Załącznik nr 2a
do SIWZ OR-IV.272.12.2017.JG

Szczegółowe wymagania co do parametrów technicznych i właściwości sprzętu infrastruktury serwerowej - poprawiony

Przełącznik sieciowy

Atrybut	Minimalne wymagania
Architektura sieci LAN	GigabitEthernet 10GigabitEthernet
SmartSwitch (WEB Managed)	Tak
Liczba portów 1000BaseT (RJ45)	48 szt.
Liczba gniazd 10GB SFP+	4 szt.
Porty komunikacji	Port konsoli
Zarządzanie, monitorowanie i konfiguracja	SNMP - Simple Network Management Protocol SNMPv1 - Simple Network Management Protocol ver. 1 SNMPv2 - Simple Network Management Protocol ver. 2 SNMPv3 - Simple Network Management Protocol ver. 3 RMON - Remote Monitoring HTTP - Hypertext Transfer Protocol HTTPS - Hypertext Transfer Protocol Secure DHCP Client - Dynamic Host Configuration Protocol (RFC 2131) zarządzanie przez przeglądarkę WWW GUI - graficzny interfejs użytkownika
Protokoły uwierzytelniania i kontroli dostępu	SSH - Secure Shall SSL - Secure Sockets Layer RADIUS - zdalne uwierzytelnianie użytkowników TACACS+ - Terminal Access Controller Access Control System
Obsługiwane protokoły routingu	CIDR - Classless Inter-Domain Routing RIP v2 - Routing Information Protocol ver. 2 VRRP - Virtual Router Redundancy Protocol
Obsługiwane protokoły i standardy	IEEE 802.1Q - Virtual LANs IEEE 802.1D - Spanning Tree IEEE 802.1s - Multiple Spanning Tree IEEE 802.3ad - Link Aggregation Control Protocol IEEE 802.1Q-in-Q - VLAN Tag GVRP - Group VLAN Registration Protocol DHCP - Dynamic Host Configuration Protocol IPv4 UDP - datagramowy protokół użytkownika ARP - Address Resolution Protocol QoS - Quality of Service (kontrola jakość usług i przepustowości) GARP - Generic Attribute Registration Protocol LLDP-MED - Link Layer Discovery Protocol - Media Endpoint Discovery Cisco Discovery Protocol TFTP - Trivial File Transfer Protocol BOOTP - BOOTstrap Protocol IEEE 802.3az - Energy Efficient Ethernet TCP/IP - Transmission Control Protocol/Internet Protocol
Rozmiar tablicy adresów MAC	16000
Algorytm przełączania	Store-and-Forward

Prędkość magistrali wew.	176 Gb/s
Przepustowość	130,95 mpps (64-byte packets)
Warstwa przełączania	3
Możliwość łączenia w stos	Tak
Typ obudowy	1U Rack
Wymagania dodatkowe	Dostawca powinien dostarczyć niezbędne okablowanie i ewentualne moduły potrzebne do połączenia ze sobą przełączników w stos. Dostawca musi zapewnić szyny i akcesoria do montażu w szafie rack 19” Gwarancja minimum 36 miesięcy

Urządzenie UTM

	Minimalne wymagania
	1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.
	2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 5. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 6. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 7. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall’u. 8. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 9. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).
	10. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 11. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 12. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 13. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 14. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 15. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 16. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.

	17. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 18. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 19. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 20. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
	21. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 22. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 23. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 24. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.
	25. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 26. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 27. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 28. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
	29. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 30. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN 31. SSL VPN musi działać w trybach Tunel i Portal. 32. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 33. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 34. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 35. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based.
	36. Urządzenie ma posiadać wbudowany filtr URL. 37. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 38. Administrator musi mieć możliwość dodawania własnych kategorii URL. 39. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 40. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 41. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL,

	c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 42. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 43. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych. 44. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 45. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 46. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 47. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.
	48. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory. 49. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP. 50. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos. 51. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 52. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. 53. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.
	54. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). 55. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia. 56. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 57. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 58. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 59. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 60. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 61. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 62. Rozwiązanie powinno wspierać technologię Link Aggregation.
	63. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 64. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 65. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 66. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 67. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 68. Urządzenie musi posiadać usługę DNS Proxy.

	69. Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 70. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 71. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 72. Komunikacja może odbywać się na porcie innym niż https (443 TCP). 73. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 74. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 75. Platforma do centralnej administracji powinna pozwalać na zarządzanie przynajmniej 5 urządzeniami w różnych lokalizacjach bez konieczności zakupu dodatkowej licencji. 76. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 77. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 78. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 79. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 80. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
	81. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 82. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 83. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 84. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. 85. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 86. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 87. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy
	88. Urządzenie ma być wyposażone w dysk twardy o pojemności co najmniej 320 GB. 89. Liczba portów Ethernet 10/100/1000Mbps – min. 12. 90. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 91. Przepustowość Firewalla – min. 5 Gbps 92. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 3 Gbps. 93. Przepustowość filtrowania Antywirusowego – min. 850 Mbps 94. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1 Gbps. 95. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500 96. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100 97. Obsługa min. VLAN 256 98. Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 20 000 nowych sesji/sekundę.

	99. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive. 100. Urządzenie jest nielimitowane na użytkowników. 101. Urządzenie ma być objęte gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od stwierdzenia awarii, taka gwarancja powinna być zapewniona przez min. 36 miesięcy.
	102. Dostawca zapewni zamawiającemu Vouchery dla 2 osób, na autoryzowane przez producenta rozwiązania szkolenie, realizowane przez autoryzowany ośrodek szkoleniowy. Ważność voucherów minimum pół roku od daty zakupu. Zamawiający ma mieć możliwość wyboru i dołączenia na dowolny termin szkolenia otwartego realizowanego wedle kalendarza ośrodka szkolącego

klaster wysokiej dostępności:

KLASTER WYSOKIEJ DOSTĘPNOŚCI	
Parametr lub warunek	**Minimalne wymagania**
Elementy klastra	- pamięć masowa – macierz dyskowa – szt1. - serwer - węzeł klastra – szt 2. - każdy element klastra jest zamontowany w obudowie przystosowanej do montażu w szafie rack 19”, - maksymalna wysokość klastra wysokiej dostępności wynosi 6U, - każdy element klastra musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego. - zamawiający dopuszcza integrację wszystkich elementów klastra w jednej obudowie, przy zapewnieniu możliwości rozbudowy o 2 dodatkowe serwery - węzły klastra,
Obudowa	- obudowa chłodzona powietrznie w standardzie przód-tył, wyposażona w redundantne wentylatory, - certyfikacja producenta do poprawnej i ciągłej pracy w temperaturze do minimum 35 stopni Celsjusza, - diodowa wizualizacja obecności zasilania dla obudowy, - diodowa sygnalizacja pracy/awarii zasilaczy i układu chłodzenia, - Dostawca musi zapewnić szyny i akcesoria do montażu w szafie rack 19”,
Zasilanie	- każdy element klastra jest wyposażony w redundantne zasilanie hot-plug charakteryzujące się sprawnością klasy Platinum (94%) o łącznej mocy wszystkich zasilaczy wchodzących w skład klastra wynoszącej minimum 3000W,
Wysoka dostępność	- oferowany klaster nie może mieć pojedynczego punktu usterki: połączenie pomiędzy elementami klastra ma być zrealizowane redundantnie, - połączenie węzłów z macierzą dyskową zrealizowane w standardzie SAS 3 12 Gbit/s, - możliwość współdzielenia dysków macierzy pomiędzy węzłami,
Gwarancja	- każdy element klastra musi być objęty minimum 36 miesięczną gwarancją producenta w trybie onsite z gwarantowanym (SLA) czasem skutecznej naprawy elementu najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime), - dyski twarde które ulegną awarii pozostają własnością Zamawiającego, - dostępność części zamiennych przez 5 lat od momentu zakupu klastra; - wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/ Firmware/ sterowników dożywotnio dla każdego oferowanego elementu klastra – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta elementu klastra, takowa licencja musi być uwzględniona w konfiguracji;
Dokumentacja, inne	- telefoniczna infolinia/linia techniczna producenta klastra, w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwerów, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; - możliwość aktualizacji i pobrania sterowników do oferowanych serwerów w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta elementu klastra,
Element klastra - pamięć masowa – macierz dyskowa – 1 szt.	

Parametr lub warunek	Minimalne wymagania
Macierz	- Minimum 16 wnęk dla dysków twardych Hotplug 2,5 cala; - Możliwość współdzielenia dysków pomiędzy węzłami klastra z zapewnieniem redundancji połączeń, - Możliwość podłączenia do 4 węzłów klastra z zapewnieniem redundancji połączeń, -obsługiwany tiering dla całej dopuszczalnej pojemności macierzy dyskowej, jeżeli są wymagane jakiekolwiek dodatkowe licencje należy takie elementy wliczyć do oferty
Dyski twarde	- Zainstalowane 8 dysków SAS 3.0 10K RPM o pojemności 600GB każdy, dyski Hotplug,
Element klastra - Serwer – węzeł – 2 szt.	
Parametr lub warunek	**Minimalne wymagania**
Płyta główna	-Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów dwunastordzeniowych, -Wsparcie dla procesorów o TDP 160W, -Minimum 2 złącza PCI Express generacji 3 o prędkości x16, -Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora (niezależne od dysków twardych),
Procesory	-Zainstalowane dwa procesory 8-rdzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECint_rate2006 min. 665 pkt; -Wymagane dołączenie do oferowanego urządzenia pełnego protokołu testów SPEC dla oferowanego modelu serwera wyposażonego w oferowane procesory, protokół poświadczony przez producenta serwera;
Pamięć RAM	-Zainstalowane 64 GB pamięci RAM typu DDR4 Registered, 2400Mhz w kościach o pojemności 32GB - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC lub Chipkill lub inne równoważne zapewniające co najmniej wymieniony poziom zabezpieczeń i pracy oraz Memory Scrubbing (tj. technologię, która koryguje zawartość pamięci RAM, poprzez odczyt uszkodzonych danych, korekcje ECC oraz ponowne zapisanie danych do pamięci RAM, w sposób cykliczny lub po wykryciu błędu przy odczycie (tzw. patrol scrubbing lub demand scrubbing)), SDDC. -Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing”; -Minimum 16 gniazd pamięci RAM na płycie głównej, obsługa minimum 1024GB pamięci RAM DDR4;
Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 3.0 obsługujący funkcje klastrowania, zapewniający fizyczny dostęp do wszystkich dysków zainstalowanych w obudowie na serwery z zachowaniem redundancji połączeń,
Dyski twarde	Dysk SSD SATA o pojemności min. 128 GB z zainstalowanym oprogramowaniem hypervisora
Kontrolery LAN	- 2x 1Gb/s LAN, ze wsparciem iSCSI i iSCSI boot i teamingu, RJ-45, niezajmująca złącz PCI Express; - dodatkowa karta sieciowa 4x 1Gb/s LAN, RJ-45
Porty	zintegrowana karta graficzna ze złączem VGA; -2x USB 3.0;
Zarządzanie	-Przyciski/wizualizacja pracy: • włącznik serwera z wizualną (np. diodową) kontrolą stanu (on/off) • diodowa sygnalizacja obecności/braku zasilania • diodowa sygnalizacja obecności błędów sprzętowych • diodowa sygnalizacja pozycji maszyny (ID) wraz z przyciskiem fizycznym pozwalającym na włączenie/wyłączenie sygnalizacji pozycji maszyny • diodowa sygnalizacja pracy każdego z dysków twardych • diodowa sygnalizacja awarii dysku -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania

	• Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • 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.).
Zainstalowany system operacyjny	-Windows Server 2012 R2 Standard z uruchomionym klastrem Hyper-V lub równoważny. Warunki równoważności: - Licencja umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server 2012 R2 Standard Edition w trybie klastra HYPER-V. Minimalne wymagania funkcjonalności: - możliwość dokonywania aktualizacji i poprawek systemu przez internet z możliwością wyboru instalowanych poprawek; -możliwość dokonywania uaktualnień sterowników urządzeń przez internet – witrynę producenta systemu; - możliwość, w ramach pojedynczej licencji zainstalowania min. 20 systemów wirtualnych, -darmowa aktualizacja w ramach wersji systemu operacyjnego przez internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat)

NAS do backupu

Nazwa elementu, parametru lub cechy	**Opis minimalnych wymagań**
Typ	Serwer NAS do backupu danych
Zastosowanie	Backup maszyn wirtualnych
Liczba zatok na dyski	12 typu hot-swap
Pojemność	12 x 4 = 48 TB
Obsługa RAID	RAID 0,1, 5, 6, 10, 5/6/10+spare
Pamięć RAM	min 4GB
Porty	4 RJ45 Gigabit Ethernet, 4 USB 3.0
Bezpieczeństwo	Obsługa szyfrowania AES 256
Wymagania dodatkowe	Obsługa VMware, Microsoft® Hyper-V oraz zaawansowanych funkcji wirtualizacji Integracja z Active Directory Obsługa protokołów: CIFS/SMB, AFP (v3.3), NFS(v3), FTP, FTPS, SFTP, TFTP, HTTP(S), Telnet, SSH, iSCSI, SNMP, SMTP, SMSC Redundantne zasilanie Wielkość max 2U, montaż w szafie rack 19”, Dostawca musi zapewnić szyny i akcesoria do montażu w szafie rack 19”
Gwarancja	Minimum 36 miesięcy

UPS dla klastra

Nazwa elementu, parametru lub cechy	Opis minimalnych wymagań
Typ	Zasilacz awaryjny
Zastosowanie	Zapewnienie ciągłości działania platformy wirtualizacyjnej, ochrona przed przepięciami i spadkami napięć
Moc	co najmniej 5000VA/4500W – dostawca musi zapewnić wystarczającą moc do podtrzymania platformy wirtualizacyjnej oraz backupu z możliwością dołączenia kilku urządzeń typu switch
Typ UPSa	on-line
Wymagania dodatkowe	Oprogramowanie do zarządzania, wspierane systemy: MS Windows Server 2012 R2, MS Windows Server 208 R2, VMware Infrastusture Dostawca musi zapewnić szyny i akcesoria do montażu w szafie rack 19”
Gwarancja	Minimum 36 miesięcy

Oprogramowanie do backupu maszyn wirtualnych

Nazwa elementu, parametru lub cechy	Opis minimalnych wymagań
Wymagania ogólne	• Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej • Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami. • Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami. • Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V
Całkowite koszty posiadania	• Oprogramowanie musi być licencjonowanie w modelu “per-CPU”. Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone • Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej • Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków • Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji • Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. • Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania • Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia • Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość akutalizacji pola „notatki” na wirtualnej maszynie • Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.

	• Oprogramowanie musi zapewniać bezpośrednią integrację z VMware vCloud Director 5.5, 5.6, 8.0, 8.10 i archiwizować również metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD • Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji • Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji • Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX) • Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Wymagania	• Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej • Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora • Oprogramowanie musi wspierać kopiowanie plików na taśmy • Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server • Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej • Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) • Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu. • Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. • Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik • Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) • Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V • Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) • Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere • Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing) • Oprogramowanie musi umożliwić uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla srodowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania • Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować jaką migrację swoimi mechanizmami • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków • Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure. • Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików

	• Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. • Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: o Linux (xt, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs) o BSD (FS, UFS2) o Windows (NTFS, FAT, FAT32, ReFS) • Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces. • Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. • Oprogramowanie musi wspierać granularne odtwarzanie dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze. • Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. • Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia. • Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych. • Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows • Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Monitoring	• System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 4.1, 5.x oraz 6.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie • System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 oraz 2016 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. • System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware • System musi mieć możliwość instalacji na systemach operacyjnych w wersjach 64 bitowych: o Microsoft Windows 2008 SP2 o Microsoft Windows 2008 R2 SP1 o Microsoft Windows 7 SP1 o Microsoft Windows 8 o Microsoft Windows 2012 o Microsoft Windows 2012 R2 o Microsoft Windows 8.1 o Microsoft Windows 10 o Microsoft Windows 2016 • System musi obsługiwać następujące bazy danych w wersjach 32 i 64 bitowych: o Microsoft SQL Server 2008 o Microsoft SQL Server 2008 R2 o Microsoft SQL Server 2012 R2 o Microsoft SQL Server 2014 o Microsoft SQL Server 2016 • System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter

	• System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn • System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel • System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk • Silnik raportowania powinien być oparty o SQL Server Reporting Services w celu zapewnienia bezpiecznego dostępu do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji • System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora • System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów • System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) • System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna • System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego • System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta • System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. • System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware • System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 5.5, 5.6, 8.0 oraz 8.10
Raportowanie	• System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 4.1, 5.x oraz 6.0, vCenter Server 4.1, 5.x oraz 6.0 jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2i 2016. • System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. • System musi być certyfikowany przez VMware i posiadać status „VMware Ready” • System musi instalować się na następujących systemach operacyjnych: o Microsoft Windows 2008 SP2 o Microsoft Windows 2008 R2 SP1 o Microsoft Windows 7 SP1 o Microsoft Windows 8 o Microsoft Windows 2012 o Microsoft Windows 2012 R2 o Microsoft Windows 8.1 o Microsoft Windows 10 o Microsoft Windows 2016 • System musi wspierać jako silnik bazodanowy następujące bazy danych: o Microsoft SQL Server 2008 o Microsoft SQL Server 2008 R2 o Microsoft SQL Server 2012 o Microsoft SQL Server 2014 o Microsoft SQL Server 2016 • System do prezentacji raportów powinien używać SQL Server Reporting Services w celu jednoczesnego dostępu do raportów wielu użytkowników z określonymi przez administrator systemu uprawnieniami. • System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V • System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF • System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc

	• System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach • Minimalny interwał czasowy dla zadań kolekcjonowania i raportowania musi wynosić min 1 godzinę • System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów • System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych • System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych • System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury • System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta • System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn wirtualnych, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. • System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'. • System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware • System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) • System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie
Wymagania dodatkowe	Licencja musi zostać dobrana pod kątem zamawianego klastra wysokiej dostępności. Licencja na minimum 36 miesięcy

Dostarczone przez Wykonawcę licencje muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia (np. certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji, wpis na stronie producenta oprogramowania, itp.)
Potwierdzenie udzielenia licencji dla Zamawiającego będzie dostępne bezpośrednio na stronie internetowej producenta oprogramowania.
Zamawiający nie dopuszcza dostawy licencji ograniczonych czasowo.