**Załącznik nr 1 do SWZ**

**Opis przedmiotu zamówienia (OPZ)**

# Przedmiot zamówienia

Przedmiotem zamówienia jest odnowienie subskrypcji i usług wsparcia technicznego producenta dla posiadanych przez Zamawiającego urządzeń Barracuda CloudGen Firewall F400 oraz Barracuda Web Application Firewall 660 wraz z usługą konfiguracji WAF i analizy konfiguracji Firewall.

# Cel i zakres zamówienia

Celem zamówienia jest zapewnienie nieprzerwanej ochrony i wsparcia technicznego producenta dla posiadanych przez Zamawiającego urządzeń:

* 2 x Barracuda CloudGen Firewall F400 (NGFW) oraz
* 2 x Barracuda Web Application Firewall 660 (WAF),

poprzez odnowienie subskrypcji oraz usług wsparcia producenta na okres 12 miesięcy.

Dodatkowo przedmiot zamówienia obejmuje również:

* usługę konfiguracji WAF w klastrze dla wskazanych serwisów Zamawiającego;
* analizę obecnej konfiguracji Firewall w klastrze zakończoną raportem z rekomendacjami.

## Zakres zamówienia

Zakres zamówienia obejmuje:

* Dostawę nowych (nieodnowionych, nie z drugiej ręki) licencji i usług wsparcia producenta dla wskazanych urządzeń, przypisanych do konkretnych numerów seryjnych.
* Usługę konfiguracji WAF dla serwisów:
  + espd.uzp.gov.pl
  + wokanda.uzp.gov.pl
  + formularz.uzp.gov.pl
  + ekomentarzpzp.uzp.gov.pl
  + miniportal.uzp.gov.pl
  + ankieta.uzp.gov.pl
  + bzp.uzp.gov.pl
* Analizę obecnej konfiguracji Firewall;
* Szkolenie/instruktaż dla administratorów Zamawiającego w zakresie konfiguracji WAF oraz Firewall.

# Słownik pojęć

* **Zamawiający** – podmiot realizujący postępowanie przetargowe.
* **Wykonawca** – podmiot składający ofertę i realizujący zamówienie.
* **Subskrypcje** – prawo do korzystania z określonych funkcjonalności urządzenia Barracuda, zgodnie z warunkami producenta.
* **Wsparcie techniczne** – usługa świadczona przez producenta lub autoryzowanego partnera, obejmująca m.in. aktualizacje, pomoc techniczną, wymianę sprzętu.
* **WAF** – Web Application Firewall.
* **NGFW** – Next Generation Firewall.
* **SN** – numer seryjny urządzenia.

# Wymagania funkcjonalne i wydajnościowe

## Subskrypcje dla Barracuda CloudGen Firewall F400

Dla każdego z urządzeń Barracuda CloudGen Firewall F400 (SN: 1559731, 1559727) należy dostarczyć i aktywować na okres minimum 12 miesięcy następujące subskrypcje (lub równoważne):

* Energize Updates
* Instant Replacement
* Malware Protection
* Advanced Threat Protection
* Advanced Remote Access

**Warunki równoważności:** Każda subskrypcja musi zapewniać kompatybilność z urządzeniem, przypisanie do konkretnego SN oraz co najmniej funkcjonalności, parametry i zakres usług odpowiadający funkcjom opisanym w załącznik nr 1 (Tabela funkcjonalności).

## Subskrypcje dlaBarracuda Web Application Firewall 660

Dla każdego z urządzeń Barracuda Web Application Firewall 660 (SN: 1249724, 3004734) należy dostarczyć i aktywować na okres minimum 12 miesięcy następujące subskrypcje (lub równoważne):

* Advanced Bot Protection License
* Active DDoS Prevention
* Advanced Threat Protection
* Energize Updates
* Instant Replacement.

**Warunki równoważności:** Każda subskrypcja musi zapewniać kompatybilność z urządzeniem, przypisanie do konkretnego SN oraz co najmniej funkcjonalności, parametry i zakres usług odpowiadający funkcjom opisanym w załącznik nr 1 (Tabela funkcjonalności).

## Usługa konfiguracji WAF w klastrze dla 7 serwisów, okres obserwacji, optymalizacja, szkolenie administratorów, dokumentacja powykonawcza

Celem usługi jest zapewnienie skutecznej ochrony aplikacji webowych Zamawiającego poprzez profesjonalną konfigurację urządzeń Barracuda Web Application Firewall 660 dla wskazanych serwisów internetowych, zgodnie z najlepszymi praktykami bezpieczeństwa oraz specyfiką chronionych aplikacji.

### Zakres usługi

Usługa obejmuje w szczególności:

1. **Wstępną analizę środowiska**:
   * Identyfikację i analizę serwisów do ochrony:
     + espd.uzp.gov.pl
     + wokanda.uzp.gov.pl
     + formularz.uzp.gov.pl
     + ankieta.uzp.gov.pl
     + ekomentarzpzp.uzp.gov.pl
     + miniportal.uzp.gov.pl
     + bzp.uzp.gov.pl (serwis archiwalny, brak aktywnych użytkowników)
   * Wszystkie wskazane serwisy są wdrożone produkcyjnie i dostępne publicznie pod wskazanymi adresami.
   * Analiza serwisów możliwa z udziałem Zamawiającego – po 30 minut na każdy serwis.
   * Z wymienionych serwisów użytkownicy korzystają bez instrukcji. Wyłącznie dla Miniportal.uzp.gov.pl jest udostępniana instrukcja – do wglądu dla Wykonawcy.
   * Powyższe serwisy nie posiadają API.
   * Powyższe serwisy są udostępniane wyłącznie z sieci Zamawiającego (bez CDN).
2. **Wdrożenie i konfigurację WAF**:
   * Dodanie wskazanych serwisów do ochrony na urządzeniu WAF.
   * Konfigurację polityk bezpieczeństwa dla każdego serwisu, w tym:
     + Ochronę przed atakami OWASP Top 10:2025 (Release Candidate)[[1]](#footnote-1) – aktualny na dzień złożenia oferty.
     + Konfigurację ochrony przed botami (Advanced Bot Protection) i atakami DDoS (Active DDoS Prevention).
     + Włączenie mechanizmów Advanced Threat Protection dla przesyłanych plików.
     + Konfigurację SSL/TLS Offloading.
     + Ustawienie reguł dostępu (IP, geolokalizacja, uwierzytelnianie).
     + Wdrożenie mechanizmów logowania i raportowania incydentów.
   * Konfigurację trybu „obserwacji” (monitoring/learning mode) na okres minimum 2 do maksymalnie 4 tygodni:
     + Zbieranie logów i alertów, analiza fałszywych alarmów.
     + Dostosowanie polityk na podstawie obserwacji ruchu i zgłoszeń użytkowników.
3. **Optymalizację i finalizację konfiguracji**:
   * Dostosowanie reguł bezpieczeństwa po okresie obserwacji, eliminacja fałszywych alarmów.
   * Zamawiający dopuszcza, że eliminacja fałszywych alarmów nie będzie możliwa w przypadku, gdy ich źródłem są niezgodności chronionych aplikacji lub infrastruktury Zamawiającego z powszechnie przyjętymi standardami (np. IETF RFC, W3C, ANSI, UNICODE, WHATWG, WaSP). W takich przypadkach Wykonawca zobowiązany jest do wskazania przyczyny oraz rekomendacji działań po stronie Zamawiającego
   * Ostateczne włączenie trybu ochrony (enforcement mode) dla wszystkich serwisów.
   * Konfiguracja powiadomień o zdarzeniach bezpieczeństwa wykrytych przez WAF, które spełnia kryteria:
     + wykrycie ataku z listy OWASP Top 10,
     + przekroczenie progów DDoS,
     + wykrycie prób przejęcia konta.
4. **Dokumentację powykonawczą**:
   * Szczegółowy opis zastosowanych polityk i reguł.
   * Instrukcję obsługi i procedurę reagowania na incydenty.
   * Raport z okresu obserwacji (statystyki, wykryte zagrożenia, działania korygujące).
5. **Szkolenie/instruktaż administratorów**:
   * Przeprowadzenie szkolenia (minimum 4 godziny) dla administratorów Zamawiającego z zakresu:
     + Zarządzania politykami WAF.
     + Analizy logów i reagowania na incydenty.
     + Samodzielnej modyfikacji reguł i obsługi alertów.
   * Przekazanie materiałów szkoleniowych.
   * Szkolenie/instruktaż dla administratorów Zamawiającego może być przeprowadzone w formie zdalnej, z wykorzystaniem platformy MS Teams Zamawiającego.

### Terminy realizacji

1. Rozpoczęcie usługi: w ciągu 20 dni roboczych od aktywowania subskrypcji WAF o których mowa w 4.2.
2. Czas trwania wstępnej analizy środowiska oraz wdrożenie i konfigurację WAF: do 7 dni roboczych od rozpoczęcia prac.
3. Okres obserwacji (monitoring/learning mode): minimum 14 dni kalendarzowych od zakończenia konfiguracji wstępnej. Maksymalny okres obserwacji: 30 dni kalendarzowych.
4. Optymalizacja i finalizacja konfiguracji: do 7 dni roboczych po zakończeniu okresu obserwacji.
5. Szkolenie administratorów: w terminie indywidualnie uzgodnionym, nie później niż 5 dni roboczych po zakończeniu finalizacji konfiguracji.
6. Przekazanie dokumentacji i raportu: do 5 dni roboczych po zakończeniu finalizacji konfiguracji.

### Wymagania mierzalne

1. Ochroną musi zostać objętych minimum 7 wskazanych serwisów Zamawiającego.
2. Okres obserwacji (monitoring/learning mode) – minimum 14 dni. Maksymalny okres obserwacji: 30 dni kalendarzowych.
3. Liczba godzin szkolenia – minimum 4.
4. Dokumentacja powykonawcza – minimum 1 egzemplarz w wersji elektronicznej.
5. Raport z okresu obserwacji – minimum 1 egzemplarz w wersji elektronicznej.

### Procedura odbioru

1. Wykonawca zgłasza Zamawiającemu gotowość do przeprowadzenia testu odbiorczego po zakończeniu konfiguracji i optymalizacji WAF oraz przekazaniu dokumentacji powykonawczej.
2. Zamawiający potwierdza termin przeprowadzenia testu w ciągu 5 dni roboczych od zgłoszenia.
3. Test odbiorczy powinien zostać przeprowadzony w terminie nie później niż 20 dni roboczych od zgłoszenia gotowości przez Wykonawcę.
4. Czas trwania testu nie powinien przekroczyć 3 dni roboczych.
5. Test obejmuje:
   1. Symulację ataków aplikacyjnych (np. SQL Injection, XSS, RCE, LFI/RFI, brute force, ataki botów, DDoS na warstwie aplikacyjnej).
   2. Próby obejścia mechanizmów WAF.
   3. Weryfikację skuteczności blokowania ataków oraz generowania alertów/logów.
   4. Weryfikację powiadomień o zdarzeniach.
6. Szczegółowy scenariusz testów zostanie uzgodniony z Wykonawcą przed rozpoczęciem testu.
7. Testy mogą być przeprowadzane na środowisku produkcyjnym lub testowym, po wcześniejszym uzgodnieniu z Zamawiającym.
8. W przypadku wykrycia poważnych zakłóceń w działaniu serwisów, testy mogą zostać wstrzymane na wniosek Zamawiającego.
9. Za pozytywny wynik testu uznaje się sytuację, w której:
   1. WAF skutecznie blokuje co najmniej 95% prób ataków zdefiniowanych w uzgodnionym scenariuszu testowym (w tym wszystkie ataki z listy OWASP Top 10).
   2. WAF generuje logi i powiadomienia zgodnie z konfiguracją.
   3. Nie występują nieuzasadnione blokady legalnego ruchu (fałszywe alarmy nie przekraczają progu ≤ 2 na serwis podczas testu).
10. W przypadku wykrycia podatności lub nieskuteczności ochrony, Wykonawca wdraża poprawki w uzgodnionym terminie.
11. W przypadku wykrycia niezgodności, podatności lub nieskuteczności ochrony Zamawiający dostarcza raport z wykazem wykrytych problemów.
12. Wykonawca zobowiązany jest do usunięcia wskazanych niezgodności w terminie do 5 dni roboczych od przekazania raportu.
13. Po wdrożeniu poprawek przeprowadzany jest powtórny test w zakresie wykrytych niezgodności, w terminie uzgodnionym z Zamawiającym.
14. Wyniki testu odbiorczego dokumentowane są w raporcie sporządzonym przez podmiot przeprowadzający test lub przez Zamawiającego.
15. Raport stanowi załącznik do protokołu odbioru usługi konfiguracji WAF.

### Kryteria odbioru

1. Potwierdzenie objęcia ochroną wszystkich wskazanych serwisów.
2. Przekazanie Zamawiającemu dokumentacji powykonawczej i raportu z okresu obserwacji.
3. Przeprowadzenie szkolenia/instruktażu i przekazanie listy obecności.
4. Pozytywny test działania WAF przeprowadzony przez podmiot trzeci, wyłoniony w planowanym postępowaniu na testy APT lub samodzielnie przez Zamawiającego.
5. Podpisanie protokołu odbioru usługi konfiguracji WAF (wzór – załącznik nr 4).

## Usługa analizy konfiguracji 2 urządzeń Barracuda CloudGen Firewall F400 w klastrze, raport z rekomendacjami, wdrożenie poprawek krytycznych

Celem usługi jest przeprowadzenie profesjonalnej analizy obecnej konfiguracji urządzeń Barracuda CloudGen Firewall F400 Zamawiającego, mającej na celu ocenę poziomu bezpieczeństwa oraz zgodności z dobrymi praktykami w zakresie ochrony przed zagrożeniami sieciowymi, w tym malware, atakami botnet, wykorzystania silnika antywirusowego, mechanizmu sandbox oraz systemów wykrywania i raportowania zagrożeń. Efektem analizy będzie raport zawierający rekomendacje usprawnień i wskazanie ewentualnych luk bezpieczeństwa.

### Zakres usługi

Usługa obejmuje w szczególności:

1. **Zebranie danych i wstępny przegląd środowiska**:
   * Inwentaryzację urządzeń Barracuda CloudGen Firewall F400 objętych analizą (numery seryjne: 1559731, 1559727).
   * Zebranie informacji o aktualnie stosowanych politykach bezpieczeństwa, wersjach oprogramowania, aktywnych subskrypcjach i licencjach.
   * W przypadku wykrycia krytycznych luk bezpieczeństwa (pozwalającej na zdalne wykonanie kodu, przejęcie konta użytkownika, dostęp do urządzenia) podczas analizy Firewall, Wykonawca zobowiązany jest do ich niezwłocznego usunięcia w ramach realizacji zamówienia, po uzyskaniu zgody Zamawiającego.
2. **Analizę konfiguracji pod kątem**:
   * **Ochrony przed malware**:
     + Sprawdzenie aktywności i ustawień silnika antywirusowego.
     + Weryfikacja zakresu skanowania (ruch web, poczta, FTP, pliki).
     + Analiza harmonogramu i aktualności sygnatur.
   * **Wykorzystania mechanizmu sandbox (Advanced Threat Protection)**:
     + Sprawdzenie aktywności i konfiguracji sandboxingu.
     + Weryfikacja limitów, polityk przesyłania plików do analizy, raportowania wyników.
   * **Wykrywania i raportowania zagrożeń**:
     + Analiza ustawień systemów IDS/IPS.
     + Ocena skuteczności i kompletności raportowania wykrytych zagrożeń.
   * **Ochrony przed atakami sieci botnet**:
     + Weryfikacja aktywności mechanizmów DNS Sinkholing, Botnet Protection, blokowania złośliwych domen/IP.
     + Sprawdzenie polityk aktualizacji baz zagrożeń.
   * **Zgodności z dobrymi praktykami**:
     + Porównanie obecnej konfiguracji z zaleceniami producenta oraz uznanymi standardami bezpieczeństwa (np. CIS Benchmarks, zalecenia Barracuda Campus).
3. **Identyfikację luk i nieprawidłowości**:
   * Wskazanie obszarów, w których konfiguracja odbiega od dobrych praktyk lub nie zapewnia optymalnego poziomu ochrony.
   * Wskazanie potencjalnych zagrożeń wynikających z obecnych ustawień.
4. **Opracowanie raportu z analizy**:
   * Szczegółowy opis stanu obecnego (konfiguracja, polityki, aktywne moduły).
   * Wykaz wykrytych nieprawidłowości, luk lub obszarów wymagających poprawy.
   * Rekomendacje zmian lub usprawnień wraz z uzasadnieniem.
   * Wskazanie priorytetów wdrożenia rekomendacji (np. krytyczne, zalecane, opcjonalne).
   * Załączniki: zrzuty ekranu, przykładowe logi, tabele porównawcze.

### Terminy realizacji

1. Rozpoczęcie usługi: w ciągu 14 dni roboczych od potwierdzenia aktywacji subskrypcji o których mowa w 4.1.
2. Czas trwania analizy: do 14 dni roboczych od rozpoczęcia prac.
3. Przekazanie raportu z analizy: do 3 dni roboczych po zakończeniu analizy.
4. Wdrożenie poprawek krytycznych: niezwłocznie po uzyskaniu zgody Zamawiającego, nie później niż 3 dni robocze od zgłoszenia.
5. W przypadku wykrycia krytycznych luk bezpieczeństwa, których usunięcie wymaga dostarczenia poprawki przez producenta urządzenia istniejącej w dniu identyfikacji luki, Wykonawca zobowiązany jest do wdrożenia..
6. Nie jest zadaniem wykonawcy usunięcie krytycznych luk bezpieczeństwa, które wymagają zmian w urządzeniach lub serwisach innych niż te, dla których zostały aktywowane subskrypcje.

### Wymagania mierzalne

* Analiza musi objąć oba urządzenia Barracuda CloudGen Firewall F400 (numery seryjne: 1559731, 1559727).
* Raport z analizy – minimum 1 egzemplarz w wersji elektronicznej (PDF).
* Raport musi zawierać co najmniej:
  + opis stanu obecnego,
  + wykaz wykrytych nieprawidłowości/luk,
  + rekomendacje zmian,
  + priorytety wdrożenia,
  + załączniki dokumentujące analizę.

### Kryteria odbioru

1. Przekazanie Zamawiającemu kompletnego raportu z analizy w wersji elektronicznej.
2. Raport zawiera elementy określone w punkcie 4.4.3.
3. Pozytywna weryfikacja raportu przez Zamawiającego (możliwość zgłoszenia uwag w terminie 5 dni roboczych).
4. Podpisanie protokołu odbioru usługi analizy konfiguracji Firewall (wzór – 8.4).

# Wymagania techniczne

1. Oferowane subskrypcje nie mogą pochodzić z rynku wtórnego.
2. Oferowane subskrypcje muszą być przypisane do konkretnych numerów seryjnych urządzeń Zamawiającego.
3. Dostarczone rozwiązania muszą być w pełni kompatybilne z posiadanymi urządzeniami.
4. W przypadku rozwiązań równoważnych – muszą zapewniać minimum funkcjonalności i parametry określone w załączniku nr 1.

# Jakość, testy, odbiory, dokumentacja

1. Odbiór dostawy następuje na podstawie protokołu odbioru, po potwierdzeniu aktywacji licencji na urządzeniach Zamawiającego.
2. Odbiór usługi konfiguracji WAF następuje po zakończeniu okresu obserwacji, wdrożeniu zasad bezpieczeństwa i przekazaniu dokumentacji powdrożeniowej.
3. Wykonawca zobowiązany jest do przeprowadzenia testów aktywacji licencji oraz działania wsparcia technicznego.
4. Wzory protokołów odbioru znajdują się w załącznikach 2-4.

# Logistyka, dostawa, aktywacja, szkolenia

1. Dostawa subskrypcji odbywa się elektronicznie. Wykonawca zobowiązany jest do dostarczenia potwierdzenia aktywacji subskrypcji.
2. Aktywacja subskrypcji następuje w terminie do 5 dni roboczych od podpisania umowy
3. Prace wdrożeniowe i testy mogą być realizowane poza godzinami pracy urzędu lub w weekendy. Godziny pracy urzędu: poniedziałek–piątek 8:00–16:00.
4. Zamawiający dopuszcza możliwość czasowego wyłączenia chronionych serwisów podczas wdrożenia WAF wyłącznie w weekendy, po wcześniejszym uzgodnieniu z Zamawiającym.
5. Usługi wsparcia świadczone są zdalnie.
6. Zamawiający zapewni Wykonawcy zdalny dostęp do urządzeń Barracuda CloudGen Firewall F400 oraz Barracuda Web Application Firewall 660 na czas realizacji usługi konfiguracji i analizy.
7. Podczas prac konfiguracyjnych i analitycznych obecny będzie przedstawiciel Zamawiającego w celu konsultacji, akceptacji zmian i udziału w testach.
8. Szkolenie/instruktaż dla administratorów Zamawiającego odbywa się zdalnie. Termin szkolenia administratorów będzie ustalany indywidualnie pomiędzy Zamawiającym a Wykonawcą po zakończeniu wdrożenia.

# Załączniki

* **Załącznik nr 1:** Tabela funkcjonalności i parametrów minimalnych subskrypcji (do wypełnienia przez Zamawiającego na podstawie obecnych licencji).
* **Załącznik nr 2:** Wzór protokołu odbioru dostawy licencji.
* **Załącznik nr 3:** Wzór protokołu odbioru usługi konfiguracji WAF.
* **Załącznik nr 4:** Wzór protokołu odbioru usługi analizy Firewall.

## Załącznik nr 1 Tabela funkcjonalności i parametrów minimalnych licencji

|  |  |  |  |
| --- | --- | --- | --- |
| Lp. | Urządzenie / Licencja/subskrypcja | Opis zakresu | Warunki równoważności |
| 1 | **Barracuda CloudGen Firewall F400 – Energize Updates** | Aktualizacje sygnatur, firmware, wsparcie techniczne | - Aktualizacje sygnatur IPS/IDS co najmniej raz na dobę;  - Wsparcie techniczne 24/7 przez e-mail, telefon w dni robocze; |
| 2 | **Barracuda CloudGen Firewall F400 – Instant Replacement** | Wymiana sprzętu w razie awarii | - Wysyłka urządzenia zamiennego w ciągu następnego dnia roboczego (Next Business Day Shipping);  - Wsparcie techniczne 24/7;  - wymiana sprzętu na nowy model po 4 latach w przypadku nieprzerwanego posiadania tej licencji |
| 3 | **Barracuda CloudGen Firewall F400 – Malware Protection** | Ochrona przed złośliwym oprogramowaniem | - Skanowanie ruchu HTTP/HTTPS, SMTP, POP3, FTP;  - Wykorzystanie co najmniej jednego silnika antywirusowego;  - Automatyczne aktualizacje sygnatur;  - Brak ograniczenia liczby skanowanych plików;  - Możliwość inspekcji SSL |
| 4 | **Barracuda CloudGen Firewall F400 – Advanced Threat Protection** | Ochrona przed zaawansowanymi zagrożeniami (zero-day, ransomware) | - Dynamiczna analiza plików w sandboxie (CPU-emulation-based);  - Wykrywanie exploitów i zagrożeń zero-day;  - Limit przesyłania plików: min. 15 plików/min, 324 000 plików/miesiąc;  - Raportowanie forensic analysis;  - DNS Sinkholing, Botnet Protection |
| 5 | **Barracuda CloudGen Firewall F400 – Advanced Remote Access** | Zaawansowany zdalny dostęp VPN | - SSL VPN z portalem webowym;  - Multi-Factor Authentication (TOTP);  - Integracja z AD FS/SAML, Azure AD;  - NAC (kontrola dostępu do sieci);  - Nieograniczona liczba jednoczesnych sesji;  - Obsługa zdalnego zarządzania dla Windows. |
| 6 | **Barracuda Web Application Firewall 660 – Advanced Bot Protection License** | Ochrona przed atakami botów | - Machine Learning Based Bot Detection;  - Credential Stuffing/Spraying Protection;  - Account Takeover Protection;  - Web & Price Scraping Protection;  - Crowd-Sourced Bot Detection;  - Dynamic Risk Score Management;  - Auto-Configuration Engine |
| 7 | **Barracuda Web Application Firewall 660 – Active DDoS Prevention** | Ochrona przed atakami DDoS | - Cloud Scrubbing Centers (geograficznie rozproszone);  - Ochrona przed UDP/ICMP floods, DNS amplification, HTTP GET/POST floods;  - SLA dostępności Cloud Scrubbing min. 99,99%;  - Heuristic Fingerprinting;  - IP Reputation Integration;  - Minimalne opóźnienie <50 ms |
| 8 | **Barracuda Web Application Firewall 660 – Advanced Threat Protection** | Ochrona przed zaawansowanymi zagrożeniami | - Multi-Layer Threat Detection (co najmniej 4 warstwy);  - Cloud-Based CPU-Emulation Sandbox;  - Full-System Emulation;  - Zero-Day Malware Detection;  - File Upload Security;  - Forensic Analysis Reports;  - GDPR-Compliant Cloud Processing |
| 9 | **Barracuda Web Application Firewall 660 – Energize Updates** | Aktualizacje sygnatur, firmware, wsparcie techniczne | - Aktualizacje sygnatur co najmniej raz na dobę;  - Aktualizacje firmware co najmniej raz na kwartał;  - Wsparcie techniczne 24/7 przez e-mail, telefon w dni robocze;  - Przypisanie do konkretnego numeru seryjnego urządzenia; |
| 10 | **Barracuda Web Application Firewall 660 – Instant Replacement** | Wymiana sprzętu w razie awarii | - Wysyłka urządzenia zamiennego w ciągu następnego dnia roboczego;  - Wsparcie techniczne 24/7;  - wymiana sprzętu na nowy model po 4 latach w przypadku nieprzerwanego posiadania tej licencji; - Przypisanie do konkretnego numeru seryjnego urządzenia |

**Wyjaśnienia do tabeli:**

* + **Parametry minimalne** należy rozumieć jako wymagania, które muszą być spełnione przez każdą oferowaną licencję/subskrypcję.
  + **Przypisanie do SN** oznacza, że licencja/subskrypcja musi być aktywowana i przypisana do konkretnego numeru seryjnego urządzenia Zamawiającego.

## Załącznik nr 2: Wzór protokołu odbioru dostawy

**PROTOKÓŁ ODBIORU DOSTAWY**

Data sporządzenia: …………………………… Miejsce sporządzenia: ……………………………

1. Zamawiający: ……………………………………………………………………………………
2. Wykonawca: ……………………………………………………………………………………
3. Przedmiot odbioru: ……. zgodnie z Umową nr ………………… z dnia ………………… .
4. Szczegóły dostawy:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Lp. | Urządzenie | Numer seryjny | Nazwa licencji/subskrypcji | Okres ważności | Data aktywacji | Uwagi |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |

5. Potwierdzenie aktywacji:

* Licencje zostały aktywowane na wskazanych urządzeniach.
* Zamawiający potwierdza dostępność funkcjonalności zgodnie z OPZ.

6. Uwagi:

…………………………………………………………………………………………………………………………

7. Oświadczenia stron:

* Zamawiający potwierdza odbiór dostawy bez zastrzeżeń / z następującymi zastrzeżeniami: ………………………………………
* Wykonawca zobowiązuje się do usunięcia wskazanych zastrzeżeń w terminie ………………… .

Podpisy:

Zamawiający: ……………………………………… Wykonawca: ………………………………………

## Załącznik nr 3: Wzór protokołu odbioru usługi konfiguracji WAF

**PROTOKÓŁ ODBIORU USŁUGI KONFIGURACJI WAF**

Data sporządzenia: …………………………… Miejsce sporządzenia: ……………………………

1. Zamawiający: ……………………………………………………………………………………
2. Wykonawca: ……………………………………………………………………………………
3. Przedmiot odbioru: Usługa konfiguracji Barracuda Web Application Firewall 660 dla serwisów Zamawiającego zgodnie z Umową nr ………………… z dnia ………………… .
4. Zakres wykonanych prac:

* Konfiguracja ochrony dla serwisów: [wymienić serwisy]
* Integracja z SIEM: TAK/NIE
* Okres obserwacji (monitoring/learning mode): ……… dni
* Optymalizacja polityk bezpieczeństwa: TAK/NIE
* Przeprowadzenie symulacji ataków: TAK/NIE
* Przekazanie dokumentacji powykonawczej: TAK/NIE
* Przeprowadzenie szkolenia administratorów: TAK/NIE Data szkolenia: ………………… Liczba uczestników: ………………… Lista obecności w załączeniu: TAK/NIE

5. Uwagi:

…………………………………………………………………………………………………………………………

6. Oświadczenia stron:

* Zamawiający potwierdza odbiór usługi bez zastrzeżeń / z następującymi zastrzeżeniami: ………………………………………
* Wykonawca zobowiązuje się do usunięcia wskazanych zastrzeżeń w terminie ………………… .

Podpisy:

Zamawiający: ……………………………………… Wykonawca: ………………………………………

## Załącznik nr 4: Wzór protokołu odbioru usługi analizy Firewall

**PROTOKÓŁ ODBIORU USŁUGI ANALIZY KONFIGURACJI FIREWALL**

Data sporządzenia: …………………………… Miejsce sporządzenia: ……………………………

1. Zamawiający: ……………………………………………………………………………………
2. Wykonawca: ……………………………………………………………………………………
3. Przedmiot odbioru: Usługa analizy konfiguracji Barracuda CloudGen Firewall zgodnie z Umową nr ………………… z dnia ………………… .
4. Zakres wykonanych prac:

* Inwentaryzacja urządzeń: TAK/NIE
* Analiza polityk bezpieczeństwa: TAK/NIE
* Analiza ochrony przed malware, botnet, sandbox: TAK/NIE
* Integracja z SIEM: TAK/NIE
* Wdrożenie poprawek krytycznych: TAK/NIE
* Przekazanie raportu z analizy: TAK/NIE Data przekazania: …………………

5. Uwagi:

…………………………………………………………………………………………………………………………

6. Oświadczenia stron:

* Zamawiający potwierdza odbiór usługi bez zastrzeżeń / z następującymi zastrzeżeniami: ………………………………………
* Wykonawca zobowiązuje się do usunięcia wskazanych zastrzeżeń w terminie ………………… .

Podpisy:

Zamawiający: ……………………………………… Wykonawca: ………………………………………

1. <https://owasp.org/Top10/> [↑](#footnote-ref-1)