Załącznik nr 3A

.....

(pieczęć firmowa Wykonawcy)

Formularz wymagań technicznych – Zadanie nr 2

Brama Anty Spam dla poczty elektronicznej – 1 szt. – Zadanie 2

Element lub warunek	Parametry minimalne	Parametry ofertowane (podać)
Wymagania ogólne systemu	1. System musi zapewniać filtrację dla minimum 100 adresów mailowych 2. System musi zapewniać wsparcie producenta na okres 3ch lat 3. System musi posiadać konsolę zarządzającą dostępną przez przeglądarkę internetową. 4. System musi umożliwiać dostęp do konsoli osobno poprzez http oraz https 5. System musi mieć możliwość implementacji wewnątrz i na zewnątrz struktury informatycznej organizacji, powinien funkcjonować niezależnie od pozostałych jej elementów. 6. Rozwiązanie musi wspierać filtrację dla serwerów znajdujących się wewnątrz i na zewnątrz struktury informatycznej danej organizacji. 7. System musi być dostępny w postaci pliku ISO pozwalającym na instalację na serwerze fizycznym, jak też w wersji na maszyny wirtualne ze wsparciem dla następujących środowisk: VMWare, Citrix, MS Hyper-V. 8. Interfejs rozwiązania musi wspierać kilka języków i posiadać także polskojęzyczny interfejs. 9. System musi zawierać główny pulpit, na którym będą wyświetlane podstawowe informacje takie jak: a.Stan systemu w tym zużycie CPU, RAM, pamięci dyskowej b. Wersję systemu i bieżącą datę c. Informacje o typie aktualnie używanego procesora d. Informacje o stanie skanerów antywirusowych e. Wykres przedstawiający informacje zbiorcze na temat procesowania wiadomości f. Informacje z ostatnich siedmiu dni w formie listy lub/i wykresu przedstawiające liczbę zablokowanych wiadomości, liczbę wystąpień wirusów, liczbę zablokowanych załączników i innych odrzuceń g. Listy najpopularniejszych nadawców wirusów i spamu oraz najpopularniejszych wirusów wykrytych przez silniki antywirusowe 10. System musi w widocznym miejscu zawierać sekcje poświęconą wsparciu technicznemu umożliwiającą utworzenie bezpiecznego połączenia z suportem producenta. 11. Konsola zarządzająca musi mieć możliwość dostosowywania wyglądu, personalizacji kolorystyki interfejsu i umieszczenia logo firmy. 12. System musi mieć możliwość obsługi certyfikatów SSL. 13. System musi mieć możliwość importu certyfikatów. 14. System musi mieć możliwość obsługi TLS. 15. System musi mieć funkcjonalność szyfrowania emaili kluczem prywatnym, i odszyfrowywania ich u odbiorcy kluczem publicznym, tak zwane DKIM 16. System musi mieć możliwość uwierzytelniania nadawcy poprzez określone mechanizmy, nie mniej niż SPF, DMARC, ARC. 17. System musi mieć możliwość wykonywania kopii zapasowych konfiguracji zarówno automatycznych na serwerze FTP lub w chmurze Amazon, jak i na żądanie, a także możliwość importu takiej konfiguracji. 18. System musi obsługiwać zdalny Syslog, osobny dla logów dotyczących maili i osobny dla	

	logów dotyczących inferface'u oraz zmian w systemie 19. System musi wspierać SNMP v2c oraz v3 20. System musi mieć możliwość pracy w klastrze (dwóch lub więcej węzłów). 21. Aktualizacja systemu musi odbywać się poprzez konsolę webową, oraz nie może mieć wpływu na działanie samego systemu (tj. żadna wiadomość mailowa nie zostanie utracona). W przypadku aktualizacji systemów działających w klastrze, musi istnieć możliwość uruchomienia tych procesów oddzielnie (np. w przypadku gdyby aktualizacja okazała się wadliwa)	
Moduł antyspamowy	1. System musi posiadać wbudowany silnik antyspamowy. 2. System musi mieć umożliwiać korzystanie z zewnętrznych baz RBL, dowolnie definiowanych przez administratora. 3. System musi mieć możliwość tworzenia przez administratora białej listy adresów IP nadawcy, pomijanych podczas filtracji RBL. 4. System musi mieć możliwość wyłączania filtracji RBL dla poszczególnych domen podpiętych do rozwiązania. 5. System musi mieć możliwość sprawdzenia poprawności odbiorcy danej wiadomości, w trybie co najmniej: dynamicznym (weryfikacja na serwerze docelowym), LDAP, listę dozwolonych odbiorców oraz poprzez wyrażenia regularne. 6. System musi być wspierany samouczącą się bazą danych Bayes'a. 7. System musi obsługiwać Passive OS Fingerprinting oraz mechanizm Penpals i analizę Botnetów. 8. System musi posiadać konfigurowalną szarą listę, z możliwością jej włączenia i wyłączenia 9. System musi pozwalać na zdefiniowanie języków, w których to muszą być napisane wiadomości, by pomyślnie przeszły weryfikację 10. System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach email oraz nazwach domen. Listy powinny być traktowane globalnie, per domena i osobno dla każdego użytkownika. 11. System musi umożliwiać tworzenie białych i czarnych list, opartych na adresach IP serwerów pocztowych nadawcy. 12. System musi mieć możliwość indywidualnego ustalania wysokości progu filtrowania wiadomości przez moduł antyspamowy dla domen jak i również dla określonych aliasów pocztowych. 13. System musi mieć możliwość rozczytywania skróconych wersji URLi 14. System musi mieć możliwość dodawania konfigurowalnych stopek do maili wychodzących, które potwierdzą że zostały one przefiltrowane przez tenże system	
Moduł antywirusowy	1. System musi zawierać dwa niezależnie działające silniki antywirusowe zewnętrznego dostawcy. 2. System musi mieć możliwość całkowitego wyłączenia silnika antywirusowego. 3. System musi samoczynnie aktualizować bazę danych dla wbudowanego silnika antywirusowego. Baza musi być aktualizowana minimum, co godzinę.	
Moduł kontroli treści	1. System musi umożliwiać blokowanie wybranych przez administratora rozszerzeń i nazw plików. 2. System musi umożliwiać blokowanie co najmniej następujących rozszerzeń plików: ade, adp, bat, chm, cmd, com, cpl, dll, doc, exe, hta, ins, isp, jar, js, jse, lib, lnk, mde, msc, msp, mst, pif, scr, sct, shb, sys, vb, vbe, vbs, vxd, wsc, wsf, wsh 3. System musi umożliwiać blokowanie co najmniej następujących typów MIME: application/ecmascript, application/javascript, application/x-javascript, application/x-msdos-program, application/x-msdownload, text/ecmascript, text/javascript 4. Wykrywanie i blokowanie rozszerzenia załącznika typu wykonywalnego powinno być odporne na zmianę nazwy i rozszerzenia, również w przypadku skompresowanego archiwum.	

	5. System musi umożliwiać blokowanie zabezpieczonych hasłem archiwów. 6. System musi umożliwiać tworzenie własnych reguł filtracji. 7. System musi umożliwiać kontrolę treści opartej na słowniku lub wyrażeniu regularnym (przykładowo blokowanie wiadomości z numerami kard kredytowych, numerami PESEL czy też innymi danymi określanymi jako wrażliwe). 8. Wszystkie wyżej wymienione funkcje powinny być dostępne dla filtracji wiadomości wychodzących i przychodzących. 9. System musi posiadać mechanizm przepisywania linków w wiadomościach, automatycznie kierujący odbiorcę na serwery zewnętrzne, które kategoryzują strony internetowe pod kątem zagrożeń: a. Funkcjonalność można ustawić osobno dla domeny i dla użytkownika systemu b. Można tworzyć wyjątki dla domen stron internetowych, które mają być nie przepisywane, osobno dla całej domeny pocztowej oraz użytkowników systemu. c. Funkcjonalność powinna pozwalać na edycję wyświetlanej strony z informacją o blokadzie, minimum o treść wyświetlanej informacji oraz o wyświetlane logo.	
Moduł powiadamiania użytkowników	1. System musi posiadać moduł powiadamiający adresata bądź odbiorcę wiadomości o podjętych przez system akcjach. 2. System musi powiadamiać o zablokowanych wiadomościach w tym wiadomościach zablokowanych przez moduł antyspamowy, antywirusowy czy moduł kontroli treści. 3. Wiadomości powinny być edytowalne i wysyłane do odbiorcy lub/i nadawcy.	
Kwarantanna	1. System musi posiadać mechanizm kwarantanny. 2. System musi zawierać wbudowaną wyszukiwarkę. 3. System musi generować raporty kwarantanny a.Raporty kwarantanny powinny być generowane automatycznie lub na żądanie b. Raporty kwarantanny powinny być personalizowane (w tym podmiana logo producenta) c. Raporty powinny być generowane dla użytkowników systemu pocztowego. d. W przypadku współpracy z serwerami pocztowymi Microsoft Exchange, raport powinien być generowany dla użytkownika tylko raz, uwzględniając jego wszystkie aliasy. 4. System musi umożliwić dostęp do kwarantanny poprzez interfejs przeglądarki internetowej dla każdego użytkownika indywidualnie z możliwością dopasowania odpowiednich uprawnień. 5. System musi umożliwić uwierzytelnianie użytkownika za pośrednictwem wewnętrznej bazy, LDAP, w oparciu o bazę kont na docelowym serwerze pocztowym (POP3, IMAP), lub bazy SQL.	
Pozostałe funkcjonalności	1. System musi mieć możliwość tworzenie wielu administratorów o zróżnicowanym poziomie uprawnień. 2. System musi mieć możliwość tworzenia grup domen przyporządkowanych odpowiednim administratorom. 3. System musi posiadać funkcję kontroli ilości przetwarzanych wiadomości dla ruchu przychodzącego i wychodzącego. 4. System musi umożliwiać wyświetlanie statystyk dotyczących aktualnego użycia licencji (liczby unikalnych kont mailowych, przez które przechodzą wiadomości). 5. System musi umożliwiać manualne ustawienie równocześnie pracujących procesów SMTP w celu optymalizacji wydajności rozwiązania względem platformy, na której jest zainstalowane. 6. System musi posiadać moduł kontroli jakości, który pozwoli zdefiniować ograniczenia odnoszące się do co najmniej: a. ilości maili, które mogą zostać wysłane z określonej jednostce czasu b. zbiorczego rozmiaru maili, które mogą zostać wysłane w określonej jednostce czasu 7. System musi mieć możliwość ujednolicenia aliasów emailowych	

	8. System powinien mieć możliwość konfiguracji raportów generowanych użytkownikom tak, aby mogły być generowane na żądanie (z opcją wyłączenia tej opcji przez administratora).	
	Oferowany producent i model:	

…….....
(data, miejscowość)

……..
(podpis i pieczątka wykonawcy
lub osoby upoważnionej)