Projekt techniczny wraz z opisem przedmiotu zamówienia

dostawa, wdrożenie i urochomienie infrastruktury IT dla tworzonego zapasowego repozytorium cyfrowego na potrzeby archiwów państwowych

smartcom przemysław purgał

2020

Spis treści

[**1.** **Wprowadzenie** 3](#_Toc70421451)

[**2.** **Słownik pojęć i skrótów** 3](#_Toc70421452)

[3. **Ogólne warunki przedmiotu zamówienia** 3](#_Toc70421453)

[**3.1.** **Przedmiot zamówienia** 3](#_Toc70421454)

[**3.2.** **Miejsce realizacji przedmiotu zamówienia** 4](#_Toc70421455)

[**3.3.** **Etapy realizacji zamówienia** 4](#_Toc70421456)

[**4.** **Główne założenia** 7](#_Toc70421457)

[**4.1.** **Opis stanu aktualnego** 7](#_Toc70421458)

[**4.2.** **Proponowana architektura projektowanego rozwiązania** 9](#_Toc70421459)

[**4.2.1.** **Rozłożenie infrastruktury** 9](#_Toc70421460)

[**4.2.2.** **Przełączniki LAN (rdzeniowe i OOB)** 10](#_Toc70421461)

[**4.2.3.** **Przełączniki SAN** 12](#_Toc70421462)

[**4.2.4.** **Routery BGP** 12](#_Toc70421463)

[**4.2.5.** **System bezpieczeństwa – firewall** 13](#_Toc70421464)

[4.2.6. **Platforma hiperkonwergentna** 14](#_Toc70421465)

[**4.2.7.** **System kopii zapasowej** 16](#_Toc70421466)

[**4.2.8.** **System kontrolera zasobów dyskowych** 17](#_Toc70421467)

[4.2.9. **System macierzy dyskowych** 18](#_Toc70421468)

[**4.2.10.** **Agregator logów** 19](#_Toc70421469)

[**4.3.** **Propozycja konfiguracja brzegu internetowego** 20](#_Toc70421470)

[**4.3.1.** **Opis problemu** 20](#_Toc70421471)

[4.3.2. **Proponowane rozwiązanie** 21](#_Toc70421472)

[**5.** **Szczegółowa specyfikacja infrastruktury sprzętowo – programowej** 24](#_Toc70421473)

[**5.1.** **Platforma hiperkonwergentna** 24](#_Toc70421474)

[**5.2.** **System kontrolera zasobów dyskowych** 29](#_Toc70421475)

[**5.3.** **System macierzy dyskowych** 32](#_Toc70421476)

[**5.4.** **System backup** 34](#_Toc70421477)

[**5.5.** **Wymagania dla serwera systemu backupu** 46](#_Toc70421478)

[**5.6.** **Przełączniki SAN** 49](#_Toc70421479)

[**5.7.** **Przełączniki OOB** 51](#_Toc70421480)

[**5.8.** **Przełączniki rdzeniowe** 55](#_Toc70421481)

[**5.9.** **Routery BGP** 57](#_Toc70421482)

[**5.10.** **System bezpieczeństwa – firewall** 61](#_Toc70421483)

[**5.11.** **Agregator logów** 66](#_Toc70421484)

[**6.** **Dodatkowe wymagania oraz warunki dostawy sprzętu i oprogramowania** 69](#_Toc70421485)

[**7.** **Rozwiązania równoważne** 70](#_Toc70421486)

[**8.** **Scenariusze testów** 70](#_Toc70421487)

[**9.** **Dokumentacja powykonawcza** 75](#_Toc70421488)

[**9.1.** **Cechy dokumentacji dostarczonej w ramach projektu** 76](#_Toc70421489)

[**10.** **Szkolenie** 76](#_Toc70421490)

[**11.** **Wdrożenie** 78](#_Toc70421491)

[**12.** **Gwarancja** 80](#_Toc70421492)

# **Wprowadzenie**

Zamawiający oczekuje dostawy platformy do stworzenia prywatnej chmury o funkcjonalnościach wyszczególnionych poniżej określonej w z OPZ jako „System”, która będzie pełniła funkcję Zapasowego Repozytorium Cyfrowego dla NAC.

Ilekroć zamawiający opisując daną funkcjonalność wskazuje, że powinna być ona opcjonalna, należy to interpretować, że w danym postępowaniu rozwiązanie powinno posiadać daną funkcjonalność, lecz nie jest wymagane dostarczenie licencji na jej uruchomienie.

# **Słownik pojęć i skrótów**

**CRC** – Centralne Repozytorium Cyfrowe działające na potrzeby Archiwów Państwowych w strukturze Narodowego Archiwum Cyfrowego

**ZCR** – projektowane Zapasowe Repozytorium Cyfrowe na potrzeby Archiwów Państwowych w strukturze Narodowego Archiwum Cyfrowego z planowanym umiejscowieniem w Archiwum Narodowym w Krakowie

**NAC** – Narodowe Archiwum Cyfrowe

**ANK** – Archiwum Narodowe w Krakowie

**System kontrolera zasobów dyskowych** –pojęcie używane naprzemiennie z Kontroler zasobów dyskowych

# **Ogólne warunki przedmiotu zamówienia**

## **Przedmiot zamówienia**

Postępowanie przetargowe obejmuje swym zakresem:

1. Dostawę sprzętu i oprogramowania dla ZRC zgodnie z wymaganiami określonymi w punktach 4 - 11.
2. Wykonanie dokumentacji przedwdrożeniowej.
3. Opracowanie scenariuszy testów dla dostarczanego Systemu
4. Montaż i konfiguracja sprzętu oraz oprogramowania zgodnie z opracowaną i zaakceptowaną dokumentacją przedwdrożeniową.
5. Przeprowadzenie testów akceptacyjnych dostarczanego sprzętu i oprogramowania zgodnie zaakceptowanym przez Zamawiającego scenariuszem testów.
6. Opracowanie dokumentacji powykonawczej dostarczonego systemu.
7. Opracowanie procedur utrzymania dostarczonego systemu
8. Szkolenia.
9. Gwarancja na dostarczony sprzęt oraz oprogramowanie.
10. Wsparcie techniczne.

## **Miejsce realizacji przedmiotu zamówienia**

Miejscem realizacji przedmiotu zamówienia jest budynek Archiwum Narodowego w Krakowie zlokalizowany na ul. Rakowicka 22, Kraków.

Przed złożeniem oferty istnieje możliwość wykonania wizji lokalnej stanu obecnego serwerowni. Wniosek o wykonanie wizji lokalnej należy złożyć nie później niż 5 dni roboczych przed jej terminem. Wniosek powinien zostać wysłany w formie elektronicznej na adres e-mail: pzabczynski@ank.gov.pl. We wniosku muszą znajdować się informacje na temat czasu oraz osób biorących udział w wizji lokalnej po stronie Wykonawcy. Zamawiający potwierdzi zaproponowany przez Wykonawcę termin przeprowadzenia wizji lokalnej, lub wyznaczy inny termin, uwzględniający termin składania ofert

## **Etapy realizacji zamówienia**

Prace realizowane w zamówieniu, Wykonawca zobowiązany jest do wykonania wg następujących etapów:

Prace realizowane w zamówieniu, Wykonawca zobowiązany jest do wykonania wg następujących etapów:

| **LP** | **Nazwa etapu** | **Opis** | **Czas trwania** |
| --- | --- | --- | --- |
| 1 | Etap I - dostawa urządzeń objętych zamówieniem | Wykonawca dostarczy sprzęt objęty zamówieniem w terminie określonym w ofercie do wskazanych przez Zamawiającego lokalizacji.  Wykonawca po zakończeniu dostawy i wdrożenia sporządzi listę dostarczanego sprzętu, wg wzoru, który dostarczy Zamawiający. Wypełnioną listę sprzętu Wykonawca przekaże Zamawiającemu na koniec dostawy, również w formie elektronicznej.  Lista zawierać będzie minimum:   * numer seryjny urządzenia, * model dostarczonego sprzętu, * imię i nazwisko osób dokonujących odbioru, * adres i numer pomieszczenia dostarczanego sprzętu, * wartość sprzętu.   Zamawiający dopuszcza dostawy i odbiory częściowe.  Etap zakończy się odbiorem częściowym przez Zamawiającego – protokół odbioru ilościowego | Czas trwania etapu: do 45 dni od daty podpisania umowy. |
| 2 | Etap II - wykonanie dokumentacji przedwdrożeniowej | Dokumentacja przedwdrożeniowa powinna uwzględniać m. in.:   * Architekturę fizyczną oraz logiczną docelowego rozwiązania. * Harmonogram zawierający niezbędne, szczegółowo opisane działania dot. realizacji wdrożenia. * Konfigurację urządzeń w zakresie sprzętowym. * Opis integracji z elementami środowiska Zamawiającego wraz z szczegółami dot. konfiguracji tych elementów. Opis zmian w konfiguracji pozostałych urządzeń sieciowych tj. przełączniki, routery, będących w posiadaniu Zamawiającego. * Plan testów akceptacyjnych zawierający scenariusze oraz procedury składające się z co najmniej: * czasu trwania testów wraz z iteracjami, * informacje na temat obiektu testu.   W przypadku wymagania przez Wykonawcę kolejnych wizji lokalnych, Zamawiający umożliwi jej przeprowadzenie. Ze względu na aktualny stan epidemiologiczny wizja lokalna musi zostać potwierdzona przez Zamawiającego. Wykonawca jest zobowiązany do wystosowania prośby o wykonanie wizji lokalnej na nie wcześniej niż 5 dni roboczych przed jej terminem. Prośba powinna zostać wysłana w formie elektronicznej na adres e-mail: pzabczynski@ank.gov.pl We wniosku muszą znajdować się informacje na temat czasu oraz osób biorących udział w wizji lokalnej po stronie Wykonawcy.  Etap zakończy się odbiorem częściowym przez Zamawiającego – dokumentu przedwdrożeniowego. | Czas trwania etapu: 21 dni od momentu podpisania umowy. |
| 3 | Etap III - wdrożenie rozwiązania | Wdrożenie rozwiązania następować będzie wg poniższego schematu:   * Podłączenie fizyczne dostarczonych urządzeń. * Uruchomienie nowo podłączonych urządzeń. * Konfiguracja nowych podłączonych urządzeń. * Weryfikacja poprawności połączeń między poszczególnymi urządzeniami zgodnie z pkt 3.2. * Instalacja dostarczonego oprogramowania. * Uruchomienie zainstalowanego oprogramowania. * Konfiguracja dostarczonego oprogramowania. * Weryfikacja poprawności działania zainstalowanego oprogramowania. * Przygotowanie całego systemu do przeprowadzenia testów akceptacyjnych.   Etap zakończy się odbiorem częściowym przez Zamawiającego. | Czas trwania etapu: wg terminów zaproponowanych w ofercie, maksy­malnie do 70 dni od momentu podpisania bez uwag protokołu odbioru kończącego etapu II, z zastrzeżeniem pkt 6. |
| 4 | Etap IV - testy powdrożeniowe | Po zakończeniu etapu wdrożenia, Wykonawca wykona testy poprawności oraz bezpieczeństwa działania nowopowstałej infrastruktury na podstawie szczegółowego opisu testów zawartego w dokumentacji przedwdrożeniowej.  Zakres testów obejmować będzie minimum:   * Weryfikację możliwości połączeń między serwerami. * Weryfikację połączeń pomiędzy serwerami a stacjami roboczymi. * Weryfikację bezpieczeństwa połączenia – sprawdzenie braku dostępu możliwości połączeń z sieci, które nie powinny mieć dostępu – test bezpieczeństwa. * Test przypadków awarii urządzeń zlokalizowanych w serwerowniach (wyłączenie urządzenia lub urządzeń). * Test przypadków awarii pojedynczego połączenia pomiędzy urządzeniami * Test przypadku awarii dysku/dysków twardych * Test przypadków awarii połączeń pomiędzy lokalizacjami. * Test dostępu do i z sieci Internet i Intranet. * Test wykrywający pętlę w warstwie 2 modelu OSI/ISO oraz pętle w sieci pomiędzy VLANami. * Test automatyczny lub manualny przełączenia awaryjnego między lokalizacjamiTesty przypadków awarii zasilania wraz z testem automatycznego i poprawnego zamknięcia systemów serwerowych.   W przypadku, gdy testy nie zakończą się pozytywnym rezultatem, Wykonawca jest zobowiązany do usunięcia usterki oraz do ponownego przeprowadzenia testów zgodnie z zaproponowaną formułą iteracji przypadku.  Etap zakończy się odbiorem częściowym przez Zamawiającego. | Czas trwania etapu: 14 dni od momentu zakończenia etapu III, z zastrzeżeniem pkt 6. |
| 5 | Etap V - wykonanie dokumentacji powykonawczej | Dokumentacja powykonawcza dostarczona przez Wykonawcę musi zawierać co najmniej:   * Opisaną końcową konfigurację urządzeń oraz schemat połączeń wraz z oznaczeniem niestandardowych rozwiązań lub obejść . * Opis przeprowadzonych testów zawierających wyniki testów wraz z wnioskami . * Opis przeszkód napotkanych w trakcie implementacji oraz opis ich rozwiązania. * Skrypty, jeżeli zostały użyte, do automatyzacji zadań wraz z ich opisem. * Pełny wydruk połączeń.   Etap zakończy się odbiorem częściowym przez Zamawiającego. | Czas trwania etapu: 21 dni od momentu zakończenia etapu III, z zastrzeżeniem pkt 6. |
| 6 | Odbiór końcowy | Na podstawie odbiorów częściowych Zamawiający dokona odbioru końcowego przedmiotu Zamówienia po zakończeniu Etapu V. | Termin odbioru wynosi najpóźniej 5 miesięcy od dnia podpisania umowy. |

# **Główne założenia**

W rozdziale tym przedstawione zostały przedstawione założenia projektowe, opis stanu aktualnego oraz proponowana architektura projektowanego rozwiązania.

## **Opis stanu aktualnego**

Serwerownia Zapasowego Repozytorium Cyfrowego znajduje się w siedzibie Archiwum Narodowego w Krakowie przy ul. Rakowickiej. Pomieszczenia wyposażone są w odpowiednią infrastrukturę teletechniczną pod ZRC. Pomieszczenia dla ZRC zlokalizowane są na 4 piętrze. Powierzchnia serwerowni przeznaczonej dla ZRC to 118,20 m2.

Pomieszczenie wyposażone jest w następujące systemy:

* System Manager for DataCenter - zarządzanie listwami zasilającymi w szafach
* klimatyzacja precyzyjna
* system UPS,
* monitoring i kontrola dostępu,
* dwa przełączniki Nexus N9K-C93108TC-EX,
* czujniki detekcji zalania ,
* System PPOŻ,
* System BMS (oświetlenie, wentylacja)

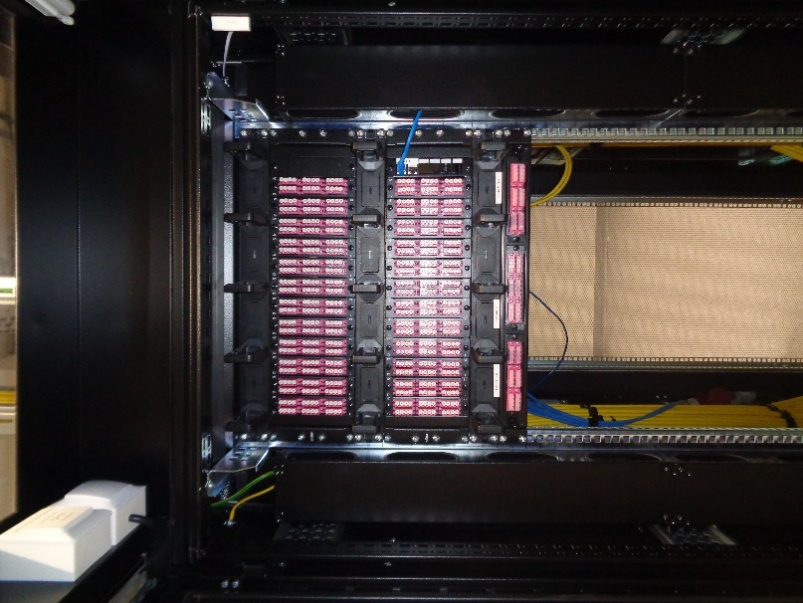
W pomieszczeniu znajduje się obudowa typu KIOSK wyposażona w 10 szaf serwerowych 42U o wymiarach 800x1200. Obudowa z jednej strony jest zamknięta stałą ścianą perforowaną, a z drugiej strony układem automatycznych szklanych drzwi przesuwnych. Drzwi otwierane są w sposób automatyczny za pomocą pilota. Dodatkowo dla celów bezpieczeństwa drzwi KIOSKu, w przypadku braku zasilania, otwierają się automatyczne. KIOSK wyposażony jest również w przycisk ewakuacyjny w celu otwarcia drzwi nawet po zaniku zasilania.

Rysunek 1 Ogólny widok KIOSKU z szafami RACK



W szafach serwerowych zainstalowany jest System Manager for DataCenter wraz z zarządzalnymi listwami zasilającymi umożliwiającymi monitorowanie zasilania oraz środowiska w szafach i KIOSKU.

Rysunek 2 Wyposażenie szaf RACK w KIOSKU - patchapnele światłowodowe

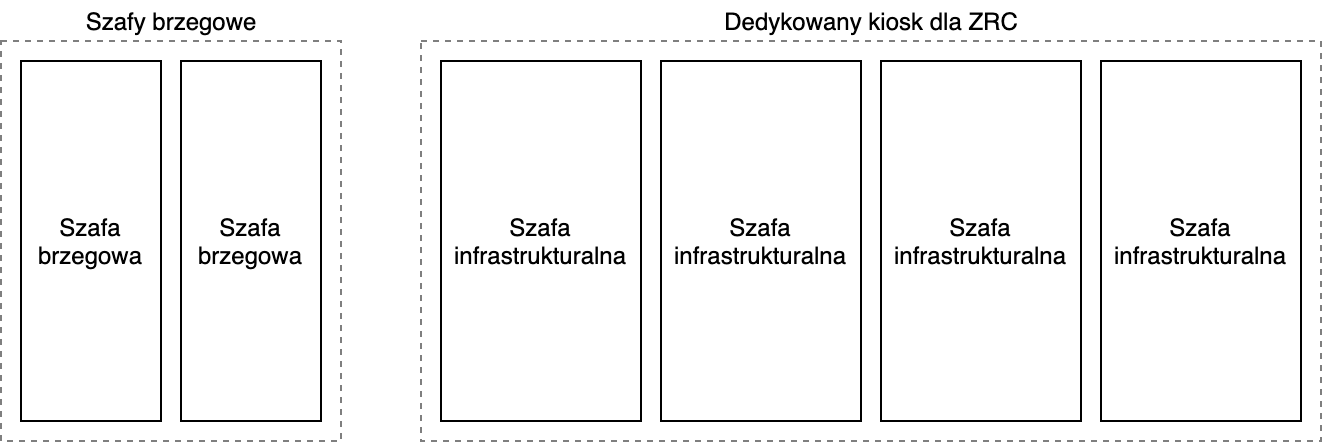


## **Proponowana architektura projektowanego rozwiązania**

### **Rozłożenie infrastruktury**

Dostarczane rozwiązanie musi być zainstalowane w 4 szafach RACK znajdujących się w KIOSKU. Szafy te połączone są z 2 szafami tzw. brzegowymi w których znajduje się przełącznik tranzytowy z sieciami zewnętrznymi i ANK. Zdecydowano się na taki podział infrastruktury, aby możliwe w jak największym stopniu rozgraniczyć zależności między infrastrukturą NAC a ANK. Poniżej przedstawiono ogólny schemat w/w koncepcji podziału fizycznego szaf.

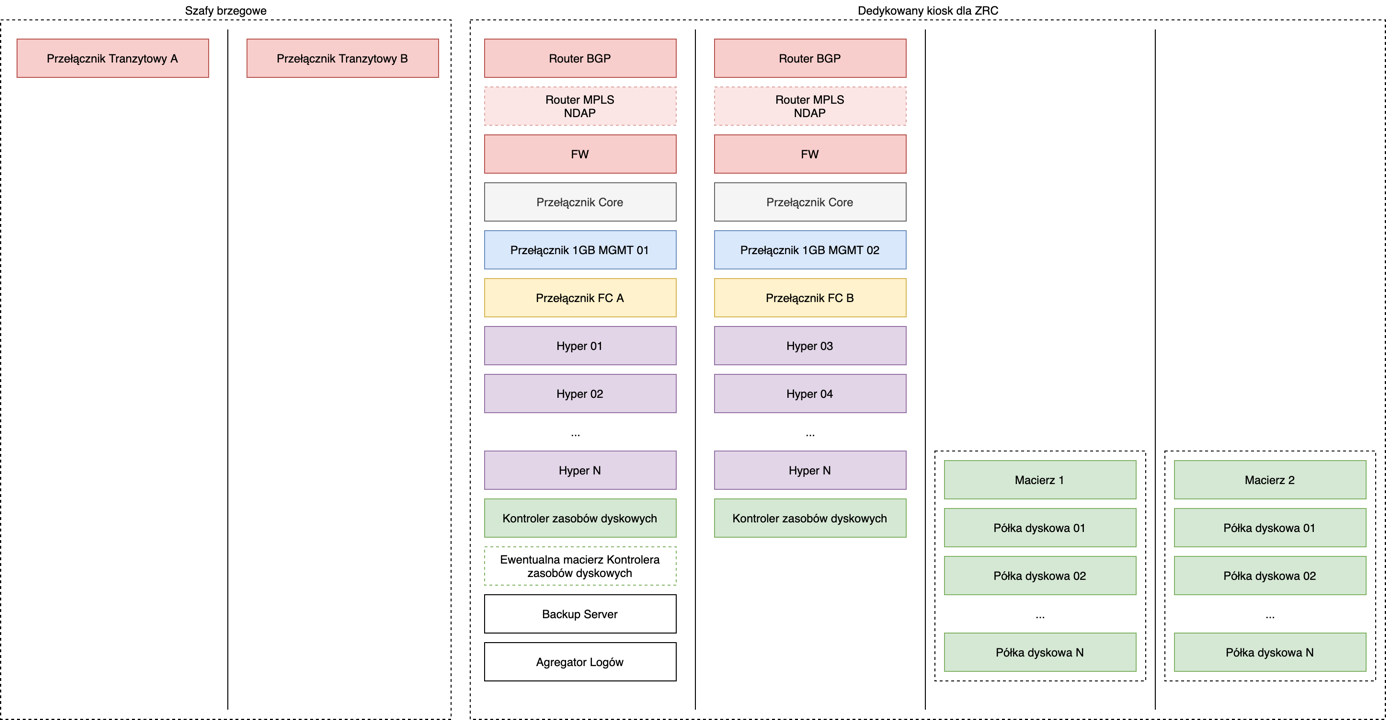
Rysunek 3 Koncepcja podziału szaf pod projekt ZRC



Każda z szaf wyposażona jest w dwie listwy BKT MPDU typ D18xIEC320C13+6xIEC320C19 wtyk IEC 60309 (32/400) o zabezpieczeniach 32A. Należy jednak założyć, ze względu na wyłącznik różnicowo-prądowy 30mA/10A na każdy obwód w szafie (są dwa per szafa), że do dyspozycji planowanej infrastruktury będzie 2 x 10A per szafa. W wypadku awarii jednego z UPS-ów do dyspozycji będzie 1x10A na szafę.

Wszystkie przewody zasilające dla urządzeń powinny zostać dostarczone w zgodzie ze standardem IEC-320-C14 (male) lub IEC-320-C20 (male). Wszystkie urządzenia muszą mieć dwa redundantne zasilacze. Planowane jest następujące rozłożenie urządzeń:

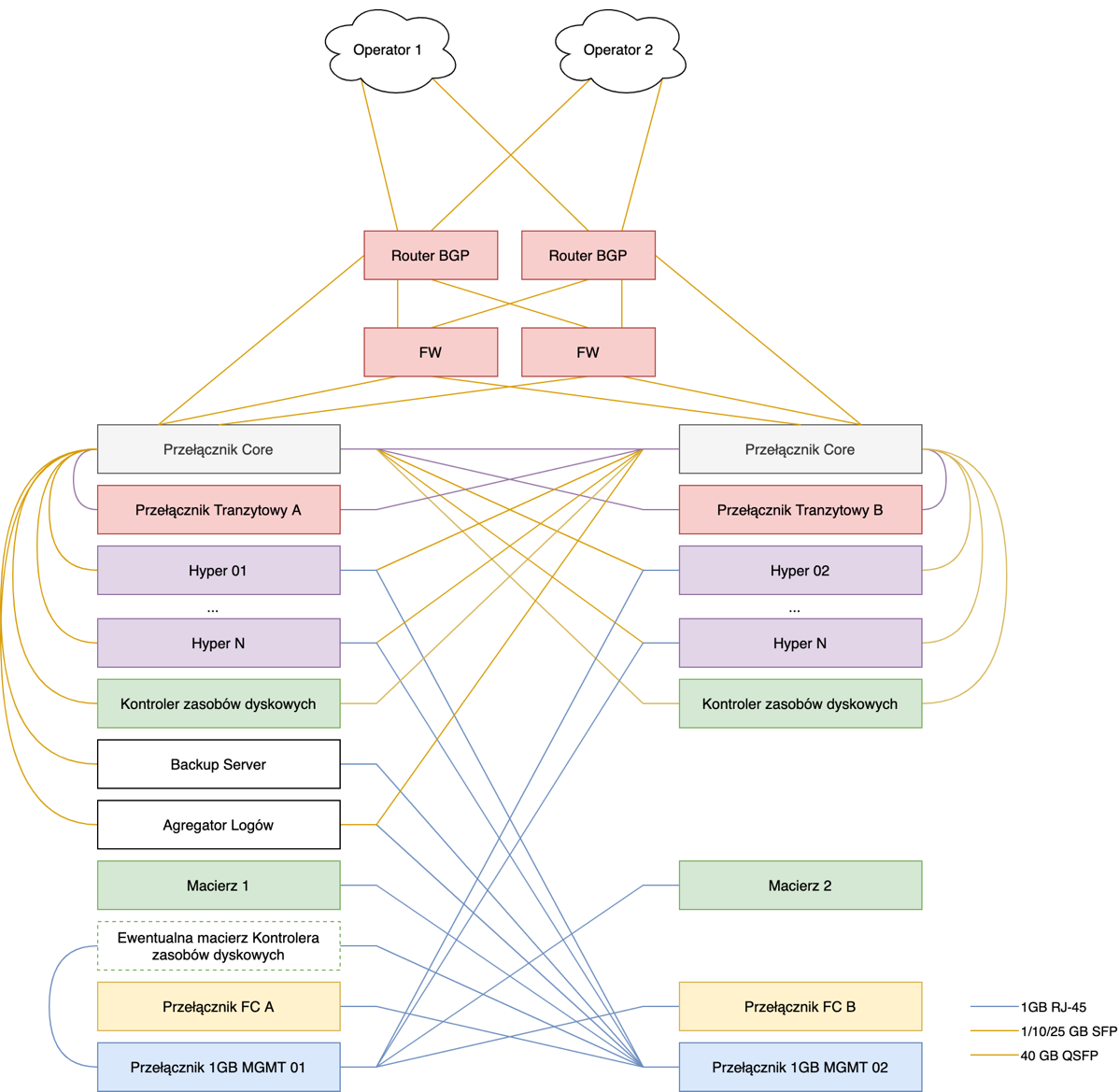
Rysunek 4 Koncepcja rozłożenia urządzeń w szafach ZRC



### **Przełączniki LAN (rdzeniowe i OOB)**

W każdej z szaf brzegowych znajduje się po jednym przełączniku Cisco Nexus N9K-C93108TC-EX (nazywane dalej tranzytowymi) wyposażony w 48 portów RJ-45 10GB oraz 6 portów 100GB QSFP28 każdy z nich wyposażony aktualnie jest w jedną wkładkę 40GB łączącą go z siecią ANK. W ramach postępowania należy dostarczyć min. 4 wkładki krótkiego zasięgu per przełącznik o przepustowości min. 40GB, aby dwie z tych wkładek połączyć z przyszłymi przełącznikami rdzeniowymi znajdującymi się w dwóch pierwszych z 4 szaf przeznaczonych pod projekt ZRC dla NAC, natomiast 2 pozostałymi połączyć je ze sobą. Przełączniki Rdzeniowe mają być tożsame konfiguracyjnie (tego samego producenta i w tej samej konfiguracji) i wyposażone w 100% w połączenia światłowodowe. Przełączniki rdzeniowe muszą posiadać min. 48 portów 1/10/25G(pracujące z trzema wymienionymi prędkościami), oraz min. 4 porty 40/100GB (pracujące z dwoma wymienionymi prędkościami) do połączenia z przełącznikami tranzytowymi każdy. Należy wyposażyć każdy z przełączników w min. 24 wkładki SFP 1/10/25GB (pracujące z trzema wymienionymi prędkościami). Wkładki muszą być zgodne i wyprodukowane przez producenta dostarczonych przełączników. Przełączniki te ze względu na skalę środowiska będą łączyć w sobie funkcję zarówno rdzenia jak i agregacji DC. Będą się do nich zbiegać wszelkie połączenia światłowodowe 1/10/25G z urządzeń aktywnych np. firewalle, serwery, macierze jak również i przełączniki OOB (Out of Band). Przełączniki OOB przewidziane są w ilości 2 szt. wyposażony w min. 24 porty RJ-45 1GB oraz min 2 porty SFP 10GB wyposażone w odpowiednie wkładki SFP aby wykonać połączenie do przełączników rdzeniowych (po jeden ścieżce do każdego z nich). Dzięki takiej konfiguracji infrastruktura przełączników będzie prezentować się następująco:

Rysunek 5 Schemat połączeń projektowanej infrastruktury ZRC



Do przedstawionej powyżej infrastruktury sieciowej podłączone zostaną urządzenia:

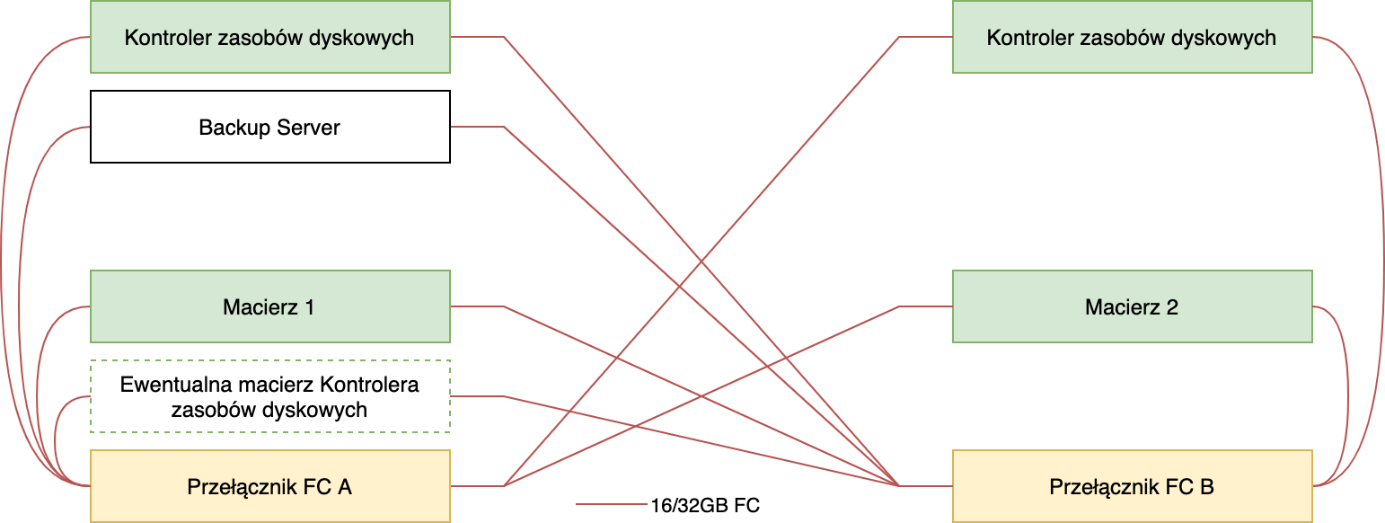
1. Przełączniki rdzeniowe
   1. Połączenie między sobą (2x40GB)
   2. Routery BGP
   3. Urządzenia Firewall
   4. Platforma hyperkonwergentna
   5. Serwer backup
   6. Kontroler zasobów dyskowych
   7. Agregator logów
   8. Przełączniki OOB
      1. Zarządzanie OOB serwerami
      2. Zarzadzanie OOB serwerem backup
      3. Zarządzanie OOB kontrolerów zasobów dyskowych
      4. Zarządzanie OOB macierzami
      5. Zarządzanie OOB przełącznikami FC
      6. Zarządzanie OOB firewall

Wszystkie połączenia do przełączników rdzeniowych należy wykonać redundantnie, jak również, gdzie to będzie możliwe połączenia interfejsów OOB. Wymagane jest, aby połączenia do przełączników rdzeniowych wykonane były poprzez interfejsy światłowodowe 10/25GB (pracujące z dwoma wymienionymi prędkościami) bez użycia jakichkolwiek konwerterów, przejściówek poza niezbędnymi wkładkami typu GBIC/Twinax. Połączenia do przełączników OOB mają być wykonane za pomocą kabli o kategorii min. 6a zakończonych złączem RJ-45.

### **Przełączniki SAN**

Zamawiający wymaga dostarczenia dwóch przełączników SAN. Mają one zostać umieszone w dwóch pierwszych szafach RACK – zgodnie z rysunkiem nr 4. Każdy z przełączników ma być wyposażony w min. 24 porty SFP Fibre Channel 32Gb obsadzone odpowiednimi wkładkami światłowodowymi (min 16 wkładek FC) i licencjami umożliwiającymi podłączanie wszystkich urządzeń FC przedstawionych w koncepcji. Porty Zarządzania/OOB mają być podpięte do przełączników OOB. Porty FC i wkładki w urządzeniach muszą być kompatybilne z prędkościami 32Gb jak również i 16 Gb. Planowaną infrastrukturę przedstawia poniższy schemat:

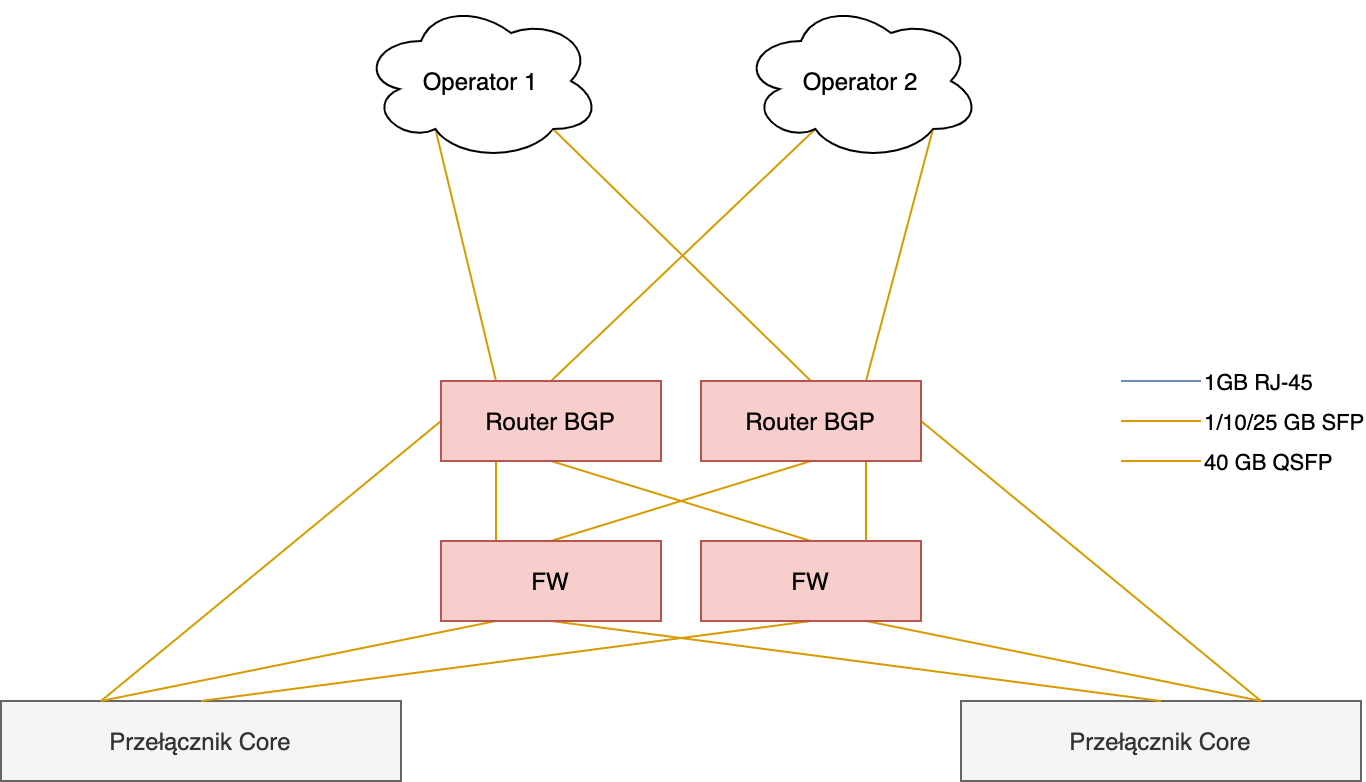
Rysunek 6 Schemat połączeń między urządzaniami ZRC



### **Routery BGP**

Brzeg sieci Zamawiającego będzie oparty o dwa routery BGP, które mają realizować wyłącznie obsługę protokołu BGP w infrastrukturze. Muszą być one wyposażone w min. 2 interfejsy 10GB SFP. Interfejsy te należy obsadzić wkładami światłowodowymi krótkiego zasięgu które pozwolą na podłączenie się do przełączników rdzeniowych (jedna ścieżka per jeden przełącznik). Urządzenie musi posiadać odpowiednie licencje o ile to wymagane pozwalające na obsługę ruchu od 5 do 10GBps. Przychodzący ruch operatorski będzie podłączany na portach SFP 1GB min. 6 szt. per urządzenie, należy je wyposażyć w min. 6 wkładek LRM (combo). Urządzenia mają działać w HA lub klastrze. Planowaną infrastrukturę przedstawia poniższy schemat:

Rysunek 7 Schemat połączeń projektowanych routrów BGP



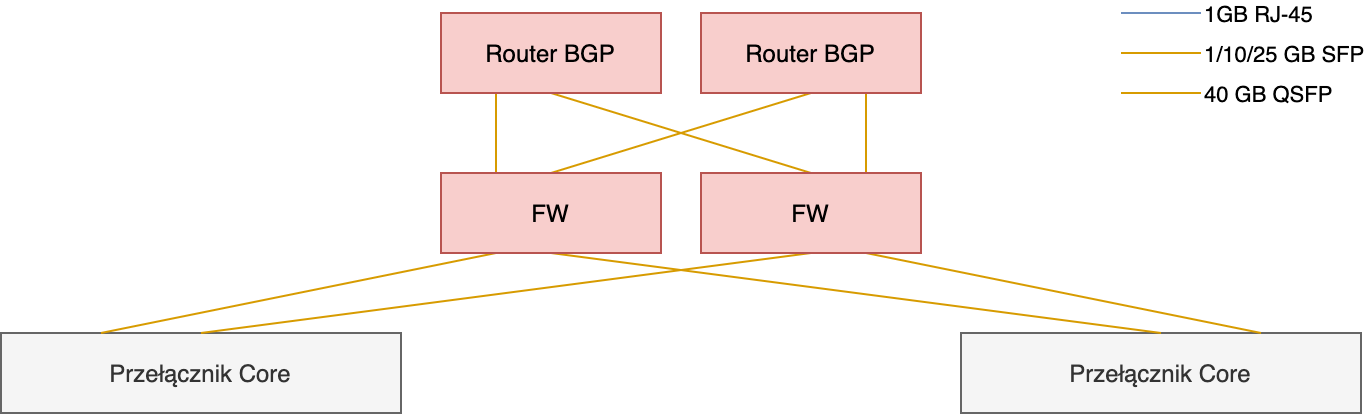
Planowane są następujące połączenia (per router):

1. 2 x 1GB SFP – Operator 1
2. 2 x 1GB SFP – Operator 2
3. 1 x 1GB SFP – Firewall A
4. 1 x 1GB SFP – Firewall B
5. 1 x 10GB SFP – Przełącznik rdzeniowy A
6. 1 x 10GB SFP – Przełącznik rdzeniowy B

### **System bezpieczeństwa – firewall**

Przewidywane są dwa urządzania typu Firewall działające w klastrze HA. Umieszczone zostaną w dwóch pierwszych szafach rack – zgodnie z rysunkiem nr 4. Urządzenia te mają być wyposażone w min. 4 porty 1GBps SFP wraz z odpowiednimi wkładkami, które umożliwią połączenie z routerami BGP (jedna ścieżka per router BGP). Dodatkowo urządzenia muszą być wyposażone w 2 porty 10GB SFP wraz z wkładkami umożliwiającymi połączenie z przełącznikami rdzeniowymi (jedna ścieżka per przełącznik rdzeniowy). Każde z urządzeń firewall musi posiadać funkcjonalność WAF (Web Application Firewall) pozwalającą na bezpieczne publikowanie stron internetowych do Internetu, oraz funkcję Load-Balancer dla min. 2 stron WWW (publikacja z użyciem protokołu HTTPS). Planowaną infrastrukturę przedstawia poniższy schemat:

Rysunek 8 Schemat połączeń projektowanych urządzeń firewall



Planowane są następujące połączenia (per firewall):

1. 1 x 1GB SFP – Router BGP A
2. 1 x 1GB SFP – Router BGP B
3. 1 x 10GB SFP – Przełącznik rdzeniowy A
4. 1 x 10GB SFP – Przełącznik rdzeniowy B

### **Platforma hiperkonwergentna**

Pod utrzymanie maszyn wirtualnych planowana jest infrastruktura hiperkonwergentna o następujących minimalnych wymaganiach użytkowych:

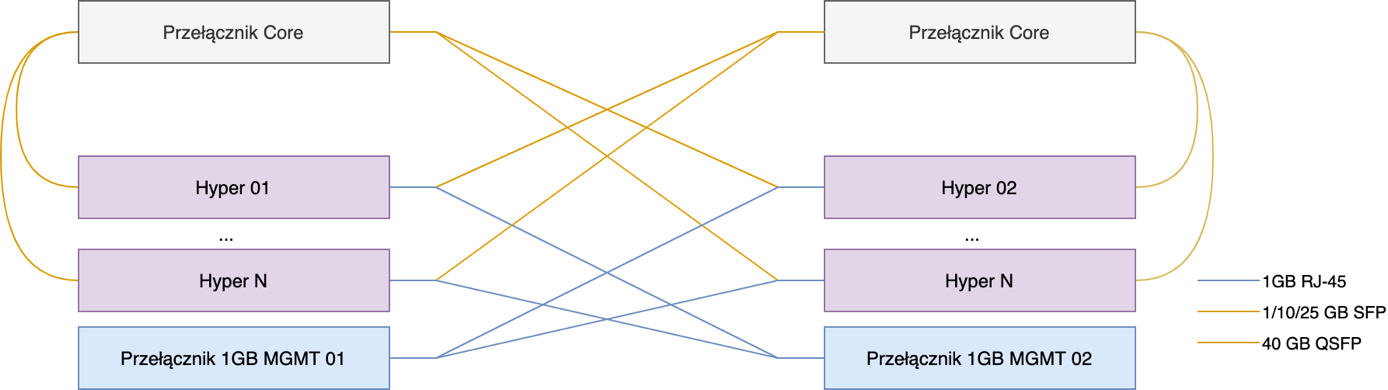
1. Ilość serwerów od 4 do 6 (włącznie) wielkości max 2U każdy
2. Sumarycznie min. 128 rdzeni procesorów, o częstotliwości min. 2,9GHz dostępnych w klastrze.
3. Przestrzeń wspólna dla środowisk realizowana za pomocą architektury „hiperkowergentnej” opartej o dyski SSD/NVMe o pojemności min. 140 TB
4. Każdy z serwerów musi posiadać min. 2 interfejsy 10/25GB SFP (pracujące z dwoma wymienionymi prędkościami) wraz z wkładkami niezbędnymi do podpięcia do przełączników rdzeniowych (po min. 2 ścieżki per przełącznik) per serwer,
5. Sumarycznie nie mniej niż 3000 GB RAM.

Serwery mają być możliwe równomiernie rozłożone między szafy RACK, a poziom ich nadmiarowości ma wynosić N+1. Celem ujednolicenia interpretacji Zamawiający postrzega rozwiązania hiperkonwergencji w podziale na 3 warstwy:

1. Oprogramowanie wirtualizacyjne
2. Oprogramowanie SDS (Software Defined Storage)
3. Platforma serwerowa

Zamawiający nie wyklucza rozwiązań opartych o różne podzespoły od różnych producentów w różnych warstwach, np. serwery jednego producenta, oprogramowanie innego. Nie dozwolone natomiast jest mieszanie producentów w pojedynczej warstwie, np. różne serwery różnych producentów jako platforma serwerowa, czy też różne hipervisory w warstwie oprogramowania wirtualizacyjnego, czy też różne technologie SDS. Rozwiązania zastosowane do stworzenia platformy hiperkonwergencji muszą być między sobą kompatybilne. Fakt ten ma być potwierdzony poprzez krzyżowe występowanie u wszystkich producentów wszystkich zastosowanych elementów na listach ich kompatybilności – np. platforma serwerowa ma się znajdować na oficjalnej liście kompatybilności oprogramowania wirtualizacyjnego i SDS, analogicznie oprogramowanie SDS na listach kompatybilności oprogramowania wirtualizacyjnego czy też producenta platformy serwerowej. Listy kompatybilności muszą być oficjalnie, publicznie dostępne. Dozwolone również jest dostarczenie platformy hiperkowergentej w całości jednego producenta. Planowaną infrastrukturę przedstawia poniższy schemat:

Rysunek 9 Schemat połączeń projektowanej platformy hiperkonwergentnej



Platforma hiperkonwergentna musi umożliwiać uruchomienie maszyn wirtualnych znajdujących się obecnie w NAC w momencie awarii ośrodka CRC. Ma ona zapewnić z jednej strony pojemność na 250 maszyn wirtualnych NAC jak również i mechanizm zapewniający tą funkcjonalność. Należy zapewnić możliwość przełączenia się do infrastruktury ZRC w czasie nie przekraczającym 4h. Dozwolone są metody replikacji asynchronicznej z aktualnej infrastruktury wirtualizacyjnej NAC – opartej o rozwiązanie VMware vSphere 6.7, lub odzyskiwanie z backupu po stornie CRC. W obu przypadkach przełączenie może być ręczne i ma się wydarzać na warstwie infrastruktury wirtualnej przy uwzględnieniu jednoczesnych zmian w konfiguracji sieci w obu ośrodkach. Rozwiązanie ma umożliwiać odwrócenie replikacji lub backup. Replikację, o której mowa można zrealizować dodatkowym oprogramowaniem, lub rozbudową posiadanej przez klienta licencji produktu CommVault o ile możliwe jest przy jego zastosowaniu wykonanie tego zadania.

### **System kopii zapasowej**

Zaplanowano w lokalizacji ZRC serwer backup i oprogramowanie do jego wykonywania i zarządzania. Serwer ma być wyposażony w min. 16 rdzeni fizycznych łącznie (w jednym lub dwóch procesorach) i rekomendowaną do działania oprogramowania ilość RAM nie mniej niż 128GB, powierzchnia wew. dysków serwera ma również być wystarczająca do działania oprogramowania, nie mniejsza niż użytkowe 8TB oparte o dyski SSD/NVMe. Serwer ma posiadać dwie 2 portowe kary FC 32GB wraz z odpowiednimi wkładkami umożliwiającymi podłączenie do przełączników FC (po 2 ścieżki per przełącznik FC). Serwer ma zostać wyposażony we wszelkie licencje (w tym na system operacyjny, jeśli wymagany) niezbędne do działania oprogramowania Backup. Serwer ma być wyposażony w min. 2 interfejsy 10/25GB SFP (pracujące z dwoma wymienionymi prędkościami) wraz z odpowiednimi wkładkami umożliwiającymi połączenie z przełącznikami rdzeniowymi (min. 1 ścieżka per przełącznik rdzeniowy).

Oprogramowanie Backup powinno być oparte o posiadane przez NAC oprogramowanie CommVault lub równoważne. Oprogramowanie należy dostarczyć w takiej ilości licencji, aby pokryć zapotrzebowanie wynikające z dostarczonej platformy hiperkonwergentnej. W przypadku dostawy oprogramowania innego niż CommVault ma być również zapewnione pokrycie licencyjne ośrodka CRC (10 CPU). Oprogramowanie nie może mieć limitu na ilość maszyn wirtualnych.

Zapotrzebowanie na przestań dyskową w serwerze kopii zapasowej zostało obliczone na podstawie już działającego systemu kopii zapasowej w CRC. W projekcie technicznym ZRC zostanie przedstawiona tabela przestawiająca harmonogramy kopii zapasowej wraz z średnim dziennym przyrostem danych.

|  |  |  |  |
| --- | --- | --- | --- |
| **Harmonogram kopii zapasowej** | | | |
| LP | Nazwa | Opis | Średni przyrost (w GB) |
| 1 | Dzienna przyrostowa | Codziennie wykonywana jest kopia przyrostowa zasobów wewnętrznych |  |
| 2 | Dzienna przyrostowa | Codziennie następuje powtórzenie kopii przyrostowej, na wypadek niezapisania jakichkolwiek danych. |  |
| 3 | Dzienna przyrostowa | Codziennie wykonywana jest kopia przyrostowa dla systemu ZOSIA, SWA |  |
| 4 | Tygodniowa | Co tydzień następuje wykonanie pełnej kopii (scalenie kopii przyrostowych) |  |

Można rozważyć także przeniesienie serwera kopii zapasowej do trzeciej lokalizacji.

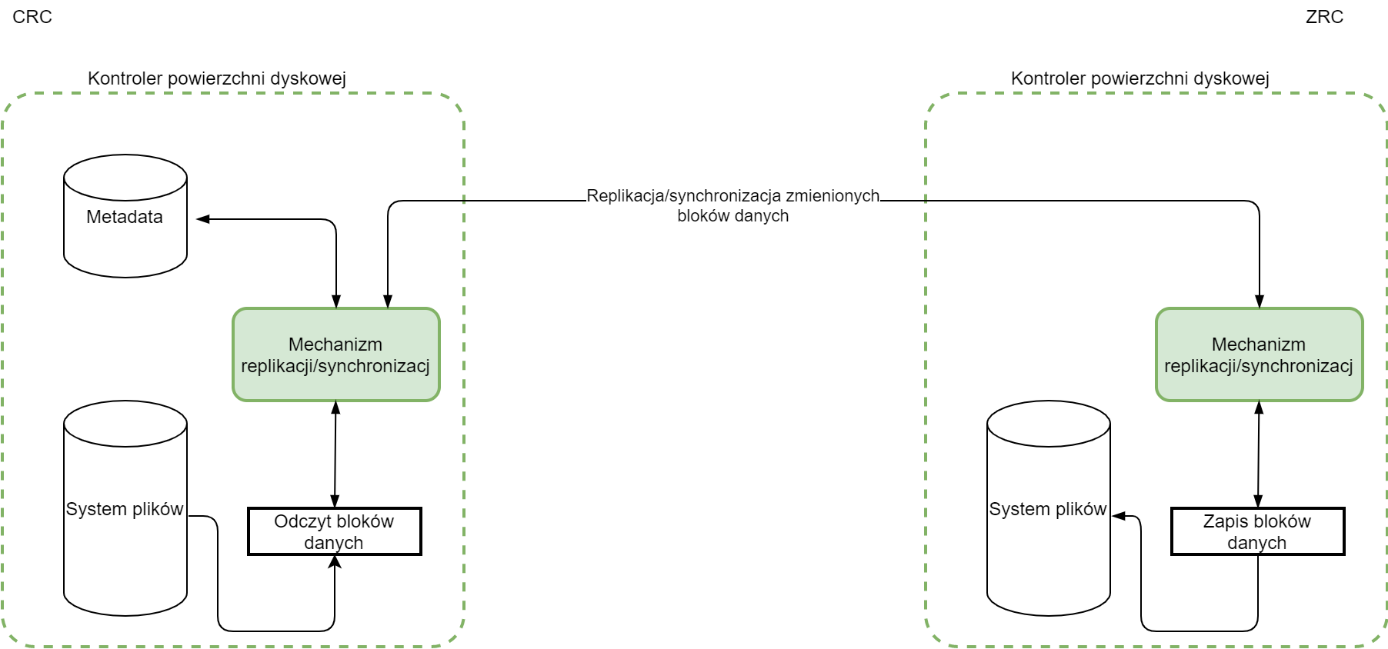
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kopie zapasowe** | | | | |
| LP | Nazwa | Miejsce składowania | Liczba kopii zapasowej | Lokalizacja |
| 1 | Maszyny wirtualne | Dyski lokalne serwera kopii zapasowej | 1 | CRC |
| 2 | Maszyny wirtualne | Taśmy | 2 | CRC/Lokalizacja zewnętrzna |
| 3 | Dane plikowe | Taśmy | 2 | CRC/Lokalizacja zewnętrzna |

### **System kontrolera zasobów dyskowych**

System kontrolera zasobów dyskowych ma zarządzać macierzą dyskową i udostępniać jej zasoby poprzez protokół NAS (NFS i CIFS) dla użytkowników jak również i serwerów w infrastrukturze. Wymagana sumaryczna wydajność urządzenia dla wskazanych protokołów ma wynosić 7GBps.

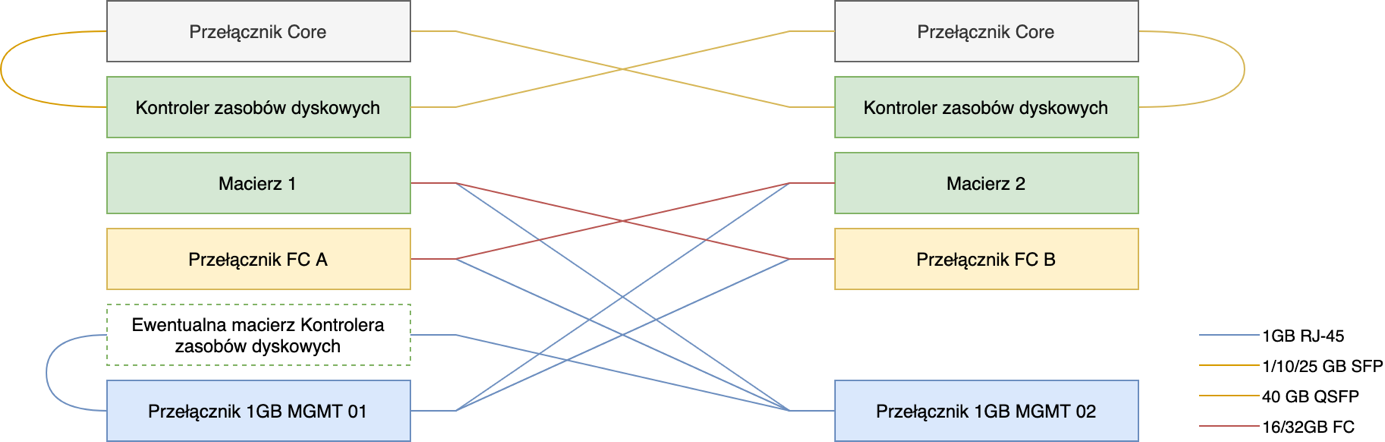
Rozwiązanie ma być zgodne z posiadanym przez Zamawiającego w podstawowym ośrodku przetwarzania danych Quantum Stronext M662XL. Ma zostać skonfigurowana replikacja zasobów dyskowych z ośrodka CRC do ZRC, replikacja ta musi się odbywać za pomocą natywnych mechanizmów zaproponowanego systemu kontrolera zasobów dyskowych. Mechanizm replikacji/synchronizacji musi przesyłać dane, tylko te które zostały zmienione. Synchronizacje/replikacje muszą się wykonywać w ramach przygotowanego harmonogramu lub być wykonywane na życzenie czyli uruchamiane ręcznie poza harmonogramem.

Rysunek 10 Proponowany schemat replikacji danych między CRC a ZRC



Rozwiązanie ma się składać z min. dwóch serwerów dostępowo-zarządczych, rozłożonych w dwóch szafach rack. Przedstawia to poniższy schemat:

Rysunek 11 Schemat połączenia projektowanych kontrolerów zasobów dyskowych

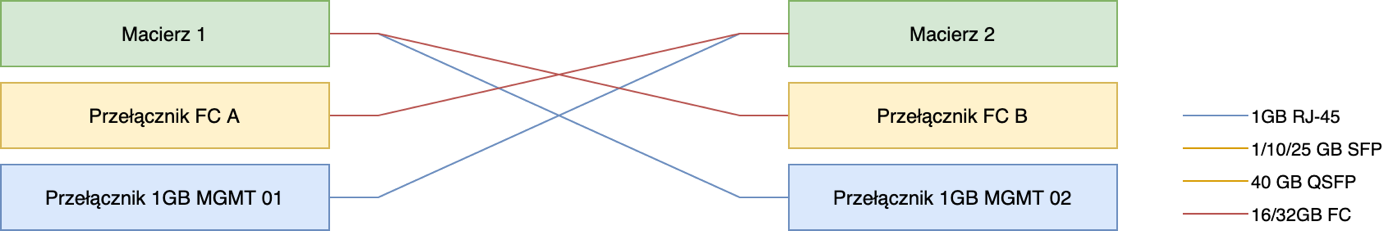


Serwery te mają być formą appliance dostarczaną przez producenta z zainstalowanym, skonfigurowanym i sklastrowanym oprogramowaniem systemu kontrolera zasobów dyskowych. Każdy z serwerów ma być wyposażony w min. 4 interfejsy Ethernet 10/25Gb (pracujące z dwoma wymienionymi prędkościami) wyposażone w wkładki światłowodowe oraz min. 2 interfejsy Fibre Channel 32Gb wyposażone w wkładki światłowodowe. Zamawiający dopuszcza dostarczenie macierzy dyskowej na metadane dla rozwiązania systemu kontrolera zasobów dyskowych, macierz taka ma zapewniać nadmiarowość komponentów np. min. 2 kontrolery, 4 porty FC per kontroler wyposażone w odpowiednie wkładki itd. Dostarczone rozwiązanie ma posiadać wszelkie licencje niezbędne do jego działania w tym nielimitowaną licencję na klientów NFS i CIFS, oraz pokrywać licencyjnie dostarczone macierze dyskowe. Kontrolery mają zostać wpięte w przełączniki rdzeniowe a w przypadku posiadania portów OOB również przełączniki OOB.

### **System macierzy dyskowych**

Zamawiający wymaga dostarczenia dwóch macierzy o sumarycznej pojemności użytkowej wynoszącej 4PB (2PB użytkowe per macierz). Powierzchnia dyskowa ma być dostarczona na dyskach NLSAS w zgodzie z najlepszymi praktykami producenta. Macierze mają zapewniać poziom zabezpieczenia danych równoznaczny lub lepszy niż poziom zapewniany przez RAID-6. Zamawiający zastrzega, że macierze będą umieszczone w dwóch oddzielnych szafach, a wszystkie komponenty macierzy mają być nadmiarowe i od siebie niezależne. Każda z macierzy ma posiadać przynajmniej dwa kontrolery wyposażone w porty FC o łącznej przepustowości min. 64Gb każdy, wyposażone w wkładki światłowodowe, mają one zostać podłączone do przełączników SAN w sposób zapewniający nadmiarowość, rekomendowany przez producenta dostarczonego rozwiązania. Interfejsy Ethernet Zarządzania/OOB mają zostać podłączone (o ile to możliwe) do przełączników OOB za pomocą połączeń miedzianych zakończonych złączem RJ-45. Przedstawia to poniższy schemat:

Rysunek 12 Schemat połączenia projektowanych macierzy

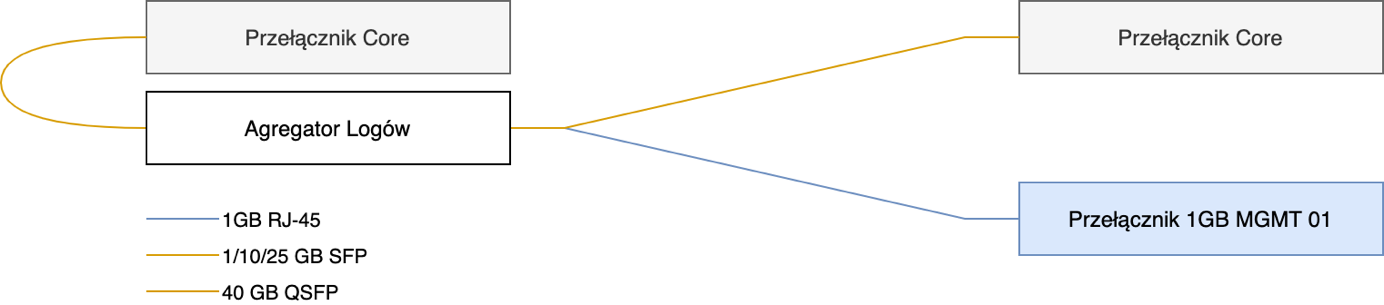


Dostarczone macierze mają być zgodne z proponowanym rozwiązaniem Systemem Kontrolera Zasobów Dyskowych i mają znajdować się na oficjalnych listach kompatybilności producentów.

### **Agregator logów**

Zamawiający wymaga dostarczenia urządzenia fizycznego do agregacji i przetwarzania logów. Ma być to appliance producenta zawierający zarówno sprzęt jak i oprogramowanie. Urządzenie to ma być wyposażone w min. 2 porty Ethernet SFP 1GB wyposażone w odpowiednie wkładki podłączone mają być do dwóch przełączników rdzeniowych – po min. jednym połączeniu. Dodatkowo urządzenia muszą posiadać min. 2 porty Ethernet RJ-45 1GB podłączone po jednym do przełączników OOB. Schemat połączenia prezentuje poniższy rysunek:

Rysunek 13 Schemat połączenia agregatora logów



Urządzenie ma zapewniać min. 8TB powierzchni użytkowej przy zastosowaniu RAID 1/10. Urządzenie ma umożliwiać przesłanie min. 150GB logów na dzień i obsługiwać min. 170 urządzeń. To urządzenie może posiadać min. jeden zasilacz.

## **Propozycja konfiguracja brzegu internetowego**

### **Opis problemu**

W proponowanym docelowym rozwiązaniu sieci NAC infrastruktura teleinformatyczną rozciągnięta jest pomiędzy trzy lokalizacje: podstawową z nich jest Warszawa (NAC WAW), oraz zapasowe w Bydgoszczy (NAC BYD) oraz Krakowie (NAC ZRC ANK).

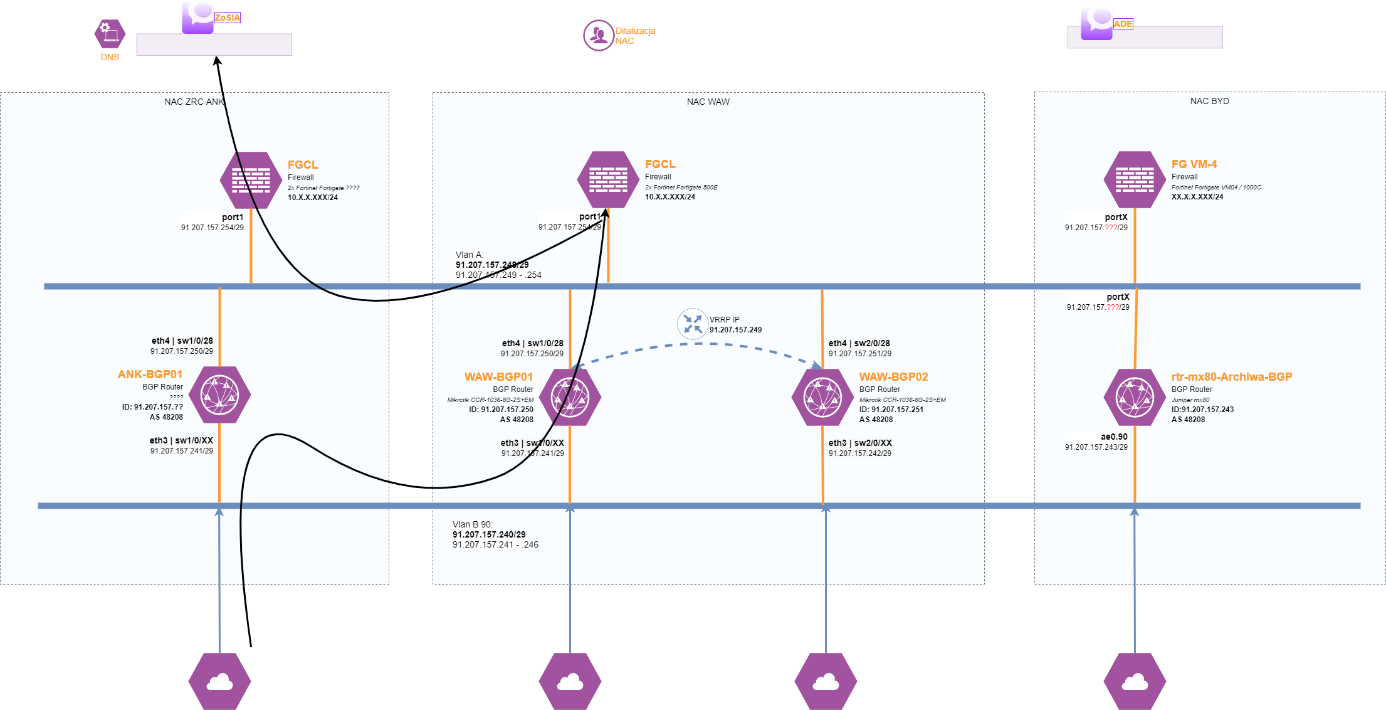
W podstawowym centrum przetwarzania danych na brzegu internetowym zainstalowana ma być para routerów obsługujących ruch za pomocą protokołu BGP. Do routerów tych podłączone zostałyby łącza internetowe. Celem zapewnienia redundancji dla ruchu inicjowanego z warszawskiego centrum przetwarzania danych pomiędzy routerami uruchomiony ma być protokół VRRP i ustawiony wirtualny adres używany jako gateway. Za wspomnianymi routerami umieszczony zostanie klaster firewalli Fortigate.

Zapasowych centrach danych zgodnie z projektem zainstalowane mają być jedynie pojedyncze Routery BGP oraz, tak jak w lokalizacji podstawowej, pojedyncze klastry firewalli.

Połączenia pomiędzy routerami BGP a firewallami w każdej lokalizacji mogą być zapewnione za pomocą kombinacji łączy warstwy drugiej i trzeciej realizowanych w technologii L2VPN, L3VPN lub transmisji danych.

W procesie analizy rozpatrywane było zachowanie się ruchu aplikacji ZoSIA oraz ADE, dla których podstawowym centrum przetwarzania danych będzie Warszawa, zaś zapasowym odpowiednio Kraków i Bydgoszcz. Działanie obu aplikacji opiera się na serwerach z nadaną adresacją prywatną. W przypadku przeniesienia aplikacji do zapasowego centrum danych, adresacja nie ulega zmianie.

W trakcie omawiania projektu zdefiniowany został problem polegające na tworzeniu się asymetrii ruchu w przypadku, gdy aplikacje nie są uruchomione w podstawowym centrum danych. Taka sytuacja może nastąpić zarówno w przypadku awarii, jaki celowego działania administracyjnego. Zamawiający zainteresowany jest możliwie najwyższym poziomem redundancji, przy jednoczesnym zachowaniu maksymalnej symetrii ruchu, i uniknięcie niepotrzebnego jego przesyłania pomiędzy lokalizacjami.



Rysunek 14 - Diagram przykładowego problemu

### **Proponowane rozwiązanie**

Przedstawione poniżej rozwiązanie pozwoli uniknąć asymetrii ruchu, i kontrolować w szczegółowy sposób zarówno trasę ruchu powrotnego dla połączeń inicjowanych z Internetu, jak i sterować ruchem wychodzącym z każdej z lokalizacji kierowanych do innych urządzeń w sieci internet. W przyjętym rozwiązaniu:

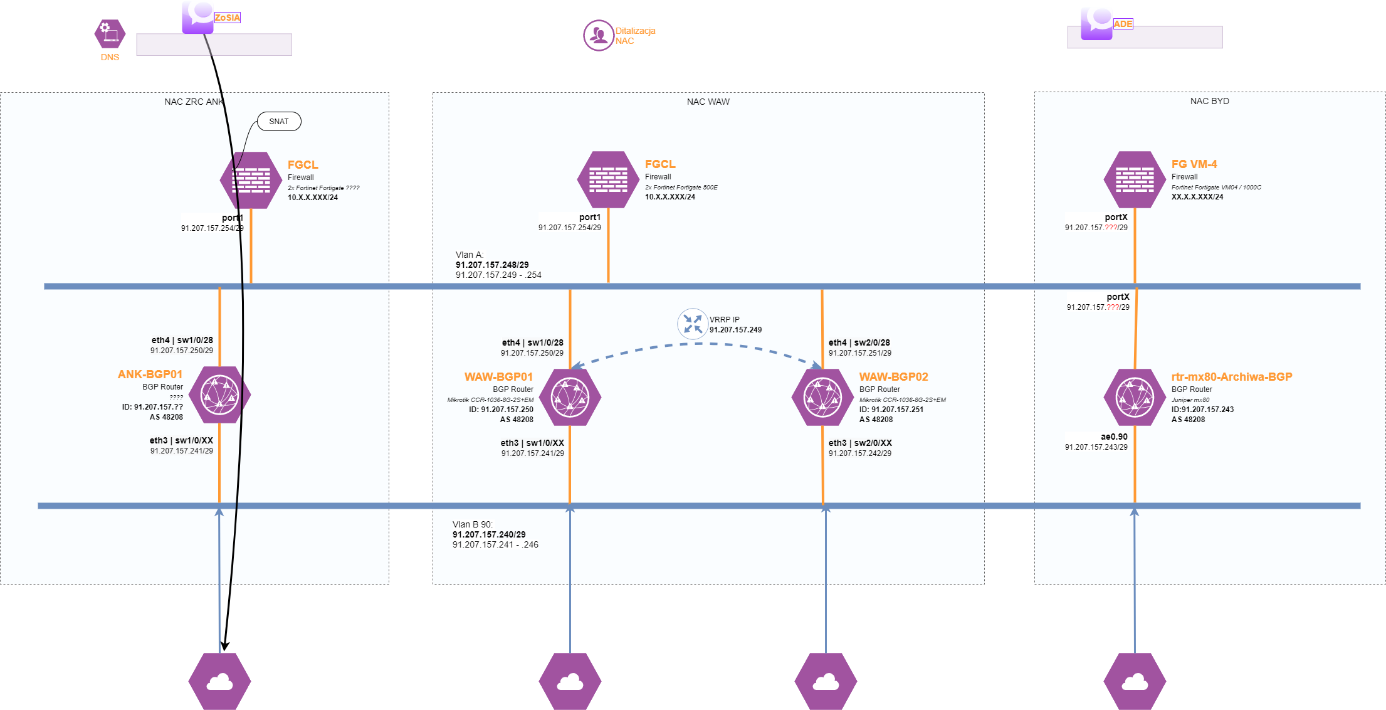
* Protokół BGP stanowi podstawę redundancji połączenia i wymiany informacji o prefiksach z siecią Internet
* Mechanizm SNAT/DNAT pozwala na sterowanie ruchem wchodzącym i wychodzącym, aby zachowana została symetria.
* Adresację serwerów aplikacyjnych nie ulega zmianie w przypadku przeniesienia ich do zapasowego centrum danych.

#### Połączenia sieciowe

W proponowanym rozwiązaniu warstwa transportowa nie gra większej roli, O ile możliwe jest dostarczenie pełnej siatki połączeń (full mesh) pomiędzy routerami i firewallami we wszystkich lokalizacjach. Połączenie to może być realizowane zarówno za pomocą pojedynczej usługi warstwy drugiej (przy czym nie jest to rekomendowane za względu na jedną dużą domenę rozgłoszeniową i potencjalnie wynikające z tego tytułu problemy sieciowe) jak i przez zestaw usług warstwy trzeciej za pośrednictwem dedykowanych połączeń Należy jednak pamiętać żeby w podstawowym centrum danych w Warszawie segment pomiędzy routera mi a klastrem firewalli był wspólny aby zapewnić redundancję dla ruchu wyjściowego inicjowanego wewnątrz data center.

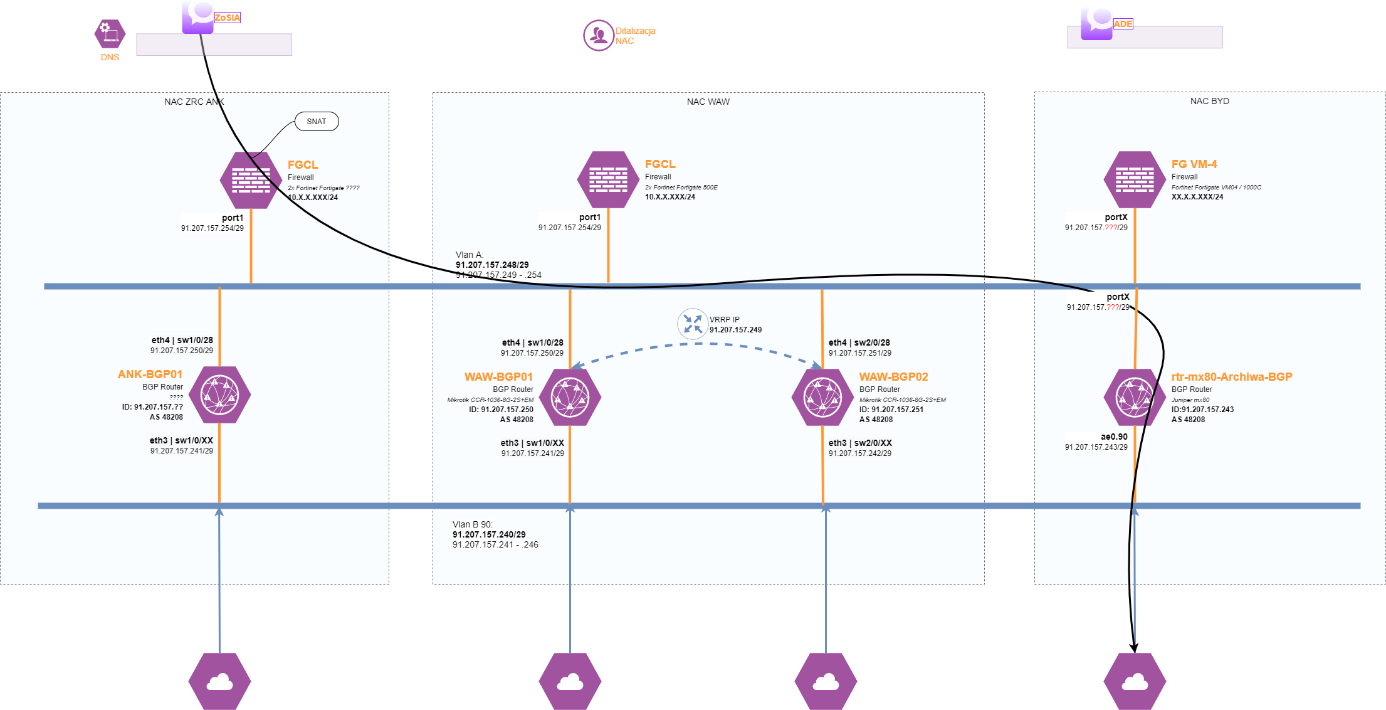
#### Ruch wychodzący

Dla ruchu wychodzącego inicjowanego w centrum przetwarzania danych, rolę bramy pełnić ma firewall zlokalizowany w danym centrum. Dokonywać on będzie odpowiedniej translacji adresów oraz przesyłać pakiety do routerów BGP które dalej prześlą je do Internetu. W przypadku awarii Łącza, bądź routerów brzegowych w danej lokalizacji, dzięki zapewnieniu pełnej sieci połączeń pomiędzy firewallami, a routerami BGP ruch zostanie przeniesiony na kolejny aktywny router. Zadanie to będzie realizowane za pomocą protokołu BGP lub protokołu z rodziny IGP, których zadaniem będzie przekazanie informacji o domyślnej bramie do firewalli.



Rysunek 15

W przypadku awarii łącza Internetowego w lokalizacji, firewall jest w stanie przesłać ruch do routera BGP w innej lokalizacji. Informacja o dostępnych bramach przesyłana powinna być za pomocą dynamicznego protokołu routingu. Nie zalecane jest stosowanie mechanizmów pozwalających na wiele jednocześnie aktywnych ścieżek (multipath). Zalecane jest aby za pomocą odpowiednich metryk urządzenie miało wprowadzone do tablicy routingu trasy zapasowe z odpowiednimi priorytetami, które będą wykorzystane w przypadku utraty informacji o podstawowej bramie.



Rysunek 16

#### Ruch przychodzący

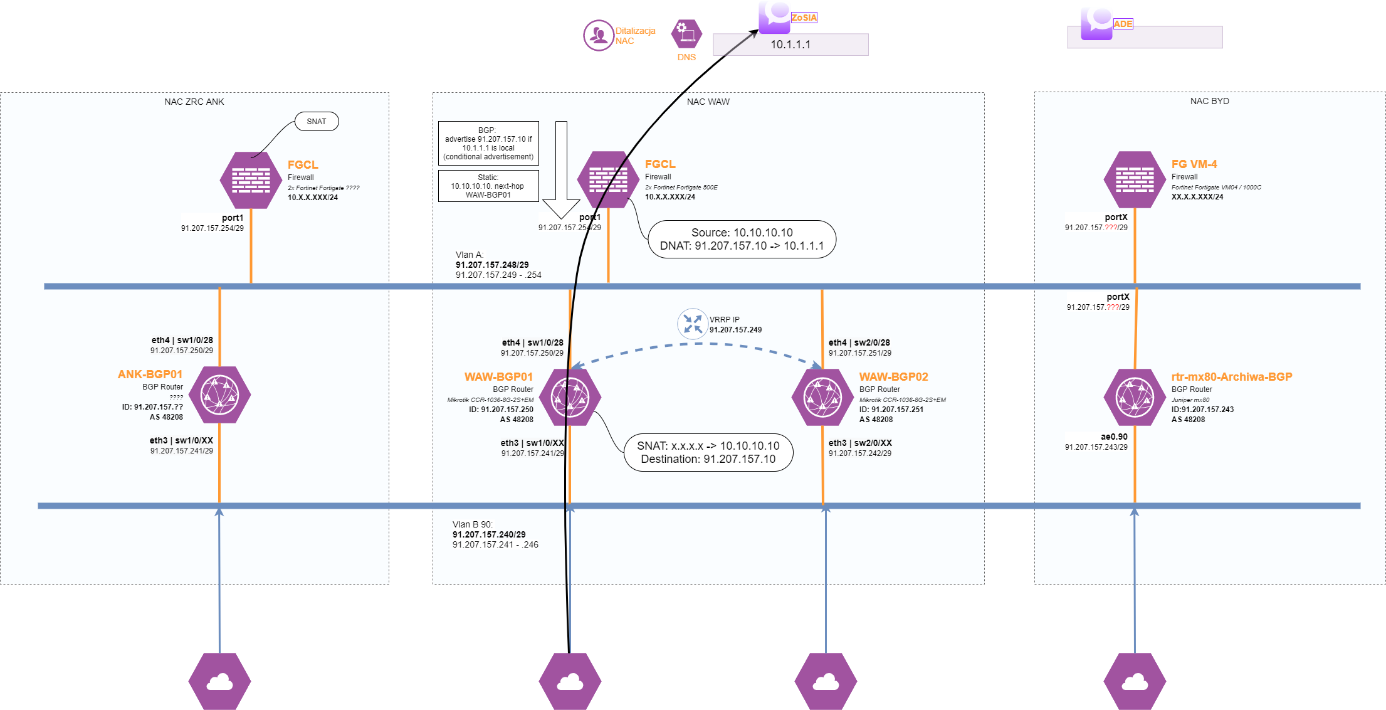
Problem z asymetrią ruchu w przypadku awarii inicjowanego z sieci Internet a skierowanego do serwerów aplikacyjnych, rozwiązany zostanie poprzez odpowiednie wdrożenie mechanizmu SNAT (Source NAT). Za odpowiednią translację adresów źródłowych odpowiedzialne będą routery BGP. Do każdego z nich powinien zostać przypisany jeden lub więcej unikalnych adresów, do których wykonana zostanie translacja SNAT połączeń przychodzących do wskazanego centrum przetwarzania danych. Adresy te muszą być unikalne dla każdego z urządzeń, czyli każdy z router ów BGP w podstawowym centrum przetwarzania danych musi mieć skonfigurowaną własną pulę adresów. Każdy z firewalli musi dysponować informacją o każdym z adresów wykorzystywanych do translacji SNAT. Rozwiązanie takie spowoduje, że ruch powrotny z serwerów aplikacyjnych zostanie zawsze skierowany z powrotem do tego samego routera BGP, przez który został on odebrany. Protokół BGP w miarę możliwości powinien zostać skonfigurowany w taki sposób, aby ruch skierowany do publicznych adresów usługi trafiał do routerów w lokalizacji, gdzie aplikacja jest w danym momencie aktywna. Jednocześnie należy pamiętać, że najmniejsza akceptowana w Internecie pocieszyć ma rozmiar /24.

Translacja adresów docelowych (publicznych adresów usług) pozostaje bez zmian i będzie realizowana na firewallach za pomocą mechanizmu DNAT (Destination NAT)

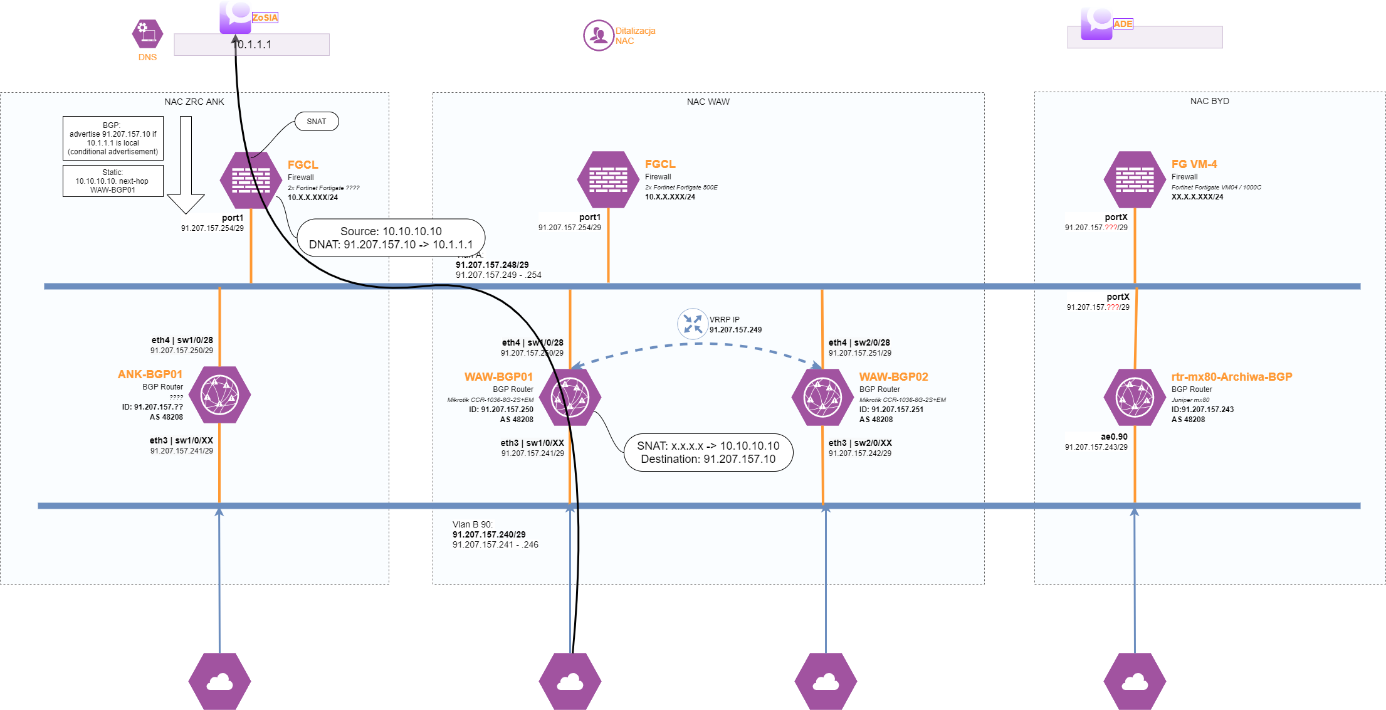
W przyjętej koncepcji podstawą do zapewnienia niezawodności opisanych mechanizmu jest zapewnienie odpowiedniej siatki połączeń pomiędzy routerami BGP oraz klastrami firewalli, oraz odpowiednia dystrybucja informacji o prefiksach pomiędzy tymi urządzeniami. Firewalle muszą mieć informację o adresach SNAT przypisanych do poszczególnych firewalli. Informacja ta może być rozgłaszana za pomocą dynamicznego protokołu routingu (BGP lub protokół z rodziny IGP) lub skonfigurowana na firewallach statycznie.

Inaczej rzecz wygląda z rozgłaszaniem pomiędzy firewallami i routerami BGP informacji o publicznych adresach IP usług. Informacja ta musi być ściśle powiązana z centrum przetwarzania danych, które jest aktywne dla wskazanej usługi. Konieczne jest zatem wdrożenie mechanizmów z rodziny BGP Conditional Advertisement dostępnych na platformie Fortinet i powiązanie rozgłaszania adresu publicznego usługi z mechanizmami z rodziny IP SLA lub podobnymi, które będą badały dostępność usługi w każdym z centrów danych.

Poniższy diagram pokazuje sytuację, gdy aplikacja znajduje się w podstawowym centrum przetwarzania danych w Warszawie, a routing BGP w sieci Internet wskazuje ścieżkę do routerów w Warszawie jako preferowaną.



W przypadku gdy aplikacja zostaje przeniesiona z Warszawy do Krakowa firewall w Warszawie zaprzestaje rozgłaszania adresu przypisanego do danej aplikacji, zaś informację o adresie publicznym rozgłaszać rozpoczyna firewall z Krakowie.



W przypadku segmentu sieci pomiędzy routerami BGP a firewallami operować można pojedynczymi adresami IP z maską /32 aby zapewnić granularność routingu do poszczególnych adresów. Sumaryzacja musi być skonfigurowana na routerach BGP aby do Internetu rozgłaszać jedynie klasy /24 lub większe.

# **Szczegółowa specyfikacja infrastruktury sprzętowo – programowej**

W ramach zamówienia należy dostarczyć:

|  |  |  |
| --- | --- | --- |
| LP | Nazwa | Ilość |
| 1 | Platforma hiperkonwergentna – min 4 serwery | 1 |
| 2 | System kontrolera zasobów dyskowych | 1 |
| 3 | System macierzy dyskowych – min 2 macierze | 1 |
| 4 | System backup wraz z dedykowanym serwerem | 1 |
| 5 | Przełączniki SAN | 2 |
| 6 | Przełączniki OOB | 2 |
| 7 | Przełączniki rdzeniowe | 2 |
| 8 | Routery BGP | 2 |
| 9 | System bezpieczeństwa - firewall | 2 |
| 10 | Agregator logów | 1 |

## **Platforma hiperkonwergentna**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Platforma musi zostać dostarczona w modelu hiperkonwergentnym tzn. z wykorzystaniem serwerów z procesorami Intel lub AMD, posiadającymi dyski wewnętrzne, które tworzą warstwę storage.

Zamawiający wymaga dostarczenia kompletnego klastra obliczeniowego, wraz z pełnym okablowaniem.

Ilekroć Zamawiający opisując daną funkcjonalność wskazuje, że powinna być ona opcjonalna, należy to interpretować, że w danym postępowaniu rozwiązanie powinno posiadać daną funkcjonalność, lecz nie jest wymagane dostarczenie licencji na jej uruchomienie.

Oferowana platforma hiperkonwergentna musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

| **LP** | **Wymagania** | |
| --- | --- | --- |
| 1 | System | 1. Rozwiązanie (sprzęt serwerowy, wirtualizator, pamięć masowa zdefiniowana programowo, ochrona i zabezpieczenie danych, zintegrowane zarządzanie) musi być dostarczone, zaprojektowane, zintegrowane oraz wspierane przez jednego dostawcę. 2. Wszystkie komponenty rozwiązania (sprzęt serwerowy , wirtualizator, pamięć masowa zdefiniowana programowo, ochrona i zabezpieczenie danych) muszą być zarządzane z jednego miejsca, za pomocą wbudowanego i zintegrowanego narzędzia. 3. Rozwiązanie musi być certyfikowane na serwerach co najmniej 3 globalnych producentów serwerów. 4. Rozwiązanie musi być niezależne od sprzętu (nie może być ograniczone do określonego dostawcy sprzętu ). Wymagana jest możliwość przenoszenia licencji lub subskrypcji pomiędzy wszystkimi wspieranymi platformami. 5. Platforma sprzętowa w zaproponowanej konfiguracji musi być certyfikowana przez producenta Systemu i znajdować się na publicznie dostępnej liście kompatybilności. 6. Możliwość wykonywania i monitorowania aktualizacji wszystkich komponentów rozwiązania za pomocą pojedynczego narzędzia zarządzania. Narzędzie musi wykonywać automatyczną weryfikację kompatybilności wersji oprogramowania. 7. Rozwiązanie musi być samo naprawialne. Oznacza to, że musi utrzymywać określony poziom odporności na awarie oraz stałą wydajność w przypadku awarii, bez konieczności interwencji administratora. Musi także przywrócić odporność tak szybko jak tylko możliwe. Np w przypadku awarii dysku twardego system musi natychmiast rozpocząć odbudowę utraconych danych nawet bez konieczności wymiany dysku twardego 8. Rozwiązanie musi być niezależne od sieci, nie może wymagać określonego sprzętu sieciowego. 9. Rozwiązanie jako opcje musi zapewniać wbudowaną funkcję udostępniania usług pamięci masowej dla maszyn wirtualnych, kontenerów oraz zewnętrznych serwerów fizycznych jako:  * blokowe zasoby iSCSI * plikowe zasoby – poprzez protokoły NFS i SMB * zasoby obiektowe – kompatybilne z Amazon S3  1. Rozwiązanie musi zapewniać możliwość udostępniania pamięci masowej jako LUN-y iSCSI do maszyn wirtualnych uruchomionych na zasobach rozwiązania. 2. Rozwiązanie jako opcja musi zapewniać możliwość udostępniania pamięci masowej jako LUN-y iSCSI, do zewnętrznych serwerów fizycznych bez wirtualizacji. 3. Rozwiązanie musi umożliwiać uruchamianie klastrów Kubernetes za pomocą kreatora (tzw. wizard), spełniając następujące kryteria:  * musi umożliwiać udostępnienie usług pamięci masowej dla klastra Kubernetes * pamięć masowa musi obsługiwać plugin CSI (Container Storage Interface) * musi zapewnić możliwość uruchomienia nieograniczonej liczby podów Kubernetes * musi zapewnić wbudowane zarządzanie i orkiestrację kontenerów * rozwiązanie musi być kompatybilne z Google Kubernetes framework  1. Rozwiązanie musi wspierać różne warstwy pamięci masowej:  * SSD i NVMe jako warstwa wydajnościowa * NL-SAS/SATA/SSD jako warstwa pojemnościowa  1. Rozwiązanie musi zapewniać zautomatyzowane, działające w czasie rzeczywistym, wielowarstwowe składowanie danych (ang. tiering) pomiędzy nośnikami SSD/NVMe (warstwa buforująca i wydajnościowa) oraz HDD/SSD (warstwa pojemnościowa), w celu zapewnienia optymalnej wydajności. 2. Jeśli wielowarstwowe składowanie (ang. tiering) nie jest dostępne, wówczas rozwiązanie musi być w całości zbudowane w oparciu o, odpowiednio, NVMe lub SSD, a także musi zostać dostarczona gwarancja ceny nośnika SSD/NVMe w całym okresie trwania kontraktu. 3. W przypadku rozwiązania opartego o technologię cache’owania danych, wymagany współczynnik warstwy wydajnościowej do warstwy pojemnościowej to minimum 30%. 4. Jeśli system plików w wyniku założeń projektowych architektury lub jako najlepsza praktyka danego producenta nie powinien być całkowicie zapełniany przez dane użytkownika, wówczas niezbędna wolna przestrzeń (ang. slack space) powinna zostać uwzględniona dodatkowo i doliczona do pojemności surowej węzła. 5. Wszystkie węzły muszą być hiperkonwergentne, a lokalne (wewnętrzne) dyski wszystkich węzłów muszą stanowić klaster prezentowany jako pojedyncza i rozproszona pula zasobów dostępna dla wszystkich węzłów kontrolowanych przez wirtualizator. Węzły obliczeniowe nie są akceptowane. 6. Rozwiązanie musi zapewniać rozbudowę wyłącznie pamięci masowej, bez dodatkowej rozbudowy CPU i RAM, a także bez dodatkowych kosztów związanych z licencjami wirtualizatora. Np. poprzez dołożenie dodatkowych dysków do wolnych slotów w serwerze albo poprzez bezprzerwową wymianę dysków twardych w serwerach na większą pojemność 7. Rozwiązanie musi zapewniać usługę kompresji danych, w trybie inline oraz w post-processie . Wymaganie dotyczy oferowanej konfiguracji All-Flash. Jeżeli wymagane są dodatkowe licencje należy je dostarczyć 8. Poniższe usługi i parametry pamięci masowej muszą być konfigurowalne osobno dla każdej maszyny wirtualnej lub kontener/datastore wystawiamy do systemu wirtualizacji:  * Kompresja * Deduplikacja online lub post-process * Erasure Coding (zabezpieczenie z pojedynczą lub podwójną parzystością pomiędzy węzłąmi) * Resilience Factor (współczynnik odporności na awarie): N+1 lub N+2  1. Rozwiązanie musi zapewniać funkcję tworzenia kopii migawkowych oraz klonów maszyn wirtualnych, także z zapewnieniem spójności z punktu widzenia aplikacji (co najmniej dla systemów operacyjnych Windows oraz Linux). Funkcja ta musi być wbudowana w platformę i realizowana na poziomie pamięci masowej. 2. Rozwiązanie musi wspierać architekturę All-NVME |
| 2 | Bezpieczeństwo | 1. System opcjonalnie musi posiadać mechanizmy szyfrowania danych 2. Opcjonalnie szyfrowanie musi odbywać się na poziomie datastore. 3. Opcjonalnie system musi posiadać wbudowany serwer KMS (Key Management Server) 4. System musi wspierać dwuskładnikowe uwierzytelnienie do Systemu 5. System musi posiadać tzw. STIG, regularnie aktualizowane i udostępniane przez producenta 6. System musi posiadać mechanizm automatycznego wykrywania odchyleń od STIG i automatycznie je naprawiać, zarówno w warstwie wirtualizacji jak i storage |
| 3 | Odporność na awarię, wysoka dostępność, backup, Disaster Recovery | 1. System musi być odporny na jednoczesną awarię co najmniej pojedynczego, dowolnych komponentów Systemu, nie powodując przerwy w pracy Systemu. 2. Opcjonalnie System musi umożliwiać replikację maszyn wirtualnych między ośrodkami z RPO = 5 minut 3. Opcjonalnie System musi umożliwiać replikację maszyn wirtualnych między ośrodkami w scenariuszu wiele do wielu dla co najmniej trzech ośrodków. 4. System musi umożliwiać konfigurację polityki replikacji per maszyna wirtualna 5. Opcjonalnie System musi posiadać narzędzie do Disaster Recovery:  * Z możliwością określenia kolejności w jakiej maszyny mają zostać uruchomione w drugim ośrodku * Z mapowaniem adresacji IP per maszyna wirtualna, pomiędzy ośrodkami * Z funkcją testowania scenariuszy DR, tzw. failover oraz failback.  1. System musi wspierać odtwarzanie pojedynczych plików ze Snapshotów 2. Opcjonalnie System musi umożliwiać replikację z RPO = 5 minut oraz scenariusze Disaster Recover dla różnych hypervisorów w dwóch ośrodkach |
| 4 | Usługi plikowe | 1. System musi posiadać wbudowane, rozproszone usługi plikowe. 2. System musi zapewniać usługi plikowe poprzez protokół NFS v3/v4 oraz SMB. 3. System musi umożliwiać jednoczesny dostęp do plików za pomocą NFS oraz SMB. 4. System musi umożliwiać rozbudowę usług plikowych w modelu scale-out, poprzez dokładanie kolejnych węzłów. Dodatkowe węzły muszą zwiększać zarówno pojemność usług plikowych jak i ich wydajność. 5. Opcjonalnie System musi posiadać możliwość replikacji zasobów plikowych pomiędzy klastrami z RPO = 5 minut. 6. System usług plikowych musi integrować się z Active Directory oraz rozwiązaniami Antywirus za pomocą protokołu ICAP 7. System usług plikowych musi wspierać CFT (Change File Tracking) 8. System musi obsługiwać szyfrowanie danych dla zasobów plikowych (tzw. data at rest encryption) |
| 5 | Usługi obiektowe | 1. System musi posiadać wbudowane, rozproszone usługi obiektowe. 2. System musi zapewniać usługi obiektowe poprzez protokół S3 3. System musi umożliwiać rozbudowę usług obiektowych w modelu scale-out, poprzez dokładanie kolejnych węzłów. Dodatkowe węzły muszą zwiększać zarówno pojemność usług plikowych jak i ich wydajność. 4. Opcjonalnie System musi posiadać możliwość replikacji zasobów plikowych pomiędzy klastrami z RPO = 1 minuta. 5. System usług obiektowych musi integrować się z Active Directory 6. System usług obiektowych musi zapewniać WORM (Write Once Read Many) oraz wersjonowanie obiektów. 7. System musi obsługiwać szyfrowanie danych dla zasobów plikowych (tzw. data at rest encryption) 8. System musi obsługiwać REST API |
| 6 | Zarządzanie | 1. Zarządzanie Systemem musi odbywać się z pojedynczej konsoli 2. Konsola do zarządzania klastrem musi być skonfigurowana w postaci wysokodostępnej. Awaria pojedynczego dowolnego elementu nie może spowodować niedostępność konsoli zarządzania. Jeżeli najlepsze praktyki danego producenta zalecają aby usługa/konsola/ system do zarządzania działał po za klastrem wirtualizacyjnym należy dodatkowo dostarczyć dodatkowe serwery oraz licencje aby system zarządzania był wysokodostępny 3. System musi umożliwiać bezprzerwową rozbudowę klastra, poprzez dołożenie kolejnych węzłów. System musi automatycznie rozłożyć równomiernie dane w klastrze, bez ingerencji administratora. 4. Konsola zarządzania Systemem musi umożliwiać podnoszenie wersji Systemu (sterowniki serwerów, hypervisor, podsystem storage) bez przerwy w pracy Systemu. Wymagane jest aby dla dostarczonej konfiguracji taki mechanizm był dostępny 5. System musi automatycznie sprawdzać kompatybilność podnoszonych elementów Systemu (sterowniki serwerów, hypervisor, podsystem storage) eliminując możliwość omyłkowego podniesienia jednego z komponentów do niewłaściwej wersji. 6. Opcjonalnie System musi udostępniać szczegółowe informacje na temat maszyn wirtualnych: 7. Wydajność maszyn wirtualnych (utylizacja CPU/RAM/IOPS oraz opóźnienie/latency) 8. Rekomendacje w temacie przypisanych zasobów (za mało / za dużo CPU lub RAM) 9. System musi wspierać REST API dla całej platformy. |
| 7 | Hypervisor | 1. Do zaproponowanego systemu należy dostarczyć licencje na oprogramowanie wirtualizacyjne na każdy dostarczony serwer. 2. Oprogramowanie wirtualizacyjne musi zapewniać mechanizmy HA w obrębię pojedynczego klastra 3. Oprogramowanie wirtualizacyjne musi posiadać mechanizm inteligentnego umiejscowienia nowych maszyn wirtualnych na serwerach o najmniejszym obciążeniu 4. Oprogramowanie wirtualizacyjne musi posiadać mechanizm Affinity Rules 5. Oprogramowanie wirtualizacyjne musi umożliwiać tworzenie i zarządzanie wirtualnymi sieciami 6. Oprogramowanie wirtualizacyjne musi automatycznie przenosić maszyny wirtualne pomiędzy węzłami w klastrze w zależności od ich obciążenia 7. Oprogramowanie wirtualizacyjne musi być w pełni zintegrowane z dostarczoną platformą chmury prywatnej i posiadać wspólną konsole zarządzania. 8. Oprogramowanie wirtualizacyjne musi posiadać mechanizmy klonowania maszyn wirtualnych. Klonowanie maszyn wirtualnych musi integrować się z podsystem dyskowym w celu szybkiego wykonywania klonów. 9. Oprogramowanie wirtualizacyjne musi posiadać wirtualny przełącznik sieciowy, umożliwiający konfigurację ustawień sieci per klaster. 10. Oprogramowanie musi być na liście wspieranych rozwiązań przez oprogramowanie do backupu firmy Commvault które posiada zamawiający. |
| 8 | Podsystem serwerowy | 1. System musi być wyposażony w procesory posiadające w sumie min. 128-rdzeni, klasy high-end posiadające wynik min 30 200 w benchmarku PassMark - CPU Mark ( Multi CPU system ) znajdującym się na stronie internetowej http://www.cpubenchmark.net/high\_end\_cpus.html 2. System musi być wyposażony w minimum 3 TB pamięci RAM 3. System musi być wyposażony w minimum 16 portów 25 Gb Ethernet SFF28 wraz z kablami o długości 3 metra 4. System musi być wyposażony w porty do zarządzania zdalnego każdym serwerem w ramach klastra. 5. Zamawiający wymaga aby rozbudowa systemu była liniowa . |
| 9 | Podsystem pamięci masowej | Zamawiający wymaga aby podsystem dyskowy udostępniał minimum 149 TiB przestrzeni użytecznej na dyskach SSD. Pojemność użyteczna nie może uwzględniać oszczędności z ewentualnej kompresji lub deduplikacji. Pojemność musi zakładać także failover na poziomie N+1 czyli pojemność 149 TiB musi być dostępna w przypadku awarii pojedynczego dowolnego serwera w ramach klastra  Jeżeli zapisy nie są realizowane bezpośrednio na wszystkie dyski zainstalowane, ale poprzez dedykowany dla serwera lub grupy dyskowej dyski, to takie dyski nie mogą być wliczane w dostarczoną pojemność i muszą mieć parametry wydajności minimum 100 000 zapisów/sec oraz wytrzymałość 20 000 TBW |
| 10 | Dodatkowe | Zamawiający wymaga aby dostarczone rozwiązanie było w pełni redundantne i kompletne, jeżeli do spełnienia wymagań, wymagane są dodatkowe licencje lub komponenty należy je dostarczyć. |
| 11 | Serwis gwarancyjny | 1. Wymagany jest serwis gwarancyjny dla Systemu świadczony przez minimum 3 lata. 2. Wymagany jest dostęp bezpośredni do Centrum serwisowego producenta rozwiązania poprzez: email, web, telefon 3. Dostępność serwisu 8x5 4. Serwis musi wspierać w rozwiązywanie problemów ze sprzętem i oprogramowaniem Systemu oraz z dostarczonym wirtualizatorem 5. Wymiana uszkodzonych podzespołów – NBD od momentu potwierdzenia usterki 6. Dostęp do poprawek (patch, hotfix, update) i nowych wersji oprogramowania (upgrade) w ramach wykupionego serwisu gwarancyjnego przez okres 3 lat. |

## **System kontrolera zasobów dyskowych**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Oferowany kontroler zasobów dyskowych musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

|  |  |  |
| --- | --- | --- |
| **LP** | **Wymagania** | |
|  | **Główne wymagania** | 1. Urządzenie musi być zbudowane w postaci appliance, tj. być dedykowanym rozwiązaniem sprzętowo programowym 2. Appliance może składać z jednego lub dwóch węzłów kontrolnych 3. Appliance może zostać rozbudowany poprzez dołożenie dodatkowych węzłów rozszerzających odpowiadających za przepływ danych wejściowych (front-end) oraz po stronie archiwum (back-end) 4. Musi zapewniać i gwarantować niezmienność przechowywanych w nim obiektów (treści) poprzez wykorzystanie technologii WORM (Write Once Read Many). Wykorzystanie technologii WORM może być realizowane przez inne urządzenie tego samego producenta. 5. Musi opierać się o zestaw polityk (polis), pozwalających na automatyczne zarządzanie przechowywanymi w archiwum obiektami, takimi jak, zakres danych polityki, wykluczenia, czas tworzenia kolejnych kopii, liczba wersji, czas usuwania danych ze strorage Tier 1 (truncate, ścianie, stubbowanie) 6. Zabezpieczenie treści odpowiednią ilością kopii. Wymagana jest możliwość zdefiniowania co najmniej 4 kopii danych na różnych nośnikach: napędy taśmowe, macierze dyskowe blokowe/plikowe/obiektowe 7. Musi istnieć możliwość trwałego usuwania danych - shredding 8. Musi istnieć integracja ze sprzętowymi mechanizmami szyfrowania danych. Wykorzystanie technologii szyfrowania danych może być realizowane przez inne urządzenie tego samego producenta. 9. Musi istnieć mechanizm indeksowania i księgowania danych. Musi być możliwość przekierowania księgowania i metadanych na dedykowaną przestrzeń dyskową (rozdzielając te dane od danych użytkowników) 10. Dane muszą być dostępne wieloma protokołami: blokowymi (FC lub iSCSI/inny dedykowany), plikowymi (NFS lub SMB) i obiektowymi S3 jednocześnie 11. Dla protokołów blokowych muszą istnieć dedykowani klienci umożliwiający jednoczesny zapis z wielu stacji na ten sam filesystem. Agenci muszą być dostępni dla środowisk min. Linux, Windows, Mac. 12. Dla systemów Windows i Mac, musi istnieć dodatkowy dedykowany agent, który będzie integrował się z systemem operacyjnym. Integracja ma polegać na: modyfikacji ikon plików tak, aby było wiadomo, czy dane posiadają swoją kopię i gdzie ta kopia się znajduje (taśma, dysk, chmura), modyfikacji menu kontekstowego tak, aby użytkownik był w stanie odtwarzać dane, wykonywać kopie, wykonywać ścinanie dla plików i katalogów (rekurencyjnie) jednym przyciskiem myszy. Dedykowani klienci muszą istnieć dla środowisk min. Windows, Mac. 13. System musi mieć możliwość replikacji lokalnej (tj. wykonywać replikację między dwoma różnymi rodzajami macierzy dyskowych) 14. System musi mieć możliwość replikacji zdalnej (tj. wykonywać replikację między różnymi urządzeniami 15. System musi mieć wewnętrzne mechanizmy ochrony (ochrona wewnętrznej bazy danych, wersjonowanie plików, księgowanie zmian) 16. System musi monitoring i raportować zużycie przestrzeni dyskowej, obciążenia, status komponentów 17. System musi integrować się oraz zarządzań dostępami z wykorzystaniem usług katalogowych (AD, LDAP) lub za pomocą wewnętrznych mechanizmów (np. unix bits) 18. Zapewniać wysoką dostępność (redundancja dostępu i danych, ochrona, wielokrotność kopii, replikacja) 19. Logowanie wszystkich wykonywanych procesów itp. 20. Pojedynczy interfejs zarządzania całym systemem archiwum zarówno w postaci panelu dostępnego przez WWW, wiersz poleceń CLI i polecenia RestAPI 21. Możliwość posadowienia pojedynczego systemu plików i jednoczesnego zapisu danych, na co najmniej 256 LUNach (urządzeniach blokowych) 22. Obsługa load-balancingu zarówno dla danych wejściowych (front-end) jak również danych zapisanych na urządzeniach rozwiązania (back-end) 23. Możliwość zdefiniowania wielu systemów plików w obrębie pojedynczego kontrolera archiwum 24. Możliwość integracji ze sprzętowymi mechanizmami sprawdzania poprawności danych oferowanych przez fizyczne biblioteki taśmowe 25. Oprogramowanie musi umożliwiać migrację danych pomiędzy różnymi poziomami archiwum, tzn. kopiować dane z dyskowych macierzy produkcyjnych (*primary*) na kolejne poziomy archiwum (*secondary*: biblioteki taśmowe ew. macierze dyskowe dużej pojemności) i usuwać dane z dysków primary zgodnie z regułami 26. Proces migracji musi być zarządzany centralnie 27. Możliwość zapisu danych na taśmach w formacie LTFS 28. Serwer zarządzający archiwum w formie klastra minimum dwu węzłowego 29. Quality of Service (gwarantowany czas odpowiedzi systemu archiwizacji) 30. Możliwość rozbudowy systemu o kolejne 64 węzły dostępowe 31. Kontrolery zasobów pracujące w klastrze muszą osiągać przepustowość na poziomie min. 5GB/s przy zapisie sekwencyjnym NAS lub DLC. 32. Możliwość zbudowania filesystemu niezarządzanego (bez dodatkowych kopii) do 5 miliardów plików lub zarządzalnego (do 4 kopii jednocześnie) do 1 miliarda plików 33. Maksymalny rozmiar pliku 2PB |
|  | **Wymagania dla roli kontrolera danych** | 1. Sprzęt musi być dostarczony w formie appliance tego samego producenta co system kontrolera zasobów dyskowych 2. Rozwiązanie należy dostarczyć w postaci klastra - tj. 2 sztuki serwerów 3. Każdy serwer powinien:    1. być wielkości 1U    2. posiadać dwa niezależne zasilacze    3. posiadać interfejsy:       * 3 x 1GbE Base-T,       * 2 x 32GbFC wraz z odpowiednimi modułami SFP oraz kablami,       * 4 x 10/25GbE SFP+ wraz z odpowiednimi modułami SFP+ oraz kablami,    4. posiadać licencję na:       * stworzenie i obsługę klastra metadanych,       * stworzenie i obsługę klastra danych dostępnych po protokołach plikowych,       * stworzenie i obsługę klastra danych dostępnych po protokołach blokowych,       * współdzielenie danych po protokołach plikowych - SMB i NFS (nielimitowane),       * współdzielenie danych po protokołach blokowych - DLC/Proxy (nielimitowane) i FC SAN (do 8 sztuk),       * replikację z rozwiązaniem StorNext M662/M662XL, 4. Dodatkowo klaster powinien mieć dedykowaną macierz za składowanie metadanych oraz indeksów. Macierz musi być tego samego producenta co system kontrolera zasobów dyskowych. Macierz musi mieć parametry:    1. wielkość 2U,    2. 6 x 0,8TB SSD 12Gb SAS,    3. 8 x 16GbFC. |
|  | **Wymagania dla serwisu całego rozwiązania** | 1. Cały system musi być jednego producenta. 2. Posiadać jeden punkt kontaktu serwisowego na terenie Polski. 3. 3 letnie wsparcie serwisowe w trybie 8x5xNBD musi być świadczone przez producenta rozwiązania lub przez Autoryzowanego Partnera Serwisowego producenta na terenie Polski. W przypadku świadczenia serwisu lub przez Autoryzowanego Partnera Serwisowego producenta na terenie Polski jedostka powinna posiadać certyfikat jakości ISO 9001:2015 w zakresie świadczenia serwisu oraz minimum 3 certyfikowanych inżynierów przez producenta w serwisie dedykowanego sprzętu i oprogramowania. |

## **System macierzy dyskowych**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Dostarczone macierze muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

|  |  |  |
| --- | --- | --- |
| **LP** | **Wymagania** | |
|  | **Obudowa** | System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''. |
|  | **Pojemność:** | 1. System musi zostać dostarczony w konfiguracji zawierającej minimum:  * dla macierzy pierwszej powierzchni użytkowej min. 1,7 PB * dla macierzy drugiej powierzchni użytkowej 0,85 PB * Zamawiający w ramach prawa opcji wymaga przedstawienia kosztu zakupu kolejnych 0,85 PB powierzchni użytkowej do drugiej macierzy  1. System w dostarczonej konfiguracji musi ponadto wspierać dyski:  * SAS 10k od 1200GB do 1800GB * NL-SAS od 4TB do 16TB  1. System musi mieć możliwość rozbudowy do minimum 300 dysków. |
|  | **Kontroler** | 1. Dwa kontrolery wyposażone w przynajmniej 64GB cache każdy.   Zamawiający dopuszcza zastosowanie kontrolerów z 8GB pamięci Cache na kontroler gdy oferowana macierz będzie wyposarzona w 5% przestrzeni na dyskach SSD z tieringiem danych lub funkcjonalnością SSD Cache dla odczytu i zapisu.  Lub  dopuszcza zastosowanie kontrolerów z 8GB pamięci Cache w sytuacji gdzie obsługa zapisów i odczytów będzie zoptymalizowana w systemie kontrolerów zasobów dyskowych, co zostanie poświadczone oficjalnym oświadczeniem zarówno przez producenta systemu kontrolerów dyskowych oraz producenta systemu macierzy dyskowych   1. W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash. |
|  | **Interfejsy** | 1. Oferowana macierz musi posiadać minimum:  * 8 portów 16Gb FC dla komunikacji frontend (tj. do hostów) * 2 porty 12Gb SAS dla komunikacji backend (tj. do półek rozszerzeń z dyskami) * 2 porty GbE dla komunikacji management (tj. do zarządzania administracyjnego oraz jako)  1. Macierz musi umożliwiać obsadzenie jej portami:  * 8 portami 10GbE SFP+ - Zamawiający dopuszcza możliwość wymiany kontrolerów macierzy  1. Zamawiający pozwala na dostarczenie macierzy, która nie spełnia warunku wymiany portów przy założeniu zaoferowania rozwiązania od razu wyposażonego w:  * 8 portów FC 16Gb   8 portów 10GbE SFP+ |
|  | **RAID** | 1. Wsparcie dla RAID:    * 0, 1, 5, 6, 10,    * DDP/ADAPT lub odpowiednik, który umożliwia tworzenia wirtualnej przestrzeni na minimum 120 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych. 2. Obliczanie sum kontrolnych (kodów parzystości) dla grup dyskowych RAID5 musi być realizowane w sposób sprzętowy przez dedykowany układ w macierzy lub procesor główny posiadający taką zdolność. |
|  | **Inne wymagania** | 1. Macierz musi posiadać wsparcie dla wielościeżkowości dla oferowanego systemu kontrolera zasobów dyskowych. 2. Macierz musi posiadać funkcjonalność wykonywania snapshotów minimum 128 per wolumen. 3. Macierz musi posiadać funkcjonalność klonowania danych 4. Macierz musi posiadać funkcjonalność replikacji danych po FC (po zainstalowaniu portów FC na macierzy) lub iSCSI w trybie asynchronicznym 5. Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie 6. Macierz musi posiadać oprogramowanie do monitoringu stanu dysków, które pozwala na identyfikowanie potencjalnie zagrożonych awarią dysków 7. Wraz z system musi zostać dostarczone narzędzie do monitoringu macierzy w kontekście:  * wydajności i opóźnień na wolumenach * wydajności I/Ops, MB/s  1. Wszystkie licencje na funkcjonalności muszą być dostarczone na maksymalną pojemność macierzy. |
|  | **Wydajność** | Kontrolery macierzy musza umożliwiać przepustowość na poziomie 7GB/s, 320k IOPS. Zamawiający wymaga dostarczenia oświadczenia producenta macierzy lub niezależnego testu potwierdzającego, że dany model macierzy osiągnie ten poziom wydajności przy zapisie mi 30%.  Kontrolery muszą działać w trybie min. asymetryczny aktywny/aktywny (ALUA). |
|  | **Gwarancja i serwis** | 1. 3 lata serwisu producenta z 2 godzinnym czasem odpowiedzi na awarie krytyczne i dostawą elementów w na następny dzień roboczy od diagnozy problemu. 2. Dostarczony system musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia. |

## **System backup**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Dostarczony system backup musi zapewniać wszystkie wymienione poniżej wymagania i funkcje

Zamawiający wymaga dostarczenia licencji backupowych które zabezpieczą dostarczoną platformę chmury prywatnej. Zamawiający wymaga dostarczenia licencji per CPU w celu rozbudowy obecnie posiadanego rozwiązania do backupu firmy Commvault ( CCID: FE7E3 ). Dostarczone licencje muszą w pełni zabezpieczać dostarczony klaster oraz stworzenie konfiguracji klastrowej dla usługi Commserve. Licencje muszą posiadać wsparcie na okres 3 lat. Jeżeli wymagane jest przez producenta aby wszystkie licencje posiadały taki sam okres wsparcia serwisowego należy je dostarczyć dla obecnych licencji oraz nowych.

Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniające poniższe wymagania.

Wymogi funkcjonalne dla systemu zarządzania danymi obejmujący backup serwerów fizycznych, aplikacji oraz maszyn wirtualnych.

Uwaga:

Pojęcie **system** wskazuje na rozwiązanie zabezpieczające dane stanowiące jedno, spójne rozwiązanie, zarządzane z poziomu jednej konsoli. Nie dopuszcza się rozwiązań pochodzących od różnych producentów, a co za tym idzie nie całkowicie niezintegrowanych pomiędzy sobą wymagających wykorzystywania różnych konsol dla zarządzania czy konfiguracji.

Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych lub pocztowych do archiwum (repozytorium dyskowe lub taśmowe) z pozostawieniem skrótów lub bez ich pozostawiania.

Jeśli przy danym punkcie wymogu występuje informacja „jako opcja” oznacza to iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność.

W celu weryfikacji funkcjonalności oferowanych przez proponowany system, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wynik negatywny - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

|  |  |
| --- | --- |
| **LP** | **Wymagania** |
| **Wymogi podstawowe** | |
| 1 | Rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych. |
| 2 | Oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia |
| 3 | Jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizyczny (minimum 2xCPU po 8 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V |
| 4 | Licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z czasem przełączenia nie dłuższym niż 15 minut. Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacja produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego |
| 5 | Rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji. |
| 6 | Oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux i Unix – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich |
| 7 | System musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów. |
| 8 | System musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania |
| 9 | Dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie |
| 10 | System musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu |
| 11 | System musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów) z jednej konsoli administracyjnej oraz także z konsoli webowej |
| 12 | Agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ |
| 13 | Automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe |
| 14 | System musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP |
| 15 | Komunikacja agentów systemu z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania |
| 16 | System musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN |
| 17 | System musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia). |
| 18 | Włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh |
| 19 | Logiczna Globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej |
| 20 | Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych. |
| 21 | Deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB. |
| 22 | System musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji |
| 23 | System musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu. |
| 24 | Proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej |
| 25 | System musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób aby awaria pojedynczego serwera nie powodowała utraty możliwości deduplikacji i odtwarzania danych |
| 26 | System musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie wykorzystuje bazę deduplikacyjną |
| 27 | Na jednym serwerze systemu (na jednej instancji systemu operacyjnego) może być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu. |
| 28 | System musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną |
| 29 | System musi zapewniać zintegrowane logowanie dla użytkownika końcowego poprzez tzw. social media (minimum poprzez Google) |
| 30 | System musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD. |
| 31 | System musi pozwalać na zarządzanie z poprzez „cmd” z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH. |
| 32 | Komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach |
| 33 | System musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych) |
| 34 | System musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail |
| 35 | Szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu. |
| 36 | Możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem |
| 37 | System musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO |
| 38 | System musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password |
| 39 | System musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrującym – minimum dla:   * Safenet * Amazon Web Services (AWS) key management service * Microsoft Azure Key Vault |
| 40 | System musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy |
| 41 | System musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:   * Zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane * Monitorowanie nietypowych aktywności na serwerach za pomocą np. metody: Honeypot * Monitorowanie dużych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji |
| 42 | System musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email. |
| 43 | System musi automatycznie wysyłać informacje o alertach, zdarzeniach oraz informacjach audytowych do syslog serwera |
| 44 | Automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach |
| 45 | System musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:   * Raport zmian/wzrostu środowiska systemu * Raport wykorzystania licencji * Raport wykonanych zadań backupowych |
| 46 | System musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail |
| 47 | System musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV |
| 48 | System musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryterii:   * Czas zadania dłuższy niż zadany * Ilość danych większa niż …. * Ilość danych mniejsza niż …. * Ilość nie zbackupowanych plików większa niż * Ilośc nie zbackupowanych plików większa niż …% * Wielkośc backupowanych danych wieksza niż … |
| 49 | Notyfikacje alertów muszą być wysyłane minimum poprzez mail. |
| 50 | Raport spełnienia wymogów SLA dla parametrów:   * Ilości dodatkowych kopii backupowych * RTO * RPO |
| 51 | System musi zapewniać funkcjonalność wznawiania zadań backupowych. |
| 52 | System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych |
| 53 | System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy |
| 54 | Funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu |
| 55 | System musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków |
| 56 | Rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego. |
| 57 | System musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych. |
| 58 | System musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji. |
| 59 | System ma realizować procesy backupu oraz odzyskiwania danych. |
| 60 | System ma umożliwić tworzenie zadań backupowych w oparciu o kalendarz. |
| 61 | System musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane backupowane i archiwizowane. |
| 62 | System musi realizować funkcjonalność weryfikacji wykonanych kopii. |
| 63 | System powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:   * Windows * Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu * Unix: AIX/Solaris * OpenVMS |
| 64 | System musi umożliwiać (jako opcja) integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage, Tintri, Kaminario, z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji.  System musi posiadać możliwość wykonywania kopii oraz archiwów na urządzenia dyskowe i taśmowe |
| 65 | System powinien umożliwiać (jako opcja) obsługę urządzeń składowania danych w chmurze, minimum: Azure, Amazon, Google Cloud |
| 66 | System musi pozwalać na odtwarzanie tylko samych uprawnień do plików |
| 67 | System musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) |
| 68 | System (jako opcja) powinien umożliwiać analizę logów z systemów zewnętrznych, na bazie zdefiniowanych kryterii powinien generować alarmy lub akcje. Minimalne wsparcie to: Windows Event Log. |
| 69 | Możliwość odtwarzania backupów plikowych poprzez udostepnienia CIFS lub NFS. A więc dostęp do zbackupowanych danych widocznych jako udostępnione przez sieć zasoby CIFS/NFS |
| 70 | System musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux |
| 71 | System musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix |
| 72 | System musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Gentoo, Mandriva, Oracle Linux, Red Flag Linux, Scientific Linux, Ubuntu, Slackware |
| 73 | System musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris |
| 74 | System musi wspierać funkcjonalność odtwarzania fizycznego serwera do środowiska wirtualnego, minimum: dla serwera Windows do środowiska Vmware |
| 75 | System musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane. |
| 76 | System musi wspierać backup całych maszyn wirtualnych dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:   * Alibaba Cloud * Amazon * Citrix Xen * Docker * Google Cloud Platform * Huawei FusionCompute * Microsoft Azure * Microsoft Azure Stack * Microsoft Hyper-V * Kubernetes * Nutanix Acropolis Hypervisor (AHV) * OpenStack * Oracle Cloud Classic * Oracle Cloud Infrastructure * Oracle VM * Red Hat OpenShift * Red Hat Virtualization * vCloud Director * VMware   To znaczy musi posiadać dedykowanego agenta do backupu minimum całej maszyny wirtualnej bez konieczności instalowania agenta wewnątrz maszyny z możliwością granularnego odtwarzania pojedynczych plików. |
| 77 | System musi wspierać wersje środowisk VMware, 5.0.x, 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 6.0, 6.0.1, 6.5, 6.7 poprzez integrację z vStorage API |
| 78 | Dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS |
| 79 | System musi wspierać środowisko Hyper-V dla:   * Microsoft Windows Server 2008 R2 SP1 * Microsoft Windows Server 2012 * Microsoft Hyper-V Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Hyper-V Server 2012 R2 * Microsoft Windows Server 2016 (z Core Edition) * Microsoft Hyper-V Server 2016 (z Core Edition) * Microsoft Windows Server, version 1709 (z Core Edition) * Microsoft Hyper-V Server, version 1709 (z Core Edition) * Microsoft Windows Server 2019 (z Core Edition) * Microsoft Hyper-V Server 2019 (z Core Edition) |
| 80 | System musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych. |
| 81 | System musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej – minimum dla Vmware. |
| 82 | System musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:   * Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure * Hyper-V do: Azure, Amazon, Vmware * Amazon do: Azure, Vmware * Azure do: Amazon, Hyper-V, Vmware |
| 83 | System musi umożliwiać konwersję serwera Windows i Linux do maszyny wirtualnej w środowisku:   * Hyper-V * Vmware |
| 84 | System musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows |
| 85 | System musi posiadać możliwość wykonywania kopii oraz archiwów na urządzenia dyskowe i taśmowe |
| 86 | Dla producentów: NetApp, EMC i HDS system musi (jako opcja) umożliwiać nie tylko integrację z mechanizmami tworzenia kopii migawkowych (tzw. Snapshot) ale musi integrować się także z mechanizmami replikacyjnymi, a więc sterować replikami wykonywanymi przez macierze |
| 87 | System musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V |
| 88 | Możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure |
| 89 | System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, Postgress, Oracle, Informix na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik. |
| 90 | System musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, Postgress, DB2, Informix konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny. Brak skryptów musi dotyczyć dowolnych typów backupów: backup automatyczny uruchamiany poprzez harmonogram, backup manualny. |
| 91 | Odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów |
| 92 | Dla silników bazodanowych MS SQL i Oracle musi istnieć mechanizm backupu logów tranzakcyjnych z częstotliwością co 1 minuta nawet w przypadku gdy serwer zarządzający systemem backupowym jest niedostępny |
| 93 | Konfiguracja agentów backupowych dla: MS SQL, Oracle, mySQL musi odbywać się poprzez interface graficzny, jakakolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie |
| 94 | System musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników |
| 95 | System musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange |
| 96 | System musi umożliwiać wykonanie kopii na gorąco aplikacji MS Exchange a następnie odzyskania pojedynczych wiadomości. Dedykowany agent do backupu Exchange musi wspierać backup środowiska Exchange DAG poprzez nazwę DAG |
| 97 | System musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, MS SQL |
| 98 | Dla minimum mySQL i PostgresSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego |
| 99 | Automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle |
| 100 | Dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio |
| 101 | Wsparcie dla backupu online dla minimum MS SQL Server 2016/2014/2012/2008/2005 |
| 102 | Dedykowany agent bazodanowy dla backupu MS SQL na platformie Linux: Ubuntu, SuSe, RHE |
| 103 | Możliwość (jako opcja) archiwizacji danych z baz Oracle do plików XML |
| 104 | Odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore) |
| 105 | Dedykowani agenci (jako opcja) do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk |
| 106 | Możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, mySQL, Oracle – zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów |
| 107 | Możliwość backupu i odtwarzania (jako opcja) dokumentów i maili dla Office 365 z:   * + SharePoint Online   + Exchange Online   + OneDrive for Business   + Teams |
| 108 | System musi zapewniać (jako opcja) backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach:   * System musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh * Dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS i Android * Dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa. * System musi zapewniać współdzielenie plików pochodzących z backupu laptopów i desktopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny. * System musi oferować możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły) * Każdy użytkownik desktopa czy laptopa musi posiadać możliwość zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to: * Odtwarzanie własnych danych * Uruchomienie backupu * Wstrzymanie backupu * Możliwość zdefiniowania innego okna backupowego * Możliwość monitorowania postępu działania zadania * Możliwość przeglądania danych z stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadając jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopii ale także przeglądać dane na stacji roboczej nawet w momencie gdy jest poza siedzibą firmy – korzysta jedynie z dostępu do internetu (do przeglądania danych nie jest potrzebne żadne dodatkowe połączenie VPN) * Zabezpieczenie przed kradzieżą, system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci wtenczas automatycznie dane zostaną zaszyfrowane * Możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany pliki zostaje skasowany albo zamieniony na skrót (stub) |
| 109 | Rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników (stub) na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix) serwerów fizycznych, archiwizacja musi korzystać z tej samej architektury systemu co backup i korzystać z tego samego repozytorium danych. |
| 110 | System musi posiadać funkcjonalności archiwizacyjne (archiwizacja plikowa) takie jak:   * Oprogramowanie musi wspierać archiwizację zgodnych z wyznaczonymi kryteriami danych z systemów produkcyjnych na inne tańsze pamięci masowe. Mechanizm ten pozwoli na zmniejszenie ilości danych na systemach produkcyjnych. * Oprogramowanie musi obsługiwać strategię wielowarstwowego aktywnego archiwum. Na przykład, umożliwiać przenoszenie zarchiwizowanych plików pomiędzy różnorodnymi urządzeniami pamięci masowej, w sposób zautomatyzowany przez politykę do wykonania krótko-, średnio- i długoterminowe okresów retencji, przy zachowaniu przejrzystego jedno- krokowego odzyskiwania dla użytkowników końcowych. * Oprogramowanie musi być zintegrowane z modułem do tworzenie kopii zapasowych w celu redukcji czasu okien backupowych przy zabezpieczaniu dużej ilości danych. * Oprogramowanie musi wspierać proces archiwizacji bezpośrednio na taśmy. * Oprogramowanie musi umożliwiać deduplikację danych archiwizowanych na poziomie bloków w celu redukcji ilości przestrzeni na dyskach fizycznych. Oprogramowanie musi umożliwiać globalną deduplikację dla archiwizacji i kopii zapasowych w celu minimalizowania zużycia pamięci masowej. * Oprogramowanie musi zapewniać przezroczysty dostęp użytkowników do danych archiwalnych poprzez mechanizm skrótów |
| 111 | System musi (jako opcja) umożliwiać rozbudowę o archiwizację poczty (minimum Exchange), archiwizacja poczty musi umożliwiać archiwizowanie maili z skrzynek pocztowych oraz archiwizowanie ruchu pocztowego (journaling) |
| 112 | Oprogramowanie musi umożliwiać (jako opcja) pełnokontekstowo indeksować maile wraz z załącznikami oraz posiadać centralną konsolę do wyszukiwania danych i monitorowania zgodności z przepisami/normami bezpieczeństwa (compliance). |
| 113 | System musi umożliwiać (jako opcja) pełnokontekstowe indeksowania treści danych dla wybranych typów plików, indeksacja musi odbywać się dla danych znajdujących się już w systemie. |
| 114 | System musi umożliwiać (jako opcja) przeprowadzanie wielu wyszukiwań (eDiscovery) i zbierać wszystkie wyniki w jednej lokalizacji. |
| 115 | System musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to iż kopia backupowa jest przechowywana w repozytorium przez określony czas (np. tydzień, miesiąc, rok….) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie |
| 116 | Musi istnieć dedykowany agent do backupu online aplikacji MongoDB |
| 117 | System musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce. Integracja z StoreOnce musi być dostępna nie tylko dla Windows ale także dla Unix i Linux. |
| 118 | System (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym |
| 119 | Musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell |
| 120 | Agent do spójnego backupu bazy HBASE – backup pełny i przyrostowy |
| 121 | Agent do backupu systemów plikowych: Lustre, GlusterFS |
| 122 | Wsparcie (jako opcja) dla replikacji maszyn wirtualnych Vmware z wykorzystaniem VIAO (VSphere APIs for I/O) |
| 123 | System musi zamierać moduł do monitorowania i zarządzania taśmami wynoszonymi z bibliotek taśmowych o funkcjonalnościami minimum:   * + Identyfikacja taśm, które muszą być wyciągnięte z biblioteki   + Identyfikacja taśm, które można z powrotem wstawić do biblioteki taśmowej   + Automatyczne przenoszenie taśm w bibliotece i notyfikacja administratorów   + Identyfikacja i monitorowanie nośników (taśm) w trakcie transportu |
| 124 | Możliwość backupu skrzynek pocztowych Google i Google drive |
| 125 | Możliwość backupu baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy |
| 126 | System musi posiadać integrację z ServiceNow o funkcjonalnościach:   * + Dedykowany plugin do ServiceNow   + Możliwość zgłaszania zdarzeń backupowych i odtworzeniowych bezpośrednio z konsoli Service Now |
| **Wymogi dla licencjonowania** | |
| 1 | Niedopuszczalne jest aby licencjonowanie było zależne od ilości danych (kopii backupowych) składowanych na dowolnych nośnikach (np. dysk, taśma VTL…) czy to z deduplikacją czy bez. |
| 2 | Niedopuszczalne jest aby licencjonowanie było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych |
| 3 | Zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu |
| 4 | Oferowana licencja oraz architektura systemu musi pozwalać na backup danych na nielimitowana ilość bibliotek taśmowych i napędów fizycznych. |
| 5 | W przypadku wielu lokalizacja licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami |
| 6 | Do dostarczonych licencji jest wymagane 36 miesięczne wparcie producenta (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień. Oferowane wsparcie serwisowe musi być świadczone przez producenta rozwiązania lub autoryzowanego partnera serwisowego producenta na terenie Polski. W przypadku serwisu świadczonego przez autoryzowanego partnera serwisowego producenta na terenie Polski wymagane jest potwierdzenie jakości świadczonych usług poprzez certyfikat ISO 9001:2015 na świadczone usługi serwisowe. |
| 7 | Zaoferowane licencje na system muszą zapewnić backup danych z środowiska o wielkości:   * + Dostarczonego środowiska chmury prywatnej   + środowisko wirtualne składające się 14 CPU (10 CPU – dla CRC oraz 4 CPU dla ZRC) wraz z aplikacjami i bazami na maszynach wirtualnych, środowisko znajduję się w oddziale Warszawskim   + środowisko serwerów fizycznych wraz z aplikacjami i bazami w ilości 1 sztuki   + środowisko laptopów i desktopów w ilości 30 sztuk |

## **Wymagania dla serwera systemu backupu**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Dostarczone serwery do systemu backup muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje oraz być kompatybilne lub wspierane przez producenta oferowanego systemu backup

|  |  |  |
| --- | --- | --- |
| **LP** | **Wymagania** | |
| 1 | Obudowa | 1. Typu Rack, wysokość maksimum 4 U; 2. Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack; 3. Możliwość instalacji minimum 12 dysków 3.5” typu Hot-Plug. |
| 2 | Płyta główna | 1. Wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów 28-rdzeniowych; 2. Wyposażona w minimum 24 gniazda pamięci RAM DDR4, obsługa minimum 3TB pamięci RAM DDR4 2933 MHz. Możliwość rozbudowy do minimum 768GB pamięci RAM bez konieczności wymiany zaoferowanych modułów DDR4; 3. Obsługa pamięci nieulotnej instalowanej w gniazdach pamięci (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci); 4. Możliwość rozbudowy do minimum 8 złączy PCI Express generacji 3, w tym minimum 3 złączy o prędkości x16; w zaoferowanej konfiguracji wymaga się minimum 5 złączy PCI Express aktywnych i wolnych do instalacji kart rozszerzeń; 5. Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; 6. Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora bez zajmowania klatek dyskowych serwera. |
| 3 | Procesory | 1. Zainstalowane minimum jeden procesor 16-rdzeniowy lub dwa procesory 8-rdzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności [SPECrate2017\_int\_base](http://www.spec.org/auto/cpu2017/Docs/result-fields.html#SPECrate2017intbase) wynik minimum 80 pkt. 2. Wynik dla oferowanego serwera wraz z oferowanymi procesorami dostępny na stronie spec.org. 3. Nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowana aplikacji i systemów operacyjnych. |
| 4 | Pamięć RAM | 1. Zainstalowane minimum 128 GB pamięci RAM typu DDR4 Registered, 2933 MHz; 2. Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC lub równoważne; 3. Wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM. |
| 5 | Kontrolery dyskowe, I/O | 1. Zainstalowany dedykowany sprzętowy kontroler SAS 3.0 ze wsparciem dla poziomów RAID: 0, 1, 5, 6, 50, 60; 2. Kontroler wyposażony w minimum 2GB pamięci podręcznej Cache oraz podtrzymanie bateryjne (dopuszcza się brak podtrzymania bateryjnego pamięci podręcznej w przypadku zaoferowania kontrolera z minimum 2GB nieulotnej pamięci Cache). |
| 6 | Dyski twarde | Zainstalowane minimum 6 dysków SSD SAS 12Gb/s Hot-Plug o pojemności 1.6TB każdy i parametrze DWPD minimum 3. |
| 7 | Interfejsy sieciowe | 1. Jedna dwuportowa karta 25/10Gbit/s w standardzie SFP+ wyposażona we wkładki optyczne typu Multimode; karta nie może zajmować jakiegokolwiek slotu PCI Express i nie może zostać osiągnięta przez zastosowanie dodatkowego adaptera (np. przejściówki podłączaniej do portu USB); 2. Jedna dwuportowa karta 32Gbit/s FC wyposażona we wkładki optyczne typu Multimode. |
| 8 | Porty | 1. Zintegrowana karta graficzna ze złączem VGA; 2. min 1x USB 2.0 lub 3.0 dostępne na froncie obudowy; 3. 2x USB 3.0 dostępne z tyłu serwera; 4. 1x USB 3.0 wewnątrz serwera; 5. Możliwość rozbudowy o dodatkowe złącze szeregowe w standardzie RS-232-C; 6. Wszystkie wymagane złącza VGA i USB nie mogą być osiągnięte poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera. |
| 9 | Zasilanie, chłodzenie | 1. Redundantne zasilacze Hot-Plug o mocy minimum 800W każdy i sprawności 94%; 2. Redundantne wentylatory Hot-Plug; 3. Dostarczone wraz z kablami C13 o długości min. 3m każdy. |
| 10 | Zarządzanie | 1. Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania/rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zrządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera; 2. Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: 3. Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; 4. Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; 5. Dostęp poprzez przeglądarkę Web (także SSL, SSH); 6. Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; 7. Zarządzanie alarmami (zdarzenia poprzez SNMP); 8. Możliwość przejęcia konsoli tekstowej; 9. Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); 10. Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych); 11. Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 8Gbit/s oferowanych przez producenta serwera); 12. Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.); 13. Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB; 14. Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); 15. Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; 16. Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; 17. Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; 18. Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; 19. karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera. |
| 11 | Wspierane OS | 1. Windows 2019 Hyper-V; 2. Windows 2016 R2 Hyper-V; 3. VMWare; 4. SuSE; 5. RHEL. |
| 12 | System operacyjny | Wymaga się dostarczenie wraz z serwerem systemu Windows Server 2019 Standard z licencją na wszystkie zainstalowane w serwerze rdzenie procesorów. |
| 13 | Gwarancja | 1. Minimum 3 lat gwarancji producenta serwera w trybie onsite z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime); 2. Wymagane jest oświadczenie Producenta oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta serwera na potrzeby oferty w niniejszym postępowaniu; 3. Dostępność części zamiennych przez 5 lat od momentu zakupu serwera; 4. Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji. |
| 14 | Dokumentacja, inne | 1. Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 (dokumenty załączyć do oferty); 2. Serwer musi posiadać deklarację CE (dokument załączyć do oferty); 3. Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty); 4. Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu w języku polskim lub angielskim; 5. Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera. |

## **Przełączniki SAN**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Dostarczone przełączniki SAN muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

|  |  |
| --- | --- |
| **LP** | **Wymagania** |
| 1 | Urządzenie musi być wyposażone w nie mniej niż 16 aktywnych portów Fibre Channel w standardzie SFP pracujących w trybie 4/8/16/32 Gbps z pełną przepustowością dla prędkości 32G FC. |
| 2 | Musi istnieć możliwość zwiększenia liczby aktywnych portów urządzenia do co najmniej 32 portów 4/8/16/32G FC pracujących z pełną przepustowością dla prędkości 32G FC. |
| 3 | 16 portów musi zostać obsadzonych wkładkami optycznymi wyposażonymi w interfejsy optyczne SW FC 32 Gb SW(short-wave); |
| 4 | Każdy port musi być wyposażony w minimum 500 buffer credits |
| 5 | Przynajmniej jeden port musi mieć możliwość wyposażenia w co najmniej 8000 kredytów i wspierać dystans do 500km (przy zachowaniu pełnej przepustowości, bez spadku wydajności związanego z odległością). |
| 6 | Urządzenie musi wspierać podział sieci SAN na wirtualne sieci SAN (wirtualne fabryki) i umożliwiać stworzenie co najmniej 32 wirtualnych sieci (fabryk) SAN; |
| 7 | Urządzenie musi oferować routing między wirtualnymi sieciami SAN |
| 8 | Urządzenie musi umożliwiać agregację nie mniej niż 16 portów fizycznych w jedno połączenie logiczne. Jeśli opisany mechanizm wymaga dodatkowej licencji musi być ona dostarczona razem z urządzeniem. W skład zagregowanego połączenia logicznego musi być możliwe włączenie dowolnego aktywnego portu przełącznika. |
| 9 | Urządzenie musi wspierać wymianę oprogramowania bez przerwy w działaniu |
| 10 | Urządzenie musi oferować mechanizmy gwarancji jakości usług (QoS). |
| 11 | Urządzenie musi posiadać dodatkową możliwość uruchomienia mechanizmów telemetrycznych:   * 1. Monitorowanie oraz inspekcja połączeń FC dla protokołów SCSI oraz NVMe z pełną wydajnością (wirespeed) z raportowaniem operacji read/write i/o rate, read/write i/o bandwidth, read/write abort, read/write failure.   2. Wykrywanie i eliminowanie problemów zatykania (slow-drain) w sieci SAN   3. Możliwość eksportu danych telemetrycznych poprzez dedykowany port lub standardowy port zarządzający.   4. Możliwość eksportu danych telemetrycznych do dowolnej aplikacji   5. Jeśli powyżej wymieniona funkcjonalność potrzebuje do pracy dodatkowej licencji na oprogramowanie to wymagane jest dostarczenie go na obecnym etapie postępowania |
| 12 | Urządzenie musi posiadać wsparcie dla następujących mechanizmów:   * 1. Sprzętowo implementowany zoning,   2. N-Port ID Virtualization (NPIV),   3. Zarządzanie/monitorowanie SNMPv3,   4. Dostęp administracyjny SSHv2,   5. Transfer plików za pomocą SFTP i SCP   6. Autoryzacja dostępu administracyjnego do przełącznika za pomocą RADIUS i TACACS+, LDAP, Microsoft Active Directory;   7. Protokół FC-SP (Fibre Channel Security Protocol) wraz z autentykacją DH-CHAP dla dołączanych przełączników i hostów   8. Filtrowanie adresów IP z których możliwe jest zarządzanie przełącznikiem   9. Interfejs programistyczny REST-API   10. Szyfrowanie sprzętowe łącza na wybranych portach z pełną wydajnością z użyciem AES 128 bit   11. Wsparcie sprzętowe dla pokazywania statystyk ruchu dla poszczególnych maszyn wirtualnych VM |
| 13 | Urządzenie musi oferować możliwość konfiguracji poprzez terminal i linię komend CLI, interfejs graficzny GUI oraz REST API. Oprogramowanie do konfiguracji i monitorowania przełącznika, musi być wyposażone w graficzny interfejs użytkownika oparty o HTML, bez konieczności instalacji oprogramowania klienckiego i zapewniać:   1. Interfejs GUI 2. Wizualizacja topologii sieci SAN 3. Konfiguracja całej sieci (fabryki) SAN oraz poszczególnych przełączników i ich portów 4. Uproszczone narzędzia konfiguracyjne 5. Narzędzia diagnostyczne łącznie analizą działania (fabryki) SAN w tym zjawiska slow-drain. 6. Wizualizacja wydajności działania 7. Wizualizacja błędów i alarmów 8. Jednoczesne zarządzanie wieloma oddzielnymi fizycznie sieciami SAN 9. Zbieranie i raportowanie danych historycznych 10. Przekazywanie zdarzeń (events) do zdalnych kolektorów 11. Wizualizacja połączeń SAN dla maszyn wirtualnych VM w środowisku VMWare ESXi |
| 14 | Urządzenie musi być wyposażone w szeregowy port konsoli oraz port USB (ten ostatni do procedury automatycznej konfiguracji przy pierwszym uruchomieniu) |
| 15 | Urządzenie musi być wyposażone w następujące narzędzia diagnostyczne   * 1. Rejestrowanie zdarzeń poprzez mechanizm „syslog”,   2. Możliwość bezzakłóceniowego monitorowania ruchu na portach przez kopiowanie ruchu z określonego portu na wybrany port monitorujący (z dołączonym zewnętrznym analizatorem),   3. Mechanizm diagnostyki portu   4. Narzędzia dla Fibre Channel odpowiadające funkcjonalnie poleceniom sieciowym ping i traceroute. |
| 16 | Urządzenie musi posiadać redundantne zasilacze i wentylatory z możliwością ich wymiany w czasie pracy |
| 17 | Urządzenie musi posiadać obudowę 1RU, przystosowaną do montażu w szafie 19” i wykonaną z metalu. |

## **Przełączniki OOB**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Dostarczone przełączniki OOBmuszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

|  |  |  |
| --- | --- | --- |
| **LP** | **Wymagania** | |
| 1 | Porty | 1. 24 porty 10/100/1000BaseT RJ-45 2. 2 porty uplink 10G SFP   Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek: Gigabit Ethernet 1000Base-T, Gigabit Ethernet 1000Base-SX, Gigabit Ethernet 1000Base-LX/LH, Gigabit Ethernet 1000Base-EX, Gigabit Ethernet 1000Base-ZX, Gigabit Ethernet 1000Base-BX-D/U, 10Gigabit Ethernet 10GBase-SR, 10Gigabit Ethernet 10GBase-LR, 10Gigabit Ethernet 10GBase-ER, 10Gigabit Ethernet 10GBase-ZR, |
| 2 | Stackowanie | 1. Przepustowość w ramach stosu - 80Gb/s, 2. 8 urządzeń w stosie, 3. Zarządzanie poprzez jeden adres IP, 4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad, |
| 3 | Zasilanie i chłodzenie | 1. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap), 2. Redundantne wentylatory, |
| 4 | Parametry wydajnościowe | 1. Przepustowość przełącznika (switching capacity): 128 Gb/s (bez podłączenia do stosu), 2. Prędkość przesyłania (forwarding rate): 95 Mpps 3. Bufor pakietów – 2MB 4. Pamięć DRAM – 2GB 5. Pamięć flash – 2GB 6. Obsługa:  * 500 aktywnych sieci VLAN * 16000 adresów MAC * 3000 tras IPv4 * 1500 tras IPv6  1. Ilość wpisów w listach kontroli dostępu Security ACL – 1000 2. 512 interfejsów SVI L3 3. Jumbo frame 9198B 4. 48 połączeń zagregowanych typu „port channel” 5. 8 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP |
| 5 | Mechanizmy związane z zapewnieniem ciągłości pracy sieci | 1. IEEE 802.1w Rapid Spanning Tree 2. Per-VLAN Rapid Spanning Tree (PVRST+) 3. IEEE 802.1s Multi-Instance Spanning Tree 4. Obsługa 64 instancji protokołu STP |
| 6 | Mechanizmy związane z bezpieczeństwem sieci | 1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level), 2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN, 3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL, 4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X, 5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC, 6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X, 7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem, 8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176, 9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www), 10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard, 11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard), 12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+, 13. Obsługa list kontroli dostępu (ACL) następujących typów: 14. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, 15. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika, 16. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN, 17. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia); 18. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika 19. Funkcja Private VLAN; |
| 7 | Mechanizmy związane z zapewnieniem jakości usług w sieci: | 1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi, 2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek, 3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority), 4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP, 5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting), 6. Kontrola sztormów dla ruchu broadcast/multicast/unicast, 7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP; |
| 8 | Obsługa protokołów i mechanizmów routingu | 1. Routing statyczny dla IPv4 i IPv6, 2. Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes 3. Policy-based routing (PBR), 4. Obsługa protokołu redundancji bramy (VRRP) |
| 9 | Zarządzanie | 1. Port konsoli, 2. Dedykowany port Ethernet do zarządzania out-of-band, 3. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją, 4. Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog, 5. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów, 6. Wsparcie dla protokoły RESTCONF, 7. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych, 8. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB, 9. Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki; |
| 10 | Dodatkowe wymagania | 1. Obsługa protokołu NTP 2. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping 3. Obsługa protokołu LLDP i LLDP-MED. 4. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC 5. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego 6. Możliwość uruchomienia funkcji serwera DHCP 7. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN 8. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.), 9. Funkcjonalność sondy IP SLA Responder, 10. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow/sFlow/JFlow 11. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie, |
| 11 | Wyposażenie urządzenia | 1. Przełącznik wyposażony w pojedynczy zasilacz, 2. Przełącznik wyposażony jest w następujące wkładki interfejsowe 10Gigabit Ethernet 10GBase-SR, 3. Możliwość montażu w szafie rack 19”. 4. Wysokość urządzenia 1 RU, |

## **Przełączniki rdzeniowe**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Dostarczone przełączniki rdzeniowe muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

|  |  |  |
| --- | --- | --- |
| **LP** | **Wymagania** | |
| 1 | **Porty** | 1. 24 aktywne, obsadzone wkładkami porty 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+ z możliwością rozbudowy do 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+ 2. 6 aktywnych portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie100Gbps na pojedynczej parze okablowania multi-mode (do 100m). |
| 2 | **Parametry wydajnościowe:** | 1. Prędkość przełączania 1.8Tbps full duplex 2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 |
| 3 | **Funkcjonalność warstwy L2** | 1. Trunking IEEE 802.1Q VLAN; 2. Wsparcie dla 3000 sieci VLAN; 3. Wsparcie sprzętowe dla 90 tysięcy adresów MAC 4. IEEE 802.1w Rapid Spanning Tree (RST) 5. IEEE 802.1s Multiple Spanning Tree (MST) 6. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU) 7. Internet Group Management Protocol (IGMP) Versions 2, 3; 8. Link Aggregation Control Protocol (LACP): IEEE 802.3ad 9. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów); 10. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN 11. Wsparcie sprzętowe dla tunelowania QinQ ~~i QinVNI~~ |
| 4 | **Funkcjonalność warstwy L3** | 1. Sprzętowe przełączanie pakietów w warstwie L3 2. Routing w oparciu o trasy statyczne 3. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. 4. Policy Based Routing (PBR) 5. VRRP 6. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6 7. Tunele GRE 8. Wsparcie sprzętowe dla minimum 750tyś prefixów LPM/ wpisów hosta w tablicy routingu IP 9. Wsparcie dla min. 32 VRF 10. Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP) 11. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast) 12. Wsparcie dla IGMPv3 oraz MSDP 13. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych |
| 5 | **Funkcjonalności związane z VXLAN** | 1. Zintegrowany, sprzętowy VXLAN Bridging/Routing 2. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) 3. Implementacja VXLAN BGP EVPN (Ethernet VPN) 4. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN) |
| 6 | **Mechanizmy związane z zapewnieniem jakości usług w sieci** | 1. Layer 2 IEEE 802.1p (CoS) oraz DSCP 2. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6) 3. Kolejkowanie bezwzględne (strict-priority) 4. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection) 5. Ograniczanie ruchu (policing) do zadanej przepływności 6. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych 7. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| 7 | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci** | 1. Obsługa list kontroli dostępu (ACL)    * + ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;      + ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);      + ACL oparte o porty (PACL); 2. DHCP Snooping 3. ARP Inspection 4. IP Source Guard 5. Unicast reverse path forwarding (uRPF) 6. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| 8 | **Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika** | 1. Port zarządzający 100/1000 Mbps; 2. Port konsoli CLI; 3. Zarządzanie In-band; 4. SSHv2; 5. Authentication, authorization, and accounting (AAA); 6. RADIUS; 7. TACACS+ 8. Syslog; 9. SNMP v1, v2c, v3; 10. Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB. 11. Role-Based Access Control RBAC; 12. IEEE 802.1ab LLDP 13. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) 14. 802.1x 15. Ograniczanie ruchu kierowanego do warstwy sterowania 16. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring) 17. Network Time Protocol (NTP); 18. Precision Time Protocol IEEE 1588 19. Diagnostyka procesu BOOT; 20. Ping 21. Traceroute |
| 9 | **Narzędzia programowania i zarządzania przełącznikiem** | 1. Powłoka Bash (wbudowana lub jako osobny moduł) do zarządzania systemem Unix/Linux przełącznika 2. Interfejs programistyczny REST API wraz z upublicznionym SDK |
| 10 | **Wyposażenie** | 1. dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych; 2. Obudowa o rozmiarach maksymalnie 2RU (rack unit), przeznaczona do montażu w szafie rackowej 19”. |

## **Routery BGP**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Dostarczone routery BGP muszą zapewniać wszystkie wymienione poniżej wymagania i funkcje

|  |  |  |
| --- | --- | --- |
| **LP** | **Wymagania** | |
| 1 | **Ogólne** | Urządzenie o architekturze modularnej, wyposażone w 6 interfejsów Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP lub równoważnych, a także w 2 interfejsy 10 Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP+ lub równoważnych. Interfejs 10GB musi być aktywne, jeżeli wymaga to licencji to musi być ona dostarczona. |
| 2 | **Porty** | Urządzenie musi dodatkowo umożliwiać rozszerzenie o co najmniej następujące typy interfejsów za pomocą modułów rozszerzeń:   * + 1. 1 port 10 GigabitEthernet;     2. 6 portów Gigabit Ethernet;     3. 2 interfejsy ATM STM1 lub 2 interfejsy STM4 |
| 3 | **Wydajność** | 1. Urządzenie pozwala na przełączanie z prędkością 10 Gbps i umożliwia rozbudowę wydajności do co najmniej 20 Gbps bez modyfikacji sprzętowych. 2. Urządzenie posiada dedykowany akcelerator kryptograficzny osiągający wydajność co najmniej 8 Gbps dla ruchu IMIX. |
| 4 | **Wymagane** **protokoły** | 1. Urządzenie obsługuje co najmniej 1 000 000 prefiksów w tablicach routing IPv4. 2. Urządzenie obsługuje co najmniej 1 000 000 prefiksów w tablicach routing IPv6. 3. Urządzenie obsługuje co najmniej 100000 tras multicast. 4. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP. 5. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP. 6. Urządzenie obsługuje Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja. 7. Urządzenie umożliwia uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu Forwarding) 8. Urządzenie umożliwia m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci. 9. Urządzenie obsługuje 8 000 instancji wirtualnych tablic routingu. 10. Urządzenie obsługuje funkcjonalność Bidirectional Forwarding Detection(BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego. 11. Urządzenie obsługuje funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF. 12. Urządzenie obsługuje multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN. 13. Urządzenie obsługuje protokół NHRP (ang. Next Hop Resolution Protocol). 14. Urządzenie obsługuje protokół GDOI (RFC 3547) |
| 5 | **Funkcjonalności związane z niezawodnością pracy** | 1. redundancja procesów routingowych realizowana poprzez uruchomienie dwóch kopii systemu operacyjnego, jeżeli do otrzymania tej funkcjonalności jest wymagana licencja to nie jest wymagane dostarczenie jej; 2. BFD dla OSPF, BGP, ISIS; 3. IP FRR; 4. BGP Prefix-Independent Convergence (PIC); 5. Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP; 6. funkcjonalność VRRP; 7. możliwość wymiany modułów w trakcie pracy (ang. hot swap). |
| 6 | **Obsługa MPLS** | Urządzenie musi obsługiwać MPLS, w szczególności: LDP, EoMPLS, VPLS, MPLS L3 VPN, MPLS TE, MPLS FRR w trybach protekcji łącza oraz węzła. |
| 7 | **Mechanizmy jakości usług (QoS):** | 1. klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN zarówno dla IPv4 jak iIPv6; 2. hierarchiczny QoS (H-QoS) -co najmniej 3 poziomy; 3. klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP; 4. dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek; 5. algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek; 6. możliwość obsługi jednej kolejki z priorytetem wstosunku do innych; 7. mechanizm ograniczania ilości ruchu w kolejce priorytetowej; 8. możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP –poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP; 9. możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting); 10. mechanizm WRED; 11. możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS. |
| 8 | **Funkcje i elementy bezpieczeństwa** | 1. sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu; 2. Unicast RPF (Reverse Path Forwarding); 3. listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL; 4. dostęp administracyjny oparty o role z przypisanymi uprawnieniami; 5. zasoby sprzętowe umożliwiające uruchomienie funkcjonalności zapory ogniowej typu statefull (ang. statefull firewall), przy czym zapora ogniowa:    * + - umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji),        - obsługuje ruch IPv4 oraz IPv6,        - umożliwia konfigurację polityk per wirtualna tablica routingu (VRF),−umożliwia obsługę 2 000000 równoczesnych sesji,        - umożliwia zestawianie 200000 nowych połączeń HTTP na sekundę,        - Jeżeli do otrzymania tej funkcjonalności jest wymagana licencja to nie jest wymagane dostarczenie jej. 6. zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością 5 Gbps (AES256) z obsługą 4 000 tuneli IPSec; 7. sieci VPN typu site-2-site oparte o IPSec; 8. dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP w relacji spoke to spoke w celu optymalizacji transmisji danych pomiędzy oddziałami; 9. bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast; 10. algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), w szczególności:     * + - Elliptic Curve Diffie-Hellman (ECDH),         - Galois Counter Mode Advanced Encryption Standard (GCM-AES) -128/256 bitów,         - Galois Message Authentication Code (GMAC-AES) -128/256 bitów,         - Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2,         - konfiguracja tuneli IPSec VPN w oparciu o protokół IKEv2,         - IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych,         - IKEv2 zarówno dla ruchu IPv4 jak i IPv6.l)funkcjonalność VPN per VRF; 11. Jeżeli do otrzymania funkcjonalności VPN IPSec jest wymagana licencja to nie jest wymagane dostarczenie jej; 12. ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU; 13. logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU; 14. możliwość uruchomienia funkcjonalności analizy i klasyfikacji pakietów w warstwie 2-7 polegającej na przeszukiwaniu pakietów pod kątem zawierania specyficznych ciągów znaków i wykrywania na tej podstawie ataków. |
| 9 | **Funkcjonalności zarządzania oraz wyposażenie** | 1. Urządzenie musi posiadać co najmniej 2 GB pamięci RAM. 2. Urządzenie musi posiadać redundantne zasilacze AC 230V zintegrowane w obudowie urządzenia. 3. Urządzenie umożliwia montaż w szafie 19”. 4. Urządzenie musi posiadać dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet 10/100/1000 oraz port AUX; 5. Musi posiadać port USB; 6. W ramach funkcjonalności urządzenie musi:    * + umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3;      + obsługuje Ethernet OAM (IEEE 802.3ah, IEEE 802.1ag, ITU-T Y.1731);      + obsługuje MPLS OAM;      + umożliwia pisanie skryptów konfiguracyjnych;      + obsługuje protokół Netflow ze wsparciem dla multicast oraz IPv4/IPv6;      + posiada narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP;      + posiada obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+;      + posiada możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej;−konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona      + urządzenie posiada możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów; |
| 10 | **Inne wymagania** | 1. Urządzenie umożliwia uruchomienie usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, przy czym klasyfikacja ta:    * 1. opiera się na kilku mechanizmach gwarantujących poprawne rozpoznawanie wielu aplikacji / protokołów;      2. udostępnia 3 atrybuty opisujące daną aplikację / protokół (atrybuty ułatwiają konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji / protokołów - na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji);      3. nie wymaga rozbudowy sprzętowej urządzenia, jedynie zakup licencji . 2. Urządzenie posiada możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt oraz punkt-wielopunkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE. 3. Urządzenie umożliwia ochronę kryptograficzną tuneli GRE. |

## **System bezpieczeństwa – firewall**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.

W celu utrzymania kompatybilności z systemem firewall posiadanym przez Zamawiającego w CRC, Zamawiający wymaga dostarczenia urządzeń Fortigate FOR-FG-500E (2 szt). Nie mniej jednak Zamawiający dopuszcza dostarczenie urządzeń innego producenta pod warunkiem spełnienia poniższych wymagań równoważnych.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

|  |  |  |
| --- | --- | --- |
| **LP** | **Wymagania** | |
| 1 | **Ogólne** | W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |
| 2 | **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 4. Monitoring stanu realizowanych połączeń VPN. 5. System musi umożliwiać agregację linków. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
| 3 | **Interfejsy, Dysk, Zasilanie:** | 1. System realizujący funkcję Firewall musi dysponować minimum:  * 10 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 2 gniazdami SFP+ 10 Gbps.  1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System musi być wyposażony w zasilanie AC. |
| 3 | **Parametry wydajnościowe:** | 1. W zakresie Firewall’a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 300 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 64 B. 4. Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 1518 B. 5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 14 Gbps. 6. Wydajność szyfrowania IPSec VPN nie mniej niż 20 Gbps. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 7 Gbps. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4.5 Gbps. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 5.5 Gbps. |
| 5 | **Funkcje Systemu Bezpieczeństwa:** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. |
| 6 | **Polityki, Firewall** | 1. System Firewall musi umożliwiać tworzenie list kontroli dostępu realizowanych bezstanowo przed funkcją FW. 2. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 3. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure * Cisco ACI. * Google Cloud Platform (GCP). * Nuage Networks VSP. * OpenStack. * VMware vCenter (ESXi). * VMware NSX. |
| 7 | **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. * Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |
| 8 | **Routing i obsługa łączy WAN** | W zakresie routingu rozwiązanie powinno zapewniać obsługę:   * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |
| 9 | **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| 10 | **Ochrona przed malware** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |
| 11 | **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| 12 | **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| 13 | **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |
| 14 | **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| 15 | **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |
| 16 | **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. |
| 17 | **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. |
| 18 | **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:   * Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.   Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. |

## **Agregator logów**

Należy podać producenta, model oraz dokładny numer katalogowy wraz ze wszystkimi modułami i licencjami, które wskazują na spełnienie poniższych wymagań:

|  |  |
| --- | --- |
| **Producent** |  |
| **Model** |  |
| **Numer katalogowy** |  |
| **Wyposażenie/licencje/**  **oprogramowanie** |  |

**Wymagania Ogólne**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

|  |  |  |
| --- | --- | --- |
| **LP** | **Wymagania** | |
| 1 | **Interfejsy, Dysk, Zasilanie:** | 1. System musi dysponować co najmniej:  * 2 portami Gigabit Ethernet RJ-45. * 2 gniazdami SFP 1 Gbps.  1. Rozwiązanie musi dysponować powierzchnią dyskową min. 8 TB. 2. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0, 1. 3. System musi być wyposażony w zasilanie AC. |
| 2 | **Parametry wydajnościowe:** | 1. System musi być w stanie przyjmować minimum 150 GB logów na dzień. 2. System musi być w stanie przeanalizować minimum 4500 logów na sekundę. 3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 170 systemów. |
| 3 | **Logowanie** | 1. Podgląd logowanych zdarzeń w czasie rzeczywistym. 2. Możliwość przeglądania logów historycznych z funkcją filtrowania. 3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:   Listę najczęściej wykrywanych ataków.  Listę najbardziej aktywnych użytkowników.  Listę najczęściej wykorzystywanych aplikacji.  Listę najczęściej odwiedzanych stron www.  Listę krajów , do których nawiązywane są połączenia.  Listę najczęściej wykorzystywanych polityk Firewall.  Informacje o realizowanych połączeniach IPSec.   1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |
| 4 | **Raportowanie** | W zakresie raportowania system musi zapewniać:   1. Generowanie raportów co najmniej w formatach: PDF, CSV. 2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3. Funkcję definiowania własnych raportów. 4. Możliwość spolszczenia raportów. 5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |
| 5 | **Korelacja logów** | W zakresie korelacji zdarzeń system musi zapewniać:   1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:  * Malware. * Aplikacje sieciowe. * Email. * IPS. * Traffic. * Systemowe: utracone połączenie VPN, utracone połączenie sieciowe. |
| 6 | **Zarządzanie** | 1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.   a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.   1. System musi umożliwiać definiowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |
| 7 | **Serwisy i licencje** | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| 8 | **Rozszerzone wsparcie serwisowe** | 1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy. 2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 przez serwisowy moduł internetowy oraz infolinię w języku polskim 8x5. Oferent winien przedłożyć dokumenty:  * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne  o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 podmiotu serwisującego.   Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. |

# **Dodatkowe wymagania oraz warunki dostawy sprzętu i oprogramowania**

1. Wykonawca opracuje plan dostaw realizowanych przez Wykonawcę. Plan dostaw musi zawierać:

* szczegółowy harmonogram dostaw do miejsca wskazanego przez Zamawiającego,
* procedurę odbioru jakościowego,
* procedurę zmian terminów w trakcie realizacji dostaw,
* procedurę obsługi uszkodzeń sprzętu w trakcie dostawy,
* specyfikację niezbędnych dokumentów i protokołów potwierdzających prawidłowość dostaw.

1. Wykonawca dostarczy całość sprzętu w miejsce wskazane przez Zamawiającego w godzinach od 8:00 do 16:00 w dni robocze od poniedziałku do piątku.
2. Odbiory sprzętu odbędą się w umówionym terminie przy obecności wyznaczonych pracowników ANK lub NAC
3. Wykonawca zapewni we własnym zakresie środki transportu oraz zasoby ludzkie umożliwiające rozładunek i transport sprzętu do pomieszczeń wskazanych przez Zamawiającego.
4. Wykonawca jest zobowiązany do wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania.
5. Wykonawca musi zapewnić, że wszystkie dostarczane sprzęty jak i oprogramowania są ze sobą kompatybilne w zakresie, w jakim wymagana jest ich wzajemna współpraca.
6. Wszystkie urządzenia muszą zawierać osprzęt wymagany przez producentów oferowanego rozwiązania (na przykład: okablowanie energetyczne, urządzenia zasilające) niezbędny do jego prawidłowego podłączenia z siecią energetyczną Zamawiającego o parametrach: 230 V ± 10% , 50 Hz
7. Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (tzn. bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej, urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania.
8. Urządzenia muszą pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń: odnawianych, demonstracyjnych lub powystawowych.
9. Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
10. Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz wszystkie muszą być objęte gwarancją producenta.
11. Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
12. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
13. Wykonawca dostarczy wszystkie licencje i klucze licencyjne wymagane do działania dostarczanego sprzętu i oprogramowania
14. W przypadku, gdy licencja oprogramowania objęta jest opłatą okresowej opieki wówczas Wykonawca poda wszystkie dane umożliwiające przedłużenie czasu opieki przez Zamawiającego

# **Rozwiązania równoważne**

W sytuacji, gdy w opisie przedmiotu zamówienia wskazywane by były znaki towarowe wskazujące na konkretne rozwiązania, w myśl artykułu 29 ust. 3 ustawy PZP, Zamawiający dopuszcza składanie ofert na produktach równoważnych, pochodzących od innych producentów, spełniających minimalne wymagania określone w niniejszym Opisie Przedmiotu Zamówienia. Udowodnienie równoważności rozwiązań spoczywa na Wykonawcy.

Zawarte w dokumentacji nazwy producenta mają na celu jedynie wskazanie oczekiwanego przez Zamawiającego wzorca jakości przedmiotu Zamówienia.

Zamawiający stosując nazwy produktów wskazuje jedynie jakościowe wymagania, przez co dopuszcza składanie ofert zawierających równoważnych o parametrach jakościowych oraz cechach użytkowych, spełniających co najmniej przedstawione wymagania.

Obowiązkiem oferenta jest udowodnienie że produkt, przez niego zaproponowany spełnia te wymagania. Służyć mogą temu zapisy zawarte w ogólnie dostępnych źródłach, katalogach lub stronach internetowych producentów.

Wykonawca do udowodnienia równoznaczności jest zobowiązany do wykazania że oferowane przez niego urządzenia oraz ich części składowe spełniają wymagania minimalne poprzez dostarczenie kart charakterystyki technicznej, certyfikatów, katalogów, opisów technicznych dotyczących tych urządzeń oraz ich elementów. Zamawiający zastrzega sobie możliwość wezwania Wykonawcy do przedstawienia oferowanego rozwiązania w celu udowodnienia jego równoważności.

# **Scenariusze testów**

Zamawiający będzie wymagał opracowania scenariuszy testów dostarczanej infrastruktury według poniższego zestawienia.

|  |  |  |  |
| --- | --- | --- | --- |
| **Numer testu** | **Nazwa testu** | **Opis testu** | **Oczekiwany rezultat testu** |
|  | Symulacja awarii Operatora | * Głównym celem testu jest zasymulowanie awarii jednego z Operatorów świadczących usługi dostępu do sieci dla ZRC. * Test należy przeprowadzić dla wszystkich Operatorów uwzględnionych w architekturze. | Podczas awarii jednego z Operatorów musi zostać automatycznie użyty alternatywny Operator w celu zapewnienia ciągłości dostępu do sieci. |
|  | Symulacja awarii pojedynczego fizycznego połączenie z routera BGP do Operatora | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy routerem BGP a Operatorem. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kabla z routera BGP lub wyłączenia portu, w który wpięty jest Operator. * Test należy przeprowadzić dla każdego połączenie z routera BGP do Operatora. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego fizycznego połączenia routera BGP do Firewall i z Firewall do routera BGP | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy routerem BGP a Firewall oraz między Firewall a routerem BGP. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kabla z routera BGP lub wyłączenia portu na jednym z urządzeń, w który wpięty jest Operator. * Test musi być przeprowadzony dla wszystkich połączeń pomiędzy tymi urządzeniami. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego routera BGP | * Celem testu jest zasymulowanie awarii pojedynczego routera BGP. * Test musi być przeprowadzony dla wszystkich routerów BGP. * Test może być przeprowadzony na zasadzie fizycznego odłączenia routera BGP od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne uruchomienie i wykorzystanie alternatywnego zapasowego routera BGP. |
|  | Symulacja awarii pojedynczego Firewall | * Celem testu jest zasymulowanie awarii pojedynczego urządzenia Firewall. * Test musi być przeprowadzony dla wszystkich urządzeń Firewall. * Test może być przeprowadzony na zasadzie fizycznego odłączenia urządzenia Firewall od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne uruchomienie i wykorzystanie alternatywnego zapasowego urządzenia Firewall. |
|  | Symulacja awarii pojedynczego fizycznego połączenia między routerem BGP a przełącznikiem Core lub pomiędzy przełącznikiem Core a routerem BGP | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy routerem BGP a przełącznikiem Core lub pomiędzy przełącznikiem Core a routerem BGP. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kabla z routera BGP lub wyłączenia portu na jednym z urządzeń, w który wpięty jest Operator. * Test musi być przeprowadzony dla wszystkich połączeń pomiędzy tymi urządzeniami. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego fizycznego połączenia między przełącznikiem Core a urządzeniem Firewall | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy przełącznikiem Core a urządzeniem Firewall lub pomiędzy urządzeniem Firewall i przełącznikiem Core. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kabla z przełącznika Core lub wyłączenia portu na jednym z urządzeń, w który wpięty jest Operator. * Test musi być przeprowadzony dla wszystkich połączeń pomiędzy tymi urządzeniami. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego przełącznika Core | * Celem testu jest zasymulowanie awarii pojedynczego przełącznika Core. * Test musi być przeprowadzony dla wszystkich przełączników Core. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika Core od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne uruchomienie i wykorzystanie alternatywnego zapasowego przełącznika Core. Mowa tu o wszystkich urządzeniach, które posiadają połączenia do przełącznika testowanego. |
|  | Symulacja awarii fizycznego połączenia pomiędzy przełącznikami Core | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy przełącznikami Core. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kabla z przełącznika Core lub wyłączenia portu na jednym z urządzeń, w który wpięty jest Operator. * Test musi być przeprowadzony dla wszystkich fizycznych połączeń pomiędzy tymi urządzeniami. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. Do zapewnienia połączenia muszą zostać wykorzystane przełączniki tranzytowe. |
|  | Symulacja awarii fizycznego połączenia pomiędzy przełącznikiem Core a Przełącznikiem Tranzytowym A lub pomiędzy przełącznikiem Tranzytowym A i przełącznikiem Core | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy przełącznikiem Core a przełącznikiem Tranzytowym A lub przełącznikiem Tranzytowym A i przełącznikiem Core. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kabla z przełącznika Core lub wyłączenia portu na jednym z urządzeń, w który wpięty jest Operator. * Test musi być przeprowadzony dla wszystkich fizycznych połączeń pomiędzy tymi urządzeniami. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii fizycznego połączenia pomiędzy przełącznikiem Core a Przełącznikiem Tranzytowym B lub pomiędzy przełącznikiem Tranzytowym B i przełącznikiem Core | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy przełącznikiem Core a przełącznikiem Tranzytowym B lub przełącznikiem Tranzytowym B i przełącznikiem Core. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kabla z przełącznika Core lub wyłączenia portu na jednym z urządzeń, w który wpięty jest Operator. * Test musi być przeprowadzony dla wszystkich fizycznych połączeń pomiędzy tymi urządzeniami. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego przełącznika Tranzytowego | * Celem testu jest zasymulowanie awarii pojedynczego przełącznika Tranzytowego. * Test musi być przeprowadzony dla wszystkich przełączników Tranzytowych. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika Tranzytowego od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne uruchomienie i wykorzystanie alternatywnego zapasowego przełącznika Tranzytowego. |
|  | Symulacja awarii pojedynczego połączenia przełącznika Core do hosta lub między hostem i przełącznikiem Core | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy przełącznikiem Core a hostem lub pomiędzy hostem a przełącznikiem Core. * Test musi być przeprowadzony dla wszystkich hostów oraz przełączników Core. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika Core od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego hosta w ZRC | * Celem testu jest zasymulowanie awarii pojedynczego hosta. * Test musi być przeprowadzony dla wszystkich hostów. * Test może być przeprowadzony na zasadzie fizycznego odłączenia hosta od zasilania. | Wynikiem przeprowadzonego testu musi być restart działających maszyn wirtualnych na innym, działającym hoście. |
|  | Symulacja awarii dysków twardych w hoście | * Celem testu jest zasymulowanie awarii dysków twardych w hoście. * Test musi być wykonany dla minimum dwóch dysków twardych. * Test może być przeprowadzony na zasadzie fizycznego wyciągnięcia dysku twardego z serwera. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe działanie maszyn wirtualnych na danym hoście. |
|  | Symulacja awarii pojedynczego połączenia pomiędzy przełącznikiem Core a systemem kontrolera zasobów dyskowych lub pomiędzy systemem kontrolera zasobów dyskowych a przełącznikiem Core | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy przełącznikiem Core i systemem kontrolera zasobów dyskowych lub pomiędzy systemem kontrolera zasobów dyskowych a przełącznikiem Core. * Test musi być przeprowadzony dla wszystkich przełączników Core oraz systemem kontrolera zasobów dyskowych. * Test może być przeprowadzony na zasadzie fizycznego odłączenia portu lub wyłączenia portu na przełączniku. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego połączenia pomiędzy przełącznikiem Core a serwerem Backup lub pomiędzy serwerem Backup a przełącznikiem Core | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy przełącznikiem Core a serwerem Buckup lub pomiędzy serwerem Backup a przełącznikiem Core. * Test musi być przeprowadzony dla wszystkich przełączników Core oraz serwerów Backup. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika Core od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego połączenia pomiędzy przełącznikiem Core a agregatorem logów lub pomiędzy agregatorem logów a przełącznikiem Core | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia pomiędzy przełącznikiem Core i agregatorem logów lub pomiędzy agregatorem logów a przełącznikiem Core. * Test musi być przeprowadzony dla wszystkich przełączników Core oraz agregatorów logów. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika Core od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego połączenia FC pomiędzy przełącznikiem FC a serwerem Backup lub pomiędzy serwerem Backup a przełącznikiem FC | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia FC pomiędzy przełącznikiem FC a serwerem Backup lub pomiędzy serwerem Backup a przełącznikiem FC * Test musi być przeprowadzony dla wszystkich przełączników FC oraz serwerów Backup. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika FC od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne bezprzerwowe przełączenie się „uszkodzonego” portu na inny zapasowy. |
|  | Symulacja awarii pojedynczego kontrolera zasobów dyskowych | * Celem testu jest zasymulowanie awarii pojedynczego kontrolera zasobów dyskowych. * Test musi być przeprowadzony dla wszystkich kontrolerów zasobów dyskowych. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kontrolera zasobów dyskowych od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne uruchomienie i wykorzystanie alternatywnego zapasowego kontrolera zasobów dyskowych. |
|  | Symulacja awarii pojedynczego połączenia FC pomiędzy kontrolerem zasobów dyskowych a przełącznikiem FC lub pomiędzy przełącznikiem FC a kontrolerem zasobów dyskowych | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia FC pomiędzy kontrolerem zasobów dyskowych a przełącznikiem FC lub pomiędzy przełącznikiem FC a kontrolerem zasobów dyskowych. * Test musi być przeprowadzony dla wszystkich przełączników FC oraz kontrolerów zasobów dyskowych. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika FC od zasilania. | Wynikiem przeprowadzonego testu musi być zachowana ciągłość połączenia. |
|  | Symulacja awarii pojedynczego przełącznika FC | * Celem testu jest zasymulowanie awarii pojedynczego przełącznika FC. * Test musi być przeprowadzony dla wszystkich przełączników FC. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika FC od zasilania. | Wynikiem przeprowadzonego testu musi być zachowana ciągłość połączenia. |
|  | Symulacja awarii pojedynczego połączenia FC pomiędzy macierzą a przełącznikiem FC lub pomiędzy przełącznikiem FC a macierzą. | * Celem testu jest zasymulowanie awarii pojedynczego fizycznego połączenia FC pomiędzy macierzą a przełącznikiem FC lub pomiędzy przełącznikiem FC a macierzą. * Test musi być przeprowadzony dla wszystkich przełączników FC oraz macierzy. * Test może być przeprowadzony na zasadzie fizycznego odłączenia przełącznika FC od zasilania. | Wynikiem przeprowadzonego testu musi być zachowana ciągłość połączenia. |
|  | Symulacja awarii pojedynczej macierzy dla kontrolera zasobów dyskowych | * Celem testu jest zasymulowanie awarii pojedynczej macierzy dla kontrolera zasobów dyskowych * Test musi być przeprowadzony dla wszystkich macierzy dla kontrolerów zasobów dyskowych. * Test może być przeprowadzony na zasadzie fizycznego odłączenia macierzy od zasilania. | Wynikiem przeprowadzonego testu musi być zachowana ciągłość połączenia. |
|  | Symulacja awarii pojedynczej macierzy | * Celem testu jest zasymulowanie awarii pojedynczej macierzy. * Test musi być przeprowadzony dla wszystkich macierzy. * Test może być przeprowadzony na zasadzie fizycznego odłączenia macierzy od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne uruchomienie i zachowanie ciągłości połączenia z wykorzystaniem alternatywnej macierzy. |
|  | Symulacja przełączenia usług z CRC do ZRC | * Test musi obejmować przełączenie awaryjne usług z CRC do ZRC w sposób ręczny lub/i automatyczny. * Testy będą obejmować usługi wykorzystujące przestrzeń dyskową, np. serwer WWW, Active Directory. | Wynikiem testu musi być przywrócenie usług do pełnej funkcjonalności w ZRC, działających uprzednio w CRC. Pełna funkcjonalność oznacza takie samo działanie usług, jak przed przełączeniem do ZRC. |
|  | Symulacja przełączenia z ZRC do CRC | * Test musi obejmować przełączenie usług z ZRC do CRC w sposób ręczny lub/i automatyczny. * Testy będą obejmować usługi wykorzystujące przestrzeń dyskową, np. serwer WWW, Active Directory. | Wynikiem testu musi być przywrócenie usług do pełnej funkcjonalności w CRC, działających uprzednio w ZRC. Pełna funkcjonalność oznacza takie samo działanie usług, jak przed przełączeniem do CRC. |
|  | Test replikacji plików | * Test ma na celu utworzenie plików na zasobie znajdującym się w CRC oraz wykonanie automatycznej lub ręcznej replikacji danych do ZRC. * Celem testu jest zweryfikowanie zreplikowanych plików z CRC. | Wynikiem testu musi być poprawne odczytanie zreplikowanych danych w ZRC. Test powinien zakończyć się w określonych ramach czasowych. Założeniem jest replikacja 100GB danych testowych w ciągu 12 godzin. |
|  | Symulacja awarii kontrolerów zasobów dyskowych | * Celem testu jest zasymulowanie awarii kontrolerów zasobów dyskowych. * Test musi być przeprowadzony dla wszystkich kontrolerów zasobów dyskowych w ZRC. * Test może być przeprowadzony na zasadzie fizycznego odłączenia kontrolera zasobów dyskowych od zasilania. | Wynikiem przeprowadzonego testu musi być automatyczne/ręczne uruchomienie i wykorzystanie alternatywnego zapasowego kontrolera zasobów dyskowych w drugiej lokalizacji. |
|  | Test wykonania kopii zapasowych i przywrócenia | * Celem testu jest wykonanie kopii zapasowych w CRC oraz testowe przywrócenie wykonanych kopii. | Wynikiem testu jest utworzenie kopii zapasowych wraz z ich przetestowaniem. |
|  | Test replikacji kopii zapasowych do ZRC | * Celem testu jest wykonanie replikacji kopii zapasowych do ZRC. | Wynikiem testu musi być poprawna replikacja danych kopii zapasowych do ZRC. |
|  | Test przywrócenia kopii zapasowych w ZRC | * Celem testu jest przywrócenie kopii zapasowych w ZRC. | Wynikiem testu musi być poprawne przywrócenie plików/danych/usług z kopii zapasowych w ZRC. |
|  | Test przypadków awarii zasilania wraz z testem automatycznego i poprawnego zamknięcia systemów serwerowych | * Celem testu jest zasymulowanie awarii zasilania przed UPSami. * Dodatkowo celem testu jest sprawdzenie czy systemy serwerowe zostaną automatycznie i poprawnie zamknięte w przypadku wystąpienia awarii zasilania. | Wynikiem testu musi być poprawne i automatyczne przełączenie się infrastruktury na zasilanie z UPSów  Dodatkowo wynikiem testów musi być automatyczne i poprawne zamknięcie się systemów serwerowych. |

# **Dokumentacja powykonawcza**

Wykonawca opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis połączeń zainstalowanych komponentów, instalacji i konfiguracji zainstalowanych komponentów infrastruktury ZRC. Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej, a także w wersji pdf. Na żądanie Zamawiającego Wykonawca dostarczy dokument w wersji drukowanej.

Dodatkowo Wykonawca opracuje dokumentację dla administratorów IT ZRC. Dokumentacja ta powinna zawierać co najmniej:

* Procedury bieżących działań administracyjno-eksploatacyjnych
* Procedury instalacji i konfiguracji
* Procedury okresowych/planowanych działań administracyjnych
* Procedury aktualizacji standardowych elementów dostarczonego sprzętu
* Procedury włączenia i wyłączenia całości dostarczanego sprzętu w przypadku prac planowych.

Jako procedurę eksploatacyjną rozumie się opis zbioru czynności eksploatacyjnych mających na celu zrealizowane określonego zadania eksploatacyjnego np. wykonanie aktualizacji oprogramowania typu firmware. Procedury muszą obejmować wszystkie czynności, jakie należy wykonać w celu monitorowania i utrzymania dostarczonej infrastruktury w poprawnym działaniu i zgodności z najnowszymi wersjami komponentów. Procedury zostaną przetestowane przez Zamawiającego przy udziale inżyniera Wykonawcy.

Dokumentacja dostarczona w trakcie realizacji zamówienia musi być wykonana w sposób spójny, zgodnie z dobrymi praktykami i zaleceniami budowy tego typu dokumentów.

## **Cechy dokumentacji dostarczonej w ramach projektu**

Dokumentacja musi zawierać spis treści, strony dokumentów muszą posiadać numerację, załączniki muszą zostać opisane w sposób jasny i ułatwiający ich identyfikacje.

Całość dokumentacji projektowej musi być dostarczona w segregatorze umożliwiającym wypięcie dowolnej strony z dokumentacji i wpięcie jej z powrotem oraz dodatkowo w wersji elektronicznej w postaci pliku tekstowego w popularnym formacie (Microsoft Office, OpenOffice etc.).

Wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzować się muszą wysoką jakością, na którą będą miały wpływ takie czynniki jak:

1. Czytelna i zrozumiała struktura zarówno poszczególnych dokumentów jak i całej dokumentacji z podziałem na rozdziały, podrozdziały i sekcje;
2. Zachowanie standardów, a także sposób pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów oraz fragmentów tego samego dokumentu jak również całej dokumentacji;
3. Kompletność dokumentu, rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia. Oznacza to w szczególności jednoznaczne i wyczerpujące przedstawienie wszystkich zagadnień w odniesieniu do systemu.
4. Spójność i niesprzeczność dokumentu, rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.
5. Nomenklatura użyta w dokumentacji musi być spójna z dokumentacją przetargową.

Cała dokumentacja, o której mowa powyżej, musi być zaakceptowana przez Zamawiającego. Wykonawca przeniesie na Zamawiającego całość majątkowych praw autorskich do stworzonej dokumentacji.

# **Szkolenie**

W ramach prowadzonego postępowania Wykonawca zapewni i opracuje:

* szkolenia i warsztaty z dostarczanych produktów infrastruktury techniczno-systemowej. Przewidywana ilość uczestników warsztatów to od 3 do 9 osób wskazanych przez Zamawiającego,
* plan warsztatów/szkoleń z zakresu wdrażanej infrastruktury. Warsztaty z zakresu każdego z typów urządzeń dostarczanych w ramach przedmiotowego postępowania powinny trwać przynajmniej:

|  |  |  |
| --- | --- | --- |
| LP | Nazwa | Ilość godzin\* |
| 1 | Platforma hiperkonwergentna | 16 |
| 2 | Kontrolera zasobów dyskowych | 16 |
| 3 | System macierzy dyskowych | 16 |
| 4 | System backup wraz z dedykowanym serwerem | 8 |
| 5 | Przełączniki SAN | 16 |
| 6 | Przełączniki rdzeniowe | 16 |
| 7 | Routery BGP | 8 |
| 8 | System bezpieczeństwa - firewall | 8 |
| 9 | Agregator logów | 8 |

\*Przy czym szkolenie nie może trwać dłużej niż 8 godzin dziennie

Dodatkowo szkolenia powinny uwzględniać uwarunkowania montażu i instalacji sprzętu w infrastrukturze Zamawiającego.

Warsztaty odbędą się w siedzibie Zamawiającego lub online. Warsztaty będą prowadzone w języku polskim. Osoba prowadzące będą posiadać odpowiednią wiedzę, przygotowanie merytoryczne umożliwiające przekazanie informacji z zakresu wdrożonych rozwiązań. Wykonawca zobowiązany będzie do przygotowania i przedstawienia Zamawiającemu, co najmniej na 5 dni przed rozpoczęciem warsztatów, odpowiednich materiałów szkoleniowych oraz harmonogram warsztatów, włączając w to materiały dla uczestników. Zamawiający zastrzega sobie prawo do żądania wprowadzenia poprawek i zmian do materiałów szkoleniowych. Harmonogram zajęć powinien zawierać:

* informacje dotyczące czasu i miejsca realizacji danego warsztatu lub szkolenia,
* informacje dotyczące tematyki prowadzonych zajęć z podziałem na zajęcia teoretyczne i praktyczne
* informacje dotyczące wiedzy i umiejętności, jakie zdobędą uczestnicy po zakończeniu szkoleń i warsztatów.

Każdy uczestnik szkolenia otrzyma certyfikat jego ukończenia. W ramach warsztatów/szkoleń uczestnicy otrzymają komplet materiałów szkoleniowych w wersji papierowej oraz elektronicznej obejmujących swoim zakresem całe szkolenie. Wszystkie materiały szkoleniowe muszą być w języku polskim lub angielskim. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych

Szkolenia/warsztaty zostaną zrealizowane w postaci voucherów z zakresu wdrażanych rozwiązań sprzętowych. Vouchery będą ważne co najmniej 12 miesięcy od dnia podpisania Protokołu Odbioru Końcowego.

Ponadto Zamawiający oczekuje dostawy 2 szt voucherów na szkolenia, z każdego niżej wymienionego zakresu. Vouchery muszą być ważne min. 12 miesięcy od daty dostawy. Vouchery będą uprawniać do odbycia szkolenia w autoryzowanych Centrach Szkoleniowych Producentów na terenie Polski:

|  |  |  |
| --- | --- | --- |
| LP | Nazwa | Ilość voucherów |
| 1 | Platforma hiperkonwergentna  A) Platforma sprzętowa  B ) System SDS  C) System wirtualizacji | A) 2  B) 2  C) 2 |
| 2 | Kontrolera zasobów dyskowych | 2 |
| 3 | System macierzy dyskowych | 2 |
| 4 | System backup wraz z dedykowanym serwerem | 2 |
| 5 | Routery BGP | 2 |

# **Wdrożenie**

Wykonawca jest zobowiązany przestrzegać obowiązujących norm oraz przepisów związanych w wykonywaniem przedmiotu Zamówienia. Wykonawca odpowiada za wszelkie uszkodzenia powstałe w ramach jego prac, oraz jest zobowiązany do ich naprawy na własny koszt.

Zamawiający wymaga wykonanie wdrożenia obejmującego swoim zakresem minimum

* Instalacja okablowania energetycznego dostarczanych urządzeń ,
* Instalacja okablowania strukturalnego/logicznego dostarczanych urządzeń,
* Instalacja dostarczonego urządzeń wchodzących w skład dostarczanej infrastruktury ZRC
* Wykonanie aktualizacji firmware wszystkich dostarczanych komponentów infrastruktury ZRC
* Wykonanie aktualizacji systemów operacyjnych
* Podłączenie infrastruktury ZRC do sieci elektrycznej oraz oznaczenie połączeń,
* Podłączenie urządzeń do sieci SAN oraz oznaczenie połączeń,
* Podłączenie urządzeń do sieci LAN oraz oznaczanie połączeń,
* Rekonfiguracja przełączników SAN: aliasy, zony, konfiguracje
* Rekonfiguracja przełączników LAN: vlan, trunk, lacp

Poniżej przedstawiono bardziej szczegółowy opis wdrożenia niektórych elementów systemu.

#### **Wdrożenie platformy hiperkonwergentnej**

W ramach wdrożenia platformy hiperkonwergentnej Wykonawca wykona:

1. Instalację, podłączenie, uruchomienie oraz skonfigurowanie platformy w lokalizacji Zamawiającego
2. Wykonanie konfiguracji HA CommServe Stand By
3. Dostawę wszystkich niezbędnych elementów koniecznych do montażu i uruchomiania urządzeń tj. pasywnego sprzętu sieciowego i okablowania
4. Instalacji serwerów fizycznych
5. Instalacji systemu hiperkonwergetnego na dostarczonych serwerach
6. Konfiguracja klastra wirtualizacyjnego
7. Konfiguracja DNS, NTP, SMTP, powiadomień
8. Konfiguracja uprawnień do systemu
9. Instalacja testowych maszyn wirtualnych
10. Wykonanie konfiguracji HA CommServe Stand By
11. Konfiguracja roli Media Agent na serwerze (Disk Library, bazy deduplikacji, Index Cache)
12. Aktualizacja systemu CommVault do aktualnej wersji i Service Pack (CommServe, Media Agencji, wszystkie iDA),
13. Rekonfiguracja CTE: subclients, Storage Polices, Schedule Polices, Auxliary Copies
14. Instalacja iDA dla VMware/Hyper-V
15. Instalacja FRE
16. Konfiguracja nowych pseudoklientów VMware/Hyper-V, iDA FS, iDA MS SQL, iDA Oracle
17. Wykonanie backup całego środowiska
18. Wykonanie odtwarzania danych (pełnych maszyn, plików maszyn, plików systemu gościa)
19. Wykonanie testu przełączenia środowiska na serwer StandBy wraz z powrotem na serwer trzeci,
20. Wykonanie testów akceptacyjnych dostarczonych urządzeń (awaria dysku, karty IO, kontrolera, zasilania, SFP+)
21. Konfigurację urządzeń zgodnie z zaakceptowaną dokumentacją przedwdrożeniową

Wdrożenie platformy hiperkonwergentnej musi być realizowane przez autoryzowanych inżynierów producenta posiadających certyfikat maksymalnie o jeden poziom niższy od najwyższego na ścieżce certyfikacyjnej producenta, uprawniający do realizacji prac.

Wykonawca zobowiązany jest do dokumentowania wszystkich czynności realizowanych w ramach wdrożenia Platformy HCI

#### **Wdrożenie Kontrolera Zasobów dyskowych**

W ramach kontrolera zasobów dyskowych Wykonawca wykona:

1. Instalację urządzeń w szafach RACK
2. Konfigurację elementów wchodzących w skład systemu:
   1. Konfiguracja serwera będącego 1 węzłem (hostname, adresacja)
   2. Konfiguracja macierzy metadanych
   3. Konfiguracja serwera będącego 2 węzłem (hostname, adresacja)
3. Testy prawidłowego działania failover`u
4. Konfigurację macierzy na których utworzony zostanie filesystem:
   1. Konfiguracja podstawowa (adresacja, hostname itp.)
   2. Konfiguracja zasobów (raid-groupy, volumeny, luny)
   3. Konfiguracja mapowania
5. Konfigurację odpowiedniego zoningu
6. Konfigurację zasobów wystawionych z macierzy na systemie Stornext (labelowanie lunów)
7. Konfigurację filesystemów
   1. Ustawienie odpowiednich parametrów FS w zależności od używanych macierzy
   2. Testy dostępności utworzonego FS
   3. Testy wydajności utworzonego FS
8. W przypadku korzystania z SAN Clientów:
   1. Instalacja aplikacji klienckich na odpowiednich hostach
   2. Wykonanie odpowiedniego zoningu
   3. Konfiguracja mapowania FS na systemach klienckich
9. Zestawienie replikacji z Quantum StorNext w NAC w Warszawie.

#### **Wdrożenie Systemu backupu wraz z dedykowanym serwerem**

Przed przystąpieniem do prac wdrożeniowych zostanie przeprowadzone przez Wykonawcę rozpoznanie środowiska informatycznego Zamawiającego. Wykonawca wykona instalację i wdrożenie systemu po akceptacji przez Zamawiającego dokumentacji przedwdrożeniowej

W ramach systemu backupu Wykonawca wykona:

1. Instruktaż wstępny – w siedzibie Zamawiającego – dla administratorów systemu
2. Instalację, konfigurację i integrację systemu z pozostałą infrastrukturą.
3. Instalacja podłączeni i skonfigurowanie serwera
4. Implementację polityk backupu dla maszyn wirtualnych.
5. Implementację polityk backupu dla serwerów bazodanowych, aplikacyjnych oraz serwerów plikowych.
6. Przygotowanie instrukcji Disaster Recovery dla wdrożonego systemu.
7. Zestawienie replikacji, środowiska wirtualnego, przy pomocy wewnętrznych mechanizmów oprogramowania CommVault lub równoważnego, pomiędzy ośrodkami NAC w Warszawie (środowisko oparte na VMware vSphere) i ANK w Krakowie (nowo dostarczane środowisko wirtualne)
8. Wykonanie testów odtworzeniowych dla wskazanych przez Zamawiającego systemów w ramach ustalonego harmonogramu.
9. Instalacja usług proxy dla VMware/Hyper-V

Wykonawca powinien posiadać status partnera producenta systemu. Wdrożenie systemu backupu musi być realizowane przez autoryzowanych inżynierów producenta posiadających certyfikat CommVault Certified Master lub równoważnego.

#### **Wdrożenie przełączników SAN**

W ramach systemu backupu Wykonawca wykona:

1. Instalację przełączników w szafie RACK
2. Konfigurację podstawowych parametrów (m.in. hostname, adres IP, domain ID)
3. Podłączanie urządzeń do przełącznika zgodnie z zaakceptowaną dokumentacją przedwdrożeniową
4. Uruchomienie na połączeniach ISL między switchami sprzętowe szyfrowanie AES-GCM z kluczem szyfrującym długości min. 128-bitów
5. Uruchomienie na połączeniach ISL między switchami sprzętową kompresję danych
6. Uruchomienie na połączeniach ISL między switchami mechanizm agregacji połączeń realizujący balansowanie danych na poziomie pojedynczych ramek.
7. Uruchomienie wbudowany w przełączniki mechanizm monitorowania wkładek SFP. Dla wszystkich zainstalowanych wkładek SFP należy zapewnić monitorowanie wartości prądu (mA), mocy odbiorczej (uW), mocy nadawczej (uW), tempertury (C), napięcia (mV). W przypadku gdy monitorowane wartości zaczną odbiegać od wartości zalecanych przez producenta, mechanizm należy tak skonfigurować aby wysyłał email na wskazane adresy administratorów, umieszczał odpowiedni komunikat w logu systemowym przełącznika oraz wysyłał trap SNMP
8. Wykonanie konfiguracji zoningu

# **Gwarancja**

1. Całość dostarczonego sprzętu i oprogramowanie musi być objęta 3 letnim serwisem i gwarancją
2. Zgłoszenia awarii następować będzie w trybie 8/5/NBD i musi być dokonywane w postaci: zgłoszenia telefonicznego, z wykorzystaniem serwisu www lub za pomocą poczty elektronicznej, wszystkie wymienione kanały komunikacji muszą być świadczone w języku polskim.
3. W ramach gwarancji Wykonawca zapewni następujące usługi:

* zdalne wsparcie techniczne Wykonawcy i producenta,
* wsparcie w miejscu instalacji
* części zamienne oraz ich instalację,
* uaktualnienia oraz instalację oprogramowania firmware, jeżeli takie uaktualnienia są rekomendowane przez Producenta
* dostęp do internetowych narzędzi serwisowych

1. Wykonawca jest zobowiązany do niezwłocznego potwierdzenia przyjęcia zgłoszenia na adres poczty elektronicznej, podany przez Zamawiającego lub telefonicznie - na numer podany podczas rejestracji zgłoszenia (czas reakcji).
2. Zamawiający musi mieć możliwość bezpośredniego zgłaszania awarii do producenta sprzętu oraz samodzielnej aktualizacji oprogramowania.
3. W okresie obowiązywania serwisu gwarancyjnego wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Uszkodzone dyski podlegające gwarancji stanowią własność Zamawiającego i pozostają u Zamawiającego, nie podlegają zwrotowi w ramach usługi gwarancyjnej
4. Usługi gwarancyjne muszą być realizowane przez autoryzowany serwis producenta albo przez Wykonawcę na terenie Polski
5. Gwarantowany czas naprawy lub dostawy nowego urządzenia wynosi maksymalnie 15 dni roboczych od momentu zgłoszenia problemu. Termin ten uwzględnia również wykonanie niezbędnych prac związanych z instalacją lub uruchomieniem naprawianych elementów.