Załącznik nr 1 a Parametry techniczne

Pakiet nr 1 poz. 1 Dostawa i rozbudowa serwera RIS/PACS wraz z UPS

UWAGA! Oferta przedstawiająca urządzenie nie spełniające warunków granicznych wymaganych przez Zamawiającego w poniższym formularzu zostanie odrzucona jako niezgodna z treścią SIWZ.

Lp.	Opis parametru wymaganego/ granicznego	Wartość wymagana /graniczna	Oferowany parametr / cecha
	SERWERY RIS/PACS - 2 szt.		
1.	Producent	(Podać)	
2.	Typ/model	(Podać)	
3.	Pełna nazwa urządzenia/systemu	(Podać)	
4.	Rok produkcji:	(Podać)	
	Obudowa:		
5.	Rack o wysokości max 1U z możliwością instalacji do 4 dysków 2.5" Hot-Plug wraz z kompletem szyn umożliwiających montaż w szafie rack z funkcjonalnością wysuwania serwera do celów serwisowych oraz z ramieniem do zarządzania przewodami.	TAK	
6.	Obudowa posiadająca przedni panel zamykany na klucz.	TAK	
7.	Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS, SSD.	TAK	
	Płyta główna:		
8.	Z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	TAK	
9.	Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.	TAK	
10.	Płyta powinna obsługiwać do 1TB pamięci RAM, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczonych dla pamięci.	TAK	
11.	Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, Lockstep.	TAK	
	Procesory:		
12.	Zainstalowane dwa procesory min. 8 rdzeni/16 wątków klasy x86 dedykowane do pracy z zaoferowanym serwerem. Procesory taktowane zegarem o częstotliwości min. 2,1 GHz oraz posiadające min. 11 MB pamięci podręcznej. Dopuszczalny pobór mocy przez pojedynczy procesor 85 W. Oferowany procesor musi być wykonany w mikroarchitekturze skylake firmy Intel.	TAK, (Podać)	
	Pamięć RAM		
13.	Minimum 192 GB pamięci RAM typu DDR4 RDIMM, Dual Rank, ECC o częstotliwości pracy 2666MHz	TAK, (Podać)	

	Karta grafiki		
14.	Zintegrowana karta graficzna umożliwiająca wyświetlanie rozdzielczości min. 1920x1200.	TAK	
	Porty zewnętrzne		
15.	– min. 4 porty USB z czego min. 3 porty USB 3.0, – 2 porty RJ45 oraz 2 porty 10Gb SFP+ – 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym) – min. 1 serial port Powyższe porty nie mogą zostać osiągnięte poprzez stosowanie dodatkowych adapterów, przejściówek.	TAK	
	Karty rozszerzeń:		
16.	Co najmniej czteroportowa karta 1 Gigabit Ethernet ze złączami BaseT	TAK	
17.	Co najmniej dwuportowa karta 10 Gigabit Ethernet ze złączami SFP+	TAK	
18.	Co najmniej dwuportowa karta Fibre Channel Host Bus Adapter 8Gbps	TAK	
	Dyski i pamięci flash:		
19.	Zainstalowane 2 dyski o pojemności min. 32 GB typu SSD.	TAK, (Podać)	
20.	Zainstalowany dedykowany do obsługi powyższych dysków sprzętowy kontroler RAID z możliwością konfiguracji poziomów RAID co najmniej 0, 1	TAK	
	Zasilanie:		
21.	Dwa redundantne zasilacze Hot Plug o mocy co najmniej 550W każdy	TAK	
	Zabezpieczenia:		
22.	Zintegrowany z płytą główną moduł TPM 2.0.	TAK	
	Zarządzanie:		
23.	Niezależna od zainstalowanego na serwerze systemu operacyjnego karta zarządzania posiadająca dedykowany port RJ-45 Gigabit Ethernet, umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - dostęp z linii komend CLI karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (SSL) oraz autentykacje i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla SNMP v1, v2c, v3; IPMI2.0; - integracja z Active Directory;	TAK	

	- możliwość obsługi przez dwóch administratorów jednocześnie; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej, - zdalna identyfikacja fizycznego serwera i obudowy za pomocą sygnalizatora optycznego. - rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI Express. Nie dopuszcza się rozwiązań serwerowych wymagających dokupowania dodatkowych licencji umożliwiających zarządzanie serwerem i dostarczających wyżej wymienione funkcjonalności.		
	Gwarancja:		
24.	Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu przez producenta bądź autoryzowany przez producenta serwis, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, przyjmowanie zgłoszeń 24 godziny na dobę, 7 dni w tygodniu, naprawa w miejscu instalacji. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.	TAK	
25.	Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera . Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.	TAK	
26.	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001.Serwer musi posiadać deklaracja CE.	TAK	
27.	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.	TAK	
28.	Możliwość sprawdzenia poprzez stronę producenta lub telefonicznego konfiguracji sprzętowej serwera, oraz statusu i warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	TAK	
	System wirtualizacji z uruchomieniem na dostarczonym sprzęcie		
29.	Producent	(Podać)	
30.	Nazwa	(Podać)	
31.	Wersja	(Podać)	
	Konsolidacja:		
32.	Warstwa wirtualizacji powinna być rozwiązaniem systemowym tzn. powinna być zainstalowana bezpośrednio na sprzęcie fizycznym.	TAK	
33.	Rozwiązanie powinno zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.	TAK	
34.	Możliwość przydzielenia dla wirtualnej maszyny większej ilości zasobów wirtualnych, niż fizycznie dostępne serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji: – od 1 do 128 vCPU	TAK	

	– do 2TB RAM – do 62 TB przestrzeni dyskowej – możliwość skonfigurowania maszyn wirtualnych z których każda może mieć od 1 do 8 wirtualnych kart sieciowych. – możliwość dołączenia do maszyny wirtualnej fizycznych zasobów dyskowych (Raw Disk Mapping)		
35.	Rozwiązanie powinno umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.	TAK	
36.	Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.	TAK	
37.	Rozwiązanie powinno wspierać następujące rodziny systemów operacyjnych gościa: Oracle Linux, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows, Solaris	TAK	
38.	Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych bez przerywania ich pracy.	TAK	
39.	Oprogramowanie do wirtualizacji powinno zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.	TAK	
40.	Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN FibreChannel, iSCSI (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek.	TAK	
41.	Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż fizycznie dostępnych	TAK	
42.	Rozwiązanie musi mieć możliwość automatycznego równoważenia obciążenia serwerów fizycznych poprzez przenoszenie pracujących wirtualnych maszyn, oraz możliwość stałego przypisania maszyny wirtualnej do konkretnego serwera fizycznego	TAK	
43.	Rozwiązanie musi mieć możliwość oszczędzania energii elektrycznej poprzez automatyczne wyłączenie serwerów fizycznych w przypadku braku obciążenia generowanego przez wirtualne maszyny i automatycznego ich włączenia w sytuacji wzrostu obciążenia.	TAK	
	Wysoka dostępność:		
44.	Rozwiązanie musi mieć możliwość automatycznego równoważenia obciążenia serwerów fizycznych poprzez przenoszenie pracujących wirtualnych maszyn	TAK	
45.	Środowisko musi zapewniać odpowiednią redundancję i taki mechanizm (wysokiej dostępności HA) aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym	TAK	
46.	Rozwiązanie musi umożliwiać dodawanie i rozszerzanie dysków wirtualnych, procesorów i pamięci RAM podczas pracy wybranych systemów,	TAK	
47.	Obsługa statycznej oraz dynamicznej agregacji portów 802.1ad	TAK	

	Obsługa potrzeb biznesu:		
48.	Rozwiązanie powinno zapewnić możliwość szybkiego tworzenia i uruchamiania nowych usług wraz z ich pełną konfiguracją i preinstalowanymi narzędziami systemowymi w celu efektywnej obsługi wymagań biznesowych.	TAK	
49.	Rozwiązanie powinno zapewnić mechanizm wykonywania kopii - klonów systemów operacyjnych wraz z ich pełną konfiguracją i danymi.	TAK	
50.	Wraz z licencjami należy dostarczyć wsparcie producenta (Asystę Techniczną) dla w/w oprogramowania na okres co najmniej 60 miesięcy licząc od daty dostawy na warunkach określonych w Istotnych dla Stron postanowieniach Umowy oraz licencji producenta oprogramowania.	TAK	
51.	Dostarczone oprogramowanie musi pozwolić na uruchomienie klastra wirtualizacji złożonego z co najmniej dwóch serwerów, oraz nie może ograniczać ilości maksymalnie dostępnych węzłów klastra.	TAK	
	Zarządzanie:		
52.	zarządzanie poprzez dedykowany dla rozwiązania interfejs WWW/https oraz CLI	TAK	
53.	możliwość uruchomienia aplikacji do zarządzania środowiskiem na fizycznym serwerze lub w maszynie wirtualnej	TAK	
54.	dostęp do funkcji obsługi wirtualnych maszyn: tworzenie, edytowanie zasobów, klonowanie, włączanie i wyłączanie, usypianie, restart, migracji, podgląd konsoli maszyny (graficznej i tekstowej) z poziomu przeglądarki	TAK	
55.	zarządzanie więcej niż jedną pulą serwerów	TAK	
56.	zarządzanie zasobami sieciowymi (funkcje Agregacji linków, obsługa VLAN, bandwidth throttling) i dyskowymi	TAK	
57.	zarządzanie aktualizacjami serwerów z poziomu menadżera - aktualizacja bez konieczności wyłączania maszyn wirtualnych	TAK	
58.	thin provisioning, thin clone, migawki, możliwość klonowania dysków wirtualnych	TAK	
59.	importowanie i tworzenie szablonów maszyn wirtualnych	TAK	
	Pozostałe prace wymagane do realizacji:		
60.	Dla zapewnienia wysokiej wydajności wymiany danych pomiędzy systemami AMMS, oraz RIS/PACS, wymagane jest uruchomienie klastra bazodanowego i testowej bazy zgodnie z zaleceniami producenta bazy danych dla uruchomionego środowiska wirtualizacji w oparciu o posiadane przez zamawiającego dwie licencje Oracle Database 11g Enterprise, na dyskach SSD skonfigurowanych w RAID10 - jeżeli do legalnego uruchomienia baz w klastrze RAC wymagane są dodatkowe licencje oprogramowania bazy danych należy je dostarczyć w ramach postępowania. Prace związane z uruchomieniem klastra bazodanowego muszą zostać wykonane przez certyfikowanego inżyniera Oracle.	TAK	
61.	Na zainstalowanych serwerach zostaną uruchomione następujące maszyny wirtualne:	TAK	

	- serwery aplikacji JBOSS dla systemu AMMS w oparciu o system operacyjny Oracle Linux - serwery mogą być zabezpieczone przed awarią fizycznych urządzeń przez uruchomienie gościa na drugim serwerze lub inne rozwiązanie oparte na oprogramowaniu dostępnym w OS gościa - wymagane jest, zachowanie dostępności uruchomionych aplikacji w razie awarii jednej z maszyn fizycznych, oraz dzielenie obciążenia w trakcie normalnej pracy, - maszyna wirtualna do obsługi systemu RIS/PACS - jako magazyn danych wykorzystane zostaną dyski 7200 rpm z włączoną deduplikacją danych, - domena AD, serwer plików i inne wymagane do poprawnego działania (wymagane dostarczenie 300 licencji dostępowych oraz dla systemów operacyjnych uruchamianych gości) , oraz inne maszyny wirtualne z aplikacjami wykorzystywanymi przez Zamawiającego (RCP, WSUS, Płatnik itp.) sumarycznie 5 maszyn z systemem Windows Server zgodnie z zaleceniami producenta oprogramowania i dobrymi praktykami. Do uruchomienia tej części wykorzystane zostaną dyski 10 krpm w RAID10 - wymagane zapewnienie procesu automatycznego uruchomienia na dostępnym serwerze w przypadku awarii jednego z urządzeń fizycznych.		
62.	Serwer zarządzania uruchomiony w formie wirtualnej maszyny na jednym z wskazanych serwerów Zamawiającego. Hypervisor na którym będzie uruchomiony musi być również zarządzany z poziomu uruchomionego serwera zarządzania.	TAK	
63.	System operacyjny dla maszyny wirtualnej i baza danych zgodne z oferowanym systemem RIS/PACS umożliwi uruchomienie dwóch maszyn wirtualnych na dwóch serwerach w sposób pozwalający na ich migrację pomiędzy węzłami klastra. Tryb wysokiej dostępności i klaster wydajnościowy musi zostać skonfigurowany na poziomie oprogramowania bazodanowego zgodnie z zaleceniami producenta oraz dobrymi praktykami.	TAK	
64.	Przedmiot zamówienia obejmuje dostarczenie/ instalację/ konfigurację licencji pozostałego oprogramowania wchodzącego w skład przedmiotu zamówienia, w ilości niezbędnej do spełnienia wymogów SIWZ.	TAK	
65.	System monitorowania parametrów pracy urządzeń (temperatury, praca wentylatorów, napięcia itp.) i warunków w serwerowni z powiadamianiem (zalanie, temperatura wilgotność, otwarcie drzwi)	TAK	
	Macierz dyskowa 1 sztuka		
66.	Producent	(Podać)	
67.	Typ/model	(Podać)	
68.	Pełna nazwa urządzenia/systemu	(Podać)	
69.	Rok produkcji:	(Podać)	
	Obudowa:		
70.	Obudowa do montażu w szafie RACK 19” za pomocą dostarczonych dedykowanych elementów.	TAK	

	Możliwość instalacji minimum 24 dyski 2,5'' w obudowie jednostki kontrolerowej.		
71.	Maksymalna wysokość rozwiązania: 4U.	TAK	
72.	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active/active lub ALUA, z funkcjonalnością SAN. Możliwość rozbudowy o funkcjonalność dostępu plikowego NAS poprzez zakup i aktywację licencji w urządzeniu (nie dopuszcza się montażu dodatkowych elementów sprzętowych lub rekonfiguracji sprzętowej urządzenia w celu aktywacji dostępu plikowego NAS). Możliwość rozbudowy do minimum 8 kontrolerów dyskowych tworzących jedną logiczną macierz bez konieczności wymiany zaoferowanej pary kontrolerów. Rozbudowa nie może odbywać się poprzez wirtualizację (podłączanie kilku macierzy przez wirtualizator zasobów dyskowych).	TAK	
	Kontrolery dyskowe:		
73.	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active/active lub ALUA, z funkcjonalnością SAN. Możliwość rozbudowy o funkcjonalność dostępu plikowego NAS poprzez zakup i aktywację licencji w urządzeniu (nie dopuszcza się montażu dodatkowych elementów sprzętowych lub rekonfiguracji sprzętowej urządzenia w celu aktywacji dostępu plikowego NAS). Możliwość rozbudowy do minimum 8 kontrolerów dyskowych tworzących jedną logiczną macierz bez konieczności wymiany zaoferowanej pary kontrolerów. Rozbudowa nie może odbywać się poprzez wirtualizację (podłączanie kilku macierzy przez wirtualizator zasobów dyskowych).	TAK	
	Wymagana przestrzeń dyskowa:		
	Macierz musi posiadać zainstalowane:		
74.	1) min. 9 dysków 1.2TB SAS 10000RPM	TAK	
75.	2) min. 5 dysków 960GB SAS SSD eMLC	TAK	
76.	3) min. 9 dysków 6TB NL-SAS 7200RPM	TAK	
	Dodatkowa półka dyskowa:		
77.	- Obudowa do montażu w szafie RACK 19" za pomocą dostarczonych dedykowanych elementów. - Możliwość instalacji minimum 25 dysków 2.5" w obudowie, połączenie z jednostką kontrolera z wykorzystaniem co najmniej dwóch dedykowanych kabli SAS 12Gbps. - Wysokość dodatkowej półki maksymalnie 2U	TAK	
	Możliwości rozbudowy macierzy:		
78.	- Możliwość rozbudowy oferowanej macierzy, do co najmniej 480 napędów dyskowych, bez wymiany kontrolerów macierzowych, tylko poprzez dodawanie półek i dysków. - Możliwość instalacji mieszanej konfiguracji dysków SAS z SSD lub NL-SAS z SSD w obrębie jednej półki dyskowej. - Obsługa samoszyfrujących dysków SAS, SSD oraz NL-SAS.	TAK	

	- Obsługa dysków SSD o pojemności powyżej 7TB.		
	Pamięć Cache:		
79.	Minimum 32GB pamięci Cache na każdy kontroler. Pamięć Cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci Cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 72 godzin. Możliwość rozbudowy pamięci Cache o minimum 1500GB z użyciem dysków SSD	TAK	
	Zabezpieczenie dyskami SPARE:		
80.	Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.	TAK	
	Dostępne interfejsy:		
81.	- Minimum 4 interfejsów 10Gb/s SFP+ z wkładkami optycznymi SFP+ typu Multimode. - Minimum 2 interfejsy 12Gb/s SAS do połączeń z półkami dyskowymi. - Wymagane jest dostarczenie wraz z macierzą 8 kabli optycznych o długości minimum 3 metrów każdy do realizacji połączeń 10Gb/s oraz dostarczenie zalecanej przez producenta ilości kabli umożliwiających podłączenie półek dyskowych.	TAK	
	Obsługiwane typy zabezpieczenia RAID:		
82.	- Kontrolery wyposażone w funkcjonalność konfiguracji poziomów RAID: RAID 0, RAID 1, RAID 10, RAID 5, RAID 50, RAID 6. Zabezpieczenia RAID realizowane za pomocą sprzętowego, dedykowanego układu. - Zamawiający dopuści alternatywnie rozwiązanie gwarantujące zabezpieczenie przed awarią trzech dysków w grupie RAID, realizowane przez oprogramowanie kontrolera przy zachowaniu nie gorszej wydajności niż w/w poziomy RAID.	TAK	
	Prezentacja dysków logicznych o pojemności większej niż zajmowana przestrzeń dyskowa (ang. Thin Provisioning):		
83.	- Możliwość tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). - Funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Jeżeli funkcjonalność wymaga dodatkowych licencji – należy je dostarczyć.	TAK	
	Serwisowalność:		
84.	Możliwość aktualizacji firmware-u kontrolerów macierzy bez przerywania dostępu do danych.	TAK	
85.	Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania.	TAK	
86.	Macierz musi umożliwiać zdalne zarządzanie oraz automatyczne informowanie centrum serwisowego o awarii.	TAK	
	Zarządzanie:		

87.	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu GUI i CLI. Możliwość tworzenia skryptów użytkownika. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagane dostarczenie w/w funkcjonalności na zainstalowaną przestrzeń dyskową.	TAK	
	Raportowanie:		
88.	Możliwość wglądu w obecne i historyczne parametry wydajnościowe oraz możliwość generowania raportów dotyczących tych parametrów. Dopuszcza się zaoferowanie oprogramowania dodatkowego w celu dostępu do parametrów historycznych.	TAK	
	Dynamiczna zmiana wielkości wolumenów:		
89.	Macierz musi umożliwiać funkcjonalność dynamicznego zwiększania rozmiaru wolumenów. Jeżeli funkcjonalność wymaga dodatkowych licencji – należy je dostarczyć.	TAK	
	Kopie wewnątrz macierzy:		
90.	Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych lub testów systemów komputerowych. Możliwość wykonania minimum 1024 kopii migawkowych LUN. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
91.	Tworzenie na żądanie pełnej fizycznej kopii danych (klon) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Możliwość utworzenia minimum 64 kopii danych LUN typu klon. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
92.	Funkcjonalność kopiowania na żądanie danych ze źródłowego zasobu LUN na docelowy zasób LUN (ang. Lun Copy). Możliwość utworzenia minimum 64 kopii LUN. Jeżeli funkcjonalność wymaga dodatkowych licencji – należy je dostarczyć.	TAK	
93.	Funkcjonalność zapisywania tych samych danych na dwóch osobnych zasobach LUN (ang. LUN mirroring). W przypadku gdy LUN źródłowy staje się niedostępny, aplikacje automatyczne mają dostęp do lustrzanego zasobu LUN. Możliwość utworzenia minimum 128 kopii lustrzanych LUN. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
	Multipathing:		
94.	Możliwość udostępniania danych do hosta wykorzystując wiele niezależnych ścieżek (ang. Multipathing). Wymagane dostarczenie w/w funkcjonalności.	TAK	
	Migracja danych wolumenu logicznego pomiędzy różnymi technologiami dyskowymi (ang. Tiering):		
95.	Macierz musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych (ang. Tiering) na poziomie całych woluminów logicznych lub jego	TAK	

	fragmentów, w szczególności macierz musi zapewniać zmianę poziomu RAID/migrację danych bez konieczności rekonfiguracji po stronie serwerów korzystających z woluminów logicznych. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.		
	Deduplikacja:		
96.	Możliwość eliminacji identycznych danych dla systemu plikowego (NAS) oraz danych blokowych LUN (SAN). Macierz musi pozwalać na włączenie deduplikacji w trybie in-line. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności jest wymagane.	TAK	
	Zarządzanie jakością usług (ang. Quality of Service):		
97.	Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe. Określanie minimalnej lub maksymalnej wydajności konkretnego wolumenu logicznego poprzez zdefiniowanie parametrów IOPS oraz przepustowości w MB/s. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
	Funkcjonalność klastra wysokiej dostępności:		
98.	Wymagana funkcjonalność umożliwiająca zastosowanie mechanizmów synchronizacji danych między dwiema macierzami dyskowymi tego samego producenta, z możliwością automatycznego i bezprzerwowego przełączenia ruchu na drugą macierz w przypadku całkowitej niedostępności pierwszej macierzy (ang. Metro Cluster). Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
	Partycjonowanie pamięci Cache:		
99.	Partycjonowanie oraz alokowanie określonej przestrzeni pamięci Cache na żądanie (ang. Cache Partitioning) dla Cache opartego o fizyczny RAM kontrolerów. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
	Rozbudowa pamięci Cache:		
100.	Możliwość wykorzystania dysków SSD do rozbudowy pamięci Cache dla operacji odczytów. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
	Migracja wolumenów:		
101.	Możliwość migracji danych ze źródłowego (source LUN) wolumenu logicznego LUN do docelowego (target LUN) wolumenu logicznego LUN bez przerywania dostarczania usług. Jeżeli funkcjonalność wymaga dodatkowych licencji – należy je dostarczyć.	TAK	
	Wirtualizacja zewnętrznych zasobów macierzy dyskowych:		
102.	Funkcjonalność wirtualizacji zasobów kilku macierzy dyskowych różnych producentów na zaoferowanym rozwiązaniu, z możliwością zarządzania zwirtualizowanymi zasobami i ich udostępniania jako własnych z pozycji panelu administracyjnego oferowanej macierzy. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
	Replikacja danych:		

103.	Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie synchronicznym i asynchronicznym. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dopuszcza się realizację replikacji synchronicznej na podstawie funkcjonalności klastra geograficznego (Metro Cluster) z wykorzystaniem dodatkowych przełączników oraz mostków SAS. Na tym etapie postępowania, dostarczenie wskazanej funkcjonalności nie jest wymagane.	TAK	
	Load-balancing:		
104.	Macierz musi optymalizować wykorzystanie dysków w ramach wszystkich pojedynczych grup RAID, tak aby wszystkie dyski wchodzące w skład tych grup, były utylizowane w równym stopniu. Jeżeli funkcjonalność wymaga dodatkowych licencji – należy je dostarczyć.	TAK	
	Zasilacze:		
105.	Minimum 2szt., redundantne, typu hot-plug. Wymaga się dostarczenia wraz z macierzą niezbędnej ilości kabli gwarantujących redundancję zasilania.	TAK	
	Certyfikaty:		
106.	Wymagane oznaczenie produktu znakiem CE, dokumenty/deklarację producenta potwierdzający spełnienie przez produkt wymagań bezpieczeństwa zgodnie z dyrektywą. Macierz musi być wyprodukowana zgodnie z normą ISO-9001. Macierz musi znajdować się na oficjalnej liście kompatybilności VMware oraz posiadać wsparcie dla VMware SRM.	TAK	
	Gwarancja:		
107.	Minimum 5 lat gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Możliwość zgłaszania awarii poprzez polską infolinię telefoniczną producenta lub autoryzowanego partnera serwisowego producenta.	TAK	
108.	Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia.	TAK	
109.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy.	TAK	
110.	Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia.	TAK	
111.	Urządzenie musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający będzie wymagał dostarczenia wraz z urządzeniem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.	TAK	
112.	W przypadku awarii dyski twarde pozostają własnością Zamawiającego.	TAK	

	Przełączniki IP SAN - 2 sztuki		
113.	Producent	(Podać)	
114.	Model	(Podać)	
115.	Rok Produkcji	(Podać)	
	Obudowa:		
116.	Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zamontowania w szafie rack	TAK	
117.	Wymagane parametry fizyczne: a) możliwość montażu w stelażu/szafie 19” b) wysokość maksymalna 1U c) wewnętrzny zasilacz 230V AC o mocy nie większym niż 155W oraz możliwość zastosowania wewnętrznego zasilacza redundantnego (nie dopuszcza się zasilacza zewnętrznego). W ramach postępowania należy dostarczyć każdy przełącznik z 2 wewnętrznymi zasilaczami z możliwością wymiany w trakcie pracy urządzenia (ang. hot-swap) d) zakres temperatur pracy ciągłej co najmniej 0 – 45 °C e) port USB umożliwiający podłączenie zewnętrznej pamięci flash f) wymiary urządzenia nie większe niż (WxDxH): 445mm x 430mm x 45mm g) waga urządzenia nie większa niż 10kg h) możliwość wymiany modułu wentylatora w trakcie pracy urządzenia (ang. hot-swap)	TAK	
	Porty:		
118.	Przełącznik musi posiadać 24 porty 10Gigabit Ethernet ze stykiem definiowanym przez moduły SFP+ z obsługą standardów 10GBase-SR, 10GBase-LR i 10GBase-ER, kable DAC o długości minimum 1m, 1000Base-SX, 1000Base-LX, 1000Base-T, modułów CWDM 1G oraz 10G, modułów DWDM 1G oraz 10G. Przełącznik musi posiadać 2 porty 40G ze stykiem definiowanym przez modułu QSFP+ z obsługą standardów 40GBase-SR4, 40GBase-LR4 oraz kable DAC o długości minimum 1m.	TAK	
119.	Wraz z przełącznikiem należy dostarczyć 12 wkładek (6 kompletów) SFP+ 10G-SR oraz kompatybilne okablowanie do podłączenia dostarczonych serwerów oraz innych urządzeń Zamawiającego (standard LC). Wkładki SFP+ muszą pochodzić od producenta oferowanych przełączników w celu zapewnienia jak najlepszej kompatybilności oraz muszą posiadać takie samo wsparcie serwisowe jak oferowane przełączniki.	TAK	
120.	Dodatkowo należy dostarczyć zgodnych z dostarczonymi urządzeniami: 18 wkładek SFP 1Gbps z patchcordami ST-LC o długości 5 metrów do podłączenia przełączników dostępowych Zamawiającego, oraz 24 (6 kompletów po 4 wkładki) 1Gbps wraz z patchcordami LC-LC do połączenia pozostałych przełączników w serwerowni Zamawiającego. Zamawiający w ramach zamówienia wymaga uruchomienia spójnej konfiguracji dla wszystkich posiadanych i dostarczonych urządzeń w	TAK	

	zakresie routingu, STP, VLAN, Link Aggregation.		
121.	Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności: a) Zarządzanie stosem poprzez jeden adres IP b) Do min. 9 jednostek w stosie c) Magistrala stackująca o wydajności większej niż 160Gb/s d) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation) e) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree f) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia wraz z kablami stackującymi o długości min. 1m. Zamawiający wymaga aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink 40G.	TAK	
	Wydajność/ funkcje:		
122.	Matryca przełączająca o wydajności min. 2,5 Tbps, wydajność przełączania przynajmniej 240 Mpps	TAK	
123.	Wbudowana pamięć RAM min. 1GB	TAK	
124.	Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 200MB	TAK	
125.	Obsługa min. 32.000 adresów MAC	TAK	
126.	Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)	TAK	
127.	Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI działających równocześnie	TAK	
128.	Obsługa ramek jumbo o wielkości min. 9216 bajtów	TAK	
129.	Obsługa protokołu GVRP	TAK	
130.	Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP	TAK	
131.	Wsparcie dla funkcjonalności PVST bądź równoważnej	TAK	
132.	Obsługa min. 8 000 tras dla routingu IPv4	TAK	
133.	Obsługa min. 4 000 tras dla routingu Ipv6	TAK	
134.	Obsługa min. 3 000 tras dla routingu statycznego Ipv4	TAK	
135.	Obsługa min. 1 000 tras dla routingu statycznego Ipv6	TAK	
136.	Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-Isv6, BGPv4, BGPv4+,RIP, RIPng, PIM-SM, PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania	TAK	

137.	Obsługa min. 64 wirtualnych tablic routingu-forwardingu (VRF)	TAK	
138.	Obsługa protokołów LLDP i LLDP-NP.	TAK	
139.	Przełącznik musi posiadać funkcjonalność DHCP Server i DHCP Relay	TAK	
140.	Obsługa ruchu multicast – IGMP v1, v2 i v3 oraz IGMP v1/2/3 Snooping	TAK	
141.	Mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) min. 4 poziomy dostępu administracyjnego poprzez konsolę b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL c) możliwość utworzenia minimum 1000 list ACL d) możliwość utworzenia minimum 2000 reguł w liście ACL e) możliwość utworzenia minimum 200 różnych przedziałów czasowych (ang. time ranges/ schedule) w celu aktywacji list kontroli ACL w zadanym okresie czasu (np. lista ACL jest aktywna w godzinach pracy) f) możliwość uwierzytelniania urządzeń na porcie celem uzyskania dostępu do sieci w oparciu o adres MAC, 802.1x oraz poprzez wbudowany w przełącznik portal www. Możliwość ustawienia wiele metod uwierzytelniania na pojedynczym porcie (np. 802.1x i Portal, 802.1x i MAC) g) zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów Ipv4 i Ipv6 h) możliwość filtrowania ruchu w oparciu o adresy MAC, Ipv4, Ipv6, porty TCP/UDP i) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny), j) możliwość synchronizacji czasu zgodnie z NTP	TAK	
142.	Obsługa funkcjonalności UDLD lub równoważnej	TAK	
143.	Wsparcie dla VRRP dla IPv4 oraz IPv6. Obsługa minimum 64 grup VRRP.	TAK	
144.	Obsługa protokołu BFD. Wsparcie BFD dla tras statycznych, RIP, OSPF, OSFPv3.	TAK	
145.	Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach: a) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP b) wsparcie dla mechanizmów QoS: WRR, DRR, SP, WRR+SP, DRR+SP	TAK	
146.	Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP	TAK	

	w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania		
147.	Wymagane opcje zarządzania: a) możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC) c) urządzenie musi posiadać wbudowany port USB muszą pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych d) dedykowany port konsoli e) dedykowany port zarządzający out-of-band Ethernet 10/100Base-T	TAK	
	Gwarancje/wsparcie:		
148.	Wraz z urządzeniami muszą zostać dostarczone: a) pełna dokumentacja w języku polskim lub angielskim b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana	TAK	
149.	Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy	TAK	
150.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski	TAK	
151.	Zamawiający wymaga, aby przełącznik posiadał 5-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia	TAK	
152.	Zamawiający wymaga, aby przełącznik posiadał gwarancję producenta typu limited life time zapewniającą wymianę uszkodzonego urządzenia przez okres minimum 3 lat od daty zakupu	TAK	
153.	Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres eksploatacji urządzeń	TAK	

	Ochrona sieci - UTM	TAK, (Podać)	
154.	Producent		
155.	Typ/model		
156.	Pełna nazwa urządzenia/systemu		
157.	Rok produkcji:		
	Wymagania ogólne:		
158.	Architektura systemu - dedykowana platforma sprzętowa opracowana przez producenta wykorzystującej wielordzeniową architekturę sprzętową.	TAK	
159.	Dedykowany system operacyjny firewalla opracowany przez producenta urządzenia.	TAK	
160.	Możliwość uruchomienia firewalla w trybie routingu, transparentnym lub hybrydowym (oba tryby uruchomione jednocześnie).	TAK	
161.	Możliwość uruchomienia funkcjonalności NAT w tym translacja adresu IP źródłowego, translacja adresu IP przeznaczenia, PAT, translacja statyczna i translacje puli adresów IP.	TAK	
162.	Możliwość usunięcia wirusa, wyświetlenie strony alarmującej, oznaczanie wiadomości mailowej oraz logowanie.	TAK	
163.	Możliwość uruchomienia funkcjonalności IPS, AV, URL filtering oraz AS. Wraz z urządzeniem ma być dostarczona subskrypcja na aktualizację wszystkich funkcjonalności UTM.	TAK	
	Redundancja, monitoring i wykrywanie awarii:		
164.	Urządzenie wyposażone w minimum 2 wewnętrzne zasilacze 230V AC. Nie dopuszcza się rozwiązań z zewnętrznym redundantnym zasilaczem.	TAK	
165.	Możliwość uruchomienia firewalla w trybie redundantnej pracy dla zwiększenie niezawodności. Możliwość pracy w trybie active/active oraz active/standby	TAK	
166.	Możliwość uruchomienia przynajmniej 100 wirtualnych firewalli. Jeśli jest wymagana licencja urządzenie powinno być dostarczone z licencją na przynajmniej 10 wirtualnych firewalli.	TAK	
167.	Wsparcie dla mechanizm redundancji systemu (klaster urządzeń) w trybie routingu jak i transparentnym.	TAK	
	Interfejsy, dysk, zasilanie:		
168.	Liczba portów Ethernet 10/100/1000Mbps – min. 8.	TAK	
169.	Liczba portów 1000Base-X ze stykiem SFP – min. 4	TAK	
170.	Urządzenie ma być wyposażone w dysk o pojemności co najmniej 1200 GB.	TAK	
171.	System musi być wyposażony w wewnętrzne zasilanie AC.	TAK	
	Parametry wydajnościowe:		
172.	Liczba równoczesnych połączeń - min. 4 000 000, Liczba nowych połączeń na sekundę – min. 70 000	TAK	

173.	Przepustowość Firewall: nie mniej niż 6 Gbps	TAK	
174.	Przepustowość Firewalla wraz z włączonym systemem IPS – min. 2 Gbps.	TAK	
175.	Możliwość utworzenia 15 000 polityk bezpieczeństwa	TAK	
176.	Liczba jednoczesnych tuneli IPsec – min. 4 000	TAK	
177.	Liczba tuneli SSL VPN – min. 100. Możliwość licencyjnego rozszerzenia do 1000. Jeżeli funkcjonalność SSL VPN wymaga licencji to należy dostarczyć wraz z urządzeniem licencję na obsługę minimum 100 równoległych sesji SSL VPN	TAK	
178.	Urządzenie jest nielimitowane na użytkowników.	TAK	
	Funkcje Systemu Bezpieczeństwa:		
179.	Możliwość konfiguracji kontroli dostępu na podstawie adresów źródłowych i docelowych, portów, typu protokołu, czasu, TOS, użytkownika oraz aplikacji rozpoznawalnej przez analizę warstwy siódmej.	TAK	
180.	Możliwość otrzymania kategorii URL z serwera kategorii dostępnego w sieci Internet. Reakcja podejmowana jest na podstawie skonfigurowanej polityki i przypisanej akcji do konkretnej grupy URL.	TAK	
181.	Możliwe reakcje modułu URL filtering - "zablokuj" lub "zezwól". Możliwość wyświetlenia częściowo spersonalizowanej strony informującej o zablokowaniu dostępu.	TAK	
182.	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: • ICSA lub równoważne dla funkcji Firewall • ICSA lub równoważne dla funkcji IPS • ICSA lub równoważne dla funkcji IPSEC ICSA lub równoważne dla funkcji SSL-TLS VPN	TAK	
183.	Wsparcie dla funkcjonalności IPS. Wykrywanie anomalii w różnych protokołach, w tym w: HTTP, SMTP, FTP, POP3, IMAP4, NETBIOS, SMB, MS_SQL, Telnet, IRC oraz DNS.	TAK	
184.	Możliwość włączenia i wyłączenia funkcji IPS globalnie dla całego urządzenia.	TAK	
185.	Automatyczna aktualizacja bazy sygnatur IPS poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji.	TAK	
186.	Kontrola postów na portalach internetowych. Kontrola ściągania i wysyłania plików poprzez określenie nazwy plików, rodzaju lub rozmiaru.	TAK	
187.	Kontrola i ograniczenie ruchu P2P na podstawie protokołu.	TAK	
	Funkcje routera:		
188.	Wspierane protokoły oraz funkcjonalności dla IPv6: TCP6, UDP6, ICMPv6, PathMTU, ACL6, IPv6 DHCP (server, relay oraz client), IPv6 DNS, ND-RA, IPv6 PPPoE oraz IPv6 QoS.	TAK	

189.	Obsługa protokołów routingu dla IPv6: BGP4+, IS-ISv6, OSPFv3 oraz RIPng.	TAK	
190.	Obsługa protokołów routingu dla IPv4: RIP, OSPF, BGP, IS-IS, obsługa rutingu multicast'owego (MSDP, PM-DM, PM-SM, IGMP oraz statycznego rutingu multicast'owego)	TAK	
	Obsługa łączy WAN		
191.	Urządzenie musi posiadać wbudowany filtr URL.	TAK	
192.	Obsługa dopasowywania wpisów w whitelist oraz blacklist w oparciu o prefiks, sufiks słowa kluczowego. Blacklist i whitelist mają wyższy priorytet niż kategoria URL. Whitelist ma wyższy priorytet niż blacklist.	TAK	
193.	Obsługa kategorii URL tworzonych przez użytkownika. Kategorie stworzone przez użytkownika mają wyższy priorytet od predefiniowanych kategorii.	TAK	
194.	Polityka filtrowania URL może być oparta o grupę adresów i określony czas.	TAK	
195.	Filtrowanie na podstawie stanu sesji (ASPF). Wsparcie dla inspekcji aplikacji opartych o protokoły TCP/UDP oraz takie protokoły jak FTP, SMTP, HTTP, RTSP, H323, SIP, MSN, detekcja na podstawie zdefiniowanych portów, blokowanie Java applet/ActiveX, Mapowanie portów do aplikacji (Port to Application Mapping (PAM)), detekcja fragmentacji.	TAK	
196.	Możliwość filtrowania stron z określeniem słów kluczowych występujących w treści strony.	TAK	
	Zarządzanie pasmem:		
197.	Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytety ruchu oraz minimalną i maksymalną wartość pasma.	TAK	
198.	Ograniczenie pasma lub priorytety mają być określane względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika.	TAK	
199.	Możliwe rodzaje reakcji na zdarzenie IPS: logowanie i blokowanie pakietów.	TAK	
200.	Automatyczne generowanie polityk na podstawie analizy ruchu przechodzącego przez firewall.	TAK	
201.	Możliwość uruchomienia przynajmniej do 8 interfejsów fizycznych jako jedno łącze logiczne w celu zwiększenia przepustowości i niezawodności połączenia.	TAK	
202.	Wsparcie dla protokołów tunelowania: SSL VPN, IPSec VPN, L2TP VPN, GRE VPN, L2TP over IPSec oraz GRE over IPSec.	TAK	
	Kontrola antywirusowa:		
203.	Wsparcie dla funkcjonalności antywirus (AV). Skanowaniu różnych protokołów w celu wykrycia wirusów. Wsparcie dla wykrywania wirusów w plikach przesyłanych przez HTTP, SMTP, POP3,IMAP,NFS,SMB oraz FTP.	TAK	
204.	Dekompresja wielokrotnie skompresowanych plików od 2 do 10 poziomów w celu skanowania AV	TAK	
205.	Możliwość wylistowania wirusów zawartych w bazie AV.	TAK	

206.	Możliwość powiązania polityk AC z regułami ACL i przypisania polityk AV do strefy.	TAK	
207.	Możliwość ustawienia poziomu skanowania antywirusowego od 1 do 3 w celu zoptymalizowania obciążenia urządzenia.	TAK	
208.	Obsługa przynajmniej 21 rodzajów algorytmów kompresji w celu skanowania AV	TAK	
	Ochrona przed atakami:		
209.	Ochrona przed atakami typu SYN flood, ICMP Flood, IP spoofing, UDP Flood, Land, Fraggle, Smurf, Winnuke, Ping of Death, Tear Drop, skanowanie adresów oraz portów, IP Option control, IP fragment, TCP label validity check, large ICMP packet, ICMP redirect packet, ICMP unreachable.	TAK	
210.	Możliwość statycznej konfiguracji tzw. blacklisty jak i mechanizm dynamicznego wpisu adresów do blacklisty na podstawie wykrytych źródeł ataku oraz połączenie ACL z blacklistą.	TAK	
211.	Wysyłanie logów z modułu IPS do zewnętrznego serwera oraz generowanie różnych rodzajów raportów umożliwiających sprawdzenie najczęściej występujących ataków, ich źródeł i przeznaczenia.	TAK	
212.	Grupowanie sygnatur IPS na kategorie.	TAK	
213.	Możliwość włączania i wyłączania jednej lub wszystkich reguł IPS w polityce oraz konfiguracji rodzaju reakcji na zdarzenie.	TAK	
214.	Możliwość definiowania sygnatur IPS przez użytkownika.	TAK	
	Zarządzanie i uwierzytelnianie:		
215.	Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia.	TAK	
216.	Możliwość zarządzania urządzeniem przy wykorzystaniu protokołów HTTP i HTTPS, SSH, Telnet oraz z poziomu linii komend.	TAK	
217.	Możliwość automatycznej aktualizacji bazy wirusów poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji.	TAK	
218.	Możliwość tworzenia kopii zapasowych, eksportowania i przywracania konfiguracji.	TAK	
219.	Integracja z wewnętrzną i zewnętrzna bazą użytkowników (local, RADIUS, TACACS, AD, LDAP)	TAK	
	Logowanie zdarzeń:		
220.	Urządzenie musi posiadać wewnętrzny dysk twardy o pojemności minimum 1200G w celu logowania i tworzenia raportów dotyczących np.: Analizy ruchu z uwzględnieniem nazwy użytkownika, adresu IP, rodzaju aplikacji, ilości transmitowanych danych Statystyki dostępu do stron www z uwzględnieniem kategorii stron www oraz dokładnych witryn www.	TAK TAK	
221.	Funkcja logowania dostępu do adresów URL. Możliwość określenia osiągniętych zasobów.	TAK	
222.	Musi istnieć możliwość logowania do serwera SYSLOG.	TAK	

223.	Wysyłanie logów z modułu IPS do zewnętrznego serwera oraz generowanie różnych rodzajów raportów umożliwiających sprawdzenie najczęściej występujących ataków, ich źródeł i przeznaczenia.	TAK	
	Gwarancja oraz wsparcie:		
224.	Zamawiający wymaga, aby firewall posiadał minimum 5-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 8x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia	TAK	
225.	Dostarczony firewall musi być nowy, nie używany w żadnych innych projektach, produkowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy. Zamawiający może podczas etapu dostawy żądać oświadczenia producenta bądź oficjalnego przedstawiciela na rynku Polskim o spełnieniu powyższego punktu.	TAK	
226.	Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski		
	Serwisy i licencje:		
227.	System musi zapewniać ochronę przed nieznanym złośliwym oprogramowaniem, na zasadzie analizy behawioralnej (sandbox). Wraz z urządzeniem należy dostarczyć licencję na funkcjonalność Sandbox na okres zgodny z okresem gwarancji, świadczoną przez producenta oferowanego urządzenia. Jeżeli producent oferowanych urządzeń typu firewall nie posiada takiej usługi Zamawiający dopuszcza możliwość zaoferowania dedykowanego urządzenia (kompatybilne z oferowanym urządzeniem typu firewall) które zostanie zainstalowane w siedzibie Zamawiającego. W takim wypadku, oferowane urządzenie musi zostać dostarczone wraz z serwisem gwarancyjnym gwarantującą wymianę uszkodzonego elementu w trybie 8x5xNBD w okresie minimum 5 letnim.	TAK	
	Ochrona poczty elektronicznej		
228.	Producent	(Podać)	
229.	Typ/model	(Podać)	
230.	Pełna nazwa urządzenia/systemu	(Podać)	
231.	Rok produkcji:	(Podać)	
	Wymagania ogólne		
232.	System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników.	TAK	
233.	Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci	TAK	

	osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.		
234.	Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o dedykowany system operacyjny oraz komercyjne bazy zabezpieczeń.	TAK	
235.	Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:	TAK	
236.	Tryb Gateway.	TAK	
237.	Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).	TAK	
	Parametry fizyczne systemu antyspamowego		
	System musi być wyposażony w interfejsy:	TAK	
238.	- 4 porty Gigabit Ethernet RJ-45.	TAK	
239.	System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 500 GB.	TAK	
240.	System musi posiadać wbudowany port konsoli szeregowej.	TAK	
241.	Zasilanie z sieci 230V/50Hz.	TAK	
	Ogólne funkcje systemu ochrony poczty		
	Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:	TAK	
242.	– Wsparcie dla co najmniej 2 domen pocztowych.	TAK	
243.	– System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 2,5 tys. wiadomości/godzinę.	TAK	
244.	– Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).	TAK	
245.	– Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.	TAK	
246.	– Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).	TAK	
247.	– Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.	TAK	
248.	– Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.	TAK	
249.	– Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.	TAK	
250.	– Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.	TAK	

251.	– Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz POP3.	TAK	
252.	– Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.	TAK	
253.	– Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.	TAK	
254.	– Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.	TAK	
255.	– Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.	TAK	
256.	– Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).	TAK	
	Kontrola antywirusowa i ochrona przed malware		
	W tym zakresie dostarczony system ochrony poczty musi zapewniać:	TAK	
257.	– Skanowanie antywirusowe wiadomości SMTP.	TAK	
258.	– Kwarantannę dla zainfekowanych plików.	TAK	
259.	– Skanowanie załączników skompresowanych.	TAK	
260.	– Definiowanie komunikatów powiadomień w języku polskim.	TAK	
261.	– Blokowanie załączników w oparciu o typ pliku.	TAK	
262.	– Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antywirusowej.	TAK	
263.	Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu. Usługa typu Sandbox nie jest przedmiotem w ramach dostawy specyfikowanego urządzenia, intencją zamawiającego jest możliwość podłączenia urządzenia do tego typu usługi w przyszłości.	TAK	
264.	Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.	TAK	
	Kontrola antyspamowa		
	System musi zapewniać poniższe funkcje i metody filtrowania spamu:		
265.	Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.	TAK	
266.	Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.	TAK	

267.	Szczegółowa kontrola nagłówka wiadomości.	TAK	
268.	Analiza Heurystyczna.	TAK	
269.	Współpraca z zewnętrznymi serwerami RBL, SURBL.	TAK	
270.	Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.	TAK	
271.	Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.	TAK	
272.	Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.	TAK	
273.	Kontrola w oparciu o Greylisting oraz SPF.	TAK	
274.	Filtrowanie treści wiadomości i załączników.	TAK	
275.	Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.	TAK	
276.	Możliwość zdefiniowania nie mniej niż 15 polityk kontroli antyspamowej.	TAK	
277.	Ochrona typu outbrake.	TAK	
278.	Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).	TAK	
279.	Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.	TAK	
	Ochrona przed atakami na usługę poczty		
	System musi zapewniać poniższe funkcje i metody filtrowania:	TAK	
280.	– Ochrona przed atakami na adres odbiorcy.	TAK	
281.	– Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.	TAK	
282.	– Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.	TAK	
283.	– Kontrola Reverse DNS (ochrona przed Anty-Spoofing).	TAK	
284.	– Weryfikacja poprawności adresu e-mail nadawcy.	TAK	
	Funkcje logowania i raportowania		
	W tym zakresie dostarczony system ochrony poczty musi zapewniać:	TAK	
285.	Logowanie do zewnętrznego serwera SYSLOG.	TAK	
286.	Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.	TAK	
287.	Logowanie informacji na temat spamu oraz niedozwolonych załączników.	TAK	
288.	Możliwość podglądu logów w czasie rzeczywistym.	TAK	

289.	Możliwość analizy przebiegu sesji SMTP.	TAK	
290.	Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.	TAK	
291.	Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.	TAK	
292.	Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.	TAK	
	Funkcje pracy w trybie wysokiej dostępności (HA)		
	System ochrony poczty musi zapewniać poniższe funkcje, w celu umożliwienia rozbudowy w przyszłości:	TAK	
293.	Konfigurację HA w każdym z trybów: gateway, transparent.	TAK	
294.	Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.	TAK	
295.	Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.	TAK	
296.	Monitorowanie stanu pracy klastra.	TAK	
	Aktualizacje sygnatur, dostęp do bazy spamu		
	W tym zakresie dostarczony system ochrony poczty musi zapewniać:	TAK	
297.	Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.	TAK	
298.	Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.	TAK	
	Zarządzanie		
	System ochrony poczty musi zapewniać poniższe funkcje:	TAK	
299.	System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.	TAK	
300.	Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.	TAK	
301.	Powinna istnieć możliwość zdefiniowania co najmniej 6 lokalnych kont administracyjnych.	TAK	
	Certyfikaty		
302.	VBSpam and VB100 rated lub Common Criteria NDPP, FIPS 140-2 Certified.	TAK	
	Serwisy i licencje		
303.	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów, obejmujące kontrolę Antyspam, URL Filtering, kontrolę antywirusową na okres 60 miesięcy.	TAK	

	Gwarancja oraz wsparcie		
304.	System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.	TAK	
	Oprogramowania do zabezpieczania danych poprzez mechanizm kopii zapasowych dedykowane dla środowisk wirtualizacyjnych – 4 licencje na okres 5 lat		
305.	Wspierane systemy operacyjne Dla hosta: - VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5 , - Hyper-V, - Citrix XenServer, - Red Hat Virtualization, - Linux KVM, - Oracle VM Server. Dla maszyn wirtualnych: - Windows 10, Windows 8/8.1/7/XP, Windows Vista, - Windows Server 2016, Windows Server 2012/2012R2, Windows Server 2008/2008R2, Windows Server 2003/2003R2, - Windows SBS 2011/2008, 2003/2003R2, - Windows Storage Server 2012/2012R2, 2008R2/2008/2003, - Windows MultiPoint Server 2012/2011/2010, - Linux OS (wiele dystrybucji), - macOS.	TAK	
306.	Możliwości zarządzania systemem kopii zapasowych i wymagania co do oczekiwanych funkcjonalności: - Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek WWW, - Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania system z poziomu tabletu), - Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych, - Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu),	TAK	

	- Definiowanie uprawnień dla administratorów system kopii zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.), - Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami, - Wsparcie dla Single Sign On dla logowania do systemu, - Zarządzanie procesem tworzenia kopii zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT, - Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem), - Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych. - Zdalna instalacja agentów kopii zapasowych na maszynach z systemem operacyjnym Windows, - Zdalne uaktualniania agentów kopii zapasowych - Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych - Możliwość zdefiniowania dedykowanej maszyny, której agent kopii zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej), - Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych, - Centralny katalog wszystkich danych zapisanych w kopiach zapasowych, - Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.		
307.	Wymagane związane z wykonywaniem kopi zapasowych: - Kopie zapasowe całych dysków i partycji, - Kopie zapasowe wybranych plików i folderów, - Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWare ESXi), - Kopie zapasowe aplikacji (Exchange, SQL, SharePoint, Active Directory), - Kopie zapasowe baz danych Oracle, - Kopie zapasowe hostów Hyper-V i VMWare ESXi, - Zapis kopii zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez producenta systemu kopi zapasowych, - Zapis kopii zapasowych na udziały sieciowe, - Zapis kopii zapasowych na serwer SFTP, - Zapis kopii zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana, - Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery),	TAK	

	- Możliwość wyszukiwania plików w kopiach zapasowych, - Szyfrowanie plików kopi zapasowych, - Wsparcie dla technologii VSS, - Deduplikacjia kopii zapasowych na poziomie bloków danych, - Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć, - Kompresja plików kopii zapasowych, - Replikacja kopii zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy), - Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych.		
308.	Wymagania związane z odtwarzaniem danych z kopii zapasowych: - Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore, - Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową, - Odtworzenie całego hosta (Hyper-V i VMWare ESXi) na takiej samej lub innej platformie sprzętowej, - Odtworzenie poszczególnych plików i folderów, - Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania), - Granularne odtwarzanie baz danych Microsoft Exchange, - Granularne odtwarzanie skrzynek pocztowych i poszczególnych wiadomości email z Microsoft Exchange, - Wyszukiwanie i podgląd odtwarzanych wiadomości email, - Granularne odtwarzanie baz danych Microsoft SQL, - Granularne odtwarzanie witryn i plików Microsoft SharePoint, - Odtwarzanie kontrolerów domeny Microsoft Active Directory, - Granularne odtwarzanie baz danych Oracle, - Dla hostów VMware ESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście, - Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.	TAK	
309.	Dodatkowe wymagania związane ochroną danych: Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń	TAK	
310.	Wymagania co do modelu licencjonowania rozwiązania - licencji dożywotnie, - model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość	TAK	

	danych, maszyn wirtualnych i aplikacji.		
	Rozbudowa istniejącej infrastruktury		
	Pamięć do serwerów HP ProLiant DL360 Gen9 (2 sztuki)		
311.	Rozbudowa pamięci RAM do 128 GB/serwer (aktualnie 64 GB/serwer)	TAK	
	Akcesoria do serwerów HP ProLiant DL360 Gen9		
312.	HPE Ethernet 10Gb 2-port 560SFP+ Adapter lub kompatybilne z posiadanym sprzętem – 1 sztuka/serwer	TAK	
313.	HPE 82Q 8Gb Dual Port PCI-e FC HBA lub kompatybilne z posiadanym sprzętem – 1 sztuka/serwer	TAK	
	Dyski		
314.	Rozbudowa serwera NAS QNAP - 8 dysków twardych o pojemności minimum 10TB SATA 7200rpm Hot-Plug o określonym przez producenta parametrze MTBF 2500000h	TAK	
	Oprogramowanie		
315.	Windows Server 2016 lub równoważny (4 sztuki) wraz z licencjami dostępowymi CAL (300 sztuk)	TAK	
316.	Dostarczone licencje MS pozwalające na uruchomienie OS w starszych wersjach	TAK	
	Oprogramowanie antywirusowe		
317.	Ochrona antywirusowa dla serwerów z oprogramowaniem MS Windows Serwer 2016 (10 licencji) z licencją 5 lat	TAK	
318.	Ochrona serwera plików Windows Wsparcie dla systemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. Wbudowana technologia do ochrony przed rootkitami i exploitami. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas	TAK	

	skanowania „na żądanie” i według harmonogramu. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. Możliwość skanowania dysków sieciowych i dysków przenośnych. Skanowanie plików spakowanych i skompresowanych. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. Aplikacja powinna wspierać mechanizm klastrowania. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony. Dodanie automatycznych wyłączeń nie wymaga restartu serwera. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.		

	Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line). Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów. Aktualizacje modułów analizy heurystycznej. Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e□mail. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma		

	pytać o hasło. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo. System antywirusowy ma być w pełni zgodny z technologią CISCO NAC. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz pamięci USB. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer		

	aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). Aplikacja musi wspierać skanowanie magazynu Hyper-V. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów. Praca programu musi być niezauważalna dla użytkownika. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.		
	Zasilacz awaryjny UPS z dodatkowymi modułami bateryjnymi	TAK, (Podać)	
319.	Producent	(Podać)	
320.	Model	(Podać)	
321.	Rok produkcji	(Podać)	
	Parametry		
322.	Moc pozorna/rzeczywista co najmniej: 3000VA/2700W	TAK	
323.	Liczba i rodzaj gniazdek - 8xIEC320 C13, 1xIEC320 C19	TAK	
324.	Czas przełączania na baterię – max. 4ms	TAK	
325.	Zimny start	TAK	
326.	Układ automatycznej regulacji napięcia (AVR)	TAK	
327.	Obudowa RACK 19” 2U	TAK	
328.	Karta zdalnego zarządzania/monitorowania SNMP	TAK	
329.	3 dodatkowe moduły bateryjne, każdy o pojemności baterii nie mniejszej niż pojemność proponowanego zasilacza awaryjnego	TAK	
330.	Czas podtrzymania dla obciążenia 100% - co najmniej 6 minut	TAK	
331.	Urządzenie musi być objęte serwisem producenta przez okres 24 miesięcy.	TAK	
332.	Wymagane dostarczenie urządzenia z kompletem szyn montażowych.	TAK	
333.	Wymagane dostarczenie dwóch dodatkowych list dystrybucyjnych zasilania z co najmniej 24 portami IEC C13 oraz 6-ścioma IEC C19, prąd znamionowy co najmniej 16A, wyświetlanie aktualnego obciążenia. Montaż pionowy.	TAK	
334.	Dla zapewnienia ciągłości zasilania ii zrównoważenia czasu podtrzymania z urządzeniami Zamawiającego wymagane jest dostarczenie transfer switcha umożliwiającego na jednoczesne	TAK	

	podłączenie zasilania z dwóch niezależnych źródeł. Jeżeli główne źródło zasilania ulegnie awarii, system automatycznie przełączy się na zasilanie ze źródła zapasowego. Dostępne porty dla urządzeń odbiorczych: 8xC13 oraz 1xC19.		
335.	**Konfiguracja oprogramowania z funkcjonującym u Zamawiającego systemem RIS/PACS**	TAK	
	POZOSTAŁE WARUNKI GWARANCJI I SERWISU		
336.	Wszystkie wymienione urządzenia dostarczone zostaną wraz z wymaganymi do pracy akcesoriami i okablowaniem (wkładki, patchcordy, kable stackujące, SAS, USB itp.)	TAK	
337.	Wszystkie czynności serwisowe, w tym przeglądy konserwacyjne, w okresie gwarancji – bezpłatne	TAK	
338.	Czas reakcji serwisu (dotyczy także reakcji zdalnej): „przyjęte zgłoszenie – podjęta naprawa” UWAGA: czas reakcji serwisu będzie liczony od chwili telefonicznego zgłoszenia awarii potwierdzonego faksem lub pocztą elektroniczną [godz]	TAK ≤ 24 GODZ	
339.	Możliwość zgłoszeń 24h/dobę, 365 dni/rok	TAK, (Podać) SPOSÓB	
340.	Wymiana podzespołu na nowy po pierwszej nieskutecznej próbie jego naprawy	TAK	
341.	Zakończenie działań serwisowych – najpóźniej w czasie nie dłuższym niż 2 dni kalendarzowe od dnia zgłoszenia awarii, jeśli naprawa nie wymaga użycia części zamiennych.	TAK	
342.	Wymogiem końcowego odbioru jest określenie i przekazanie wszystkich dokumentów gwarancyjnych wraz ze wskazaniem sposobu realizacji postępowania gwarancyjnego	TAK	
343.	Dostępność części w okresie pogwarancyjnym 5 lat od daty dostawy	TAK	
344.	W ramach oferty wykonawca zobowiązany jest, po dokonanej instalacji, do odebrania wszelkich opakowań po zainstalowanym sprzęcie oraz innych niewykorzystanych materiałów oraz ich utylizację na własny koszt.	TAK	
345.	Termin montażu i uruchomienia do 6 tygodni liczone od daty obustronnego podpisania umowy	TAK	
346.	Oferenci zobowiązani są załączyć przed rozpoczęciem prac harmonogram dostawy/wdrożenia do akceptacji.	TAK	