Załącznik nr 3 B do SIWZ

Warunki techniczne - część druga zamówienia

Urządzenie zabezpieczające UTM – 1 sztuka

Lp.	Nazwa komponentu	Wymagane minimalne, parametry techniczne
1.	Funkcje i parametry pracy	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym. 5. System realizujący funkcję Firewall powinien dysponować minimum 7 portami Ethernet 10/100/1000 Base-TX 6. System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 7. W zakresie Firewall'a obsługa nie mniej niż 1,5 mln. jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę 8. Przepustowość Firewall'a: nie mniej niż 2 Gbps 9. Wydajność szyfrowania VPN IPSec: nie mniej niż 180 Mbps 10. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej. 11. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń. 12. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych: • Kontrola dostępu - zapora ogniowa klasy Stateful Inspection • Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS • Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN • Ochrona przed atakami - Intrusion Prevention System • Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM. • Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP • Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości

		pasma • Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów) • Możliwość analizy ruchu szyfrowanego protokołem SSL • Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) 13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 700 Mbps 14. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 160 Mbps 15. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż: • Tworzenie połączeń w topologii Site-to-site oraz Client-to-site • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Praca w topologii Hub and Spoke oraz Mesh • Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth 16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. 17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. 18. Translacja adresów NAT adresu źródłowego i docelowego. 19. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci. 20. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ 21. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR. 22. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. 23. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP 24. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW. 25. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL. 26. System zabezpieczeń musi umożliwiać weryfikację tożsamości użytkowników za pomocą nie mniej niż:

		• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu • haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych • Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory 27. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty: • ICSA lub EAL4 dla funkcji Firewall • ICSA lub NSS Labs dla funkcji IPS • ICSA dla funkcji: SSL VPN, IPSec VPN 28. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
2.	Serwisy i licencje	Wykonawca, którego oferta zostanie wybrana, zobowiązany jest do dostarczenia licencji aktywacyjnych dla wszystkich wymaganych funkcji ochronnych, upoważniających do pobierania aktualizacji baz zabezpieczeń przez okres 1 roku.
3.	Gwarancja i certyfikaty	Urządzenie powinno być objęte serwisem gwarancyjnym producenta lub Autoryzowanego Partnera Serwisowego przez okres 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Wykonawca winien w Załączniku nr 5 B do SIWZ złożyć oświadczenie, w którym potwierdzi wymagany serwis gwarancyjny (podając numer modułu internetowego i infolinii telefonicznej producenta lub Autoryzowanego Partnera Serwisowego) na terenie Rzeczpospolitej Polskiej. Podmiot serwisujący winien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5. **Oświadczenie Wykonawcy w Załączniku nr 5 B do SIWZ.**
4.	Dodatkowo	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.