Załącznik nr 1 do oferty

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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| --- | --- | --- | --- |
| 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 = 1 minuta. 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 = 1 minuta. 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 . | Model procesora  ……………….  Ilość Pamięci RAM  ………………….  Ilość portów Ethernet 25Gb  ………………. |
| 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 | Oferowana przestrzeń dyskowa:  …………………… |
| 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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
|  | **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. | Podać parametry oferowanych serwerów:  ………………….. |
|  | **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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
|  | **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. | Podać pojemność dla każdej macierzy wraz z rodzajami dysków:  …………………  Podać jakie dyski wspiera macierz:…..  Możliwość rozbudowy do:  ……………….. |
|  | **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+ | Podać rodzaj i liczbę oferowanych portów:  …………………  Podać rodzaj i liczbę portów możliwych do rozbudowy:  …………. |
|  | **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** | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| **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 kryteriów:   * 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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| 1 | Obudowa | 1. Typu Rack, wysokość maksimum 4U; 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. | Model oferowanego procesora:  ……………………. |
| 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. | Ilość i rodzaj oferowanej 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. | Ilość i rodzaj oferowanych dysków:  ……………….. |
| 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. | Ilość i rodzaj oferowanych portów:  ……………….. |
| 8 | Porty | 1. Zintegrowana karta graficzna ze złączem VGA; 2. 2x 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. | Ilość i rodzaj oferowanych portów:  ……………….. |
| 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** | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| 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. | Ilość i rodzaj oferowanych portów:  ……………….. |
| 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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| 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, | Ilość i rodzaj oferowanych portów:  ……………….. |
| 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 | Podać:  Ilość pamięci flash: ………….  Ilość pamięci DRAM: ……….  Przepustowość:  …………………..  Prędkość przesyłania: …………………. |
| 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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| 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). | Ilość i rodzaj oferowanych portów:  ……………….. |
| 2 | **Parametry wydajnościowe:** | 1. Prędkość przełączania 1.8Tbps full duplex 2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3 | Prędkość przełączania:  …………………. |
| 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 |  |
| 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 (control plane policing) 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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| 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. | Ilość i rodzaj oferowanych portów:  ……………….. |
| 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 | Ilość i rodzaj dodatkowych portów:  ……………….. |
| 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. | Przełączanie z prędkością:  ………………  Możliwość rozbudowy do:  …………….. |
| 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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| 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. | Ilość i rodzaj oferowanych portów:  ……………….. |
| 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. | 1. W zakresie Firewall’a obsługa: ……… jednoczesnych połączeń oraz …………………… nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: ………….. dla pakietów 512 B. 3. Przepustowość Stateful Firewall: ………… dla pakietów 64 B. 4. Przepustowość Stateful Firewall: ………… dla pakietów 1518 B. 5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: ……… 6. Wydajność szyfrowania IPSec VPN ………………. 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 - ……………. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - ……….. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – ………….. |
| 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** | | **Potwierdzenie spełnienia warunków**  **Spełnia/nie spełnia** |
| 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. | Ilość i rodzaj oferowanych portów: ………………….  Oferowana przestrzeń dyskowa: …………………. |
| 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. | Podać parametry wydajnościowe:  ……………………… |
| 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. |  |