Załącznik nr 2 do SWZ – Opis przedmiotu zamówienia/umowy - Specyfikacja techniczna.

I. Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest:

   Rozbudowa systemu firewall o kolejne elementy mające na celu separacje podsieci serwerowych od podsieci stacji roboczych wraz z rozbudową systemu poczty elektronicznej o kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników, całość wraz z instalacją i konfiguracją. Nowe elementy systemu bezpieczeństwa powinny być niezależne od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia, natomiast muszą ze sobą współpracować jeśli istnieje taka konieczność. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

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

   W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

   Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

   Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie dotyczące ochrony poczty musi pracować w oparciu o komercyjne bazy zabezpieczeń.

   Dostarczone rozwiązanie do ochrony poczty elektronicznej musi mieć możliwość pracy w każdym trybów:

   1. Tryb Gateway.
   2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

2. Przedmiot zamówienia szczegółowo opisany został we wzorze umowy stanowiącym załącznik numer 5 do niniejszej SWZ, w tym w załącznikach do tej umowy.

Zadanie nr 1-Urządzenia brzegowe- Firewall.

Tabela numer 1:

Opis przedmiotu zamówienia dla centralnego kontrolera sieci bezprzewodowej	**Wypełnia Wykonawca podając proponowane rozwiązania i/lub parametry techniczne i/lub potwierdzając spełnienie wymagań z kolumny „Opis przedmiotu zamówienia dla centralnego kontrolera sieci bezprzewodowej"**
Nazwa producenta i nazwa produktu	**Nazwa producenta .....** **Nazwa produktu .....**
Ilość urządzeń: 2 szt.	Spełnia / nie spełnia
Ilość wkładek SFP+ 10Gbps – min. 4 (dopuszczone są zamienniki, kompatybilne z dostarczonym urządzeniem)	Podać wartość liczbową dla ilości dostarczonych wkładek SFP+: ..... Oryginał / zamiennik (niepotrzebne skreślić)
Patchcordy niezbędne do podłączenia urządzeń do istniejącej infrastruktury	Spełnia / nie spełnia
Minimalne wymagane funkcjonalności	
System musi wspierać protokoły IPv4 oraz IPv6 w zakresie: • Firewall	Spełnia / nie spełnia

• Ochrony w warstwie aplikacji • Protokołów routingu dynamicznego	
Przepustowość Intrusion Prevention System – min. 12 Gbps	Podać wartość liczbową Gbps dla przepustowosc IPS ……..
Przepustowość Next Generation FireWall – min. 10 Gbps	Podać wartość liczbową Gbps dla przepustowości NGFW ……..
Przepustowość Threat Protection – min. 9 Gbps	Podać wartość liczbową Gbps dla przepustowości Threat Protection ……..
Obsługa nie mniej niż 7mln jednoczesnych połączeń	Polać ilość obsługiwanych jednoczesnych połączeń ……..
Obsługa nie mniej niż 450 tys. nowych połączeń	Polać ilość obsługiwanych nowych połączeń ……..
Wydajność szyfrowania IPSec VPN nie mniej niż 50 Gbps dla pakietów 512B	Podać wartość liczbową Gbps dla szyfrowania IPSec ……..
Przepustowość Stateful Firewall nie mniej niż 40Gbps dla pakietów 512B	Podać wartość liczbową Gbps dla przepustowości Stateful Firewall ……..
Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 6 Gbps	Podać wartość liczbową Gbps dla ruchu Enterprise Traffic Mix ……..
Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 5 Gbps	Podać wartość liczbową Gbps dla ruchu Enterprise Mix z włączonymi funkcjami IPS, Application Control, Antyvirus ……..
Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4.6 Gbps	Podać wartość liczbową Gbps dla inspekcji komunikacji szyfrowanej SSL dla ruchu http ……..
Redundancja, monitoring i wykrywanie awarii	
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.	Spełnia / nie spełnia
W ramach postępowania system musi zostać dostarczony w postaci redundantnej.	Spełnia / nie spełnia
Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych	Spełnia / nie spełnia
Monitoring stanu realizowanych połączeń VPN	Spełnia / nie spełnia
System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych	Spełnia / nie spełnia
System musi być wyposażony w redundantne zasilanie AC	Spełnia / nie spełnia
Interfejsy, dysk, zasilanie	
System realizujący funkcję Firewall musi dysponować minimum: • Min. 18 portów Gigabit Ethernet RJ-45 • Min. 4 gniazda SFP+ 10Gbps	Spełnia / nie spełnia
System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.	Spełnia / nie spełnia
W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.	Spełnia / nie spełnia
Funkcje systemu bezpieczeństwa	
Kontrola dostępu - zapora ogniowa klasy Stateful Inspection	Spełnia / nie spełnia

Kontrola Aplikacji	Spełnia / nie spełnia
Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN	Spełnia / nie spełnia
Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS	Spełnia / nie spełnia
Ochrona przed atakami - Intrusion Prevention System	Spełnia / nie spełnia
Kontrola stron WWW	Spełnia / nie spełnia
Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3	Spełnia / nie spełnia
Zarządzanie pasmem (QoS, Traffic shaping)	Spełnia / nie spełnia
Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)	Spełnia / nie spełnia
Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site	Spełnia / nie spełnia
Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2	Spełnia / nie spełnia
Analiza ruchu szyfrowanego protokołem SSH	Spełnia / nie spełnia
Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system	Spełnia / nie spełnia
Firewall i polityki	
Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń	Spełnia / nie spełnia
System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu.\ • Dedykowany ALG (Application Level Gateway) dla protokołu SIP	Spełnia / nie spełnia
W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN	Spełnia / nie spełnia
Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików	Spełnia / nie spełnia
Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS). • Microsoft Azure • Google Cloud Platform (GCP). • OpenStack. • VMware NSX	Spełnia / nie spełnia
Połączenia VPN	
System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2.	Spełnia / nie spełnia

• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site	
System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN	Spełnia / nie spełnia
Routing i obsługa łączy WAN	
Obsługa routingu statycznego	Spełnia / nie spełnia
Obsługa routingu opartego o polityki (Policy Based Routing)	Spełnia / nie spełnia
Obsługa protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP, PIM	Spełnia / nie spełnia
Zarządzanie pasmem	
System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.	Spełnia / nie spełnia
Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.	Spełnia / nie spełnia
System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL	Spełnia / nie spełnia
Ochrona przed malware i atakami	
Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).	Spełnia / nie spełnia
System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.	Spełnia / nie spełnia
System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).	Spełnia / nie spełnia
System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.	Spełnia / nie spełnia

System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	Spełnia / nie spełnia
Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.	Spełnia / nie spełnia
Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.	Spełnia / nie spełnia
System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.	Spełnia / nie spełnia
Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	Spełnia / nie spełnia
Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.	Spełnia / nie spełnia
System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.	Spełnia / nie spełnia
Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.	Spełnia / nie spełnia
Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	Spełnia / nie spełnia
Kontrola aplikacji, kontrola WWW	
Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.	Spełnia / nie spełnia
Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.	Spełnia / nie spełnia
Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.	Spełnia / nie spełnia
Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.	Spełnia / nie spełnia
Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	Spełnia / nie spełnia
Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.	Spełnia / nie spełnia
W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.	Spełnia / nie spełnia
Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.	Spełnia / nie spełnia
Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.	Spełnia / nie spełnia
Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.	Spełnia / nie spełnia
Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.	Spełnia / nie spełnia
W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.	Spełnia / nie spełnia

Zarządzanie	
Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.	Spełnia / nie spełnia
Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.	Spełnia / nie spełnia
Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.	Spełnia / nie spełnia
System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow	Spełnia / nie spełnia
System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.	Spełnia / nie spełnia
Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.	Spełnia / nie spełnia
Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.	Spełnia / nie spełnia
Logowanie, uwierzytelnianie użytkowników w ramach sesji	
System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.\ • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.	Spełnia / nie spełnia
Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego	Spełnia / nie spełnia
Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	Spełnia / nie spełnia
Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu http.	Spełnia / nie spełnia
Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej	Spełnia / nie spełnia
W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona	Spełnia / nie spełnia

możliwość jednoczesnego wysyłania logów do wielu serwerów logowania	
Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu	Spełnia / nie spełnia
Musi istnieć możliwość logowania do serwera SYSLOG	Spełnia / nie spełnia
Rozwiązanie musi być kompatybilne z używanym w Szpitalu systemem FortiAnalyzer do zbierania i analizowania logów	Spełnia / nie spełnia
Gwarancja, serwis, licencje certyfikaty	
Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	Spełnia / nie spełnia
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum 12 miesięcy	Spełnia / nie spełnia
Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall. Wykonawca załączy do oferty.	Spełnia / nie spełnia

Zadanie nr 2-System zabezpieczający dla poczty elektronicznej

Tabela numer 2:

Opis przedmiotu zamówienia dla przełączników sieciowych	**Wypełnia Wykonawca podając proponowane rozwiązania i/lub parametry techniczne i/lub potwierdzając spełnienie wymagań z kolumny „Opis przedmiotu zamówienia dla centralnego kontrolera sieci bezprzewodowej”**
Nazwa producenta i nazwa produktu	**Nazwa producenta** …… **Nazwa produktu** ……
Min. 1 szt.	**Podać ilość** ……
Minimalne wymagane funkcjonalności	
Możliwość pracy w trybie Gateway	Spełnia / nie spełnia
Możliwość pracy w trybie transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej)	Spełnia / nie spełnia
System musi obsługiwać co najmniej 4 interfejsy sieciowe	Podać liczbę interfejsów sieciowych ……
System musi wspierać powierzchnię dyskową o pojemności co najmniej 1 TB	Podać pojemność wspieranej powierzchni dyskowej ……
Ogólne funkcje systemu ochrony poczty	
Wsparcie dla co najmniej 20 domen pocztowych	Spełnia / nie spełnia
System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę	Spełnia / nie spełnia

Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all)	Spełnia / nie spełnia
Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP	Spełnia / nie spełnia
Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości)	Spełnia / nie spełnia
Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie	Spełnia / nie spełnia
Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej	Spełnia / nie spełnia
Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów	Spełnia / nie spełnia
Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP	Spełnia / nie spełnia
Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika	Spełnia / nie spełnia
Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora	Spełnia / nie spełnia
Dostęp do kwarantanny użytkownika możliwy poprzez WebMail	Spełnia / nie spełnia
Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki	Spełnia / nie spełnia
Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI	Spełnia / nie spełnia
Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu	Spełnia / nie spełnia
Białe i czarne listy adresów mailowych dla poszczególnych użytkowników	Spełnia / nie spełnia
Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika	Spełnia / nie spełnia
Kontrola antywirusowa i ochrona przed malware	
Skanowanie antywirusowe wiadomości SMTP	Spełnia / nie spełnia
Kwarantannę dla zainfekowanych plików	Spełnia / nie spełnia
Skanowanie załączników skompresowanych	Spełnia / nie spełnia
Definiowanie komunikatów powiadomień w języku polskim	Spełnia / nie spełnia
Blokowanie załączników w oparciu o typ pliku	Spełnia / nie spełnia
Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej	Spełnia / nie spełnia
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	Spełnia / nie spełnia

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	Spełnia / nie spełnia
Ochronę typu wirus outbrake	Spełnia / nie spełnia
Ochrona przed atakami na usługę poczty	
Ochrona przed atakami na adres odbiorcy (m.in. email bombing)	Spełnia / nie spełnia
Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu	Spełnia / nie spełnia
Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu	Spełnia / nie spełnia
Kontrola Reverse DNS (ochrona przed Anty-Spoofing)	Spełnia / nie spełnia
Weryfikacja poprawności adresu e-mail nadawcy	Spełnia / nie spełnia
Funkcje logowania i raportowania	
Logowanie do zewnętrznego serwera SYSLOG	Spełnia / nie spełnia
Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku	Spełnia / nie spełnia
Logowanie informacji na temat spamu oraz niedozwolonych załączników	Spełnia / nie spełnia
Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych	Spełnia / nie spełnia
Możliwość analizy przebiegu sesji SMTP	Spełnia / nie spełnia
Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych	Spełnia / nie spełnia
Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu	Spełnia / nie spełnia
Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu	Spełnia / nie spełnia
Rozwiązanie musi być kompatybilne z używanym w Szpitalu systemem FortiAnalyzer do zbierania i analizowania logów	Spełnia / nie spełnia
Funkcje pracy w trybie wysokiej dostępności (HA)	
Konfigurację HA w każdym z trybów: gateway, transparent	Spełnia / nie spełnia
Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP	Spełnia / nie spełnia
Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu	Spełnia / nie spełnia
Monitorowanie stanu pracy klastra	Spełnia / nie spełnia
Aktualizacje sygnatur, dostęp do bazy spamu	
Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym	Spełnia / nie spełnia
Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę	Spełnia / nie spełnia
Zarządzanie	

System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH	Spełnia / nie spełnia
Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy	Spełnia / nie spełnia
Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych	Spełnia / nie spełnia
Serwisy i licencje, certyfikaty	
System musi być dostarczony w modelu „na własność" tj. Niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.	Spełnia / nie spełnia
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:	Spełnia / nie spełnia
Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified	Spełnia / nie spełnia
Gwarancja	
System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.	Spełnia / nie spełnia
Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 8x5 / 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 8x5 / 24x7. Oferent winien przedłożyć dokumenty: • Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). Wykonawca załączy do oferty. • Certyfikat ISO 9001 podmiotu serwisującego. Wykonawca załączy do oferty.	Spełnia / nie spełnia

1. Zakres wdrożenia:
   Konfiguracja dostarczonego sprzętu i oprogramowania (w związku ze specyfiką wdrożenia, prace mają być realizowane przez osobę z certyfikatem o najwyższym poziomie certyfikacji w programie certyfikacyjnym producenta). Wykonawca załączy do oferty dla zadania nr 1 i 2.

   Wymagania dla rozbudowy systemu firewall
   1. Stworzenie klastra urządzeń
   2. Rejestracja urządzeń i wsparcia w systemie producenta
   3. Migracja ustawień systemowych z istniejących urządzeń wraz z optymalizacją ustawień
   4. Migracja konfiguracji sieciowej z istniejących urządzeń, uwzględniająca konieczność zmiany interfejsów
   5. Migracja polityk zezwalających na ruch pomiędzy segmentami sieci z istniejących urządzeń wraz z optymalizacją pod kątem bezpieczeństwa,
   6. Aktualizacja do najnowszej zalecanej wersji oprogramowania,
   7. Przełączenia sieci na nowy klaster urządzeń
   8. Wykonanie testów poprawności pracy klastra
   9. Podłączenie klastra do systemu zbierania logów posiadanego przez Zamawiającego
   10. Sporządzenie dokumentacji architektury, połączeń między urządzeniami oraz konfiguracji systemu

   Wymagania dla rozbudowy systemu ochrony poczty elektronicznej:

1. Instalacja serwera wirtualnego w środowisku Zamawiającego
2. Rejestracja urządzenia i wsparcia w systemie producenta
3. Konfiguracja systemu
4. Wprowadzenie niezbędnych zmian w środowisku pocztowym Zamawiającego
5. Wykonanie testów poprawności pracy systemu ochrony poczty
6. Podłączenie systemu ochrony poczty do systemu zbierania logów posiadanego przez Zamawiającego
7. Sporządzenie dokumentacji architektury, połączeń między urządzeniami oraz konfiguracji systemu

2. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

3. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
4. Oznaczenie przedmiotu zamówienia według CPV:
    1. 32420000-3 Urządzenia sieciowe
    2. 48000000-8 Pakiety oprogramowania i systemy informatyczne

5. Opis kryteriów, którymi Zamawiający będzie kierował się przy wyborze oferty.

1. Oferty zostaną ocenione przez Zamawiającego w oparciu o następujące kryteria i ich znaczenie:

Kryterium	Znaczenie procentowe	Maksymalna liczba punktów jakie może otrzymać oferta za kryterium
Cena z podatkiem VAT (C)	100%	100 punktów

2. Zasady oceny w kryterium "Cena" (C).

W kryterium "Cena" oferta otrzyma zaokrągloną do dwóch miejsc po przecinku liczbę punktów wynikającą z działania:

$$Pi(C) = \frac{Min(C)}{Ci} * 100 \text{ pkt}$$

gdzie:

i – numer oferty

Ci – oferta cenowa o numerze i

Min (C) – oferta cenowa o najniższej cenie

Pi (C) – liczba punktów jakie otrzyma oferta „i" za kryterium „Cena z podatkiem VAT (C)";

3. Zasady obliczania końcowej oceny za wszystkie kryteria

$$Pi = Pi(C)$$

gdzie:

Pi (C) – liczba punktów jakie otrzyma oferta „i" za kryterium „Cena z podatkiem VAT (C)", obliczona w pkt 2,

Maksymalna nota to 100 pkt. Wygrywa oferta z największą liczbą zdobytych punktów.

W przypadku dwóch zwycięskich ofert o tej samej liczbie punktów, kryterium wyboru będzie niższa cena.