Szczegółowy opis przedmiotu zamówienia

|  |  |
| --- | --- |
|  | |
| **Urządzenie UTM (Unified Threat Management) wraz z 3 letnią subskrypcją 1 szt** | |
|
|
|
| **Parametr** | **Charakterystyka (minimalne wymagania)** |
| **Architektura systemu ochrony** | System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania dlatego urządzenie ochronne nie może posiadać dysku magnetycznego, w zamian powinno używać pamięci FLASH. |
| **System operacyjny** | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu, urządzenie powinno pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego.  Wszystkie dostępne funkcje ochronne oraz zastosowane technologie a także system operacyjny muszą pochodzić od jednego producenta. |
| **Ilość i rodzaj interfejsów:** | * 2 x GE RJ45 WAN, * 2 x GE RJ45 LAN, * 2 x GE RJ45 DMZ, * 2 x GE RJ45 High Availability, * 1 x RJ45 Console Port * 2 x USB w tym min. 1 umożliwiający podłączenie modemu USB, |
| **Montaż w szafach RACK** | Montaż w szafie 19", z dostępem do wszystkich portów z przodu urządzenia. |
| **Pamięć wewnętrzna:** | Pamięć o pojemności min. 30 Gb do celów logowania i raportowania. |
| **Funkcjonalności:** | Najważniejsze funkcje:  Firewall:   * NAT, PAT oraz Bridge, (Translacja adresów NAT adresu źródłowego i NAT adresu docelowego), * Policy-Based NAT, * VLAN Tagging (802.1Q), min 254 interfejsy, * Wsparcie dla protokołu IPv6,   IPS:   * Automatyczna aktualizacja bazy danych, * Sensor IPS, DoS, * Wsparcie dla protokołu IPv6, * Antywirus/Antyspyware: * Automatyczna aktualizacja, * Proxy-Based Antywirus, * Proxy-Flow Antywirus, * Kwarantanna, * Wsparcie dla protokołu IPv6, * Ochrona dla protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP   VPN:   * IPSec VPN, SSL VPN, * Autentyfikacja DES, 3DES, AES, SHA-1/MD5, * PPTP, L2TP, VPN Client Pass Through, * SSL Single Sign-On Bookmarks, * Two-Factor Authentication, * Dostępność klienta VPN (IPSec VPN, SSL VPN - bez dodatkowych opłat)   WAN   * Buforowanie WEB, * Bezpieczne tunele, * Tryb transparentny,   Inspekcja ruchu SSL   * Protokoły: HTTPS, SMTPS, POP3S, IMAPS, * Inspekcja: Antivirus, Web Filtering, Antispam, Data Loss Prevention, * SSL Offload,   Mechanizm ochrony przed wyciekiem poufnych informacji (DLP)   * Identyfikacja oraz kontrola danych w ruchu, * Wbudowana baza wzorców, * Kontrola formatu plików, * Wsparcie dla symboli międzynarodowych,   Kontrola aplikacji   * Identyfikacji oraz kontrola aplikacji, * Kształtowanie ruchu, * Kontrola aplikacji bez względu na port oraz protokół (np. Facebook, BitTorrent, Skype, eDonkey), |
| **Dodatkowe**  **funkcjonalności** | * Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN. * Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall’a, Antywirus’a, IPS’a, Web Filter’a. * Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety) * Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach oraz powinien umożliwiać skanowanie archiwów (ZIP, RAR) * Ochrona IPS:   + powinna opierać się co najmniej na analizie protokołów i sygnatur   + Baza wykrywanych ataków powinna zawierać co najmniej 3000 wpisów.   + Administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur.   + możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. * Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. * Baza filtra WWW o wielkości co najmniej 20 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. * Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. |
| **Połączenia VPN** | W zakresie realizowanych funkcjonalności 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 * Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF * Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth |
| **Uwierzytelnianie użytkowników:** | System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania 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 bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny. |
| **Wydajność:** | * Przepustowość Firewall - nie mniej niż 2500 Mbps, * Ilość jednoczesnych sesji TCP – nie mniej niż 2000000, * Ilość nowych sesji TCP – nie mniej niż 20000/sek, * Przepustowość IPSec VPN – nie mniej niż 400 Mbps, * Przepustowość IPS – nie mniej niż 500 Mbps, * Przepustowość skanera antywirusowego - nie mniej niż 300 Mbps, |
| **Funkcjonalność zapewniająca niezawodność (High Availability):** | Monitorowanie i wykrywanie uszkodzenia elementów sprzętowych i oprogramowania systemu zabezpieczeń oraz połączeń sieciowych. Połączenie dwóch identycznych urządzeń w klaster:  Tryby pracy:   * Active – Active, * Active – Passive. |
| **Konfiguracja i zarządzanie:** | Konfiguracja poprzez terminal, linię komend a także GUI. Dostęp do urządzenia musi być szyfrowany. Zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. System powinien umożliwiać aktualizację oprogramowania oraz zapisanie konfiguracji i odtworzenie z pamięci USB. |
| **Raportowanie:** | Urządzenie powinno mieć możliwość współpracy z zewnętrznym (sprzętowym) modułem raportowania: zbieranie logów z urządzeń, generowanie raportów. |
| **Certyfikaty:** | * ICSA lub EAL4 dla funkcji Firewall * ICSA lub NSS Labs dla funkcji IPS * ICSA dla funkcji: SSL VPN, IPSec VPN |
| **Licencje (subskrypcje):** | Licencja na urządzenie - bez limitu chronionych użytkowników.  Dostawca dostarczy licencje aktywacyjne, aktualizacje wszystkich modułów urządzenia ( tzn. FIREWALL, IPS, WEB FILTERING, obsługa kanałów VPN, ochrona Antyspam i Antywirus), na okres nie krótszy niż 36 miesięcy . |
| **Wsparcie techniczne** | Wsparcie techniczne telefonicznie w języku polskim w trybie 8 godzin 5 dni w tygodniu świadczone przez uprawnionych inżynierów posiadających aktualne certyfikaty producenta (należy podać numer telefonu). |
| **Gwarancja:** | System powinien być objęty serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. Warunki gwarancji wraz z kartą gwarancyjną należy załączyć do sprzętu w wersji papierowej.  Zgłoszenia serwisowe przyjmowane w trybie 8 godzin 5 dni w tygodniu przez infolinię (należy podać numer infolinii). |
| **Szkolenie** | Dostawca musi zapewnić 3-dniowe (18 godzinne) szkolenie 3 osób obejmujące konfigurację systemu, przeprowadzone przez uprawnionego inżyniera posiadającego aktualny certyfikat producenta. Miejsce szkolenia: LODR w Końskowoli. |