**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI IV**

|  |
| --- |
| **Parametry wymagane** |
| **Urządzenie sieciowe klasy UTM – 1 szt.**  |
| 1 | **Architektura systemu ochrony** – system ochrony musi być zbudowany przy użyciu pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanych układów. Producent musi udzielić odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). |
| 2 | **System operacyjny** – dla zapewnienia wysokiej sprawności i skuteczności działania systemu, urządzenie ochronne musi pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia. |
| 3 | **Parametry fizyczne systemu** – nie mniej niż 10 portów Ethernet 10/100/1000 Base-TX (w tym minimum dwa niezależne fizyczne porty WAN), port USB do obsługi modemów sieci 3G/4G. |
| 4 | **Funkcjonalności podstawowe i uzupełniające** – system ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności:1. kontrolę dostępu – zaporę ogniową klasy Stateful Inspection, ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, NNTP),
2. poufność danych – IPSec VPN oraz SSL VPN,
3. ochronę przed atakami – Intrusion Prevention System [IPS/IDS],
4. kontrolę treści i kategoryzację odwiedzanych stron WWW – Web\URL Filter,
5. kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP),
6. kontrolę pasma oraz ruchu [QoS, Traffic shaping],
7. kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM, P2P, VoIP, Web-mail),
8. zapobieganie przed wyciekiem informacji poufnej - DLP (Data Leak Prevention),
9. obsługę sieci VLAN (802.1q).
 |
| 5 | **Zasada działania (tryby)** – urządzenie musi umożliwiać ustawienie jednego z dwóch trybów pracy: jako router/NAT (3.warstwa ISO-OSI) i jako most /transparent bridge/. |
| 6 | **Polityka bezpieczeństwa (firewall)** – polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać: adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie, zarządzanie pasmem sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ). Urządzenie musi 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) oraz niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP:1. nie mniej niż 4000 sygnatur ataków,
2. możliwość dodawania własnych sygnatur ataków,
3. możliwość wykrywania anomalii protokołów i ruchu.
 |
| 8 | **Moduł antywirusowy** – antywirus musi mieć możliwość transferu częściowo przeskanowanego pliku do klienta w celu zapobiegnięcia przekroczenia dopuszczalnego czasu oczekiwania (timeout). Antywirus musi przeprowadzać sprawdzanie danych zarówno po bazie sygnatur wirusów, jak i heurystycznie. |
| 9 | **Moduł antyspamowy** – moduł antyspamowy musi pracować w obrębie protokołów SMTP, POP3 i IMAP. Klasyfikacja wiadomości musi bazować na wielu czynnikach, takich jak:1. sprawdzenie zdefiniowanych przez administratora adresów IP hostów, które brały udział w dostarczeniu wiadomości,
2. sprawdzenie zdefiniowanych przez administratora adresów pocztowych,
3. RBL, ORDBL,
4. sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych.
 |
| 10 | **Filtracja stron WWW** – moduł filtracji stron www musi umożliwiać blokowanie stron w oparciu o:1. białe i czarne listy URL,
2. zawarte w stronie słowa kluczowe,
3. dynamicznie definiowane przez producenta kategorie.
 |
| 11 | **Translacja adresów** – statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT. |
| 12 | **Wirtualizacja i routing dynamiczny** – możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 8 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. Obsługiwane protokoły routingu dynamicznego – co najmniej RIPv2, OSPF, BGP-4 i PIM. |
| 13 | **Połączenia VPN** – tworzenie połączeń w topologii Site-to-Site oraz Client-to-Site. 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:1. haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia,
2. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
3. haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych.

Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych. |
| 15 | **Wydajność** – obsługa nie mniej niż 700 000 jednoczesnych połączeń i 35 000 nowych połączeń na sekundę. Przepływność nie mniejsza niż 6 Gbps dla ruchu nieszyfrowanego i 6,5 Gbps dla VPN (3DES). Obsługa nie mniej niż 200 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 mieć możliwość uwierzytelniania za pomocą:1. haseł statycznych,
2. haseł dynamicznych (RADIUS, RSA SecureID).

System musi umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. |
| 18 | **Raportowanie** – system musi mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym:1. zbieranie logów z urządzeń bezpieczeństwa,
2. generowanie raportów,
3. skanowanie podatności stacji w sieci,
4. zdalną kwarantannę dla modułu antywirusowego.
 |
| 19 | **Gwarancja, serwis oraz aktualizacje** – wykonawca musi dostarczyć wraz z urządzeniem licencje aktywacyjne dla funkcji bezpieczeństwa (w tym min. antywirus, antyspyware/antymalware, IPS, kontrola aplikacji, filtrowanie stron www, ochrona przed wyciekiem informacji, antyspam) na okres 36 miesięcy, licząc od dnia dostarczenia urządzenia. Urządzenie musi być objęte serwisem gwarancyjnym producenta przez okres 36 miesięcy, w trybie 24/7, w tym wsparciem technicznym producenta polegającym na dostarczeniu aktualnego oprogramowania, a także na pomocy technicznej świadczonej telefonicznie oraz naprawie lub wymianie uszkodzonego sprzętu. |
| 20 | **Certyfikaty** – producent urządzeń musi posiadać co najmniej następujące certyfikaty: ISO 9001, UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, SSL, Network IPS, Antywirus. |
| 21 | **Inne wymagania** – oferowane urządzenie musi zapewniać pełną kompatybilność i bezproblemową współpracę z już wdrożonymi przez zamawiającego rozwiązaniami, opartymi o posiadane i użytkowane urządzenia firmy FORTIGATE - model 600E, punkty dostępowe FAP-U433F, szczególnie w zakresie zarządzania, zestawiania i utrzymywania połączeń gateway-to-gateway VPN (IPSec i SSL) oraz raportowania (Forti Analyzer). |