Urządzenie zabezpieczające sieć		
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 nie może posiadać twardego dysku, w zamian używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanych układów ASIC. 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 odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.
3.	Parametry fizyczne systemu	Nie mniej niż **7** portów Ethernet 10/100 Base-TX, oraz nie mniej niż **2** porty 10/100/1000 Base-TX.
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności: • 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]. • kontrolę treści i kategoryzację odwiedzanych stron WWW – Web\URL Filter • kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) • kontrolę pasma oraz ruchu [QoS, Traffic shaping] • kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM, P2P, VoIP, Web-mail) • zapobieganie przed wyciekiem informacji poufnej - DLP (Data Leak Prevention)
5.	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: • jako router/NAT (3.warstwa ISO-OSI) lub • jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.
6.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń, zarządzanie pasmem sieci (m.in. pasma gwarantowane i maksymalne, pasmo na stację roboczą, priorytety, oznaczenia DiffServ). Urządzenie powinno umożliwiać utworzenie nie mniej niż **5 000** polityk firewall'a

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 4000 sygnatur ataków. • Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie • Możliwość dodawania własnych sygnatur ataków • Możliwość wykrywania anomalii protokołów i ruchu
8.	Moduł antywirusowy	Moduł powinien posiadać minimum dwa tryby pracy skanera: potokowy (flow-based) i plikowy (file-based). Antywirus powinien mieć możliwość transferu częściowo przeskanowanego plik do klienta w celu zapobiegnięcia przekroczenia dopuszczalnego czasu oczekiwania (timeout). Antywirus powinien przeprowadzać sprawdzanie danych zarówno po bazie sygnatur wirusów jak i heurystycznie.
9.	Moduł antyspam	Zawarty moduł antyspamowy powinien pracować w obrębie protokołów SMTP, POP3 i IMAP Klasyfikacja wiadomości powinna bazować na wielu czynnikach, takich jak: • sprawdzenie zdefiniowanych przez administratora adresów IP hostów, które brały udział w dostarczeniu wiadomości, • sprawdzenie zdefiniowanych przez administratora adresów pocztowych, • RBL, ORDBL • Sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych Oprócz powyższego mechanizm antyspamowy powinien umożliwiać skorzystanie z zewnętrznej, wieloczynnikowej bazy spamu.
10.	Filtracja stron WWW	Moduł filtracji stron www powinien umożliwiać blokowanie stron w oparciu o: • białe i czarne listy URL • o zawarte w stronie słowa kluczowe • dynamicznie definiowane przez producenta kategorie.
11.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT. NAT traversal dla protokołów SIP i H323
12.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny. 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.
13.	Połączenia VPN	Wymagane nie mniej niż: • Tworzenie połączeń w topologii Site-to-Site oraz Client-to-Site • Dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki: o firewall o antywirus o web filtering o antyspam • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności • Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

14.	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 statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP • haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.
15.	Wydajność	Obsługa nie mniej niż **1 000 000** jednoczesnych połączeń i **12 000** nowych połączeń na sekundę Przepływność nie mniejsza niż **700 Mb/s** dla ruchu nieszyfrowanego i **140 Mb/s** dla VPN (3DES). Obsługa nie mniej niż **1000** jednoczesnych tuneli VPN
16.	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
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, RSA SecureID) 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.	Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: • Zbieranie logów z urządzeń bezpieczeństwa • Generowanie raportów • Skanowanie podatności stacji w sieci • Zdalną kwarantannę dla modułu antywirusowego
19.	Serwis oraz aktualizacje	Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 1 roku. System powinien być objęty serwisem gwarancyjnym producenta przez okres 1 roku z możliwością przedłużenia Dostawca musi zatrudniać minimum jednego inżyniera posiadającego aktualne certyfikaty techniczne producenta. Dostawca musi okazać zaświadczenie informujące o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem do naprawy u dystrybutora na terenie polski.