*Załącznik nr 1 do formularza ofertowego*

*Załącznik nr …….. do umowy*

*pieczęć Wykonawcy*

**FORMULARZ TECHNICZNY**

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

1. **Rozwiązanie NAS typ A – 1 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Oferowane rozwiązanie ma spełniać dwie role: dodatkowej przestrzeni dyskowej (tier II) dla istniejącej Jednolitej Infrastruktury Bazodanowej oraz centralnego urządzenia NAS świadczącego usługę systemu pamięci masowej typu NAS i pamięci obiektowej. |  |
| 2 | Podsystem pamięci masowej spełniający wymagania NAS Typ A musi:  • być podłączony do istniejącej Jednolitej Infrastruktury Bazodanowej za pomocą interfejsów o przepustowości całkowitej wynoszącej minimum 80 Gb/s realizowanych  w technologii InfiniBand 40Gb/s lub 10 Gb Ethernet (łącze optyczne), połączenia muszą być redundantne;  • zapewniać przepustowość dla ładowania danych bazodanowych do istniejącej Jednolitej Infrastruktury Bazodanowej nie niższą niż 2GB/s;  • umożliwiać obsługę protokołów plikowych: NFS v3/v4, CIFS/SMB v2/v3, HTTP, FTP, Obiekty (REST). Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej |  |
| 3 | System pamięci masowej ma być dostarczony w zestawie z szafą/szafami RACK 19” o wysokości maksymalnej 42U i głębokości maksymalnej 1200mm. |  |
| 4 | Kontrolery podsystemu pamięci masowej muszą obsługiwać zarządzaną przestrzeń dyskową, jej konfigurację, obsługę RAID i wszystkie wymienione niżej serwisy danych oraz zaawansowane funkcje monitoringu. Wymagane jest aby kontrolery pracowały w układzie Activ-Activ Concurent. Wymagane jest aby kontrolery oferowanego urządzenia były rozwiązaniem jednolitym technologicznie - wszystkie wymagane zapytaniem funkcjonalności myszą być możliwe do uruchomienia bez konieczności instalacji dodatkowych "głowic" czy urządzeń czy modułów zewnętrznych tego samego producenta lub firm trzecich. Ten sam wymóg dotyczy wymaganych zapytaniem interfejsów - instalacja łączy Ethernet, Fibre Channel i InfiniBand. Zamawiający nie dopuszcza spełnienia wymogu poprzez użycie wszelkiego typu wirtualizatorów i urządzeń warstw pośrednich. |  |
| 5 | W celu zapewnienia odpowiedniej wydajności, pojedynczy kontroler podsystemu pamięci masowej musi posiadać sumarycznie nie mniej niż 8 jednostek CPU, a sumaryczna liczba rdzeni obliczeniowych nie może być mniejsza niż 144. |  |
| 6 | Kontrolery modułu pamięci podsystemu pamięci masowej muszą być wyposażone w szybką pamięć cache w oparciu o pamięć DRAM, a sumaryczna ilość pamięci cache dla całej macierzy musi być nie mniejsza niż 3000 GB. |  |
| 7 | Podsystem pamięci masowej musi umożliwiać rozbudowę pamięci DRAM o pamięć Cache L2 typu flash SSD. Rozbudowa do co najmniej 486 TB pamięci Cache L2 poprzez dokładanie węzłów. |  |
| 8 | Podsystem pamięci masowej musi być wyposażony w:  • minimum 8 interfejsów 10Gb Base-T Ethernet;  • minimum 4 interfejsy, po dwa na każdy kontroler w technologii InfiniBand 40Gb/s  i 4 interfejsy 10Gb Ethernet SFP+ lub 12 interfejsów 10Gb Ethernet SFP+;  • minimum 4 interfejsy 16Gb FC i obsługiwać protokół NDMP. |  |
| 9 | Podsystem pamięci masowej musi:  • posiadać funkcjonalność oraz licencje umożliwiające wykonanie kompresji danych oraz kopii chwilowych (snapshot) dla całej oferowanej przestrzeni dyskowej;  • mieć funkcjonalność zdalnej replikacji asynchronicznej. Jeżeli funkcjonalność ta wymaga licencji - powinna być ona zawarta w ofercie dla pełnej pojemności macierzy wyznaczonej jej zakresem skalowalności. System replikacji ma być w pełni kompatybilny z systemem pamięci masowej NAS typ B, oferowanym dla lokalizacji zapasowej (wymagania pkt.7.2). Połącznie w zespół replikacji zdalnej dwóch macierzy ma być rozwiązaniem jednolitym technologicznie i nie może wymagać instalacji urządzeń firm trzecich;  • wspierać możliwość transparentnej migracji danych z innych urządzeń świadczących sieciowe usługi plikowe. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej;  • mieć możliwość wykonywania cienkich (ang. thin clone / thin copy) kopii danych w trybie odczytu i zapisu. Jeżeli funkcjonalność ta wymaga licencji - powinna być ona zawarta  w ofercie dla pełnej pojemności macierzy wyznaczonej jej zakresem skalowalności;  • mieć funkcjonalność szyfrowania danych mechanizmem AES 256-bit dla całej oferowanej przestrzeni dyskowej. |  |
| 10 | Podsystem pamięci masowej musi:  • umożliwiać równoczesną obsługę wielu poziomów RAID tj. co najmniej RAID 0, 1, 5, 6  i 10 lub równoważnych;  • być wyposażony w minimum 1600 GB pamięci flash SSD dla danych, pełniącej funkcję akceleratora dla klasycznych dysków obrotowych;  • być wyposażony w minimum 2460 TB netto w RAID 6 na dyskach nie mniejszych niż 10 TB (poj. dysku brutto);  • umożliwiać rozbudowę przestrzeni dyskowej poprzez dołożenie dodatkowych dysków twardych / dodatkowych półek dyskowych, do wielkości 7,2 PB przestrzeni surowej przy wykorzystaniu dysków nie większych niż 10 TB oraz bez konieczności zmiany architektury/generacji macierzy. |  |
| 11 | Pojedyncza półka dyskowa do oferowanego podsystemu pamięci masowej musi mieć możliwość obsługi min. 24 napędów dyskowych. |  |
| 12 | Dyski przeznaczone na dane muszą znajdować się w półkach dyskowych. W kontrolerach macierzowych mogą znajdować się jedynie pamięć cache oraz dyski przeznaczone na system operacyjny modułu pamięci masowej. |  |
| 13 | Podsystem pamięci masowej musi:  • umożliwiać zarządzanie zarówno z poziomu linii komend (CLI), jak również poprzez interfejs graficzny (GUI). Dostęp do urządzenia bezpośrednio z poziomu standardowych przeglądarek internetowych oraz klientów SSH. Wymagane jest wsparcie dla następujących metod zarządzania macierzą: HTTPS, SSH, SNMP v1/v2c, RESTful API;  • posiadać narzędzie umożliwiające obserwację danych wydajnościowych oraz ich graficzną prezentację w postaci wykresów. Monitorowanie wydajności macierzy musi być możliwe na podstawie parametrów takich jak: przepustowość sieci, przepustowość dysków, liczba operacji I/O dla dysków oraz kontrolerów, opóźnienia zapisów/odczytów. Statystyki pracy elementów urządzenia muszą być widoczne w czasie rzeczywistym. Jeżeli uruchomienie takiej funkcjonalność wymaga licencji lub oprogramowania, taka licencja/oprogramowanie musi zostać dostarczona;  • mieć możliwość gromadzenia oraz prezentowania graficznego bieżących oraz historycznych danych wydajnościowych w postaci wykresów w GUI urządzenia. |  |

1. **Rozwiązanie NAS typ B - 1 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Kontrolery podsystemu pamięci NAS muszą obsługiwać zarządzaną przestrzeń dyskową, jej konfigurację, obsługę RAID i wszystkie wymienione niżej serwisy danych oraz zaawansowane funkcje monitoringu. Wymagane jest aby kontrolery pracowały w układzie Activ-Activ Concurent. Wymagane jest aby kontrolery oferowanego urządzenia były rozwiązaniem jednolitym technologicznie - wszystkie wymagane zapytaniem funkcjonalności myszą być możliwe do uruchomienia bez konieczności instalacji dodatkowych "głowic" czy urządzeń czy modułów zewnętrznych tego samego producenta lub firm trzecich. Ten sam wymóg dotyczy wymaganych zapytaniem interfejsów - instalacja łączy Ethernet, Fibre Channel i InfiniBand. Zamawiający nie dopuszcza spełnienia wymogu poprzez użycie wszelkiego typu wirtualizatorów i urządzeń warstw pośrednich. |  |
| 2 | W celu zapewnienia odpowiedniej wydajności, pojedynczy kontroler macierzy dyskowej typu NAS musi posiadać sumarycznie nie mniej niż 2 jednostki CPU, a sumaryczna liczba rdzeni obliczeniowych nie może być mniejsza niż 36 na kontroler |  |
| 3 | Kontrolery modułu pamięci masowej muszą być wyposażone w szybką pamięć cache  w oparciu o pamięć DRAM, a sumaryczna ilość pamięci cache dla całej macierzy musi być nie mniejsza niż 1500 GB. |  |
| 4 | Podsystem pamięci masowej musi umożliwiać rozbudowę pamięci DRAM o pamięć Cache L2 typu flash SSD. Rozbudowa do co najmniej 204TB pamięci Cache L2 poprzez dokładanie węzłów. |  |
| 5 | System pamięci masowej ma być dostarczony w zestawie z szafą/szafami RACK 19” o wysokości maksymalnej 42U i głębokości maksymalnej 1200mm |  |
| 6 | Podsystem pamięci masowej musi być wyposażony w:  • minimum 8 interfejsy 10Gb Base-T Ethernet,  • minimum 4 interfejsy 10Gb Ethernet SFP+,  • minimum 4 interfejsy 16Gb FC i obsługiwać protokół NDMP. |  |
| 7 | Podsystem pamięci masowej musi:  • umożliwiać obsługę protokołów plikowych: NFS v3/v4, CIFS/SMB v2/v3, HTTP, FTP, Obiekty (REST). Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej;  • mieć funkcjonalność zdalnej replikacji asynchronicznej. Jeżeli funkcjonalność ta wymaga licencji - powinna być ona zawarta w ofercie dla pełnej pojemności NAS wyznaczonej jej zakresem skalowalności. System replikacji ma być w pełni kompatybilny z usługą podsystemu pamięci masowej pełniącym funkcję dodatkowej przestrzeni dyskowej (tear II) dla istniejącej Jednolitej Infrastruktury Bazodanowej oraz urządzenia NAS lokalizacji centralnej (NAS typ A wymagania pkt. 7.1). Połącznie w zespół replikacji zdalnej dwóch macierzy typu NAS ma być rozwiązaniem jednolitym technologicznie i nie może wymagać instalacji urządzeń firm trzecich;  • wspierać możliwość transparentnej migracji danych z innych urządzeń świadczących sieciowe usługi plikowe. Jeżeli uruchomienie tej funkcjonalności wymaga dodatkowych licencji, takie licencje muszą zostać dostarczone dla całej oferowanej przestrzeni dyskowej;  • posiadać funkcjonalność oraz licencje umożliwiające wykonanie kompresji danych oraz kopii chwilowych (snapshot) dla całej oferowanej przestrzeni dyskowej;  • mieć możliwość wykonywania cienkich (ang. thin clone / thin copy) kopii danych w trybie odczytu i zapisu.  • mieć funkcjonalność szyfrowania danych mechanizmem AES 256-bit dla całej oferowanej przestrzeni dyskowej. |  |
| 8 | Podsystem pamięci masowej musi:  • umożliwiać równoczesną obsługę wielu poziomów RAID tj. co najmniej RAID 0, 1, 5, 6  i 10 lub równoważnych;  • być wyposażony w minimum 2280 TB netto w RAID 6 na dyskach nie mniejszych niż 10TB (poj. dysku brutto).  • być wyposażony w minimum 800 GB pamięci flash SSD dla danych, pełniącej funkcję akceleratora dla klasycznych dysków obrotowych.  • umożliwiać rozbudowę przestrzeni dyskowej poprzez dołożenie dodatkowych dysków twardych / dodatkowych półek dyskowych, do wielkości 3,0 PB przestrzeni surowej przy wykorzystaniu dysków nie większych niż 10 TB oraz bez konieczności zmiany architektury/generacji macierzy. |  |
| 9 | Pojedyncza półka dyskowa do oferowanego modułu pamięci masowej musi mieć możliwość obsługi minimum 24 napędów dyskowych. |  |
| 10 | Dyski przeznaczone na dane muszą znajdować się w półkach dyskowych. W kontrolerach macierzowych mogą znajdować się jedynie pamięć cache oraz dyski przeznaczone na system operacyjny modułu pamięci masowej. |  |
| 11 | Podsystem pamięci masowej musi:  • umożliwiać zarządzanie zarówno z poziomu linii komend (CLI), jak również poprzez interfejs graficzny (GUI). Dostęp do urządzenia bezpośrednio z poziomu standardowych przeglądarek internetowych oraz klientów SSH. Wymagane jest wsparcie dla następujących metod zarządzania macierzą: HTTPS, SSH, SNMP v1/v2c, RESTful API;  • posiadać narzędzie umożliwiające obserwację danych wydajnościowych oraz ich graficzną prezentację w postaci wykresów. Monitorowanie wydajności macierzy musi być możliwe na podstawie parametrów takich jak: przepustowość sieci, przepustowość dysków, liczba operacji I/O dla dysków oraz kontrolerów, opóźnienia zapisów/odczytów. Statystyki pracy elementów urządzenia muszą być widoczne w czasie rzeczywistym. Jeżeli uruchomienie takiej funkcjonalność wymaga licencji lub oprogramowania, taka licencja/oprogramowanie musi zostać dostarczona;  • mieć możliwość gromadzenia oraz prezentowania graficznego bieżących oraz historycznych danych wydajnościowych w postaci wykresów w GUI urządzenia. |  |

1. **Macierz blokowa – 1 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Macierz musi być przystosowana do montażu w szafie rack 19” |  |
| 2 | Oferowane urządzenie musi posiadać minimum 2 kontrolery pracujące w trybie Active-Active z funkcją Mirrored cache. |  |
| 3 | Komunikacja pomiędzy wszystkimi kontrolerami macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się w szczególności komunikacji z wykorzystaniem protokołów FC/Ethernet/Infiniband. |  |
| 4 | Dla zapewnienia najwyższej wydajności, maksymalna konfiguracja macierzy musi wspierać tworzenie wolumenów rozłożonych na wszystkich dyskach macierzy (tzw. wide-striping) i ich jednoczesne, aktywne udostępnianie ze wszystkich kontrolerów macierzy. |  |
| 5 | Macierz musi posiadać min. 128 GiB wbudowanej pamięci cache (bez posiłkowania się dyskami SSD),posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych. |  |
| 6 | Macierz musi posiadać min. 8 interfejsów FC 16Gb i 4 interfejsy 1Gb |  |
| 7 | Macierz musi obsługiwać dyski SSD, SAS i Nearline SAS. Musi umożliwiać mieszanie napędów dyskowych SSD, SAS i Nearline SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”. być wyposażona w dyski posiadające podwójne interfejsy.obsługiwać mechanizmy RAID zgodne z RAID0, RAID1 lub RAID10, RAID5 lub RAID50 oraz RAID6 lub RAID60 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). |  |
| 8 | Rozłożenie dysków w macierzy musi zapewniać redundancję pozwalającą na nieprzerwaną pracę i dostęp do wszystkich danych w sytuacji awarii pojedynczego komponentu sprzętowego typu: kontroler,półka dyskowa, dysk, zasilacz. |  |
| 9 | Możliwość definiowania różnych poziomów RAID na tych samych dyskach fizycznych. Jeżeli nie jest możliwe uzyskanie takiej funkcjonalności, dla uzyskania podobnej wydajności wymagane jest zrealizowanie żądanej pojemności większą o 50% liczbą dysków fizycznych. |  |
| 10 | Macierz musi umożliwiać definiowanie globalnych dysków spare lub odpowiedniej zapasowej przestrzeni dyskowej. Oferowana konfiguracja dyskowa musi zawierać rekomendowaną przez producenta ilość dysków spare lub odpowiednią zapasową przestrzeń dyskową. |  |
| 11 | Wymagana minimalna wielkość użytkowej przestrzeni dyskowej:  • SSD: min. 50TiB w RAID 6, przy zastosowaniu min. 24 dysków  • SAS 10k: min. 460TiB w RAID 6, przy zastosowaniu min. 360 dysków |  |
| 12 | Macierz musi, w dostarczonej konfiguracji, przy obciążeniu losowym (ang. random) o charakterystyce R/W = 50%/50% dla bloku 8 kB, być w stanie osiagnąć dla poszczególnych typów dysków, minimalną wydajność na poziomie:  • SSD: 200 tys. IOps  • SAS 10k: 40 tys.Iops  Wykonawca jest zobowiązany do przedstawienia, dla zaproponowanej konfiguracji, szacunków wydajności na podstawie danych katalogowych lub raportu z dedykowanego narzędzia producenta. |  |
| 13 | Możliwość rozbudowy do min. 576 dysków twardych bez konieczności dodawania lub wymiany kontrolerów macierzy. |  |
| 14 | Zarządzanie grupami dyskowymi oraz dyskami logicznymi:  • Macierz musi umożliwiać dynamiczne zwiększania pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych.  • Macierz musi umożliwiać zmianę technologii dyskowej oraz poziomu zabezpieczenia RAID dla wolumenu dyskowego w sposób transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy." |  |
| 15 | Thin Provisioning:  • Macierz musi umożliwiać tworzenie zasobów dyskowych typu Thick oraz Thin.  • Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny, bez konieczności ręcznego uruchamiania dodatkowych procesów na kontrolerach macierzy (wymagana obsługa standardu T10 SCSI UNMAP).  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy. |  |
| 16 | Macierz musi umożliwiać wykonywanie na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach danej macierzy, za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa ma być wykonywana bez alokowania dodatkowej przestrzeni dyskowej na jej potrzeby. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy. |  |
|  | Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone)  w ramach danej macierzy, za pomocą wewnętrznych kontrolerów macierzowych. Wykonana kopia danych musi mieć możliwość zabezpieczenia innym poziomem RAID oraz innej grupie/puli dyskowej niż dane źródłowe.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy. |  |
| 17 | Macierz dyskowa musi umożliwiać migrację danych, bez przerywania do nich dostępu, pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy.  Funkcjonalność musi umożliwiać istnienie zasobu LUN, który fizycznie będzie znajdował się na różnych typach dysków (SSD, SAS, NL) obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy. |  |
| 18 | Macierz musi umożliwiać replikację zdalną w następujących trybach: jeden do jednego, jeden do wielu, wiele do jednego oraz replikację jednego wolumenu logicznego (tych samych danych) do dwóch innych niezależnych ośrodków za pomocą replikacji synchronicznej i asynchronicznej. Oprogramowanie musi zapewniać funkcjonalność zawieszania i ponownej przyrostowej resynchronizacji kopii z oryginałem oraz zamiany ról oryginału i kopii (dla określonej pary dysków logicznych LUN macierzy) z poziomu interfejsu administratora.  Macierz musi umożliwiać zdalną replikację danych typu online do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.  Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem różnych portów macierzy FC/IP. |  |
| 19 | Macierz musi umożliwiać konfigurację gwarancji wydajności typ QoS (możliwość definiowania progów minimalnych i maksymalnych) dla wybranych wolumenów logicznych w zakresie takich parametrów jak: wydajność w IOPS, wydajność w MB/s, opóźnienie w ms.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy. |  |
| 20 | Macierz musi umożliwiać deduplikację i kompresję danych na poziomie blokowym (co najmniej w odniesieniu do danych na dyskach SSD). Musi istnieć możliwość uruchomienia deduplikacji i kompresji (niezależnie i łącznie) na poziomie pojedynczych wolumenów logicznych. Deduplikacja i kompresja danych musi odbywać się w locie, przed zapisaniem danych na dyskach macierzy. Musi istnieć możliwość wykonania operacji odwrotnej – wyłączenia deduplikacji i kompresji na określonych wolumenach logicznych. Deduplikacja i kompresja nie mogą być realizowane za pomocą zewnętrznego urządzenia lub oprogramowania.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy. |  |
| 21 | Macierz musi umożliwiać podział macierzy na minimum 8 odseparowanych macierzy logicznych zarządzanych przez dedykowanych administratorów.  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy. |  |
| 22 | Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. |  |
| 23 | Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory,mieć możliwość zasilania z dwóch niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy,umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez wyłączania dostępu do danych,umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii. |  |
| 24 | Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. |  |
| 25 | Macierz musi umożliwiać tworzenie skryptów użytkownika do automatyzacji różnych zadań. |  |
| 26 | Oprogramowanie do zarządzania macierzą musi zapewniać stałe monitorowanie jej stanu oraz umożliwiać konfigurowanie jej zasobów dyskowych.  Narzędzie musi pozwalać na obserwację danych wydajnościowych oraz prezentację ich w postaci wykresów oraz czytelnych raportów.  Wymagane jest monitorowanie bieżących parametrów pracy macierzy, w tym minimum:  • prezentowanie stanu macierzy, adresu zarządzającego IP macierzą, nazwy macierzy (model), numeru seryjnego i poziomu oprogramowania układowego macierzy;  • prezentowanie dostępnej przestrzeni na macierzy z zaznaczeniem przestrzeni wolnej do zapisu i już zapisanej (zaalokowanej);  • prezentacji w formie graficznej grup dyskowych, dysków, szablonów dysków. Konieczne jest prezentowanie tych danych w formie mapy określającej powiązania logiczne pomiędzy tymi komponentami – np. które dyski (wolumeny) należą do danej grupy dyskowej;  • tworzeniu szablonów dysków, składających się z nazwy, przyporządkowania do grupy dyskowej, pojemności dysku, typu (Thin, Full), sposobu udostępniania (prywatny dysk dedykowany serwerowi lub dysk współdzielony pomiędzy kilkoma serwerami). Z danego szablonu musi istnieć możliwość tworzenia dysku (wolumenu) o wskazanych w szablonie parametrach;  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej pojemności macierzy. |  |
| 27 | Wymaga się aby oprogramowanie do zarządzania macierzą pochodziło od producenta macierzy. |  |
| 28 | Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności - co najmniej dwoma ścieżkami. Macierz dyskowa musi wspierać obsługę minimum 128 hostów podłączonych poprzez sieć SAN. wspierać między innymi następujące systemy operacyjne na podłaczonych hostach: Windows, Linux, VMware, IBM AIX, Oracle Solaris, HP-UX. Macierz musi posiadać wsparcie dla różnych systemów klastrowych, co najmniej VMware Metrocluster, HPE Serviceguard Metrocuster, Microsoft Cluster. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów. |  |
| 29 | Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów.  Preferowane jest rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. W przypadku stosowania rozwiązań firmowych/własnych – konieczna jest ich certyfikacja dla platform: Windows 2012+, Linux RedHat 7.x+, Suse12+, VMware 5,5+  Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby hostów wspieranych przez oferowaną macierz. |  |
| 30 | Instalacja lub uruchamianie dodatkowej funkcjonalności macierzy dyskowej nie może powodować zmniejszenia dostępnego obszaru pamięci cache danych kontrolerów macierzowych. |  |
| 31 | Wymiana dysków SSD w ramach wsparcia technicznego producenta, w związku ze zużyciem bloków pamięci > 95%, w oferowanej macierzy blokowej, musi być zgodna z ofertą Wykonawcy - „Czas Trwania Wsparcia Technicznego”. |  |

1. **Serwery blade – 4 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  | |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  | |
| 1 | Zainstalowane 2 procesory, minimum 12 rdzeni każdy, x86 - 64 Bit osiągające w testach SPECint\_rate2006 wynik Base nie gorszy niż 1100 punktów w konfiguracji dwuprocesorowej. |  |
| 2 | Zainstalowane 1TB RAM DDR4 LoadReduces DIMM w modułach min. 64GB. Minimum 16 slotów na pamięć. |  |
| 3 | Minimum jeden wewnętrzny port USB umożliwiający instalację pamięci Flash. |  |
| 4 | Minimum 2 sloty PCI-Express x8 (szybkość slotu). |  |
| 5 | Dwa Interfejsy SAN FC 16Gb. |  |
| 6 | Minimum 2 Interfejsy sieciowe 20GbE lub minimum 4 interfejsy sieciowe 10GbE |  |
| 7 | Wspierane systemy operacyjne: MS Windows 2012 R2, MS Windows 2016, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware 6.0, VMware 6.5, VMware 6.7. |  |

1. **Serwery bazodanowe – 2 szt.**

| ID | Wymaganie |  | |
| --- | --- | --- | --- |
|  | Nazwa producenta | |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* | |  |
| 1 | Zainstalowane 1 procesor, maksimum 6 rdzeni, x86 - 64 Bit osiągający w testach SPECint\_rate2006 wynik nie gorszy niż 300 punktów. |  | |
| 2 | Zainstalowane 4 procesory, minimum 24 rdzeni każdy, x86 - 64 bit z taktowaniem min. 2,1GHz i mocą nie przekraczającą 145W. |  | |
| 3 | Zainstalowane 2048 GB RAM DDR4 LoadReduces DIMM w modułach min. 64GB. |  | |
| 4 | 2 dyski SSD typu Hot Swap każdy o pojemności minimum 240GB. |  | |
| 5 | Kontroler dysków obsługujący poziomy RAID 0/1 z 2GB Cache podtrzymywanym bateryjnie. |  | |
| 6 | 4 redundantne zasilacze typu Hot-plug. |  | |
| 7 | Zestaw redundantnych wentylatorów. |  | |
| 8 | Minimum 2 sloty PCI-Express x16 (szybkość slotu). |  | |
| 9 | Dwa interfejsy SAN FC 16Gb. |  | |
| 10 | Minimum 2 interfejsy sieciowe 1GbE i 4 interfejsy sieciowe 10GbE z wkładkami SFP+ SR. |  | |
| 11 | Wspierane systemy operacyjne: MS Windows 2012 R2, MS Windows 2016, Red Hat Enterprise Linux, CentOS. |  | |
| 12 | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.  Wraz z serwerem należy dostarczyć oprogramowanie do zarządzania serwerem, pozwalające na:  a) Inwentaryzację sprzętu serwerowego, monitoring zdrowia - „health status”,  b) zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci),  c) zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego,  d) zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu,  e) monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć i zasilania. |  | |

1. **Serwery RACK – 5 szt.**

|  |  |  |
| --- | --- | --- |
| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Zainstalowany 1 procesor, maksimum 6 rdzeni, x86 - 64 Bit osiągający w testach SPECint\_rate2006 wynik Base nie gorszy niż 812 punktów w konfiguracji dwuprocesorowej. |  |
| 2 | Zainstalowane 512GB RAM DDR4 LoadReduces DIMM w modułach min. 64GB. |  |
| 3 | 2 dyski SSD typu Hot Swap, każdy o pojemności minimum 960GB. |  |
| 4 | Kontroler dysków obsługujący poziomy RAID 0/1 z 2GB Cache podtrzymywanym bateryjnie. |  |
| 5 | 2 redundantne zasilacze typu Hot-plug o mocy min. 500W |  |
| 6 | Zestaw redundantnych wentylatorów. |  |
| 7 | Minimum 2 sloty PCI-Express x16 (szybkość slotu). |  |
| 8 | Dwa Interfejsy SAN FC 16Gb. |  |
| 9 | Minimum 4 Interfejsy sieciowe 1GbE i 2 Interfejsy sieciowe 10GbE (wkładki SFP+ SR) |  |
| 10 | Wspierane systemy operacyjne: MS Windows 2012 R2, MS Windows 2016, Red Hat Enterprise Linux, CentOS. |  |
| 11 | Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną.  Wraz z serwerem należy dostarczyć oprogramowanie do zarządzania serwerem, pozwalające na:  a. Inwentaryzację sprzętu serwerowego, monitoring zdrowia - „health status”,  b. zautomatyzowane instalacje systemu operacyjnego z wykorzystaniem mechanizmu PXE (bootowanie z sieci),  c. zautomatyzowane, personalizowane, zrównoleglone instalacje systemów operacyjnych oraz aplikacji z wykorzystaniem tzw. plików odpowiedzi dostarczanych przez producenta oprogramowania użytkowego,  d. zautomatyzowane, zrównoleglone kopiowanie środowisk, połączone z natychmiastową personalizacją systemu,  e. monitorowanie utylizacji następujących podzespołów serwera: procesor, pamięć i zasilania. |  |

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

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. |  |
| 2 | System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 18 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 9 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 4 000 000 jednoczesnych połączeń. |  |
| 3 | System zabezpieczeń firewall musi być wyposażony w co najmniej 4 porty Ethernet 100/1G/10G, 16 portów 1G/10G SFP/SFP+, 4 porty 40G QSFP+. |  |
| 4 | Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. |  |
| 5 | System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN. |  |
| 6 | System zabezpieczeń firewall musi obsługiwać nie mniej niż 20 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF. |  |
| 7 | System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7). |  |
| 8 | System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną. |  |
| 9 | Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 18 Gbit/s. |  |
| 10 | System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. |  |
| 11 | System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |  |
| 12 | System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji. |  |
| 13 | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |  |
| 14 | System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL. |  |
| 15 | System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. |  |
| 16 | Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. |  |
| 17 | System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. |  |
| **Wymagania ochrony: IPS, AV, anty-spyware, URL, zero-day:** | | |
| 18 | System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |  |
| 19 | System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. |  |
| 20 | System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |  |
| 21 | System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |  |
| 22 | System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |  |
| 23 | System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |  |
| 24 | System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. |  |
| 25 | System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa). |  |
| 26 | System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. |  |
| 27 | System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty. |  |
| 28 | System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. |  |
| **Wymagania w zakresie: NAT, DoS, IPSEC VPN, SSL VPN, QoS:** | | |
| 29 | System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. |  |
| 30 | System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. |  |
| 31 | System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |  |
| 32 | System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji. |  |
| 33 | System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0. |  |
| 34 | System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego. |  |
| 35 | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego. |  |
| **Wymagania w zakresie zarządzania i raportowania** | | |
| 36 | Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem. |  |
| 37 | System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. |  |
| 38 | System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. |  |
| **Dostęp do urządzenia i zarządzanie z sieci** | | |
| 39 | Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. |  |
| 40 | System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos. |  |
| 41 | System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). |  |
| 42 | System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa. |  |
| 43 | System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach. |  |
| 44 | System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia. |  |
| 45 | System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www. |  |
| **Wymagania w zakresie środowiska wirtualnego Vmware** | | |
| 47 | System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla. |  |
| **Wymagania rozszerzone w zakresie wymagań podstawowych** | | |
| 48 | Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.). |  |
| 49 | Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ). |  |
| 50 | System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. |  |
| 51 | Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM). |  |
| 52 | Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. |  |
| 53 | Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS. |  |
| 54 | System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |  |
| 55 | System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. |  |
| 56 | System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików. |  |
| 57 | System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. |  |
| 58 | System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji. |  |
| 59 | System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH. |  |
| **Wymagania rozszerzone w zakresie identyfikacji użytkowników** | | |
| 60 | System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. |  |
| 61 | System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. |  |
| 62 | Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |  |
| **Wymagania rozszerzone w zakresie identyfikacji użytkowników** | | |
| 63 | System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. |  |
| 64 | System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia. |  |
| 65 | Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej. |  |
| **Wymagania rozszerzone w zakresie ochrony IPS, AV, anty-spyware, URL, zero-day** | | |
| 66 | System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. |  |
| 67 | System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |  |
| 68 | System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. |  |
| 69 | System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole). |  |
| **Wymagania rozszerzone w zakresie NAT, DoS, IPSEC VPN, SSL VPN, QoS** | | |
| 70 | System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach. |  |
| 71 | System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników. |  |
| **Wymagania rozszerzone w zakresie zarządzania i raportowania** | | |
| 72 | System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami. |  |
| 73 | System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). |  |
| 74 | System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB (RAID 1). Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji. |  |
| 75 | System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu. |  |
| 76 | System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa. |  |
| 77 | System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. |  |
| 78 | System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni. |  |

1. **Router BGP – 2 szt.**

| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
| --- | --- | --- |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Urządzenie musi być wyposażone w minimum: w 4 porty typu Combo 1GEthernet (1Gbase-T/SFP), 2 porty 10GbEthernet SFP+, 16 portów SFP. Porty SFP mają być obsadzone wkładkami SFP: 4x1000Base-LX, 4x1000Base-SX, 8x1000Base-T. Wkładki SFP/SFP+ muszą pochodzić od producenta urządzenia. |  |
| 2 | Urządzenie musi posiadać minimum jeden wolny slot na rozbudowę o dodatkowe porty. |  |
| 3 | Musi istnieć możliwość rozbudowy urządzenia do 36 portów 1GbEthernet lub 6 portów 10GbEthernet. Rozbudowa może być wykonana poprzez wymianę istniejących portów. |  |
| 4 | Urządzenie musi posiadać dodatkowo:  • port konsoli szeregowy RJ-45,  • port USB,  • port Ethernet do zarządzania out-of-band. |  |
| 5 | Wysokość urządzenia nie może przekraczać 2U. |  |
| 6 | Urządzenie musi być wyposażone w dwa redundantne zasilacze 230V. Musi jednak istnieć możliwość jego wyposażenia w dwa redundantne zasilacze na prąd stały. |  |
| 7 | Urządzenie musi posiadać możliwość wymiany wentylatorów. |  |
| 8 | Urządzenie musi posiadać modularny system operacyjny. |  |
| 9 | Wymagana jest minimalna przepustowość urządzenia: 20Gbps i 15Mpps |  |
| 10 | Wymagana jest wydajność dla IPSec na poziomie minimum: 4.8Gbps. |  |
| 11 | Wymagana jest tablica routingu RIB była wielkości 4mln |  |
| 12 | Urządzenie musi być zbudowane w technologii pozwalającej na połączenie dwóch urządzeń tego typu w klaster działający jako jedno logiczne urządzenie. |  |
| 13 | Wymagana jest ochrona procesora przed atakami DoS |  |
| 14 | Wymagane jest wsparcie dla:  • protokołów routingu: RIP/RIPng, OSPF/OSPFv3, IS-IS/IS-ISv6, BGP/BGP4+, PIM/PIM6, MSDP, MBGP, policy based routing,  • protokołów MPLS: LDP, MPLS TE, L3 VPN, L2 VPN, VPLS, Multicast VPN, 6PE, 6vPE  • rozwiązań związanych z bezpieczeństwem: filtrowanie pakietów, pełnostanowy firewall, wykrywanie ataków, ochrona control plane przez ograniczanie ruchu, uRPF, L2TP, GRE, IPSec VPN, Auto-discovery VPN (ADVPN) i Group Domain VPN (GDVPN)  • funkcji QoS: kolejkowanie, zapobieganie przeciążeniom, priorytetyzacja, hierarchiczny QoS |  |
| 15 | Wymagane jest wsparcie dla następujących standardów BGP:  - RFC 1657 Definitions of Managed Objects for BGPv4  - RFC 1772 Application of the BGP  - RFC 1773 Experience with the BGP-4 Protocol  - RFC 1774 BGP-4 Protocol Analysis  - RFC 1965 BGP4 confederations  - RFC 1966 BGP Route Reflection An alternative to full mesh IBGP  - RFC 1997 BGP Communities Attribute  - RFC 1998 PPP Gandalf FZA Compression Protocol  - RFC 2385 BGP Session Protection via TCP MD5  - RFC 2439 BGP Route Flap Damping  - RFC 2842 Capability Advertisement with BGP-4  - RFC 2858 BGP-4 Multi-Protocol Extensions  - RFC 2918 Route Refresh Capability  - RFC 4271 A Border Gateway Protocol 4 (BGP-4)  - RFC 4272 BGP Security Vulnerabilities Analysis  - RFC 4274 BGP-4 Protocol Analysis  - RFC 4275 BGP-4 MIB Implementation Survey  - RFC 4276 BGP-4 Implementation Report  - RFC 4277 Experience with the BGP-4 Protocol  - RFC 4360 BGP Extended Communities Attribute  - RFC 4451 BGP MULTI\_EXIT\_DISC (MED) Considerations  - RFC 4456 BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)  - RFC 4486 Subcodes for BGP Cease Notification Message  - RFC 4724 Graceful Restart Mechanism for BGP  - RFC 4760 Multiprotocol Extensions for BGP-4  - RFC 4893 BGP Support for Four-octet AS Number Space  - RFC 5065 Autonomous System Confederations for BGP RFC 5291 Outbound Route Filtering Capability for BGP-4  - RFC 5292 Address-Prefix-Based Outbound Route Filter for BGP-4  - RFC 5398 Autonomous System (AS) Number Reservation for Documentation Use  - RFC 5883 BFD for Multihop Paths |  |
| 16 | Wsparcie dla następujących standardów i protokołów związanych z zarządzaniem urządzeniem:  - RFC 1155 Structure and Mgmt Information (SMIv1)  - RFC 1157 SNMPv1/v2c  - RFC 1305 NTPv3  - RFC 1901 (Community based SNMPv2)  - RFC 1901-1907 SNMPv2c, SMIv2 and Revised MIB-II  - RFC 1902 (SNMPv2)  - RFC 1908 (SNMP v1/2 Coexistence)  - RFC 1945 Hypertext Transfer Protocol -- HTTP/1.0  - RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1  - RFC 2271 FrameWork  - RFC 2452 MIB for TCP6  - RFC 2454 MIB for UDP6  - RFC 2573 (SNMPv3 Applications)  - RFC 2576 (Coexistence between SNMP V1, V2, V3)  - RFC 2578-2580 SMIv2  - RFC 2579 (SMIv2 Text Conventions)  - RFC 2580 (SMIv2 Conformance)  - RFC 2819 (RMON groups Alarm, Event, History and Statistics only)  - RFC 2819 RMON  - RFC 3410 (Management Framework)  - RFC 3416 (SNMP Protocol Operations v2)  - RFC 3417 (SNMP Transport Mappings)  - SNMP v3 and RMON RFC support  - SSHv1/SSHv2 Secure Shell  - TACACS/TACACS+ |  |
| 17 | Wsparcie dla następujących protokołów związanych z QoS:  - IEEE 802.1P (CoS)  - RFC 2309 Recommendations on queue management and congestion avoidance in the Internet  - RFC 2474 DiffServ Precedence, including 8 queues/port  - RFC 2474 DiffServ precedence, with 4 queues per port  - RFC 2474 DS Field in the IPv4 and IPv6 Headers  - RFC 2474 DSCP DiffServ  - RFC 2474, with 4 queues per port  - RFC 2475 DiffServ Architecture  - RFC 2597 DiffServ Assured Forwarding (AF)  - RFC 2597 DiffServ Assured Forwarding (AF)- partial support  - RFC 2598 DiffServ Expedited Forwarding (EF)  - RFC 2697 A Single Rate Three Color Marker  - RFC 2698 A Two Rate Three Color Marker  - RFC 2751 Signaled Preemption Priority Policy Element  - RFC 3247 Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)  - RFC 3260 New Terminology and Clarifications for DiffServ  - RFC 3662 A Lower Effort Per-Domain Behavior (PDB) for Differentiated Services  - RFC 4594 Configuration Guidelines for DiffServ Service Classes |  |
| 18 | Wsparcie dla następujących standardów sieciowych RFC i IETF:  - IEEE 802.1ad Q-in-Q  - IEEE 802.1ag Service Layer OAM  - IEEE 802.1AX-2008 Link Aggregation  - IEEE 802.1D MAC Bridges  - IEEE 802.1p Priority  - IEEE 802.1Q (GVRP)  - IEEE 802.1Q VLANs  - IEEE 802.1s Multiple Spanning Trees  - IEEE 802.1v VLAN classification by Protocol and Port  - IEEE 802.1w Rapid Reconfiguration of Spanning Tree  - IEEE 802.1X PAE  - IEEE 802.3 Type 10BASE-T  - IEEE 802.3ab 1000BASE-T  - IEEE 802.3ac (VLAN Tagging Extension)  - IEEE 802.3ad Link Aggregation (LAG)  - IEEE 802.3ae 10-Gigabit Ethernet  - IEEE 802.3ag Ethernet OAM  - IEEE 802.3z 1000BASE-X  - RFC 1305 NTPv3  - RFC 3623 Graceful OSPF Restart  - RFC 3704 Unicast Reverse Path Forwarding (URPF)  - RFC 3706 A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers  - RFC 3768 Virtual Router Redundancy Protocol (VRRP)  - RFC 3784 ISIS TE support  - RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)  - RFC 5880 Bidirectional Forwarding Detection |  |

1. **Przełącznik SAN – 2 szt.**

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

1. **Komplet pamięci RAM – 4 komplety.**

|  |  |  |
| --- | --- | --- |
| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | 32 sztuki pamięci RAM 32GB dla Serwera BL660c Gen8, zgodnie z poniższym:  1. DIMM Capacity - 32GB  2. DIMM Native Speed (MHz) - 1333  3. Voltage – LV |  |

1. **Oprogramowanie do wykonywania kopii zapasowej środowiska wirtualizacji – 1 komplet (73 szt.)**

|  |  |  |
| --- | --- | --- |
| ID | Wymaganie | Parametry techniczne sprzętu oferowanego przez Wykonawcę |
|  | Nazwa producenta |  |
|  | Identyfikacja produktu - *Typ produktu, model ...* |  |
| 1 | Oferowane licencje muszą zapewnić backup / odtwarzanie środowiska VMware składającego się z 17 serwerów ESX posiadających łącznie 60 fizycznych procesorów |  |
| 2 | System centralnego backupu musi umożliwiać dla powyżej definiowanego środowiska VMware backup/odtwarzanie nielimitowanej liczby maszyn wirtualnych: Zarówno backup obrazów maszyn wirtualnych jak również backup ze środka maszyn wirtualnych wszystkimi dostępnymi agentami oprogramowania backupowego |  |
| 3 | Wymaga się by w ramach oferowanych licencji system umożliwiał backup maszyn wirtualnych w każdym trybie:  a) Jako obrazy maszyn wirtualnych VMware(pliki vmdk)  b) Ze środka, agentem plikowym / bazodanowym / aplikacyjnym dla systemów plików Oracle, SQL, Sybase, DB2, Exchange, Lotus, Sharepoint |  |
| 4 | Musi być możliwość backupu jak powyżej dla dowolnej liczby maszyn wirtualnych w ramach zaintonowanych serwerów ESX. |  |
| 5 | Serwer backupu musi być dostarczony do zainstalowania na 2 fizycznych serwerach zarządzających backupem i odtwarzaniem całości zabezpieczanego środowiska. |  |
| 6 | Oferowany system musi tworzyć centralny system backupu wykonujący kopie zapasowe oraz zapewniać przechowywanie wszystkich zdeduplikowanych kopii zapasowych na dyskach posiadanego prze Zamawiającego de-duplikatora. |  |
| 7 | Całość backupów musi być składowana na posiadanym przez Zamawiającego de-duplikatorze EMC DataDomain.. |  |
| 8 | Oprogramowanie backupowe musi być wspierane (kompatybilne) z posiadanym przez Zamawiającego de-duplikatorem EMC DataDomain. |  |
| 9 | Każdy z serwerów backupu musi umożliwiać:  a) zarządzanie backupem lokalnego środowiska i związanych z nim zdalnych lokalizacji  b) przechowywanie backupów na dyskach posiadanego przez Zamawiającego de-duplikatora  c) zarządzanie replikacją między przez Zamawiającego de-duplikatorami  d) odtworzenie zreplikowanych backupów ze zdalnego urządzenia backupowego również w przypadku całkowitego zniszczenia zdalnego ośrodka czyli zniszczenia całości zdalnego środowiska backupu  e) stanowić kompletny system centralnego backupu z agentami do backupu plików, baz danych, środowisk wirtualnych. |  |
| 10 | Dostarczony system musi przechowywać kopie zapasowe na dyskach posiadanego przez Zamawiającego de-duplikatora EMC DataDomain. |  |
| 11 | Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, Debian, CentOS, Ubnutu, Novell OES), FreeBSD. |  |
| 12 | Backup zasobów plików z powyższych systemów musi podlegać de-duplikacji ze zmiennym blokiem na zabezpieczanej maszynie zgodnie z wymaganiami w mniejszej specyfikacji. |  |
| 13 | Oprogramowanie backupowe musi umożliwiać backup całych obrazów maszyn wirtualnych systemu VMware. |  |
| 14 | Oprogramowanie backupowe musi w trakcie backupu przesyłać do posiadanego przez Zamawiającego de-duplikatora tylko unikalne bloki, czyli bloki nie znajdujące się na oferowanym de-duplikatorze skracając czas backupu, obciążenie procesora i zmniejszając ruch w sieci WAN / LAN. |  |
| 15 | Włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera backupowego. |  |
| 16 | Oprogramowanie backupowe nie może odczytywać tych plików z systemu dyskowego, które się nie zmieniły w stosunku do ostatniego backupu. Raz zbackupowany plik nie może być nigdy więcej odczytany, chyba, że zmieni się jego zawartość. |  |
| 17 | W konsoli oprogramowania backupowego musi być możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy musza być automatycznie usunięte. |  |
| 18 | Oferowanie oprogramowanie backupowe musi mieć możliwość tworzenia z poziomu GUI (konsoli graficznej) polityk typu Dziadek – ojciec –syn, to znaczy utworzenia polityki w której zdefiniowano:  a) Czas przechowywania backupów dziennych,  b) Czas przechowywania backupów tygodniowych,  c) Czas przechowywania backupów miesięcznych,  d) Czas przechowywania backupów rocznych. |  |
| 19 | Oferowane rozwiązanie musi umożliwiać tworzenie wykluczeń, czyli elementów nie podlegających backupowi w ramach zadania backupowego. Musi istnieć możliwość tworzenia wykluczeń dla dowolnej kombinacji następujących elementów:  a) wybranych typów plików,  b) dla całych katalogów,  c) dla pojedynczych plików |  |
| 20 | Oferowane rozwiązanie musi mieć możliwość zdefiniowania by ostatni backup dowolnego zbioru danych nigdy się nie przeterminował. Oznacza to, że jeśli dany zasób nie jest backupowany to automatycznie ostatnie ważny backup tego zasobu jest trzymany bezterminowo. Jedynie administrator może zdecydować o jego usunięciu. |  |
| 21 | Serwery backupu muszą zarządzać replikacją backupów znajdujących się na de-duplikatorze. Całość konfiguracji replikacji backupów musi odbywać się z konsoli serwera backupu. Konfiguracja zadań replikacji nie może wymagać jakichkolwiek działań na de-duplikatorze |  |
| 22 | Wymaga się by replikacja między backupów znajdujących się na de-duplikatorach odbywała się w obu kierunkach jednocześnie:  a) Backupy z de-duplikatora z ośrodka podstawowego do de-duplikatora z ośrodka zapasowego  b) Backupy z de-duplikatora z ośrodka zapasowego do de-duplikatora z ośrodka podstawowego |  |
| 23 | Całość replikacji zarządzana tylko i wyłącznie z poziomu oprogramowania backupowego (serwerów backupu) |  |
| 24 | Musi istnieć możliwość zdefiniowania kalendarza replikacji między serwerami oraz zdefiniowania które zadania backupowe podlegają replikacji. |  |
| 25 | Serwer backupu musi udostępniać (pokazywać w konsoli GUI) backupy które zostały do niego zreplikowane ze zdalnej lokalizacji. Musi być możliwość odtworzenia backupów zreplikowanych do lokalnego serwera backupu / de-duplikatora ze zdalnej lokalizacji. Odtworzenie musi dobywać się poprzez interfejs GUI. Odtworzenie musi być możliwe w przypadku całkowitej niedostępności zdalnego systemu backupu (nieodstępność zdalnego serwera backupu oraz zdalnego de-duplikatora). |  |
| 26 | Każdy serwer backupu w każdej lokalizacji musi udostępniać (pokazywać w konsoli GUI) zarówno lokalne backupy jak wszystkie również backupy zreplikowane do ośrodka zdalnego. |  |
| 27 | W przypadku odtwarzania danych w ośrodku A w trakcie definiowania zadania odtwarzania musi być możliwość zdefiniowania czy odtwarzamy backupy z lokalnej kopii (znajdujące się na lokalnym oferowanym de-duplikatorze) czy też odtwarzamy ze zdalnej kopii z ośrodka B (znajdujące się na zdalnym oferowanym de-duplikatorze w lokalizacji B). |  |
| 28 | Konsola zarządzająca systemem backupowym musi integrować się z Active Directory. Musi być możliwość przydzielania użytkownikom i grupom Active Directory dostępnych ról (min, administrator, monitoring, tylko wykonywanie odtworzenia) w systemie backupowym. |  |
| 29 | Konsola musi udostępniać raporty dotyczące zajętości przestrzeni przeznaczonej na deduplikaty. |  |
| 30 | Oprogramowanie backupowe musi mieć możliwość limitowania wielkości zadania backupowego. Jeśli zadanie backupowe przekroczy zdefiniowaną wielkość wówczas nie może być zapisane w systemie backupowych |  |
| 31 | Oprogramowanie backupowe musi umożliwiać ograniczenie mocy procesora używanej do wykonywania zdania backupu tak by odpowiednia moc procesora zostawić dla innych zadań. |  |
| 32 | Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware 6.0. |  |
| 33 | Oprogramowanie backupowe musi umożliwiać dla środowisk VMware następujące typy backupu:  a. Backup całych maszyn wirtualnych  b. Backup pojedynczych, wybranych dysków maszyny wirtualnej vmdk  c. W trakcie backupu odczytowi z systemu dyskowego mają podlegać tylko zmienione bloki wirtualnych maszyn systemu VMware (wymagane wykorzystanie mechanizmu CBT systemu VMware)  d. Wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane przy pomocy technologii CBT systemu VMware to znaczy do medium backupowego z systemu VMware muszą być transferowane tylko zmienione bloki. |  |
| 34 | Jednocześnie z punktu widzenia systemu backupowego musza to być backupy pełne (full backupy). To znaczy z punktu widzenia systemu backupu muszą to być backupy identyczne z wykonywanym od zera pełnym backupem.  a. Musi istnieć możliwość zastosowania wyrażeń regularnych do określenia które wirtualne dyski VMware mają być backupowane.  b. Wykonywanie backupu obrazów maszyn wirtualnych VMware nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk) |  |
| 35 | Powyższe metody backupu maszyn wirtualnych muszą podlegać de-duplikacji ze zmiennym blokiem przed wysłaniem danych do medium backupowego zgodnie z wymaganiami dla de-duplikacji powyżej. |  |
| 36 | Powyższe metody backupu muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. |  |
| 37 | Oferowany system musi pozwalać na szybkie odtworzenie  a. całych obrazów maszyn wirtualnych  b. pojedynczych dysków maszyny wirtualnej z backupu całej maszyny wirtualnej |  |
| 38 | Rozwiązanie backupowe musi umożliwiać odtworzenie obrazów maszyn wirtualnych VMware dostarczając następujące funkcjonalności:  a. Odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu.  b. Odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu.  c. Odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux.  d. Możliwość zamontowania na dowolnym serwerze (fizycznym lub wirtualnym) zbackupowanych obrazów maszyn wirtualnych Windows (plików vmdk maszyny wirtualnej Windows). Powyższa metoda nie może fizycznie odtwarzać backupów a jedynie pozwalać na przeglądanie zawartości plików vmdk w backupie z poziomu Eksploratora Plików Windows na dowolnej maszynie. |  |
| 39 | Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend. |  |
| 40 | Rozwiązanie backupowe musi umożliwiać uruchomienie maszyny wirtualnej bezpośrednio z medium backupowego bez konieczności odtwarzania (Instant Access). |  |
| 41 | Oprogramowanie backupowe musi mieć możliwość prezentacji (bez konieczności odtworzenia) zbackupowanych obrazów maszyn wirtualnych VMware (plików vmdk) jako katalogów na maszynie fizycznej celem ich przeszukiwania (wymagane przeszukiwanie po nazwach plikó jak również zawartości plików) z poziomu systemu operacyjnego maszyny fizycznej. |  |
| 42 | Oprogramowanie backupowe musi mieć możliwość backupu / odtworzenia w trybie „image backup” (backup plików vmdk) maszyn wirtualnych znajdujących się na serwerach VMware ESX bez udziału vCenter. |  |
| 43 | Skalowalność rozwiązania dla środowisk VMware musi być na poziomie:  a. Minimum 3000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu.  b. Minimum 100 maszyn wirtualnych backupowanych w ciągu godziny w ramach pojedynczej instancji systemu backupu. |  |
| 44 | Rozwiązanie backupowe musi umożliwiać backup i odtwarzanie w tym samym czasie minimum 50 maszyn wirtualnych VMware. |  |
| 45 | Oprogramowanie backupowe musi mieć możliwość automatycznego sprawdzania (weryfikacji) zbackupowanych maszyn wirtualnych VMware. Musi istnieć możliwość ustawienia kalendarza weryfikacji maszyn wirtualnych VMware. |  |
| 46 | Weryfikacja maszyn wirtualnych musi zapewniać minimum:  a. Odtworzenie maszyny wirtualnej na zdefiniowanym Data Center / Data Store,  b. Weryfikacja podstawowych procesów,  c. Możliwość dołączenia własnego skryptu weryfikującego wybrane elementy maszyny wirtualnej. |  |
| 47 | Informacja w konsoli systemu backupu o poprawnej / niepoprawnej weryfikacji maszyny wirtualnej. |  |
| 48 | Administrator (właściciel) danej maszyny wirtualnej VMware musi mieć możliwość samodzielnego (bez konieczności kontaktu z administratorem backupu czy tez administratorem VMware) odtworzenia pojedynczych plików z dowolnego backupu obrazu jego maszyny wirtualnej. |  |
| 49 | Oprogramowanie backupowe musi zawsze przechowywać pełne backupy obrazów maszyn wirtualnych środowiska VMware/HyperV dla każdej wykonanej w przeszłości kopii zapasowej. Każdy backup obrazu maszyny wirtualnej musi być backupem pełnym. |  |
| 50 | Rozwiązanie backupowe musi pozwalać automatyczne polityki backupowe dla:  a. Folderu,  b. Resource Pool systemu VMware. |  |
| 51 | Oznacza to, że dodanie maszyny wirtualnej do folderu, hosta czy resource pooli w systemie VMware spowoduje automatyczne backupowanie dodanej maszyny wirtualnej zgodnie z polityka zdefiniowana dla folderu hosta czy resource pooli w systemie VMware. |  |
| 52 | Rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych. |  |
| 53 | Oferowany system musi automatycznie naprawiać problemy związane ze snapshotami VMware. W przypadku gdy system VMware nie usunie snapshotu, oprogramowanie backupowe musi automatycznie ponawiać usunięcie snapshotu a w przypadku konieczności automatycznie konsolidować maszyny wirtualne VMware. |  |
| 54 | Backup oraz odtworzenie maszyn wirtualnych VMware musi być możliwy z poziomu graficznego interfejsu, linii komend oraz przez REST API. |  |
| 55 | Musi istnieć możliwość odtworzenia danych:  a. z zabezpieczanego serwera / komputera,  b. z konsoli systemu backupowego. |  |
| 56 | System backupu musi mieć funkcjonalność wyrzutu na taśmę. |  |
| 57 | Opcja wyrzutu na taśmę musi być elementem niniejszej oferty. |  |
| 58 | System backupu musi mieć możliwość bezpośredniego raportowania o błędach do serwisu producenta. |  |
| 59 | System backupu musi mieć możliwość instalacji agentów jako plików msi. Musi istnieć możliwość automatyzacji agentów poprzez uruchomienie skryptu instalującego agenta na zabezpieczanej maszynie i przyporządkowującego maszynę automatycznie do określonej polityki backupowej. |  |
| 60 | System backupu musi mieć możliwość automatycznej samo-aktualizacji poprzez automatyczne ściąganie nowych wersji od producenta. |  |
| 61 | System backupu musi mieć możliwość automatycznej aktualizacji oprogramowania agentów wykonywanej bezpośrednio z serwera backupu. |  |
| 62 | W ramach licencji musi być zapewniona możliwość monitorowania, raportowania. |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_, dnia \_\_\_\_\_\_\_\_\_2018 r.

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

(podpis i pieczęć Wykonawcy)