

Szczegółowy Opis Przedmiotu Zamówienia

I. Przedmiot zamówienia

Przedmiotem zamówienia jest odnowienie licencji subskrypcyjnej do posiadanego przez Zamawiającego systemu ochrony aplikacji webowych (WAF), (dalej jako: „System”) lub dostawa rozwiązania równoważnego wraz z świadczeniem usługi wsparcia przez Wykonawcę:

1. Odnowienie licencji subskrypcyjnej dla dwóch maszyn wirtualnych FortiWeb VM02 działających w klastrze HA na okres 36 miesięcy lub 60 miesięcy od dnia 25.11.2025 r.

- 1) dostęp do aktualizacji oprogramowania (firmware) oraz baz sygnatur (m.in. WAF, IPS, AV, Botnet, GeoIP).
- 2) dostęp do wsparcia technicznego producenta (Fortinet Support) w trybie 24/7.
- 3) zachowanie ciągłości działania systemu ochrony aplikacji webowych (WAF).
- 4) odnowienie licencji na dodatkowe moduły:
 - a) AV,
 - b) IP Reputation,
 - c) FortiSandbox,
 - d) Credential Stuffing Defense,
 - e) GEO DB,
 - f) Threat Analytics.
- 5) odnowienie licencji subskrypcyjnej wraz ze wsparciem producenta na wszystkie moduły muszą dotyczyć maszyn wirtualnych o numerach seryjnych :
 - a) FVVM02TM22002136 (Primary),
 - b) FVVM02TM22002137 (Secondary).

2. Świadczenie usługi wsparcia technicznego przez wykonawcę:

Wykonawca zapewni usługę wsparcia technicznego i konsultacji dla Systemu, która będzie realizowana przez zespół minimum 2 specjalistów posiadających aktualny certyfikat Fortinet Certified Professional (FCP) - Public Cloud Security lub minimum 1 specjalistę posiadającego aktualny certyfikat Fortinet Certified Solution Specialist Public Cloud Security, wydane przez producenta Systemu.

Usługa wsparcia będzie świadczone w dni robocze w języku polskim lub angielskim w okresie 36/60 miesięcy od dnia 25.11.2025 r., w wymiarze nie przekraczającym 20 roboczogodzin. Usługa wsparcia obejmuje w szczególności:

- 1) udzielanie konsultacji i wsparcia technicznego;
- 2) świadczenie pomocy zdalnej administratorom Zamawiającego;

II. Wymagania dla rozwiązania równoważnego

Zamawiający dopuszcza dostarczenie rozwiązania równoważnego spełniającego wymagania określone w Załączniku nr 1 do SOPZ.



Opis wymagań dla oprogramowania równoważnego

1. Wymagania ogólne

- 1) elementy Systemu muszą działać w oparciu o dedykowane oprogramowanie;
- 2) wszystkie funkcje podstawowe Systemu oraz zastosowane w nich moduły muszą pochodzić od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowanych w Systemie były opracowane przez firmy trzecie;
- 3) możliwość implementacji systemu w trybach:
 - a) reverse proxy;
 - b) inline transparent;
 - c) Offline Sniffing;
 - d) Web Cache Communication Protocol (WCCP).
- 4) System nie może posiadać ograniczeń co do ilości chronionych aplikacji web;
- 5) możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu, tj.: możliwość zdefiniowania minimum 4 zestawów grup administratorów, w których każdy zestaw nie może mieć możliwość wglądu i zmiany konfiguracji innych grup administratorów, w szczególności do polityk, domen/serwerów, kwerend LDAP, logów, raportów;
- 6) System musi mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active lub w trybie synchronizacji konfiguracji;
- 7) System musi być dostarczony w formie dwóch maszyn wirtualnych (działających w trybie HA lub w trybie synchronizacji konfiguracji);
- 8) możliwość instalacji systemu na platformach: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure.

2. Parametry wydajnościowe: (Wymagania wydajnościowe)

- 1) przepustowość dla ruchu http – min. 100 Mbps;
- 2) wsparcie dla minimum 2 vCPU;
- 3) System musi umożliwiać skalowanie wydajności poprzez zmianę licencji;
- 4) możliwość skonfigurowania do czterech interfejsów sieciowych (do 10 dla VMware ESX).

3. Wymagania funkcjonalne

- 1) obsługa protokołów: http 1.1, http 2.0, FTP;
- 2) automatyczne tworzenie profili ochronnych aplikacji na bazie zaobserwowanego ruchu;
- 3) możliwość wyboru trybu wymuszania wyuczonego schematu bez konieczności akceptacji przez administratora;

-
- 4) automatyczne tworzenie profilu ochrony przed botami na bazie zaobserwowanego ruchu użytkowników;
 - 5) podział obciążenia na kilkanaście serwerów (load balancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:
 - a) Round Robin,
 - b) Weighted Round Robin,
 - c) Least Connection.
 - 6) wsparcie dla mechanizmów session persistence:
 - a) Source IP,
 - b) HTTP Header,
 - c) URL parameter,
 - d) Insert Cookie,
 - e) Rewrite Cookie,
 - f) Persistent Cookie,
 - g) Embedded Cookie,
 - h) ASP Session ID,
 - i) PHP Session ID,
 - j) JSP Session ID,
 - k) SSL Session ID.
 - 7) terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2, TLS 1.3;
 - 8) możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa;
 - 9) ochrona aplikacji www przed takimi zagrożeniami jak:
 - a) SQL and OS Command Injection,
 - b) Cross Site Scripting (XSS),
 - c) Cross Site Request Forgery,
 - d) Outbound Data Leakage,
 - e) HTTP Request Smuggling,
 - f) Buffer Overflow,
 - g) Encoding Attacks,
 - h) Cookie Tampering / Poisoning,
 - i) Session Hijacking,
 - j) Broken Access Control,
 - k) Forceful Browsing /Directory Traversal,
 - l) Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP,

-
- m) DoS w warstwie aplikacji,
 - n) Ochrona przed atakami typu Brute force,
 - o) Ochrona przed atakami clickjacking,
 - p) Ochrona przed credential stuffing.
- 10) mechanizmy ochrony przed wyciekiem informacji poufnych;
 - 11) filtrowanie ruchu do aplikacji w oparciu o geolokalizację;
 - 12) analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania;
 - 13) możliwość integracji z zewnętrznymi systemami uwierzytelniania dwuskładnikowego;
 - 14) wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy;
 - 15) wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure” oraz „http only”;
 - 16) content routing na bazie parametrów http oraz certyfikatów X.509;
 - 17) ochrona przed Web Scraping;
 - 18) wsparcie dla kompresji danych oraz cache;
 - 19) publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos);
 - 20) wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3;
 - 21) ochrona przed atakami typu SLOW ();
 - 22) możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji;
 - 23) Dodanie wyjątków dla sygnatur na podstawie wielu parametrów:
 - a) Metoda HTTP,
 - b) IP Klienta,
 - c) Host,
 - d) URI,
 - e) Cały URL,
 - f) Parametr,
 - g) Cookie,
 - h) http Header,
 - i) JSON Elements.
 - 24) funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwarded-For”;
 - 25) wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej;
 - 26) możliwość konfigurowania własnych stron z informacjami o błędzie per polityka;
 - 27) ustawienie wymaganej sekwencji otwieranych stron;
 - 28) sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload’u HTML;
 - 29) wsparcie dla walidacji OpenAPI, JSON i XML;

- 30) blokowania „Illegal XML Format” oraz „Illegal JSON Format”;
- 31) możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy;
- 32) przydzielanie różnych certyfikatów dla różnych nazw domenowych;
- 33) ochrona przed atakami MiTB (Man-in-the-Browser) przynajmniej dla Anti-keylogger, Obfuscate;
- 34) URL Encryption.

4. Wymagania dodatkowe

- 1) Kontrola antywirusowa dla komunikacji http realizowana na firewall'u aplikacyjnym. Muszą zostać dostarczone wszystkie licencje niezbędne do uruchomienia tej funkcjonalności;
- 2) skaner aplikacji WWW realizowany bezpośrednio na firewall'u aplikacyjnym. Muszą zostać dostarczone wszystkie licencje niezbędne do uruchomienia tej funkcji;
- 3) ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall'u aplikacyjnym. Muszą zostać dostarczone wszystkie licencje niezbędne do uruchomienia tej funkcji;
- 4) dekodowanie Base64 oraz CSS;
- 5) domyślne szablony ochrony dla Exchange, SharePoint i WordPress;
- 6) uwierzytelnianie użytkowników w oparciu o protokół SAML;
- 7) rozpoznawanie prawidłowo zalogowanych użytkowników dla chronionej aplikacji www;
- 8) wsparcie dla CAPTCHA i Real Browser Enforcement do weryfikacji użytkowników;
- 9) budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa;
- 10) możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day;
- 11) możliwość znakowania przez administratorów systemu za pomocą znaczników (flag) lub komentarza zdarzeń zalogowanych przez urządzenie w celu późniejszej ich analizy;
- 12) ochrona przed botami dla: strony internetowej, aplikacji mobilnej, interfejsu API - przy zastosowaniu funkcji biometrycznych;
- 13) Cross-Origin Resource Sharing (CORS) protection.

5. Zarządzanie

- 1) System musi umożliwiać zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API;
- 2) System musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture;
- 3) możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych.
- 4) Możliwość zdefiniowania ról określających uprawnienia dla kont administratorów (RBAC). Zamawiający wymaga, aby w oprogramowaniu była możliwość zdefiniowania roli administratora mającego uprawnienia read only.

6. Logowanie i Raportowanie

- 1) System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów;
- 2) możliwość logowania zdarzeń Rozwiązania do zewnętrznego serwera syslog i SIEM – Zamawiający posiada oprogramowanie Splunk ES;
- 3) obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem;
- 4) powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.

7. Sygnatury, subskrypcje

- 1) Bazy sygnatur wykorzystywane przez funkcje ochronne muszą być systematycznie aktualizowane zgodnie ze zdefiniowanym harmonogramem, nie rzadziej niż raz dziennie;
- 2) System musi być dostarczony wraz ze wszystkimi licencjami, subskrypcjami i wsparciem producenta, umożliwiającymi użytkowanie Systemu z jego wszystkim funkcjonalnościami przez okres minimum 36 (60) miesięcy;
- 3) System musi być dostarczony wraz ze wszystkimi licencjami i subskrypcjami, upoważniającymi do korzystania z aktualnych baz funkcji ochronnych i serwisów. Muszą one obejmować również: kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP przez okres 36 (60) miesięcy;
- 4) gwarancja dostępności najnowszej wersji oprogramowania Systemu oraz poprawek i uaktualnień w trakcie trwania umowy;
- 5) wszystkie niestandardowe MIB'y dla Systemu muszą zostać dostarczone przez Wykonawcę.

8. Usługa wdrożeniowa

Wykonawca zobowiązuje się do wdrożenia systemu przy udziale Zamawiającego w terminie do dnia 23.11.2025 r.

Usługa wdrożeniowa obejmuje:

- 1) instalację Systemu wraz z konfiguracją w trybie HA (active-passive lub synchronizacji konfiguracji) na platformie Zamawiającego;
- 2) konfigurację LDAP;
- 3) konfigurację logowania poprzez SSO;
- 4) uruchomienie ADFS Proxy oraz stworzenie polityk;
- 5) integrację z posiadanym przez Zamawiającego systemem SIEM – SPLUNK. Zamawiający wymaga dedykowanej aplikacji w oprogramowaniu Splunk (threat monitoring) dostarczanej przez producenta oferowanego WAF za pośrednictwem portalu splunkbase.
- 6) Implementację polityk na nowym systemie (migracja z posiadanego systemu)

Wykonawca przed przystąpieniem do wdrożenia przedstawi analizę przedwdrożeniową zawierającą szczegółową koncepcję uwzględniającą elementy wdrożenia (w szczególności topologię sieci oraz integrację

z innymi wewnętrznymi systemami i aplikacjami), ryzyka związane z wdrożeniem oraz szczegółowy harmonogram prac.

Do realizacji wdrożenia Systemu Wykonawca skieruje min. 2 osoby posiadające aktualny certyfikat autoryzowany przez producenta Systemu, potwierdzający zaawansowaną wiedzę z wdrażanego Systemu.

Wdrożenie będzie realizowane z udziałem przedstawicieli Zamawiającego poprzez zdalne połączenie lub obecność w siedzibie Zamawiającego.

Usługa wdrożeniowa realizowana w godzinach pracy nie może wpływać na dostępność obecnie wykorzystywanej usługi WAF przez Zamawiającego.

9. Dokumentacja

- 1) analiza przedwdrożeniowa, o której mowa w pkt 8;
- 2) Instrukcja dla Administratora systemu w formie elektronicznej zawierającą minimum:
 - a) opis wraz z procedurami instalacji i konfiguracji całego Systemu,
 - b) plan odtwarzania systemu po awarii (w tym procedurę tworzenia i przywracania Systemu) itp. oraz postępowania w sytuacjach awaryjnych (w postaci wykazu typowych problemów i sposoby ich rozwiązywania).

10. Usługa szkoleniowa

- 1) Wykonawca zapewni przeprowadzenie certyfikowanych szkoleń dla 4 administratorów Zamawiającego obejmujących co najmniej następujące zagadnienia: wdrożenie Systemu, podstawowa konfiguracja Systemu, zarządzanie, funkcjonalności Systemu, rozwiązywanie problemów;
- 2) szkolenie stacjonarne lub online w wymiarze minimum 3 dni, zakończone certyfikowanym przez producenta zaoferowanego rozwiązania egzaminem.
- 3) szkolenie odbędzie się w terminie ustalonym przez strony, nie później niż w terminie 3 miesięcy od dnia odbioru Systemu.

11. Wsparcie techniczne

Wykonawca zapewni usługę wsparcia technicznego i konsultacji dla Systemu, która będzie realizowana przez zespół min. 2 specjalistów po stronie Wykonawcy posiadających aktualny certyfikat autoryzowany przez producenta Systemu, potwierdzający zaawansowaną wiedzę z Systemu.

Usługa wsparcia będzie świadczona w dni robocze w języku polskim lub angielskim w okresie 36 (60) miesięcy od dnia odbioru Systemu, w wymiarze nie przekraczającym 80 roboczogodzin. Usługa wsparcia obejmuje w szczególności:

- 1) udzielanie konsultacji i wsparcia technicznego;
- 2) świadczenie pomocy zdalnej administratorom Zamawiającego.