Opis zakresu szacowania

1. Przedmiot szacowania:

Przedmiotem szacowania jest dostawa **rozwiązania do obsługi oraz filtrowania poczty elektronicznej (klaster dwóch urządzeń)** wraz z gwarancją oraz niezbędnymi licencjami wymaganymi do wdrożenia rozwiązania w infrastrukturze teleinformatycznej Głównego Inspektoratu Farmaceutycznego.

Za prawidłowo zrealizowaną dostawę uznaje się dostarczenie rozwiązania do obsługi poczty zgodnego ze specyfikacją zamieszczoną w pkt. 2

2. Wymagania ogólne

Rozwiązanie do ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware bez limitu licencyjnego na ilość chronionych kont użytkowników.

Dopuszcza się aby poszczególne elementy wchodzące w skład rozwiązania 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 również powinno posiadać co najmniej dwie z poniższych certyfikacji:

- VBSpam, Common Criteria NDPP, VB100 rated, FIPS 140-2 Certified.

Wymagania minimalne jakie muszą zostać spełnione przez pojedyncze urządzenie:

Parametr	Charakterystyka
Fizyczne	• 4 porty Gigabit Ethernet RJ-45. • lokalną przestrzeń dyskowa o pojemności minimum 1 TB . • Wbudowany port konsoli szeregowej. • Zasilanie z sieci 230V/50Hz.
Ogólne	• Praca w trybie transparentnym nie wymagającym rekonfiguracji środowiska pocztowego lub w trybie Gateway. • Wsparcie dla co najmniej 20 domen pocztowych. • Rozwiązanie 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 (np. reguły opóźniania dostarczenia wiadomości).

	• 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 danym czasie. • 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. • Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora. • Dostęp do kwarantanny użytkownika możliwy poprzez WebMail. • Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki. • Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku rozwiązania oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI. • Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora. • Białe i czarne listy adresów mailowych dla poszczególnych użytkowników. • 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 antyspamowa	• 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 typu discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. • Ochronę typu wirus outbrake. • Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości. • 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 rozwiązania 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 rozwiązaniowa 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). • Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata. • Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych • Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje typu discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
Ochrona przed atakami na usługę poczty	• Ochrona przed atakami na adres odbiorcy (m.in. 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.
Logowanie oraz raportowanie	• Logowanie do zewnętrznego serwera SYSLOG oraz do posiadanego przez Zamawiającego urządzenia FortiAnalyzer z możliwością raportowania. • Logowanie zmian konfiguracji oraz krytycznych zdarzeń rozwiązaniowych 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 rozwiązania w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych. • Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora rozwiązania. • Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora.
Tryb wysokiej dostępności	• Konfigurację HA w każdym z trybów: gateway, transparent. • Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.

(HA) oraz zarządzanie	• Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora rozwiązania. • Monitorowanie stanu pracy klastra. • W ramach postępowania wymaganym jest dostarczenie rozwiązania w formie klastra realizującego funkcje podstawowe, gdzie każdy jego element charakteryzuje się parametrami fizycznymi i funkcjonalnymi opisanymi w tym dokumencie. • Rozwiązanie 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 4 lokalnych kont administracyjnych.
Aktualizacje sygnatur, dostęp do bazy spamu	• Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym. • Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Gwarancja oraz wsparcie

1. Rozwiązanie musi być objęte serwisem gwarancyjnym producenta, 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 24/7.

2. Zamawiający wymaga, aby pierwszą linię wsparcia świadczył Wykonawca. Jeżeli producent zaoferowanego rozwiązania posiada certyfikację serwisową dla realizacji takiego wymogu to Wykonawca musi ją posiadać.

3. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim **przez 8 godzin dziennie w dni robocze**. W tym celu musi zatrudniać co najmniej dwóch inżynierów z aktualnym certyfikatem technicznym oferowanego rozwiązania oraz posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.

4. Wykonawca w ramach dostawy, dokona konfiguracji rozwiązania do ochrony poczty według wytycznych zamawiającego.

Licencje

W ramach zaoferowanego rozwiązania należy dostarczyć niezbędne licencje upoważniające do korzystania z aktualnych baz i funkcji ochronnych producenta, które powinny obejmować ochronę antywirusową, Antyspam, URL Filtering, Virus Outbrake, Sandbox w chmurze, Click Protect, Content Disarm, Reconstruction, Business Email Compromise.