**Załącznik nr 2b do SWZ**

**Opis zaoferowanego sprzętu**

**Część 2 - Dostawa urządzenia UTM oraz migracja danych ze starego urządzenia na nowe**

|  |  |
| --- | --- |
| Nazwa |  |
| Liczba obsługiwanych komputerów w sieci |  |
| Przepustowość Firewall |  |
| Przepustowość IPS |  |
| Przepustowość Antywirusa |  |
| Obsługa jednoczesnych połączeń sieciowych |  |
| Ilość nowych sesji na sekundę |  |
| Przepustowość IPSec VPN  |  |
| Przepustowość IPSec (AES256/SHA2) |  |
| Liczba tuneli IPSec VPN |  |
| Liczba SSL VPN |  |
| Liczba jednoczesnych klientów SSL VPN |  |
| Dedykowane oprogramowanie klienckie VPN |  |
| VPN Server |  |
| Wsparcie dla IKE v1 oraz v2 |  |
| Wsparcie VLAN w oparciu o standard 802.1Q |  |
| Ilość sieci VLAN |  |
| Firewall klasy Stateful Inspection |  |
| Instrusion Prevention System (IPS) |  |
| Intrusion Detection System (IDS) |  |
| Zarządzanie pasmem (QoS) |  |
| Kontrola aplikacji |  |
| Skaner antywirusowy (HTTP, POP3, SMTP, FTP, SSL) |  |
| Moduł antyspam |  |
| Filtrowanie stron WWW (HTTP, HTTPS) |  |
| Wsparcie protokołów |  |
| High Availability (Active/Passive) |  |
| Interfejsy sieciowe |  |
| Administracja urządzenia |  |
| Podręczniki |  |
| Dwuskładnikowe uwierzytelnianie |  |
| Pamięć wewnętrzna |  |
| Wielkość pamięci lokalnej |  |
| Monitorowanie w czasie rzeczywistym |  |
| Logowanie zdarzeń |  |
| Tworzenie raportów |  |
| Automatyczna aktualizacja plików sygnatur antywirusowych |  |
| Automatyczna aktualizacja sygnatur IPS |  |
| Wydzielone strefy bezpieczeństwa (np. DMZ) |  |
| Rozszerzenie funkcjonalności |  |
| Gwarancja |  |
| Serwis |  |
| Wdrożenie |  |
| Wsparcie techniczne |  |
| Przeniesienie konfiguracji z obecnego urządzenia |  |
| Certyfikaty europejskie (Certyfikacja NATO, Certyfikacja EU Restricted) |  |
| Wymagane certyfikaty |  |