**Załącznik nr 1e do SWZ**

**Opis Przedmiotu Zamówienia**

**„Oprogramowanie Web Filtering, Antispam, IoT Detection, Industrial Security, Security Rating do UTM”.**

1. Przedmiotem zamówienia jest dostawa licencji na dodatkowe funkcjonalności, serwis i wsparcie techniczne dla urządzenia UTM Fortigate 80F-POE na minimalny okres do 12.03.2026 r.

Wydłużenie okresu licencji stanowi kryterium oceny ofert.

Model posiadanego urządzenia UTM: FortiGate 80F-PoE

Data ważności aktualnie posiadanej licencji UTP: 2025-11-15

**Wymagania dla licencji:**

* W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Kontrola Aplikacji, IPS, Antywirus, Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

* Aktualizacje oprogramowania i całodobowe wsparcie techniczne w trybie 24x7
* Ochrona przed zagrożeniami typu zero-day
* Zaawansowana analiza zagrożeń w chmurze
* Kontrola aplikacji i filtrowanie treści
* Ochrona przed złośliwym oprogramowaniem i atakami
* Raportowanie i zarządzanie w chmurze

Minimalne lub równoważne funkcje oprogramowania:

* **Antyspam**Zatrzymywanie niechcianej korespondencji i eliminacja ryzyka dotarcia za jej pośrednictwem do niebezpiecznych treści.
* **Antivirus**  
  Chroni przed najnowszymi wirusami, oprogramowaniem szpiegującym i innymi zagrożeniami. Wykorzystuje wiodące w branży zaawansowane silniki wykrywania, aby zapobiec przedostawaniu się nowych i ewoluujących zagrożeń do sieci i uzyskiwaniu dostępu do jej bezcennej zawartości.
* **Intrusion Prevention**  
  Aby zidentyfikować zagrożenia, IPS analizuje pakiety danych, szukając wzorców, o których wiadomo, że istnieją w zagrożeniach. Po rozpoznaniu jednego z tych wzorców IPS zatrzymuje atak. W niektórych przypadkach system IPS wykryje jedynie niebezpieczny pakiet danych, a zespół IT może następnie wybrać, w jaki sposób chce zaradzić zagrożeniu. Kroki podjęte w celu powstrzymania ataku mogą być zautomatyzowane lub wykonane ręcznie. UTM zarejestruje również złośliwe zdarzenie. Dzienniki te mogą być następnie analizowane i wykorzystywane do zapobiegania innym atakom w przyszłości.
* **Web Filtering**  
  Funkcja filtrowania sieci UTM może uniemożliwić użytkownikom oglądanie określonych witryn internetowych lub adresów URL (Uniform Resource Locator). Odbywa się to poprzez zatrzymanie przeglądarek użytkowników przed ładowaniem stron z tych witryn na ich urządzenie. Możesz skonfigurować filtry internetowe, aby kierować reklamy na określone witryny zgodnie z celami Twojej organizacji.
* **Anti-malware**  
  UTM można wstępnie skonfigurować w celu wykrywania znanego złośliwego oprogramowania, filtrowania go ze strumieni danych i blokowania przed penetracją systemu. UTM można również skonfigurować do wykrywania nowych zagrożeń złośliwym oprogramowaniem za pomocą analizy heurystycznej, która obejmuje reguły analizujące zachowanie i cechy plików.
* **IP Reputation & Anti-botnet Security**  
  Usługa agreguje dane dotyczące szkodliwego źródła IP z rozproszonej sieci obejmującej czujniki zagrożeń, zespoły CERT, MITRE, kooperacyjną konkurencję i inne globalne źródła, które współpracują w celu dostarczania aktualnych informacji o zagrożeniach dotyczących wrogich źródeł.
* **Sandbox Cloud**  
  Zaawansowane rozwiązanie do wykrywania zagrożeń, które przeprowadza dynamiczną analizę w celu zidentyfikowania nieznanego wcześniej złośliwego oprogramowania.