oryginalnej kopii backup’owej bądź ze zreplikowanej kopii backup’owej. |
| 21 | Oprogramowanie backupowe musi mieć możliwość klonowania backupów między dowolnymi mediami:   1. De-duplikacyjnymi 2. Dyskowymi (CIFS, MIN. NFS V.4 I SMB V.3) 3. Taśmowymi 4. Macierzami |
| 22 | Oprogramowanie backupowe musi zapewniać różny czas ważności danych na podstawowym nośniku i nośniku zawierającym kopię (replikę backupu). Definicja czasu przechowywania kopii (repliki) musi być określenia w momencie definiowania zadania duplikacji/kopiowania zarówno z interfejsu graficznego jak i z linii poleceń (command line). |
| 23 | Oprogramowanie backupowe musi pozwalać na następujące rodzaje backupu systemu plików:   1. Pełny 2. Różnicowy (wymagane minimum 5 poziomów backupu różnicowego) 3. Inkrementalny |
| 24 | Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych w jeden pełen backup. Proces ten musi być niewidoczny dla systemu plików którego dotyczą backupy pełne i inkrementalne. Proces odtworzenia danych z połączonego backupu pełnego i inkrementalnego musi być identyczny z odtworzeniem danych z normalnie wykonanego backupu pełnego w zakresie zarządzania. |
| 25 | W przypadku konsoli oprogramowania backupowego wymagana jest możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte. |
| 26 | Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows 2012,2012R2,2016 (także Microsoft Cluster) , Linux (Red Hat, Ubuntu). |
| 27 | Oprogramowanie backupowe musi zapewnić (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS SQL 2016, PostgreSQL 9.5, VMware 6.5 i wyżej, HyperV. |
| 28 | Oprogramowanie backupowe musi zapewnić odtwarzanie pojedynczego serwera Windows bez ponownej instalacji systemu operacyjnego. |
| 29 | W przypadku zabezpieczania baz danych i aplikacji wymagana jest możliwość realizacji kopii zapasowej kilkoma strumieniami jednocześnie (minimum 10 jednoczesnych strumieni). |
| 30 | Oprogramowanie backupowe musi posiadać funkcjonalność podziału danych (plików, baz danych, obrazów maszyn wirtualnych) na bloki. System musi się dopasowywać do struktury dokumentu zapewniając podział na bloki w ramach pojedynczego dokumentu w celu polepszenia efektywności deduplikacji.  Podział na bloki musi następować bezpośrednio na zabezpieczanym serwerze. |
| 31 | Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być ponownie odczytywany, chyba, że zmieni się jego zawartość. |
| 32 | Wymaga się aby oprogramowanie backupowe realizowało wyłącznie - logicznie pełne backupy systemu plików. Z zabezpieczanego systemu plików muszą odczytywane tylko nowe lub zmienione pliki, do oferowanego de-duplikatora muszą być przesyłane dane po de-duplikacji, jednak każdy finalny backup musi być logicznie pełnym backupem. W wewnętrznej strukturze systemu musi być przechowywana informacja o każdym backupie i należących do niego danych (blokach), dzięki czemu odtworzenie jakichkolwiek danych plikowych musi być pojedynczym zadaniem identycznym z odtworzeniem danych z pełnego backupu. |
| 33 | Wymagana możliwość tworzenia z poziomu GUI (konsoli graficznej) w przypadku oferowanego oprogramowania backupowego, polityk typu Dziadek – ojciec –syn, to znaczy tworzenia polityk w których zdefiniowano:   1. Czas przechowywania backupów dziennych 2. Czas przechowywania backupów tygodniowych 3. Czas przechowywania backupów miesięcznych 4. Czas przechowywania backupów rocznych |
| 34 | Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Wymagana możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:   1. wybranych typów plików, np. dla plików z rozszerzeniem doc 2. dla całych katalogów (np.: c:\windows). 3. dla pojedynczych plików |
| 35 | Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min, administrator, monitoring, tylko wykonywanie odtworzeń) w systemie backupowym. |
| 36 | Bloki przesyłane z zabezpieczanych serwerów do oferowanego de-duplikatora muszą być kompresowane i szyfrowane algorytmem z kluczem minimum 256-bitowym. |
| 37 | Wymagane szyfrowanie danych na medium dyskowym przechowującym backupy (de-duplikaty). |
| 38 | Wymagana jest autentykacja komunikacji między klientem a serwerem backupu oparta na certyfikatach. |
| 39 | Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.5 i nowszych oraz Hyper-V.  Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu:   1. Backup całych maszyn wirtualnych 2. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk 3. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane 4. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware) 5. Wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk)   Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla de-duplikacji powyżej.  Powyższe metody backupu muszą być wbudowane w oferowany system backupu, nie mogą wymagać tworzenia skryptów/dodatkowych komend. |
| 40 | Oferowany system musi pozwalać na szybkie odtworzenie   1. całych obrazów maszyn wirtualnych 2. pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej |
| 41 | Wymaga się aby oferowane rozwiązanie backupowe umożliwiało odtwarzanie obrazów maszyn wirtualnych VMware z następującymi funkcjonalnościami:   1. odtwarzanie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu 2. odtwarzanie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu   Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne nie mogą generować konieczności wykorzystania dodatkowych skryptów/ komend. |
| 42 | Oferowane rozwiązanie backupowe musi umożliwiać uruchomienie maszyn wirtualnych bezpośrednio z oferowanych deduplikatorów w oparciu o zrealizowany backup, bez konieczności odtwarzania backupu (tzw. Instant Access, wymagana możliwość jednoczesnego uruchomienia min. 20 maszyn wirtualnych) – wymagane oficjalne wsparcie zarówno w przypadku oferowanych deduplikatorów (dla oferowanej aplikacji backupowej) oraz aplikacji backup’owej (dla oferowanych deduplikatorów). |
| 43 | Oferowane oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej w celu ich przeszukiwania (wymagane przeszukiwanie po nazwach plików z poziomu systemu operacyjnego maszyny fizycznej. |
| 44 | Oferowane oprogramowanie backupowe musi mieć możliwość backupu/odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter. |
| 45 | Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym. |
| 46 | Oferowane rozwiązanie backupowe musi umożliwiać na tworzenie automatycznych polityk backupowych dla:   1. Folderu 2. Resource Pool systemu VMware.   Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware. |
| 47 | Wymaga się, aby inicjowanie backupu oraz odtwarzanie maszyn wirtualnych VMware dostępne było z poziomu graficznego interfejsu, linii komend oraz przez REST API |
| 48 | Oferowane oprogramowanie backupowe musi zapewniać spójny backup MSSQL przy backupie obrazów maszyn wirtualnych środowiska Hyper-V |
| 49 | W przypadku systemów Windows 2012, Windows 2016 wymagana funkcjonalność Bare Metal Recovery - automatycznego odtworzenia całego serwera (system operacyjny + ustawienia systemu operacyjnego + dane) w jednym kroku bezpośrednio z oferowanego urządzenia,  Funkcjonalność ta musi być wbudowana w rozwiązanie backupowe. |
| 50 | Oferowany system backupu musi posiadać integralną funkcjonalność wyrzutu danych na taśmę, funkcjonalność ta musi być realizowana poprzez zastosowanie gotowego modułu producenta systemu:   1. niewymagającego dodatkowych skryptów 2. niewymagającego dodatkowego oprogramowania poza dostarczonym przez producenta 3. zawierającego interfejs GUI producenta 4. posiadającego pełne wsparcie producenta |
| 51 | Oferowany system backupu musi być dostępny (dla backupu i odtwarzania) przez 24h na dobę 7 dni w tygodniu, wyklucza się istnienie okresów w przypadku których system backupowy nie może wykonywać backupu lub odtwarzania (tzw. BLACKOUT WINDOWS). |
| 52 | Oferowany system backupu musi mieć możliwość instalacji agentów jako plików msi. Wymagana możliwość automatyzacji instalacji agentów poprzez uruchomienie skryptu na zabezpieczanej maszynie, przyporządkowującego maszynę automatycznie do określonej polityki backupowej. |
| 53 | Oferowany system backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu. |
| 54 | Oferowany system musi pozwalać na backup serwerów NAS z następującymi funkcjonalnościami:   1. w trakcie backupu z systemu NAS muszą być wysyłane do medium backupowego tylko zmienione pliki od ostatniego backupu 2. w przypadku odtwarzania danych z backupu, uprawnienia użytkowników również są odtwarzane 3. integracja z protokołem NDMP systemów NAS |
| 55 | W ramach oferowanych licencji wymaga się następujących funkcjonalności – dotyczących monitorowania, raportowania oraz przeszukiwania backupów |
| 56 | W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów:   1. Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych) 2. Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych danych) 3. Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów 4. Zbiorcze zestawienie zabezpieczanych serwerów które w sposób ciągły (kilka razy pod rząd) maja problem z backupami 5. Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii) 6. Najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów) 7. Lista najwolniejszych/najszybszych zabezpieczanych maszyn 8. Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego 9. Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu do którego się dotwarzamy) 10. Liczba danych backupowanych dziennie 11. Liczba zadań backupowych dziennie 12. Zużycie mediów backupowych i napędów taśmowych 13. Aktualna konfiguracja systemu backupowego 14. Historia zmian konfiguracji systemu backupowego 15. Posiadane licencje systemu backupowego |
| 57 | W ramach dostarczonych licencji wymagana możliwość przeszukiwania backupów z poziomu graficznego interface’u (GUI), wymagana możliwość wyszukania dowolnych fraz w nazwach plików. |
| 58 | W ramach oferowanych licencji wymaga się następujących funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk VMware. Licencja dla min. 100 maszyn wirtualnych dla każdego z trzech środowisk. |
| 59 | Integracja na poziomie VMware vCenter Plug-in (ORCHESTRATION, MANAGEMENT) , vSphere Web Client GUI |
| 60 | wsparcie dla HA, DRS, S-DRS, VMotion, S-VMotion |
| 61 | rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie ESXi |
| 62 | skalowalność zapewniająca wsparcie dla 2000 VM w obrębie poj. vCenter |
| 63 | zabezpieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla VMware ESXi 5.5 oraz 6.0 |
| 64 | możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM) |
| 65 | zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT’ów ) na poziomie VMDK oraz RDM, niezależnie od użytego storage’u (tzw. Storage Agnostic -warunkiem jest wsparcie przez VMware), wymagane wsparcie dla połączeń: FC, FCoE, iSCSI, NAS oraz DAS |
| 66 | wsparcie dla replikacji (bi-directional) asynchronicznej (realizowanej na poziomie dostarczanego oprogramowania), połączonych z mechanizmem tzw. JOURNALING umożliwiającego odnotowanie wszystkich zmian zabezpieczanego środowiska |
| 67 | odporność na krótkotrwałe problemy (przeciążenie, zaniki) związane z siecią WAN |
| 68 | wbudowana funkcjonalność kompresji w przypadku transmisji danych poprzez WAN |
| 69 | wsparcie dla równoległej replikacji zabezpieczanego środowiska do różnych ośrodków docelowych (min. 3-ech), wsparcie dla replikacji równoległej musi być zapewnione również na poziomie grup konsystencji (CONSISTENCY GROUP) |
| 70 | proponowane rozwiązanie musi umożliwiać:   1. stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska zbudowanego w oparciu o VMware 2. operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami 3. MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe |
| 71 | równoległe wsparcie środowisk lokalnych oraz zdalnych, wymagana jest możliwość pracy w 3-ech trybach, tzw.: CDP (Continuous Data Protection - tryb replikacji lokalnej), CRR (Continuous Remote Replication - tryb replikacji zdalnej), CLR (Continuous Local and Remote Replication - połączenie CDP oraz CLR - tryb replikacji lokalnej oraz zdalnej) w ramach dostarczonych licencji |
| 72 | granularność umożliwiająca pominięcie określonych plików VMDK związanych z wirtualnymi serwerami VM objętych protekcją |
| 73 | architektura FAULT-TOLERANCE |
| 74 | działanie rozwiązania będącego przedmiotem zamówienia nie może mieć żadnego negatywnego wpływu na wydajność zabezpieczanych maszyn i aplikacji |
| 75 | wyskalowanie systemu musi gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie pojedynczych sekund |
| 76 | możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie |
| 77 | możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM) |
| 78 | możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację |
| 79 | możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM) |
| 80 | możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK |
| 81 | możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, …) |
| 82 | możliwość skryptowego tworzenia planów RECOVERY |

**OPROGRAMOWANIE DO ZARZĄDZANIA HSM– sztuk 1**

Tabela 18. Minimalne wymagania na oprogramowanie do zarządzania HSM

|  |  |
| --- | --- |
| **Lp** | **Opis wymaganej funkcjonalności** |
| 1. | System musi być oparty o centralny serwer zarządzający |
| 2. | Serwer zarządzający musi pozwalać na wdrożenie w trybie wysokiej dostępności (HA) |
| 3. | Serwer zarządzający musi umożliwiać zastosowanie wewnętrznej lub zewnętrznej bazy danych (m.in. Oracle Database lub PostgreSQL), |
| 4. | System musi być dostarczony w architekturze klastra wysokiej dostępności |
| 5. | System musi mieć możliwość wdrożenia w środowisku wirtualnym |
| 6. | Dane wrażliwe przeznaczone do zarządzania modułami kryptograficznymi, system musi przechowywać w formie zaszyfrowanej a klucze szyfrujące przechowywać w dedykowanym module tzw. root-of-trust lub logicznej, separowanej instancji HSM w trybie wysokiej dostępności |
| 7. | Komunikacja pomiędzy Systemem zarządzania a modułami kryptograficznymi musi odbywać się przy pomocy interfejsu zbudowanego w oparciu o uniwersalne praktyki REST API (tzw. REST API framework) |
| 8. | System musi posiadać webowy interfejs zarządzania dostępny przez przeglądarkę internetową. |
| 9. | System musi pozwalać na zdefiniowanie do co najmniej:   * do 1000 Usług Kryptograficznych * do 1000 Organizacji * do 1000 Użytkowników w ramach Organizacji |
| 10 | System musi być dostarczony wraz z niezbędnymi licencjami do obsługi wszystkich partycji dostarczonych z modułami kryptograficznymi, |
| 11. | System musi być skalowalny poziomo poprzez możliwość docelowego obsłużenia co najmniej 10 modułów kryptograficznych HSM w wersji sieciowej |
| 12. | Z Systemem musi być dostarczona odpowiednia liczba licencji umożliwiająca obsługę co najmniej 15 niezależnych systemów klienckich przez dowolnie skonfigurowaną usługę kryptograficzną |
| 13. | System musi posiadać możliwość automatycznego wykrywania i importowania konfiguracji modułów kryptograficznych |
| 14. | Z poziomu interfejsu administracyjnego, w formie konsoli typu Dashboard, musi być możliwe monitorowanie podstawowych parametrów modułów kryptograficznych takich jak: obciążenie procesorów, ilość wykonywanych operacji na sekundę, czy też zajętość zasobów pamięci |
| 15. | Monitorowanie musi obejmować możliwość analizy historycznej trendów monitorowanych parametrów |
| 16. | System musi umożliwiać zdefiniowanie następujących obiektów logicznych:   * Użytkownika należącego do Organizacji * Usługi Kryptograficznej tworzonej z Szablonu Usługi Kryptograficznej * Zasobu określającego cechy partycji i urządzenia HSM. Powinna istnieć możliwość grupowania Zasobów w Pule Zasobów. |
| 17. | Szablon Usługi powinien definiować, co najmniej następujące parametry Usługi Kryptograficznej:   * Wysoką dostępność, * Wydajność (normalna lub wysoka) * Sposób uwierzytelniania (hasło lub MFA), * Rozmiar przestrzeni przeznaczonej na klucze (w kilobajtach), * Sposób wykonywania kopii kluczy kryptograficznych (backup, bez kopii) |
| 18. | Oprogramowanie musi posiadać interfejs dostępny przez przeglądarkę internetową |
| 19. | Oprogramowanie musi posiadać możliwość kreowania wirtualnych HSM |
| 20. | Oprogramowanie musi umożliwiać tworzenie kryptoserwisów automatyzujących wykorzystanie posiadanych urządzeń HSM |
| 21. | Oprogramowanie musi umożliwiać tworzenie ról w grupie Administrator oraz Użytkownik |
| 22. | Członkowie grupy Użytkownik mają mieć możliwość logowania do portalu selfservice w celu pobrania pliku instalacyjnego zawierającego konfiguracją urządzeń HSM przygotowanego przez Członka grupy Administratorzy w postaci kryptoserwisu. |
| 23. | Monitorowanie działania urządzeń HSM w szczególności:   * HealthCheck * Monitorowanie obciążenia |
| 24. | Musi istnieć możliwość tworzenia raportów nt. wykorzystanych Zasobów i Usług Kryptograficznych. Powinna istnieć możliwość eksportu raportów do pliku w formacie CSV. |
| 25. | Raport dotyczący Usługi Kryptograficznej musi zawierać:   * Nazwę usługi * Kto i kiedy stworzył usługę * Informację czy Usługa Kryptograficzna jest zainicjalizowana i kto wykonał inicjalizację * Ilość klientów (serwerów) przypisanych do usługi |
| 26. | Jeżeli Usługa Kryptograficzna pracuje w trybie wysokiej dostępności powinny być dostępne szczegółowe informacje nt. pracy układu HA |
| 27. | Raport dotyczący Zasobów (urządzeń) musi zawierać:   * Nazwę urządzenia * Wersję oprogramowania i oprogramowania układowego zainstalowanego w urządzeniu * Ilość klientów (serwerów) autoryzowanych do uwierzytelnienia się w urządzeniu * Detaliczne dane nt. stworzonych partycji w urządzeniu (jak numer seryjny, etykieta partycji, ilość obiektów na partycji, itp.) * Ilość wolnego i wykorzystanego miejsce na przechowywanie materiału kryptograficznego w urządzeniu. |