Załącznik nr 1

Opis Przedmiotu Zamówienia
„Przedłużenie licencji dla urządzeń Sophos”

1. **Przedmiot Zamówienia**

Przedłużenie licencji na 3 lata dla urządzeń i specyfikacji:

* 2 urządzenia Sophos XB2133SEU SN:GP/9778/S/2019 (licencja Total Protect 3-letnia (EU power cord) działające w trybie active – passive),
* 2 urządzenia Sophos XB8B3CSEK SN:GP/9778/S/2019 (licencja Total Protect 3-letnia (EU/UK/US power cord)),
1. **Minimalny zakres techniczny licencji :**
	1. Network Protection - Podstawowy moduł sieciowy UTM, który odpowiada za zaawansowaną konfigurację routingu, firewall, VPN, DHCP, NAT, zarządzania logami i raportami.
	2. konfigurowanie wszystkich ustawień systemowych poprzez interfejs webowy bez potrzeby korzystania z linii poleceń czy zewnętrznych narzędzi do zarządzania.
	3. możliwość śledzenia wszystkich zmian w konfiguracji.
	4. implementacja technologii typu intrusion prevention filtruje ponad 11 000 ataków i zagrożeń typu „zero-day”.
	5. możliwość przeglądania wielu raportów i wykresów, które pokazują aktywność w sieci dla zdefiniowanych przedziałów czasowych, użytkowników i grup.
	6. możliwość wykorzystania SSL, IPsec, L2TP lub PPTP.
	7. Zapewniać ochronne przed atakami: DoS, DDoS i skanowaniem portów.
	8. VPN site-to-site: SSL, IPsec, AES-256/3DES-256 bitów, PFS, RSA, certyfikaty X.509, pre-shared key.
	9. Zdalny dostęp: SSL, IPsec, wsparcie dla iPhone/iPad/klienta Cisco VPN.
	10. Dostęp do portalu oparty na HTML5 nie wymaga SSH, dodatkowych wtyczek lub kontrolek ActiveX do zdalnych sesji.
	11. Śledzenie połączeń: FTP, IRC, PPTP, TFTP.
	12. Reguły i konfiguracja z oparciu o tożsamość użytkowników z wykorzystaniem Sophos Authentication Agent.
	13. Routing: statyczny, OSPF, BGP, Multicast (PIM-SM).
	14. Link-balancing dla interfejsu WAN w dowolnej kombinacji portów 3G/UMTS/Ethernet: 32 połączenia internetowe, sprawdzanie stanu łącza, błyskawiczne przełączanie w przypadku awarii, automatyczne i ważone równoważenie łącza.
	15. Bezobsługowy klaster active/passive high availability.
	16. Logowanie: zdalny syslog, rotacja logów w nocy, archiwizacja logów: email/FTP/SMB/SSH.
	17. Raportowanie: filtr pakietów, zapobieganie włamaniom (IPS), przepustowość, zakres czasu dzień/tydzień/miesiąc/ rok, anonimowe raporty.
	18. Raporty w oparciu o tożsamość użytkowników.
	19. Eksport raportów do PDF lub CSV.
	20. Planowanie i archiwizacja raportów.
	21. Wsparcie dla: Active Directory, eDirectory.
	22. Single sign on: Active Directory, eDirectory Wsparcie dla SSL.
	23. Narzędzia: sprawdzanie ustawień serwera, testowanie loginów/haseł, czyszczenie cache.
	24. Graficzna przeglądarka dla użytkowników i grup.
	25. Automatyczne tworzenie użytkowników.
	26. Planowane synchronizacje urządzeń back-end.
	27. Web Protection - Moduł do kreowania polityk bezpieczeństwa i dostępu do stron www.
	28. Możliwość blokowania stron niewłaściwych.
	29. Blokowanie wysyłania informacji poufnych w tle z już zainfekowanych komputerów.
	30. Możliwość tworzenia raportów z zachowaniem anonimowości użytkowników, by przestrzegać prawa do ochrony prywatności.
	31. Wsparcie dla oddzielnie filtrujących proxy w różnych trybach.
	32. Możliwość powielania profili bezpieczeństwa.
	33. Możliwość tworzenia komunikatów dla użytkowników w różnych językach.
	34. Możliwość umieszczenia firmowego logo na zablokowanych stronach.
	35. Ograniczanie dostępu do YouTube z wykorzystaniem zintegrowanej funkcji YouTube for Schools.
	36. Widoczność ruchu w czasie rzeczywistym z możliwością blokowania lub ograniczenia pasma.
	37. Email Protection - Filtr antyspamowy i antywirusowy dla serwerów poczty, możliwość szyfrowania wiadomości i załączników, możliwość kreowania polityk bezpiecznego oraz ograniczonego dostępu do wysyłanych wiadomości, panel administracyjny z kwarantanną dla użytkowników.
	38. Filtr antyspamowy - Doskonale identyfikuje wiadomości typu spam niezależnie od użytego w nich języka czy treści, używając wielu różnych metod wykrywania niechcianej poczty.
	39. Ochrona przed malware - Blokada wirusów, wyłudzanie danych poprzez podszywanie się pod inne organizacje oraz niechcianą korespondencję używając dwóch komercyjnych silników antywirusowych, sprawdzania typów MIME oraz filtrów rozszerzeń.
	40. Globalne czarne- i białe listy dla domen i adresów.