*Załącznik nr 1 do Zapytania ofertowego*

**Opis Przedmiotu Zamówienia**

Dostawa zapory sieciowej typu UTM wraz z licencjami i usługami wsparcia technicznego na okres 36 miesięcy na potrzeby Urzędu Miasta Ostrowca Świętokrzyskiego

I. Warunki uczestnictwa w postępowaniu:

1. Na realizację części zamówienia będzie zawierana umowa..
2. Oferowany sprzęt ma być fabrycznie nowy, nieużywany oraz nieeksponowany na wystawach lub imprezach targowych, sprawny technicznie, bezpieczny, kompletny i gotowy do pracy, musi spełniać wymagania techniczno-funkcjonalne wyszczególnione w poniższym Opisie Przedmiotu Zamówienia.
3. W ramach przedmiotowego zamówienia, Zamawiający wymaga dostarczenia sprzętu i licencji, którego parametry minimalne wskazane zostały poniżej. Zamawiający akceptuje sprzęt oraz akcesoria o wyższych (lepszych) parametrach użytkowych lub wykonany w nowszej technologii pod warunkiem, że produkty zaoferowane przez Wykonawcę spełniają wszystkie parametry minimalne.
4. Wykonawca w swej ofercie zawrze wszelkie koszty związane z dostarczeniem przedmiotu zamówienia danej części.
5. Oferta Wykonawcy musi obejmować pełny określony zakres przedmiotu zamówienia.
6. Wszystkie oferowane produkty mają pochodzić z oficjalnego kanału dystrybucyjnego producenta, posiadać wszystkie wymagane certyfikaty i oznaczenia oraz spełniać wszystkie wymagane prawem normy.
7. Wykonawca dostarczy Wykonawcy kartę katalogową producenta sprzętu i oprogramowania lub link do specyfikacji technicznej producenta oferowanego sprzętu i oprogramowania.

II. Wymagane parametry urządzenia:

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Nazwa parametru** | **Wymagania minimalne zapory sieciowej typu UTM** | **Dane techniczne oferowanego urządzenia**  \*niepotrzebne skreślić |
| 1 | **Ofertowany produkt** | W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta | Proszę podać  (producent, model)  ………………….........................………………….........................  ………………….........................………………….........................  ………………….........................…………………......................... |
| 2 | **Przepustowość zapory sieciowej** | Min.27 Gbit/s | TAK\* NIE\* |
| 3 | **Przepustowość VPN** | Min. 2 Gbit/s | TAK\* NIE\* |
| 4 | **Przepustowość IPS/IDS** | Min. 5000 Mbit/s | TAK\* NIE\* |
| 5 | **Liczba wirtualnych zapór ogniowych** | Min. 10 | TAK\* NIE\* |
| 6 | **Lliczba połączeń zapory Firewall** | Min. 3000000 | TAK\* NIE\* |
| 7 | **Liczba połączeń zapory Firewall na sekundę** | Min. 280000 | TAK\* NIE\* |
| 8 | **Opóźnienie firewalla** | Max. 4,78 µs | TAK\* NIE\* |
| 9 | **Szyfrowanie / bezpieczeństwo** | Min. 256-bit AES, SHA-256 | TAK\* NIE\* |
| 10 | **Diody LED** | TAK | TAK\* NIE\* |
| 11 | **Liczba portów USB 2.0** | Min. 1 | TAK\* NIE\* |
| 12 | Ilość portów Ethernet LAN (RJ-45) | Min. 16 | TAK\* NIE\* |
| 13 | Port konsoli | RJ-45 | TAK\* NIE\* |
| 14 | Prędkość transferu danych przez Ethernet LAN | Min. 1000 Mbit/s | TAK\* NIE\* |
| 15 | Liczba portów konsoli | Min. 1 | TAK\* NIE\* |
| 16 | **Liczba zainstalowanych modułów SFP+** | Min. 4 | TAK\* NIE\* |
| 17 | **Ilość slotów Modułu SFP+** | Min. 4 | TAK\* NIE\* |
| 18 | **Możliwości montowania w stelażu** | Tak | TAK\* NIE\* |
| 19 | **Układ** | Max. 1U | TAK\* NIE\* |
| 20 | **Częstotliwość wejściowa AC** | 50 - 60 Hz | TAK\* NIE\* |
| 21 | **Zakres temperatur (eksploatacja)** | Min. 0 - 40 °C | TAK\* NIE\* |
| 22 | **Szerokość produktu** | Max. 435 mm | TAK\* NIE\* |
| 23 | **Głębokość produktu** | Max .345 mm | TAK\* NIE\* |
| 24 | **Wysokość produkt** | Max. 45 mm | TAK\* NIE\* |
| 25 | **Przepustowość VPN** | Min. 2000 Mbit/s | TAK\* NIE\* |
| 26 | **Przepustowość Firewall** | Min. 27000 Mbit/s | TAK\* NIE\* |
| 27 | **Antywirus** | zaawansowana technologia zapewniająca bezpieczeństwo sieci przed infekcjami, pozwalająca m.in. na analizę sygnaturową czy behawioralną zagrożeń | TAK\* NIE\* |
| 28 | **Moduły antyspyware i antymalware** | ochrona sieci przed szpiegującym i szkodliwym oprogramowaniem | TAK\* NIE\* |
| 29 | **Zapora sieciowa** | zabezpieczanie sieci organizacji przed niepowołanym dostępem | TAK\* NIE\* |
| 30 | **VPN** | możliwość budowania wirtualnych sieci prywatnych | TAK\* NIE\* |
| 31 | **Ochrona przed włamaniami** | moduł IPS (Intrusion Prevention System) wykrywający i blokujący tego rodzaju działania w czasie rzeczywistym | TAK\* NIE\* |
| 32 | **Kontroler firmowej sieci bezprzewodowej** | nadzoruje wykorzystywanie aplikacji biznesowych oraz przestrzeganie poziomów dostępu przez użytkowników | TAK\* NIE\* |
| 33 | **Kontrola aplikacji** | umożliwia analizę aplikacji używanych na poszczególnych urządzeniach końcowych, w razie potrzeby blokując instalację/użycie niebezpiecznego oprogramowania | TAK\* NIE\* |
| 34 | **Ochrona sieci przed wyciekami informacji** | odpowiedni moduł monitorujący przepływ danych o szczególnym (poufnym) znaczeniu dla działalności organizacji | TAK\* NIE\* |
| 35 | **Obsługa IPv6** | rozwiązania w pełni przystosowane również do pracy z najnowszą pulą adresów | TAK\* NIE\* |
| 36 | **Filtrowanie sieci (web filtering)** | narzędzia ograniczające korzystanie z Internetu, mające na celu m.in. zwiększenie produktywności pracowników i utrzymanie przepustowości łącza | TAK\* NIE\* |
| 37 | **Atyspam** | zatrzymywanie niechcianej korespondencji i eliminacja ryzyka dotarcia za jej pośrednictwem do niebezpiecznych treści | TAK\* NIE\* |
| 38 | **System ochrony IPS** | najważniejszy element utm-a, czyli sygnatury ataków stricte sieciowych i wzorce towarzyszących im anomalii, dodatkowo konfigurowalny o polityki i sensory. | TAK\* NIE\* |
| 39 | **Ilość zamontowanych zasilaczy** | Min. 2 | TAK\* NIE\* |
| 40 | Gwarancja | Min. 36 miesięcy | Proszę podać ilość m-cy  **……………………………** |

III. Usługi wsparcia technicznego:

1. Świadczone będą na podstawie wykupionego wsparcia producenta urządzenia wymienionego w tabeli w pkt 1. Obsługa zgłoszeń w okresie wykupionej usługi wsparcia technicznego producenta będzie świadczona w języku polskim.

2. Są dostępne 24 godziny na dobę, 7 dni w tygodniu, przez okres 3 lat.

3. Gwarantują reakcję w ciągu 1 godziny w przypadku problemów krytycznych i w następnym dniu roboczym w sprawach niekrytycznych.

4. Obejmują usługę urządzenia zastępczego w razie awarii.

5. Zapewniają kompleksową gamę funkcji zabezpieczeń w celu ochrony: aplikacji, treści, urządzeń, sieci i Internetu;

6. Obejmują podstawowe elementy zabezpieczeń:

- **Bezpieczeństwo sieci i plików:** obejmuje IPS, który zapewnia monitorowanie ruchu sieciowego, analizę pod kątem złośliwej zawartości i AI/ML do wykrywania zagrożeń w czasie rzeczywistym za pomocą wirtualnego łatania, podczas gdy oprogramowanie antymalware daje gwarancję ochrony w czasie rzeczywistym przed wszystkimi zagrożeniami, zwiększa ochronę poprzez analizę zagrożeń, i zapewnia wielowarstwowe bezpieczeństwo. Kontrola aplikacji natomiast zwiększa zgodność z wymogami bezpieczeństwa i zapewnia widoczność aplikacji w czasie rzeczywistym.

- **Bezpieczeństwo Web/DNS**: obejmuje funkcję Web Filtering, która zatrzymuje zagrożenia internetowe, blokuje złośliwe witryny i treści oraz sprawdza łącza e-mail pod kątem potencjalnych zagrożeń. Reputacja IP i antybotnet zapobiegają komunikacji botnetów, blokują ataki DDoS ze znanych źródeł i oferują funkcję „ustaw i zapomnij”. Bezpieczeństwo DNS chroni przed atakami DNS, szyfruje ruch w celu zapewnienia prywatności użytkowników i zapewnia niezawodność dzięki filtrowaniu FortiGuard. Dodatkowo obejmuje DNSSEC, blokowanie tunelowania DNS, ochronę przed atakami typu Flood DNS i chroni przed atakami DoS/DDoS.

- **SaaS i bezpieczeństwo danych**: obejmuje technologię DLP, która zapewnia widoczność i ochronę danych w sieciach i chmurach, a także użytkowników. Upraszcza to wdrażanie zgodności i prywatności, podczas gdy CASB chroni dane w ruchu i w spoczynku, egzekwuje główne standardy zgodności i zarządza zagrożeniami dla kont i użytkowników oraz wykorzystaniem aplikacji w chmurze. Usługa Attack Surface Security zapewnia oceny bezpieczeństwa i zgodności oraz oceny ryzyka, a także wykrywa i klasyfikuje urządzenia IoT oraz koryguje ich słabe punkty.

- **Zapobieganie zagrożeniom Zero-Day:** oferuje wbudowaną ochronę przed złośliwym oprogramowaniem w celu analizowania i filtrowania nieznanych plików w czasie rzeczywistym, zapewniając subsekundową ochronę przed zagrożeniami typu Zero-Day we wszystkich NGFW.

- **Zabezpieczenie powierzchni ataku:** wykrywanie urządzeń IoT, korelacja podatności w zabezpieczeniach IoT, ocena bezpieczeństwa, kontrola naruszeń.

- **Data Loss Prevention**