Załącznik nr 2 cz. III_do IPU

Wymagania techniczno – funkcjonalne dotyczące kompleksowego systemu zabezpieczeń struktur sieciowych – Specyfikacja techniczno-funkcjonalna urządzenia bezpieczeństwa

Lp.	Parametr	Wymagania techniczne
1.	Architektura systemu ochrony	System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania. Dlatego, główne urządzenie ochronne [gateway] nie może posiadać twardego dysku, w zamian używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu układu sprzętowo – programowego procesora. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli Zamawiającemu licencji bez limitu chronionych użytkowników (licencja na urządzenie w tym licencje na oprogramowanie). Uwaga: Dziennik zdarzeń lub inne działania wymagające systemów dyskowych muszą być realizowane na dedykowanych do tego celu urządzeniach.
2.	System operacyjny	Urządzenie musi być sterowane przez opracowany przez producenta zabezpieczeń dedykowany system operacyjny czasu rzeczywistego (tzn. nie powinien to być zmodyfikowany system operacyjny ogólnego przeznaczenia jak Linux, czy FreeBSD). Funkcjonowanie zabezpieczeń musi być wspomagane sprzętowo za pomocą specjalizowanych układów scalonych (np. ASIC). Nie dopuszcza się stosowania komercyjnych systemów operacyjnych ogólnego przeznaczenia.
3.	Ilość/rodzaj portów	Nie mniej niż **4 porty Ethernet 10/100** oraz min **2 porty elektryczne Ethernet 10/100/1000.** Nie mniej niż **8 interfejsów wirtualnych** definiowanych jako VLANy w oparciu o standard IEEE802.1q
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę ogniową klasy Stateful Inspection • ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM) • poufność danych - IPSec VPN oraz SSL VPN • ochronę przed atakami - Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających: • kontrolę pasma oraz ruchu [QoS i Traffic shaping] • kontrolę komunikatorów sieciowych (IM) oraz aplikacji P2P
5.	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: • jako router/NAT (3.warastwa ISO-OSI) • jako most /transparent bridge Tryb pracy zabezpieczeń ustalany winien być w konfiguracji.
6.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).
7.	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. • Nie mniej niż 2100 sygnatur ataków. • Aktualizacja bazy sygnatur musi odbywać się na żądanie, bądź zgodnie z zaprogramowanym harmonogramem. Sposób aktualizacji bazy sygnatur ma być ustalany w konfiguracji. Aktualizacja ma być wykonywana przez Wykonawcę w sposób ciągły. • Możliwość wykrywania anomalii protokołów i ruchu
8.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT.
9.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu co najmniej 5 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu. Urządzenie może wykonywać routing IP na bazie adresu przeznaczenia pakietów oraz adresu źródłowego. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.
10.	Połączenia VPN	Wymagane nie mniej niż: • Tworzenie połączeń w topologii Meshed Site-to-site VPN • Tworzenie połączeń w topologii Hub-Spoke Site-to-site VPN • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Konfiguracja w oparciu o politykę bezpieczeństwa (Policy-based VPN) • Obsługa IPSec NAT Traversal dla konfiguracji VPN Client-to-site oraz Site-to-site • Interface based VPN umożliwiający rozgłaszanie tunelu przez dynamiczne protokoły routingu
11.	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: • haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia • haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych
12.	Infrastruktura klucza publicznego	Urządzenie musi współpracować z wiodącymi urzędami certyfikacji, nie mniej niż: • Verisign • Entrust • Microsoft • wspierać standardy PKI (PKCS 7, PKCS 10)
13.	Wydajność	Przepływność firewalla nie mniejsza niż **400 Mbps** w tym obsługa nie mniej niż 100 000 jednoczesnych połączeń Przepływność nie mniejsza niż **200 Mbps** dla VPN (3DES). Obsługa nie mniej niż 1000 jednoczesnych tuneli VPN
14.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive
15.	Obudowa	Obudowa ma mieć możliwość zamontowania w szafie 19”.

Wymagania techniczno – funkcjonalne dotyczące kompleksowego systemu zabezpieczeń struktur sieciowych – Specyfikacja techniczno-funkcjonalna urządzenia bezpieczeństwa

Lp.	Parametr	Wymagania techniczne
16.	Zasilania i wentylacja	Zasilanie z sieci 230V/50Hz.
17.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: • haseł statycznych • haseł dynamicznych (RADIUS,) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla systemu urządzenie powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
18.	Certyfikaty	System lub jego funkcje ochronne muszą posiadać minimum certyfikaty: EAL4+, NSS Approved, ICSA dla funkcji : Firewall, VPN, SSL/TLS, IPS. Antywirus.
19.	Zarządzanie	System centralnego zarządzania umożliwiający: • Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej • Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości • Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia • Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia • Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) • Zapis i zdalne wykonywanie skryptów na urządzeniach
20.	Raportowanie	System powinien być wyposażony w moduł raportowania i korelacji logów umożliwiający: • Zbieranie logów z urządzenia bezpieczeństwa • Generowanie raportów • Skaner podatności • pojemność zastosowanych dysków powinna umożliwić co najmniej **3 miesięczną archiwizację logów**
21.	Integracja systemu zarządzania	Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centalnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów.
22.	Inne	Zamawiający wymaga, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem fabrycznie nowym, nie używanym, wyprodukowanym nie wcześniej niż 6 miesięcy przed wszczęciem postępowania, Zamawiający wymaga, że sprzęt dostarczony w ramach realizacji umowy będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji świadczonej przez producenta sprzętu, Zamawiający wymaga, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży producenta, co oznacza, że będzie on sprzętem nowym i posiadającym stosowny pakiet usług gwarancyjnych kierowanych również do użytkowników z obszaru Rzeczpospolitej Polskiej, Wraz z dostawą sprzętu należy dostarczyć dokument wydany przez przedstawiciela producenta, poświadczający datę produkcji sprzętu. Dodatkowo: • W okresie obowiązywania umowy Wykonawca zobowiązany jest do zapewnienia utrzymania najnowszych wersji oprogramowania urządzenia, aktualizacja oprogramowania dokonywana jest przez Wykonawcę.. • Rozwiązanie musi umożliwić wykonywanie filtracji URL oraz kontroli antywirusowej przy pomocy produktów firm trzecich.