

OPIS PRZEDMIOTU ZAMÓWIENIA

Część II

1. Specyfikacja urządzenia do zarządzania pocztą e-mail

Wymagania ogólne	• System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników, • Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci 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, • Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń, • Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: - Tryb Gateway, - Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).
Parametry fizyczne systemu antyspamowego	• System musi być wyposażony w interfejsy: porty Gigabit Ethernet RJ-45, • System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB, • System musi posiadać wbudowany port konsoli szeregowej, • Zasilanie z sieci 230V/50Hz.
Funkcja serwera poczty	• W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych, • Moduł serwera poczty musi integrować się z serwerem LDAP obsługującym tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.
Funkcje serwera poczty	Dostarczony system musi zapewniać: • Obsługę serwisów pocztowych: SMTP, POP3, IMAP, • Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2), • Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników, • Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2), • Polski interfejs użytkownika przy dostępie przez WebMail, • Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP, • Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP.

Ogólne funkcje systemu ochrony poczty	• Wsparcie dla co najmniej 20 domen pocztowych, • System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys. wiadomości/godzinę, • Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all), • Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP, • Zarządzanie kolejkami wiadomości (w tym: reguły opóźniania dostarczenia wiadomości), • Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej, • Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów, • Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP, • Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika, • Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz IMAP, • Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki, • Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI, • Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu, • Białe i czarne listy adresów mailowych dla poszczególnych użytkowników, • Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Prevention).
Kontrola antywirusowa i ochrona przed malware	Dostarczony system ochrony poczty musi zapewniać: • Skanowanie antywirusowe wiadomości SMTP, • Kwarantannę dla zainfekowanych plików, • Skanowanie załączników skompresowanych, • Definiowanie komunikatów powiadomień w języku polskim, • Blokowanie załączników w oparciu o typ pliku, • Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej, • 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, • 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, • Ochronę typu wirus outbrake.

Kontrola antyspamowa	System musi zapewniać poniższe funkcje i metody filtrowania spamu: • Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta, • Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania, • Szczegółowa kontrola nagłówka wiadomości, • Analiza Heurystyczna • Współpraca z zewnętrznymi serwerami RBL, SURBL, • Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen, • Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników, • Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF, • Kontrola w oparciu o Greylisting oraz SPF, • Filtrowanie treści wiadomości i załączników, • Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości, • Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej, • Ochrona typu outbrake, • Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking), • 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.
Ochrona przed atakami na usługę poczty	System musi zapewniać poniższe funkcje i metody filtrowania: • Ochrona przed atakami na adres odbiorcy (w tym: email bombing), • Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu, • Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu, • Kontrola Reverse DNS (ochrona przed Anty-Spoofing), • Weryfikacja poprawności adresu e-mail nadawcy.
Funkcje logowania i raportowania	Dostarczony system ochrony poczty musi zapewniać: • Logowanie do zewnętrznego serwera SYSLOG, • Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku, • Logowanie informacji na temat spamu oraz niedozwolonych załączników, • Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych, • Możliwość analizy przebiegu sesji SMTP, • Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych, • Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu, • Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Funkcje pracy w trybie wysokiej dostępności (HA)	System ochrony poczty musi zapewniać poniższe funkcje: • Konfigurację HA w każdym z trybów: gateway, transparent, • Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP, • Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu, • Monitorowanie stanu pracy klastra.
Aktualizacje sygnatur, dostęp do bazy spamu	Dostarczony system ochrony poczty musi zapewniać: • Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym, • Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.
Zarządzanie	System ochrony poczty musi zapewniać poniższe funkcje: • System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, • Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy, • Powinna istnieć możliwość zdefiniowania co najmniej 7 lokalnych kont administracyjnych.
Certyfikaty	VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified. Oferent winien przedłożyć dokumenty: - Oświadczenie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej), - Certyfikat ISO 9001 podmiotu serwisującego, - Certyfikat Inżyniera posiadającego certyfikację minimum NS7.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Kontrolę Antyspam, • URL Filtering, • kontrolę antywirusową, • ochronę typu virus outbreak na okres 12 miesięcy.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres min. 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.
Rozszerzone wsparcie serwisowe	• System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 8 godzin/ od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres min. 12 miesięcy. • 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 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7.