1. Przedmiot zamówienia – opis ogólny

Przedmiotem zamówienia jest:

1. **przedłużenie** posiadanej przez Zamawiającego licencji Fortinet FortiMail VM02 na okres 24 miesięcy,
2. **rozbudowa** posiadanego systemu o dodatkową instancję Fortinet FortiMail VM02, celem zbudowania środowiska wysokiej dostępności (HA) – dostarczenie nowej licencji na okres 24 miesięcy,
3. zapewnienie usługi wsparcia technicznego producenta dla obu instancji na okres 24 miesięcy.

System FortiMail pełni funkcję bramki ochrony poczty elektronicznej – pośredniczy w ruchu SMTP pomiędzy klientami Zamawiającego a usługą Microsoft Office 365, realizując wielowarstwowe filtrowanie antyspamowe, antywirusowe, ochronę przed wyciekiem danych (DLP), kontrolę treści oraz ochronę przed atakami na usługę pocztową. Rozbudowa o drugą instancję umożliwi pracę w trybie wysokiej dostępności (Active-Passive), eliminując pojedynczy punkt awarii.

Zamawiający dopuszcza zaoferowanie rozwiązania równoważnego polegającego na stworzeniu klastra obejmującego 2 instancje.

2. Stan obecny

Zamawiający posiada:

1. Jedną instancję systemu ochrony poczty Fortinet FortiMail VM02 (sn: FEVM02TM23001113), obejmującą następujące oprogramowanie i usługi:
    a. Firmware & General Updates (Web/Online),
    b. Enhanced Support (poziom Premium),
    c. Telephone Support (poziom Premium),
    d. Advanced Malware Protection (Web/Online),
    e. FortiMail-Office365-Protection (Web/Online),
    f. URI Click Protection (Web/Online),
    g. AntiSpam (Web/Online),
    h. FortiGuard Virus Outbreak Protection Service (Web/Online),
    i. FortiSandbox Cloud (Web/Online),
    j. Content Disarm & Reconstruction (Web/Online).
2. Okres obowiązywania obecnej licencji i wsparcia upływa 2026-08-15.
3. System pracuje jako virtual appliance w środowisku wirtualizacyjnym VMware.
4. System jest zintegrowany z:
    a. Microsoft Office 365 (poprzez dedykowane API – skanowanie skrzynek pocztowych w czasie rzeczywistym),
    b. systemem SIEM (przesyłanie logów, reguły korelacyjne).

5. System pracuje w trybie pojedynczej instancji – brak wysokiej dostępności.

3. Minimalne wymagania dla rozwiązania równoważnego

W przypadku zaoferowania rozwiązania równoważnego musi ono spełniać poniższe wymagania minimalne. Wymagania podyktowane są koniecznością zachowania ciągłości działania systemu ochrony poczty oraz kompatybilności z istniejącą infrastrukturą i systemami zewnętrznymi Zamawiającego.

3.1. Kompatybilność

1. Rozwiązanie musi być w pełni kompatybilne w zakresie tworzenia klastra wysokiej dostępności (HA), obejmującego synchronizację konfiguracji, polityk bezpieczeństwa oraz kolejek wiadomości.
2. Rozwiązanie musi wspierać tryb pracy Active-Active i Active-Passive.
3. Rozwiązanie musi umożliwiać tryb synchronizacji konfiguracji dla scenariuszy, w których każda instancja występuje pod innym adresem IP.
4. Rozwiązanie musi umożliwiać monitorowanie stanu pracy klastra oraz wykrywanie awarii poszczególnych węzłów z powiadamianiem administratora.
5. Rozwiązanie musi pracować w trybie Gateway, tożsamym z trybem istniejącej instancji.
6. Rozwiązanie musi być dostarczone jako virtual appliance kompatybilny ze środowiskiem wirtualizacyjnym VMware (vSphere) wykorzystywanym przez Zamawiającego.
7. Rozwiązanie musi integrować się z Microsoft Office 365 poprzez API umożliwiające skanowanie skrzynek pocztowych w czasie rzeczywistym.
8. Rozwiązanie musi umożliwiać przesyłanie logów systemowych w czasie rzeczywistym do systemu SIEM Zamawiającego.

3.2. Funkcje logowania i raportowania

1. Rozwiązanie musi umożliwiać logowanie do zewnętrznego serwera SYSLOG.
2. Rozwiązanie musi logować zmiany konfiguracji oraz krytyczne zdarzenia systemowe (np. przepełnienie dysku).
3. Rozwiązanie musi logować informacje na temat obsługiwanych wiadomości, spamu oraz niedozwolonych załączników.
4. Rozwiązanie musi umożliwiać podgląd logów w czasie rzeczywistym.
5. Rozwiązanie musi powiadamiać administratora w przypadku wykrycia wirusów w przesyłanych wiadomościach.
6. Rozwiązanie musi posiadać predefiniowane szablony raportów oraz umożliwiać ich edycję przez administratora.
7. Rozwiązanie musi umożliwiać generowanie raportów zgodnie z harmonogramem oraz na żądanie administratora.
8. Rozwiązanie musi przechowywać logi pełnej historii zdarzeń takich jak (ale nie ograniczonych do): logowanie i próby logowania, operacje na zasobach, modyfikacje uprawnień użytkowników, dodawanie grup i użytkowników, kasowanie obiektów.

3.3. Ogólne funkcje systemu ochrony poczty

1. Rozwiązanie musi wspierać co najmniej 50 domen pocztowych.
2. Rozwiązanie musi umożliwiać tworzenie polityk filtrowania poczty w oparciu o: adresy mailowe, nazwy domenowe, adresy IP, w tym definiowanie reguł all-all.
3. Rozwiązanie musi realizować email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
4. Rozwiązanie musi umożliwiać zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
5. Rozwiązanie musi zapewniać ochronę i analizę zarówno poczty przychodzącej, jak i wychodzącej.
6. Rozwiązanie musi zapewniać szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
7. Rozwiązanie musi umożliwiać tworzenie polityk kontroli antywirusowej oraz antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
8. Rozwiązanie musi zapewniać kwarantannę poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania wiadomości z kwarantanny przez użytkownika.
9. Rozwiązanie musi realizować backup konfiguracji lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
10. Rozwiązanie musi umożliwiać definiowanie białych i czarnych list adresów mailowych definiowanych globalnie oraz dla domen wskazanych przez administratora, a także funkcjonalność definiowania białych i czarnych list dla poszczególnych użytkowników.
11. Rozwiązanie musi zapobiegać przed wyciekiem informacji poufnej (DLP) pozwalające na czytanie metadanych w przesyłanych plikach, czytanie treści wiadomości (w tym nagłówków) oraz wyzwalanie akcji takich jak: zablokowanie wiadomości (reject oraz discard), dodanie nagłówka do wiadomości, powiadomienie użytkownika, poddanie kwarantannie, zaszyfrowanie wiadomości, dodanie BCC (UDW).
12. Rozwiązanie musi wspierać TLS (serwer-serwer) z kontrolą szyfrów i ich egzekwowaniem.
13. Rozwiązanie musi wspierać geolokalizację adresów IP i umożliwiać wykorzystanie geolokalizacji w politykach (np. blokowanie konkretnego państwa).
14. Rozwiązanie musi integrować się (poprzez API) z Microsoft Office 365 umożliwiając skanowanie w czasie rzeczywistym skrzynek pocztowych.
15. Rozwiązanie musi być zgodne ze standardami SMTP RFC.
16. Rozwiązanie musi obsługiwać DANE (DNS-based Authentication of Named Entities).
17. Rozwiązanie musi umożliwiać pracę w trybie Gateway.

3.4. Kontrola antywirusowa

1. Rozwiązanie musi realizować skanowanie antywirusowe wiadomości SMTP.
2. Rozwiązanie musi zapewniać kwarantannę dla zainfekowanych plików.
3. Rozwiązanie musi realizować skanowanie załączników skompresowanych oraz archiwów zagnieżdżonych.
4. Rozwiązanie musi umożliwiać definiowanie komunikatów powiadomień w języku polskim.
5. Rozwiązanie musi umożliwiać blokowanie załączników w oparciu o typ pliku.

6. Rozwiązanie musi umożliwiać zdefiniowanie nie mniej niż 50 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość integracji mechanizmów ochrony antywirusowej z rozwiązaniami sandboxowymi w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania oceny zagrożenia.
8. Rozwiązanie musi umożliwiać definiowanie różnych akcji dla poszczególnych metod wykrywania złośliwego oprogramowania dla wiadomości przychodzących i wychodzących, obejmujących co najmniej: tagowanie wiadomości, dodawanie nagłówka, dopisywanie ostrzeżenia w treści wiadomości, poddawanie kwarantannie, odrzucanie (discard oraz deny), dodanie BCC (UDW).

3.5. Kontrola antyspamowa

1. Rozwiązanie musi realizować filtrowanie w oparciu o reputację adresów źródłowych IP oraz domen pocztowych w oparciu o bazy reputacji producenta.
2. Rozwiązanie musi realizować filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Rozwiązanie musi realizować szczegółową kontrolę nagłówka wiadomości.
4. Rozwiązanie musi realizować analizę heurystyczną.
5. Rozwiązanie musi współpracować z zewnętrznymi serwerami RBL, SURBL.
6. Rozwiązanie musi realizować filtrowanie w oparciu o filtry Bayesa z możliwością uczenia przez administratora globalnie dla całego systemu lub poszczególnych chronionych domen.
7. Rozwiązanie musi umożliwiać dostrajanie filtrów Bayesa przez poszczególnych użytkowników.
8. Rozwiązanie musi realizować wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Rozwiązanie musi realizować wykrywanie spamu w oparciu o mechanizm analizy behawioralnej analizującej podobieństwa między skanowanym emailem a znanym spamem znajdującym się w bazie spamu dostarczonej przez producenta oferowanego rozwiązania.
10. Rozwiązanie musi realizować wykrywanie spamu w oparciu o mechanizm analizy podszywania się (impersonacją) – ręczne i automatyczne wykrywanie podszywania się pod adres email/osobę.
11. Rozwiązanie musi realizować kontrolę w oparciu o Greylisting.
12. Rozwiązanie musi realizować filtrowanie treści wiadomości i załączników.
13. Rozwiązanie musi zapewniać kwarantannę zarówno użytkowników, jak i systemową z możliwością edycji nagłówka wiadomości.
14. Rozwiązanie musi umożliwiać zdefiniowanie nie mniej niż 200 polityk kontroli antyspamowej dla całego systemu.
15. Rozwiązanie musi realizować skanowanie antyspamowe z wydajnością minimum 50 000 wiadomości na godzinę.
16. Rozwiązanie musi zapewniać ochronę typu outbreak.
17. Rozwiązanie musi realizować filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
18. Rozwiązanie musi wspierać SPF, DKIM, DMARC oraz ARC.

19. Rozwiązanie musi umożliwiać ochronę w oparciu o wyrażenia regularne i zdefiniowany przez administratora słownik wyrazów.
20. Rozwiązanie musi umożliwiać definiowanie różnych akcji dla poszczególnych metod wykrywania spamu dla wiadomości przychodzących i wychodzących, obejmujących co najmniej: tagowanie wiadomości, dodawanie nagłówka, dopisywanie ostrzeżenia w treści wiadomości, poddawanie kwarantannie, odrzucanie (discard oraz deny), dodanie BCC (UDW).

3.6. Ochrona treści

1. Rozwiązanie musi realizować wykrywanie aktywnej zawartości w plikach PDF i dokumentach Office.
2. Rozwiązanie musi realizować neutralizację dokumentów Office i PDF (usuwanie makr, aktywnej zawartości, załączników i innych).
3. Rozwiązanie musi realizować ponowne skanowanie w poszukiwaniu zagrożeń przy zwolnieniu z kwarantanny.
4. Rozwiązanie musi realizować wykrywanie typów MIME i typów plików.
5. Rozwiązanie musi umożliwiać tworzenie własnych filtrów plików.
6. Rozwiązanie musi umożliwiać odszyfrowywanie archiwów, plików PDF i dokumentów przy użyciu wbudowanych i zdefiniowanych przez administratora list haseł.
7. Rozwiązanie musi realizować filtrowanie adresów URL z możliwością tworzenia własnych kategorii adresów, które mają być filtrowane. Baza adresów URL powinna być dostarczona przez producenta oferowanego rozwiązania.
8. Rozwiązanie musi realizować neutralizację treści HTML wiadomości e-mail poprzez usunięcie hiperłączy lub przepisanie adresów URL.
9. Rozwiązanie musi realizować ochronę hiperłączy poprzez nadpisanie URL i przekierowanie do portalu weryfikującego kliknięty link (URI Click Protection).
10. Rozwiązanie musi wspierać S/MIME.
11. Rozwiązanie musi umożliwiać automatyczne i bezagentowe szyfrowanie wiadomości na podstawie wybranych przez administratora atrybutów, takich jak treść tematu, treść wiadomości lub domena odbiorcy, w trybie Push i Pull.

3.7. Ochrona przed atakami na usługę poczty

1. Rozwiązanie musi zapewniać ochronę przed atakami na adres odbiorcy.
2. Rozwiązanie musi umożliwiać ograniczenie liczby połączeń oraz jednoczesnych połączeń.
3. Rozwiązanie musi umożliwiać definiowanie maksymalnej liczby wiadomości pocztowych otrzymywanych w jednostce czasu.
4. Rozwiązanie musi realizować kontrolę Reverse DNS (ochrona Anty-Spoofing).
5. Rozwiązanie musi realizować weryfikację poprawności adresu e-mail nadawcy.
6. Rozwiązanie musi zapewniać ochronę przed BEC (Business Email Compromise), tj. atakami phishingowymi lub socjotechnicznymi, których celem jest przede wszystkim kadra kierownicza wyższego szczebla oraz pracownicy działów finansowych.

3.8. Funkcje pracy w trybie wysokiej dostępności (HA)

1. Rozwiązanie musi umożliwiać konfigurację HA w trybie Gateway.
2. Rozwiązanie musi wspierać tryb Active-Passive z synchronizacją polityk i wiadomości, gdzie klaster występuje pod jednym adresem IP.
3. Rozwiązanie musi umożliwiać tryb synchronizacji konfiguracji dla scenariuszy, gdy każde z urządzeń występuje pod innym adresem IP.
4. Rozwiązanie musi realizować wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.
5. Rozwiązanie musi umożliwiać monitorowanie stanu pracy klastra.

3.9. Zarządzanie i administracja

1. Rozwiązanie musi umożliwiać zarządzanie lokalne z wykorzystaniem protokołów HTTPS oraz SSH.
2. Rozwiązanie musi wspierać SAML 2.0 SSO i ADFS.
3. Rozwiązanie musi obsługiwać SNMP przy użyciu standardowych i prywatnych MIB z pułapkami opartymi na progach.
4. Rozwiązanie musi umożliwiać tworzenie kont administratora przypisywanych do konkretnych domen obsługiwanych przez system.

3.10. Aktualizacje sygnatur i bazy danych

1. Rozwiązanie musi pracować w oparciu o bazę spamu oraz URL aktualizowane w czasie rzeczywistym.
2. Rozwiązanie musi umożliwiać planowanie aktualizacji definicji sygnatur zgodnie z harmonogramem, z częstotliwością co najmniej raz na godzinę.

3.11. Szkolenie dla rozwiązania równoważnego

1. Wykonawca zapewni przeprowadzenie szkolenia dla administratorów Zamawiającego z zakresu administrowania oferowanym rozwiązaniem.
2. Szkolenie musi obejmować co najmniej: konfigurację podstawową i zaawansowaną, zarządzanie politykami bezpieczeństwa, monitorowanie pracy systemu, analizę logów i zdarzeń, obsługę mechanizmów aktualizacji, utrzymanie ciągłości działania oraz procedury reagowania na incydenty i usuwania podstawowych problemów eksploatacyjnych.
3. Szkolenie musi zostać przeprowadzone przez osobę posiadającą wiedzę i doświadczenie w zakresie oferowanego rozwiązania.
4. Materiały szkoleniowe oraz dokumentacja przekazywana w ramach szkolenia muszą zostać dostarczone w języku polskim lub angielskim.
5. W przypadku zaoferowania rozwiązania równoważnego szkolenie musi dotyczyć bezpośrednio zaoferowanego rozwiązania równoważnego i obejmować wszystkie funkcjonalności niezbędne do jego samodzielnej administracji przez Zamawiającego. Minimalny wymiar szkolenia wynosi 8 godzin zegarowych.

6. Szkolenie musi zostać przeprowadzone dla co najmniej 2 administratorów Zamawiającego.

3.12. Usługa wdrożenia dla rozwiązania równoważnego

1. W przypadku zaoferowania rozwiązania równoważnego Wykonawca zobowiązany jest do wykonania usługi wdrożenia oferowanego rozwiązania.
2. Usługa wdrożenia musi obejmować co najmniej: instalację, konfigurację, uruchomienie produkcyjne, integrację z istniejącym środowiskiem Zamawiającego, konfigurację mechanizmów wysokiej dostępności (HA), migrację lub odtworzenie niezbędnych ustawień i polityk oraz weryfikację poprawności działania rozwiązania.
3. W ramach wdrożenia Wykonawca przygotuje i przekaże dokumentację powdrożeniową w języku polskim, zawierającą opis wykonanych czynności, konfiguracji oraz rekomendacje eksploatacyjne i administracyjne.
4. Dokumentacja powdrożeniowa musi zostać przekazana w języku polskim.
5. Celem usługi wdrożenia jest zapewnienie pełnej gotowości oferowanego rozwiązania równoważnego do pracy w środowisku Zamawiającego oraz umożliwienie jego prawidłowego utrzymania i administracji.
6. Wdrożenie musi obejmować przeprowadzenie testów powdrożeniowych oraz odbiór potwierdzający poprawność uruchomienia i działania rozwiązania w środowisku Zamawiającego.

4. Wymagania licencyjne

1. Zamawiający wymaga dostarczenia licencji terminowych na okres 24 miesięcy, obowiązujących od dnia 2026-08-16.
2. Dla istniejącej instancji FortiMail VM02 – przedłużenie licencji obejmującej następujący zakres subskrypcji i usług:
    a. Firmware & General Updates,
    b. Enhanced Support (poziom Premium),
    c. Telephone Support (poziom Premium),
    d. Advanced Malware Protection,
    e. FortiMail-Office365-Protection,
    f. URI Click Protection,
    g. AntiSpam,
    h. FortiGuard Virus Outbreak Protection Service,
    i. FortiSandbox Cloud,
    j. Content Disarm & Reconstruction.
3. Dla nowej instancji HA – dostarczenie licencji w zakresie tożsamym z pkt 2.
4. Obie licencje muszą umożliwiać:
    a. samodzielne pobieranie aktualizacji oprogramowania, sygnatur i poprawek bezpośrednio od producenta poprzez dedykowane konto,
    b. zakładanie zgłoszeń serwisowych 24 godziny na dobę, 7 dni w tygodniu poprzez dedykowany, zabezpieczony kanał komunikacji elektronicznej.

5. Dla rozwiązania równoważnego – licencje muszą zapewniać zakres funkcjonalny i usługowy nie gorszy niż określony w pkt 2–4, w szczególności w zakresie wszystkich wymienionych subskrypcji i poziomu wsparcia.

5. Wsparcie techniczne i SLA

1. Okres wsparcia technicznego: 24 miesiące od dnia rozpoczęcia obowiązywania licencji (od 2026-08-16).
2. Wsparcie techniczne świadczone przez producenta w trybie zdalnym, z dostępem do kanału webowego oraz telefonicznego.
3. Minimalnie wymagany przez Zamawiającego zakres obsługi zgłoszeń: 8×5 (dni robocze, godziny 8:00–16:00 czasu lokalnego), przy czym dopuszczalne jest świadczenie wsparcia w szerszym zakresie wynikającym z warunków producenta.
4. Minimalnie wymagany przez Zamawiającego czas reakcji na zgłoszenie serwisowe: do 24 godzin od przyjęcia zgłoszenia, przy czym dopuszczalne są krótsze czasy reakcji wynikające z warunków producenta.
5. Kanał zgłoszeń serwisowych: dedykowany, zabezpieczony kanał komunikacji elektronicznej producenta, dostępny 24h/7 dni w tygodniu.
6. Wsparcie techniczne obejmuje:
    a. nieograniczony dostęp do aktualizacji oprogramowania (firmware) i poprawek,
    b. nieograniczony dostęp do aktualizacji baz sygnatur (antyspamowych, antywirusowych, URL),
    c. dostęp do bazy wiedzy i dokumentacji technicznej producenta,
    d. możliwość zakładania i śledzenia zgłoszeń serwisowych.
7. Szczegółowe warunki wsparcia technicznego regulują warunki licencyjne i serwisowe producenta, przy czym wymagania określone w niniejszym dokumencie należy traktować jako minimalne. Świadczenie wsparcia w szerszym zakresie, w tym z krótszym czasem reakcji lub większą dostępnością, jest dopuszczalne.