Załącznik nr 3 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup systemu przeznaczanego do ochrony infrastruktury sieciowej, posiadającego rozwiązania integrujące następujące funkcje: filtrowania treści stron internetowych, posiadający możliwość wykrywania intruzów włączając w to antywirus, firewall, VPN, kontrolę pasma oraz zapewniający silną i skuteczną ochronę systemów pocztowych przed spamem, wirusami, spoofingiem, phishingiem i atakami typu spyware. Zamawiający wymaga systemu opartego o akcelerowane sprzętowo rozwiązania i nie dopuszcza zastosowania systemów operacyjnych ogólnego przeznaczenia.

1) ZINTEGROWANA PLATFORMA BEZPIECZEŃSTWA

Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie typu UTM powinno pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego oraz musi być zbudowane przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania. Dlatego, główne urządzenie ochronne nie może posiadać twardego dysku, w zamian używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanych układów ASIC. Urządzenie powinno posiadać wbudowaną wewnętrzną pamięć dyskową o pojemności minimum 16 GB, realizowaną w postaci dysków SSD.
Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).
Podstawowy system ochrony (UTM) musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych:

- kontrolę dostępu - zaporę ogniową klasy Stateful Inspection,
- ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, NNTP),
- poufność danych - IPSec VPN oraz SSL VPN,
- ochronę przed atakami - Intrusion Prevention System [IPS/IDS],

oraz funkcjonalności uzupełniających:

- kontrolę treści i kategoryzację odwiedzanych stron WWW – Web\URL Filter,
- kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) ,
- kontrolę pasma oraz ruchu [QoS, Traffic shaping],
- kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM, P2P, VoIP, Web-mail),
- zapobieganie przed wyciekiem informacji poufnej - DLP (Data Leak Prevention),
- SSL proxy z możliwością pełniej analizy szyfrowanej komunikacji dla wybranych protokołów.

W zakresie zapewnienia bezpieczeństwa system musi posiadać możliwość wykrywania i blokowania ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Dla ochrony sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP oferowane rozwiązanie powinno zawierać:

- Nie mniej niż 4000 sygnatur ataków.
- Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie
- Możliwość dodawania własnych sygnatur ataków
- Możliwość wykrywania anomalii protokołów i ruchu

Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie, zarządzanie pasmem sieci (m.in. pasma gwarantowane i maksymalne, priorytety,

oznaczenia DiffServ). Urządzenie powinno umożliwiać utworzenie nie mniej niż 10 000 polityk firewall'a

Moduł Filtrowania stron WWW

Moduł filtracji stron www powinien umożliwiać blokowanie stron w oparciu o:

- białe i czarne listy URL
- zawarte w stronie słowa kluczowe
- dynamicznie definiowane przez producenta kategorie.

Moduł antywirusowy

Antywirus powinien mieć możliwość transferu częściowo przeskanowanego pliku do klienta w celu zapobiegnięcia przekroczenia dopuszczalnego czasu oczekiwania (timeout). Antywirus powinien przeprowadzać sprawdzanie danych zarówno po bazie sygnatur wirusów jak i heurystycznie.

Moduł antyspam

Zawarty moduł antyspamowy powinien pracować w obrębie protokołów SMTP, POP3 i IMAP

Klasyfikacja wiadomości powinna bazować na wielu czynnikach, takich jak:

- sprawdzenie zdefiniowanych przez administratora adresów IP hostów, które brały udział w dostarczeniu wiadomości,
- sprawdzenie zdefiniowanych przez administratora adresów pocztowych,
- RBL, ORDBL
- Sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych

Oprócz powyższego mechanizm antyspamowy powinien umożliwiać skorzystanie z zewnętrznej, wieloczynnikowej bazy spamu.

Parametry techniczne:

Urządzenie zabezpieczające sieć	
Parametr	**Wymagania techniczne**
Obudowa	Obudowa ma mieć możliwość zamontowania w szafie 19".
Zasilanie	Zasilanie z sieci 230V/50Hz.
Parametry fizyczne systemu	– nie mniej niż 2 interfejsy SFP o przepustowości 1Gb – nie mniej niż 18 interfejsów Ethernet 10/100/1000 Base-TX. – obudowa ma mieć możliwość zamontowania w szafie 19".
Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT. NAT traversal dla protokołów SIP i H323
Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.
Połączenia VPN	Wymagane nie mniej niż: – tworzenie połączeń w topologii Site-to-Site oraz Client-to-Site – dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki: a) firewall b) antywirus c) web filtering d) antyspam – monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności – konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) – obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive
Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: – jako router/NAT (3.warstwa ISO-OSI) lub – jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.
Wydajność	Obsługa nie mniej niż 1 400 000 jednoczesnych połączeń i 77 000 nowych połączeń na sekundę Przepływność nie mniejsza niż 3 Gb/s dla ruchu nieszyfrowanego i 1,3 Gb/s dla VPN (3DES). Obsługa nie mniej niż 2 000 jednoczesnych tuneli VPN site-to-site Obsługa nie mniej niż 5 000 jednoczesnych tuneli VPN client-to-gateway. Obsługa nie mniej niż 300 jednoczesnych tuneli SSL VPN
Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: – haseł statycznych – haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla systemu urządzenie powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: – haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia – haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP – haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.
Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: – zbieranie logów z urządzeń bezpieczeństwa – generowanie raportów – skanowanie podatności stacji w sieci – zdalną kwarantannę dla modułu antywirusowego

2) ZINTEGROWANY SYSTEM OCHRONY POCZTY ELEKTRONICZNEJ

Zintegrowane rozwiązanie musi być zaprojektowane, by chronić serwer poczty elektronicznej *oraz stacje robocze* przed spamem, wirusami, spoofingiem, phishingiem i atakami typu spyware. System musi być zbudowany w oparciu o architekturę, w której możliwa jest redundancja podstawowych komponentów (dyski twarde, zasilacze) lub redundancja na poziomie platformy (tryb HA) oraz powinien zapewniać kompleksową ochronę antyspamową, antywirusową i antyspyware'ową. Dla trybu wysokiej dostępności (HA) system musi zapewniać:

- konfigurację HA [Active-Passive] w każdym z trybów: gateway, transparent, serwer,

- tryb Active-Passive z syncronizacją polityk i wiadomości, gdzie cluster występuje pod jednym adresem IP,
- tryb synchronizacji konfiguracji dla scenariuszy rozległych (osobne adresy IP),
- wykrywanie awarii i powiadamianie administratora,
- monitorowanie stanu połączeń.

Jednocześnie, w celu zagwarantowania bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).
Wymagane jest również (dla zapewnienia wysokiej sprawności i skuteczności działania systemu) aby urządzenie pracowało w oparciu o dedykowany system operacyjny czasu rzeczywistego oraz było wyposażone w minimum 4 porty Ethernet 10/100/1000 Base-TX. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia. Urządzenie powinno mieć możliwość pracy w trzech niżej wymienionych trybach:

1. Tryb Gateway,
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej),
3. Tryb serwera pocztowego.

Opisywany system musi realizować poniższe funkcjonalności w każdym z trzech trybów pracy:

- Wsparcie dla wielu domen pocztowych,
- Polityki filtrowania tworzone w oparciu o adresy mailowe, nazwy domenowe, adresy IP (w szczególności reguła all-all),
- Email routing oraz zarządzanie kolejkami bazujące na politykach ,
- Ochrona poczty przychodzącej oraz wychodzącej,
- Granularne, wielowarstwowe polityki wykrywania spamu oraz wirusów,
- Skanowanie Antywirusowe oraz Antyspamowe definiowane na użytkownika w oparciu o atrybuty LDAP,
- Routing poczty (email routing) w oparciu o LDAP,
- Kwarantanna poczty z dziennym podsumowaniem (możliwość samodzielnego zwalniania plików z kwarantanny przez użytkownika),
- Dostęp do kwarantanny poprzez WebMail lub POP3,
- Archiwizacja poczty przychodzącej i wychodzącej, backup poczty do różnych miejsc przeznaczenia,
- Uwierzytelnianie SMTP w oparciu o protokoły: LDAP, RADIUS, POP3, IMAP,
- Mechanizmy reputacji nadawcy wiadomości,
- Whitelist'y definiowane dla użytkownika

oraz system musi zapewniać następujące funkcjonalności w trybie serwera pocztowego:

- Obsługę serwisów pocztowych: SMTP, POP3, IMAP
- Wsparcie SMTP over SSL
- Definiowanie powierzchni dyskowej dla użytkowników
- Szyfrowany dostęp do poczty poprzez WebMail
- Polski interfejs użytkownika przy dostępie przez WebMail
- Kalendarz na WebMail'u
- Lokalne konta użytkowników oraz uwierzytelnianie w oparciu o LDAP
- Synchronizacja książki adresowej z LDAP

Dla zapewnienia płynnej komunikacji (wydajności) rozwiązanie musi zapewniać:

- ochrona minimum 400 domen pocztowych
- obsługa minimum 1000 lokalnych skrzynek pocztowych w trybie serwer
- obsługę nie mniej niż 150 profili antywirusowych lub antyspamowych
- skanowanie Antyspamowe minimum 320 000 tyś wiadomości/godzinę

Moduł ochrony antywirusowej i antyspyware'owej

System musi realizować:

- Skanowanie antywirusowe wiadomości SMTP
- Kwarantannę dla zainfekowanych plików
- Skanowanie załączników skompresowanych
- Definiowanie komunikatów powiadomień w języku polskim
- Blokowanie załączników ze względu na typ pliku

Moduł ochrony antyspamowej

System musi obsługiwać poniższe metody filtrowania spamu:

- Heurystyczna analiza poczty z dynamiczną aktualizacją reguł
- Filtrowanie treści załączników, filtrowanie wiadomości po słowach kluczowych
- Szczegółowa kontrola nagłówka wiadomości
- Filtrowanie w oparciu o filtry Bayes'a, z możliwością dostrajania dla poszczególnych użytkowników
- Filtrowanie poczty w oparciu o sumy kontrolne spamu
- Wykrywanie spamu w oparciu a analizę plików graficznych oraz plików PDF
- Analiza poczty w oparciu o dynamiczną bazę spamu dostarczaną przez tego samego producenta
- Współpraca z zewnętrznymi serwerami RBL
- Kontrola w oparciu o Greylist'y
- Białe i czarne listy definiowane globalnie oraz per użytkownik
- Weryfikacja źródłowego adresu IP
- Mechanizmy reputacji użytkownika
- Możliwe akcje dla poczty: Accept, Relay, Reject,, Discard, Kwarnatanna, Oznaczanie (Tagging)

Opisywany system musi zapewniać ochronę przed atakami DoS: Denial of Service (Mail Bombing), ochronę przed atakami na adres odbiorcy oraz poprzez definiowanie maksymalnych ilości wiadomości pocztowych, kontrolę Reverse DNS (Anty-Spoofing), i weryfikację poprawności adresu e-mail nadawcy. Dodatkowo dla zapewnienia bezpieczeństwa wiadomości powinien zawierać mechanizmy:

- szyfrowania wysyłanych wiadomości pocztowych, bez konieczności instalowania jakichkolwiek aplikacji na stacjach klienckich, administrator powinien mieć możliwość włączenia tej funkcjonalności dla wybranych użytkowników,
- wsparcie dla szyfrowanej komunikacji Gateway-to-Gateway,
- wsparcie dla szyfrowanych protokołów: HTTPS, SMTPS, IMAPS, POP3S.

Istotną funkcją w zintegrowanym systemie ochrony poczty elektronicznej jest aktualizacja sygantur i dostęp do bazy spamu. W tym zakresie system musi zapewniać:

- pracę w oparciu o bazę spamu uaktualnianą w czasie rzeczywistym,
- planowanie aktualizacji szczepionek antywirusowych w czasie (Scheduler),
- wymuszoną aktualizację bazy wirusów (tryb push).

W zakresie prezentacji logów ze zdarzeń i ich raportowanie rozwiązanie musi zapewnić:

- możliwość definiowania polityki w oparciu w wbudowany kreator konfiguracji,
- logowanie SNMP dla zdarzeń systemowych oz możliwością definiowania progów,
- logowanie do zewnętrznego serwera SYSLOG,
- logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych,
- powiadamianie o działalności wirusów,
- logowanie informacji na temat spamu oraz niedozwolonych załączników,
- predefiniowane szablony raportów,
- możliwość planowania czasu generowania raportów,
- możliwość podglądu logów w czasie rzeczywistym,
- oraz archiwizację poczty w oparciu o zestaw filtrów (np. słowa kluczowe).

Zarządzanie i Raportowanie powinno się odbywać z wykorzystaniem konsoli szeregowej RS-232 oraz za pomocą lokalnego interfejsu zarządzania poprzez szyfrowane połączenie HTTPS, SSH. Interfejs zarządzania powinien posiadać możliwość definiowania wyglądu interfejsu zarządzania z możliwością wstawienia logo firmy.

Parametry techniczne:

Urządzenie zabezpieczające pocztę elektroniczną	
Parametr	**Wymagania techniczne**
Obudowa	Obudowa ma mieć możliwość zamontowania w szafie 19”.
Zasilanie	Zasilanie z sieci 230V/50Hz.
Powierzchnia dyskowa	minimum 2 TB
Parametry fizyczne	RAID (0, 1)
	4 porty Ethernet 10/100/1000 Base-TX
	Powierzchnia dyskowa - minimum 2 TB

3) SYSTEM ZBIERAJĄCY I ANALIZUJĄCY ZDARZENIA

System logowania i raportowania powinien stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców. Zamawiający wymaga dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i hardware pochodziły od jednego producenta. Również jak w ww. rozwiązaniach zaproponowany sprzęt musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
Urządzenie powinno być wyposażone w dysk HDD minimum 1 TB, posiadać minimum 4 porty ethernet 10/100/1000, zasilane z sieci 230V/50Hz oraz mieć możliwość zamontowania w szafie 19".
W zakresie wydajności urządzenie powinno zagwarantować obsługę do 150 urządzeń sieciowych z jednoczesnym zapewnieniem wydajności na poziomie 350 logów/sekundę.
Podstawowe funkcjonalności systemu logowania i raportowania:

- składowanie oraz archiwizacja logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników,
- gromadzenie zawartości przesyłanych za pośrednictwem protokołów Web, FTP, email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci,
- kwarantanna dla współpracujących z nim urządzeń, kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki,
- prezentacja archiwalnych logów przy zastosowaniu funkcji filtrujących, oraz przeszukiwanie wszystkich zgromadzonych danych,
- prezentacja nowych logów w czasie rzeczywistym,
- analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z jej zapisu i późniejszej analizy,
- możliwość eksportu zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych),
- możliwość przechowywania danych w wbudowanej lub zewnętrznej bazie danych SQL.
- tworzenie raportów aktywności użytkowników, ruchu w sieci, itp. na podstawie danych zgromadzonych w logach.

Ponadto system powinien umożliwiać analizę podatności stacji w sieci wraz z możliwością raportowania wykrytych luk oraz planowaną aktualizację bazy sprawdzeń (scheduler)
Zarządzanie i Raportowanie powinno się odbywać z wykorzystaniem konsoli szeregowej RS-232 oraz za pomocą lokalnego interfejsu zarządzania poprzez szyfrowane połączenie HTTPS, SSH.

4) SERWIS ORAZ AKTUALIZACJE DO ZAMAWIANEGO SYSTEMU OCHRONY INFRASTRUKTURY SIECIOWEJ

Zamawiający wymaga dostarczenia dla całości rozwiązania licencji aktywacyjnych dla funkcji bezpieczeństwa na okres 1 roku. System powinien być objęty serwisem gwarancyjnym producenta również przez okres jednego roku oraz **dostawca** powinien zapewnić:

- pierwszą linie wsparcia technicznego telefonicznie w języku polskim w trybie 8x5.
- zdalną pomoc w konfiguracji wspieranych urządzeń,
- rozwiązywanie bieżących problemów występujących podczas pracy z systemem,
- pomoc w przypadku ewentualnych ataków sieciowych,
- usuwanie skutków awarii systemu,
- analizę logów systemu,
- pomoc w opracowaniu metodologii wdrażania nowych funkcjonalności urządzeń,
- pośrednictwo w kontaktach z producentem urządzeń,
- możliwość zgłoszenia serwisowego telefonicznie, przez pocztę elektroniczną oraz dedykowany portal wsparcia technicznego,

- okresowe wizyty „prewencyjne” realizowane w czasie dogodnym dla Klienta,
- dostęp do lokalnego portalu wsparcia, oferującego informacje na temat nowych wersji oprogramowania, poprawek, FAQ etc.,
- czas reakcji na zgłoszenie serwisowe nie przekraczający 8 godzin.

Instalacja i konfiguracja systemu powinna być przeprowadzona przez uprawnionego inżyniera posiadającego aktualny certyfikat producenta.

Usługa wdrożenia urządzeń obejmuje:

- analizę obecnych polityk bezpieczeństwa oraz infrastruktury sieciowej (optymalizacja zgodna z aktualnymi trendami panującymi w sferze zagrożeń sieciowych).
- przygotowanie środowiska (rejestracja i instalacja urządzeń, aktualizacja oprogramowania).
- konfigurację urządzeń zgodnie z założeniami polityki urzędu (interfejsy sieciowe, routing, polityki firewall, DNS, Web filtering, anti-spam, anti-virus, controla aplikacji, ips, ids, virtual private network, integracja z domeną, zarządzanie pasmem, uwierzytelnianie użytkowników, sieci bezprzewodowe, redundancja dostępu do internetu, end point NAC, logowanie oraz raportowanie, alerty administracyjne, dostosowanie do współpracy z zewnętrznym systemem logowania i raportowania)
- weryfikację poprawności implementacji (testy akceptacyjne).
- kopię bezpieczeństwa konfiguracji wdrożonych urządzeń.
- instruktarz obsługi urządzenia poprzez GUI.

W celu zapewnienia odpowiedniego poziomu wsparcia technicznego dostawca musi zatrudniać minimum 3 inżynierów posiadających certyfikaty producenta oferowanego rozwiązania, potwierdzające wiedzę techniczną na poziomie zaawansowanym z minimum 2 letnim doświadczeniem w instalacji i konfiguracji oferowanego rozwiązania.

Dostawca musi okazać zaświadczenie informujące o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem do naprawy u dystrybutora na terenie polski.

W celu potwierdzenia wysokiej skuteczności systemów bezpieczeństwa producent oferowanych systemów musi posiadać certyfikaty: ISO 9001, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus oraz dla dostarczonego systemu ochrony poczty powinien posiadać co najmniej poniższe certyfikaty: ICSA dla funkcjonalności Antyspam, VBSpam Platinium, Common Criteria EAL 2+, FIPS 140-2 Validation.