**Załącznik nr 2 do SWZ**

**Opis Przedmiotu zamówienia – wymagania minimalne**

**Niniejszy załącznik należy złożyć wraz z ofertą pod rygorem jej odrzucenia**

Prawą stronę tabeli (kol. 2) należy wypełnić stosując słowa „spełnia” lub „nie spełnia”.

W przypadku, gdy Wykonawca zaproponuje produkt równoważny – informacje dotyczące proponowanych rozwiązań równoważnych musi podać w kol. 2 oraz wykazać, że spełniają one wymagania Zamawiającego.

W przypadku, gdy Wykonawca w którejkolwiek z pozycji wpisze słowa „nie spełnia” lub zaoferuje niższe wartości oferta zostanie odrzucona, gdyż jej treść jest niezgodna z warunkami zamówienia.

|  |  |
| --- | --- |
| **Wymagania minimalne** | **Kolumnę wypełnia wykonawca** |
| **nazwa oferowanego produktu:** |  |
| **Rok produkcji** |  |
| **Kraj pochodzenia:** |  |
| **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:  1. Tryb Gateway.  2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). |  |
| **Parametry fizyczne systemu antyspamowego**  1. System musi być wyposażony w interfejsy:  • 4 porty Gigabit Ethernet RJ-45.  • 2 gniazda SFP 1 Gbps.  2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 2 TB z możliwością obsługi mechanizmu RAID 1 lub 5 lub 10.  3. System musi posiadać wbudowany port konsoli szeregowej.  4. Redundantne zasilanie z sieci 230V/50Hz. |  |
| **Ogólne funkcje systemu ochrony poczty**  Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:  1. Wsparcie dla co najmniej 500 domen pocztowych.  2. Co najmniej 1500 lokalnych kont pocztowych w trybie serwerowym  3. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 400 tys. wiadomości/godzinę.  4. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).  5. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.  6. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).  7. 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.  8. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.  9. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.  10. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.  11. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.  12. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.  13. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.  14. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.  15. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.  16. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.  17. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.  18. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention).  19. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. |  |
| **Kontrola antywirusowa i ochrona przed malware**  W tym zakresie dostarczony system ochrony poczty musi zapewniać:  1. Skanowanie antywirusowe wiadomości SMTP.  2. Kwarantannę dla zainfekowanych plików.  3. Skanowanie załączników skompresowanych.  4. Definiowanie komunikatów powiadomień w języku polskim.  5. Blokowanie załączników w oparciu o typ pliku.  6. Możliwość zdefiniowania nie mniej niż 400 polityk kontroli antywirusowej.  7. 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.  8. 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.  9. Ochronę typu wirus outbrake. |  |
| **Kontrola antyspamowa**  System musi zapewniać poniższe funkcje i metody filtrowania spamu:  1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.  2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.  3. Szczegółowa kontrola nagłówka wiadomości.  4. Analiza Heurystyczna.  5. Współpraca z zewnętrznymi serwerami RBL, SURBL.  6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.  7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.  8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.  9. Kontrola w oparciu o Greylisting oraz SPF.  10. Filtrowanie treści wiadomości i załączników.  11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.  12. Możliwość zdefiniowania nie mniej niż 400 polityk kontroli antyspamowej.  13. Ochrona typu outbrake.  14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: phishing, hacking).  15. 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:  1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).  2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.  3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.  4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).  5. Weryfikacja poprawności adresu e-mail nadawcy. |  |
| **Funkcje logowania i raportowania**  W tym zakresie dostarczony system ochrony poczty musi zapewniać:  1. Logowanie do zewnętrznego serwera SYSLOG.  2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.  3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.  4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.  5. Możliwość analizy przebiegu sesji SMTP.  6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.  7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.  8. 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:  1. Konfigurację HA w każdym z trybów: gateway, transparent.  2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.  3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.  4. Monitorowanie stanu pracy klastra. |  |
| **Aktualizacje sygnatur, dostęp do bazy spamu**  W tym zakresie dostarczony system ochrony poczty musi zapewniać:  1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.  2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. |  |
| **Zarządzanie**  System ochrony poczty musi zapewniać poniższe funkcje:  1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.  2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.  3. Powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych. |  |
| **Certyfikaty**  Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:  1. VBSpam, VB100 rated, Common Criteria evaluation in process (NIAP), FIPS 140-3 Certified. |  |
|  |  |
| **Gwarancja oraz wsparcie techniczne, serwisu i licencji**  Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min 12 miesięcy (parametr punktowany), 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.  **Serwisy i licencje**  W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  1. Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbrake na okres min. 12 miesięcy (parametr punktowany). | **Oświadczenie wykonawcy (parametr punktowany):**  Deklaracja wykonawcy ……………..miesięcy  **Punktacja:**  12 miesięcy - 0%, (0 pkt)  24 miesiące - 10%,(10 pkt)  36 miesiące- 20% (20 pkt) |
| Konfiguracja systemu z przeniesieniem kont pocztowych (Zamawiający posiada Fortimail 400F):  po stronie zamawiającego 0% (0 pkt), po stronie wykonawcy 20% (20,00 pkt) | **Oświadczenie wykonawcy (parametr punktowany):**  Deklaracja wykonawcy ………………………………..  **Punktacja:**  - po stronie zamawiającego 0% (0 pkt),  - po stronie wykonawcy 20% (20,00 pkt) |

# Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca/wykonawca 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.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż oferent (wykonawca) posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. Dokument należy złożyć wraz z ofertą. W przypadku niezłożenia lub złożenia dokumentu niekompletnego, Zamawiający zastrzega na podstawie art. 107 ustawy pzp, możliwość wezwania do ich złożenia lub uzupełnienia w wyznaczonym przez Zamawiającego terminie.

.............................................

*(podpis Wykonawcy)*

Przez podpis należy rozumieć elektroniczny: podpis kwalifikowalny lub podpis osobisty lub podpis zaufany