*Załącznik nr 1*

 *do formularza ofertowego*

**Wykaz parametrów technicznych oferowanego sprzętu**

**Tabela 1 Parametry techniczne oferowanego sprzętu**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Parametr techniczny** | **Parametry minimalne** | **Parametry oferowane** |
| **Urządzenie Firewall (2 szt. ) – typ** …………………………………….. **/ model** …………………………………………… |
| 1 | Budowa i praca urządzenia | Dedykowane rozwiązanie sprzętowe |  |
| Zintegrowany moduł komunikacji, zawierający ścianę ogniową, router oraz filtr zawartości (antywirus, IPS, application security ). |  |
| Dedykowany system operacyjny |  |
| Składowanie obrazu systemu operacyjnego, polityk oraz konfiguracji w pamięci FLASH |  |
| Brak konieczności wykorzystania dysków twardych |  |
| 2 | Wydajność i przepustowość (wg danych producenta) | Wydajność zapory ogniowej dla ruchu mieszanego (IMIX) – nie mniej niż 200 Mb/s |  |
| Wydajność szyfrowania – niemniej niż 65 Mb/s (3DES+SHA-1) oraz (AES256+SHA-1) |  |
| Ilość jednoczesnych sesji – nie mniej niż 32000 |  |
| Ilość nowych sesji na sekundę – nie mniej niż 1800 |  |
| Ilość polityk na urządzeniu – nie mniej niż 384 |  |
| Wydajność systemu IPS – nie mniej niż 75Mb/s |  |
| Ilość obsługiwanych tuneli VPN IPsec – nie mniej niż 128 |  |
| Fizyczne interfejsy sieciowe:- Ethernet / Fast Ethernet – nie mniej niż 8 ( w tym interfejsy WAN)- ADSL2+ Annex A – minimum 1 szt. |  |
| Port USB – minimum 2 szt.  |  |
| 3 | Translacja adresów | Source NAT z translacją adres-port (PAT) |  |
| Statyczny NAT |  |
| Destination NAT z PAT |  |
| NAT/PAT w oparciu o polityki |  |
| Wirtualne IP – nie mniej niż 4 |  |
| Mapowanie IP – nie mniej niż 300 |  |
| Możliwość grupowania wirtualnych i mapowanych adresów IPMinimum dwa interfejsy WAN (untrust) |  |
| 4 | Firewall, UTM, VPN | Firewall stanowy i bezstanowy |  |
| Wykrywanie ataków sieciowych |  |
| Ochrona przeciwko atakom DoS i DDoS |  |
| Ochrona przed anomaliami protokołów |  |
| Ochrona przed zdeformowanymi pakietami |  |
| Ochrona przed atakami wykorzystującymi fragmentację pakietów |  |
| Ochrona przed atakami brute force |  |
| Ochrona SYN Cookie |  |
| Kontrola protokołów na podstawie sygnatur |  |
| Polityki bazujące na roli użytkownika |  |
| Możliwość tworzenia własnych sygnatur |  |
| Aktualizacje kilka razy w tygodniu |  |
| Zarządzanie przepustowością łącza i priorytetyzacja pakietów |  |
| Skanowanie protokołów: POP3, HTTP, SMTP, IMAP, FTP |  |
| Możliwość zintegrowania z zewnętrznym systemem filtrowania WWW |  |
| Liczba równoczesnych tuneli VPN – nie mniej niż 128 |  |
| Liczba interfejsów tuneli VPN – nie mniej niż 10 |  |
| Algorytmy szyfrowania: DES (56 bitów), 3DES (168 bitów), AES (256-bitów) |  |
| Metody uwierzytelnienia: MD5, SHA-1, SHA-2 |  |
| Obsługa kluczy: manualny, IKEv1, IKEv2, PKI (X.509) |  |
| Bezpieczna wymiana kluczy (DH Groups) – 1,2 5 |  |
| Przeciwdziałanie atakom *reply* |  |
| Dynamiczne tunele VPN remote access |  |
| Ilość użytkowników VPN remote access – nie mniej niż 2 |  |
| IPSec NAT Traversal |  |
| Redundantne bramy VPN |  |
| 6 | Uwierzytelnianie użytkowników i kontrola dostępu | Wewnętrzna baza użytkowników  |  |
| Możliwość autoryzacji RADIUS, LDAP, RSA SecurID |  |
| Uwierzytelnianie VPN XAUTH |  |
| Uwierzytelnianie oparte o WWW |  |
| Uwierzytelnianie 802.1X |  |
| 7 | Rejestrowanie i monitorowanie | Wysyłanie logów do serwerów syslog  |  |
| Monitorowanie przez SNMP |  |
| Standardowa lub własna baza MIB |  |
| Śledzenie tras (traceroute) |  |
| Monitorowanie wydajności w czasie rzeczywistym |  |
| Monitorowanie sesji, pakietów, wysycenia łącza |  |
| 8 | Funkcjonalności wirtualne | Maksymalna liczba stref bezpieczeństwa – nie mniej niż 10 |  |
| Maksymalna liczba wirtualnych routerów z niezależnymi tablicami routingu – nie mniej niż 3 |  |
| Maksymalna liczba sieci VLAN – nie mniej niż 16 |  |
| 9 | Funkcje wysokiej dostępności (HA) | Możliwość połączenia urządzeń w trybie:* + 1. Active/Active dla trybu pracy L3,
		2. Active/Passive dla trybu L3
 |  |
| Synchronizacja konfiguracji urządzeń |  |
| Synchronizacja sesji firewalla i VPN |  |
| Przywracanie sesji po zmianach routingu |  |
| Wykrywanie awarii urządzenia |  |
| Wykrywanie niedostępności połączenia |  |
| Obsługa protokołu VRRP |  |
| 10 | Routing | Obsługa protokołów routingu dynamicznego - RIP w wersji 1, 2, OSPF, BGP |  |
| Maksymalna ilość instancji BGP – nie mniej niż 5 |  |
| Maksymalna ilość instancji RIPv1/v2 – nie mniej niż 4 |  |
| Maksymalna ilość instancji OSPF – nie mniej niż 4 |  |
| Maksymalna ilość tras statycznych – nie mniej niż 8K  |  |
| Routing oparty o adres źródłowy |  |
| Routing oparty o polityki |  |
| ECMP (Equal-cost multipath) |  |
| RPF (Reverse Path Forwarding) |  |
| Multicast (IGMPv1/v2/v3) |  |
| SDP (Session Description Protocol) |  |
| DVMRP (Distance Vector Multicast Routing Protocol) |  |
| 11 | Zarządzanie adresami IP | Statyczne adresy IP |  |
| Klient DHCP |  |
| Klient PPPoE |  |
| Wbudowany serwer DHCP |  |
| Przekazywanie (relay) DHCP |  |
| 12 | Wsparcie dla PKI | Obsługa żądań certyfikatów (PKCS #7, PKCS #10) |  |
| Wsparcie dla Certificate Authorities:  |  |
| 13 | Administrowanie | Zarządzanie przez interfejs linii komend (CLI): port konsoli |  |
| Zarządzanie przez interfejs linii komend (CLI): telnet , SSH (v1,5; v2.0) |  |
| Zarządzanie przez WebUI:  |  |
| Konfiguracja ratunkowa za pomocą przycisku |  |
| Potwierdzanie zmian konfiguracji przed ich wdrożeniem |  |
| Wsparcie dla zewnętrznej bazy administratorów – RADIUS, LDAP, SecurID |  |
| Ograniczenie dostępu do zarządzania urządzeniem tylko z określonych sieci. |  |
| Zróżnicowanie poziomów uprawnień użytkowników  |  |
| Aktualizacja oprogramowania za pomocą:TFTP, USB  |  |
| Przywracanie poprzedniej wersji konfiguracji |  |
| 14 | Mechanizmy zarządzania ruchem | Obsługa protokołu 802.1p, DSCP |  |
| Kolejkowanie na podstawie klas ruchu z priorytetyzacją |  |
| Możliwość określenia gwarantowanego pasma |  |
| Możliwość określenia maksymalnego pasma |  |
| Priorytetyzacja wykorzystania pasma |  |
| Kolejnowanie na podstawie VLAN, DLCI, interfejsów, wielo-polowych filtrów |  |
| 15 | Sieci bezprzewodowe | Możliwość podłączenia modemu USB 3G |  |
| 16 | Pamięć RAM i FLASH | Pamięć DRAM – nie mniej niż 2 GB |  |
| Pamięć FLASH – nie mniej niż 2 GB |  |
| Możliwość użycia portu USB do podłączenia zewnętrznej pamięci. |  |
| 17 | IPv6 | OSPFv3 |  |
| RIPng |  |
| ISIS |  |
| BGP |  |
| NAT64 |  |
| 18 | Zasilanie | Zasilanie 230V AC (50 Hz), kabel zasilający w komplecie |  |
| 19 | Gwarancja | Minimum 24 miesiące gwarancji w miejscu używania urządzenia na terenie kraju. |  |
| 20 | Inne | Urządzenie powinno być wyposażone w taką ilość pamięci, która pozwala na pełne, poprawne działanie wszystkich obsługiwanych funkcji UTM oraz ich aktualizację. |  |
| Urządzenie wyposażone w podstawki do montażu na półce, |  |
| Urządzenie powinno umożliwić zestawienie i utrzymywanie połączenia VPN IPSec z firewallem Fortinet Fortigate 800 |  |
| 21 | Dokumentacja | Kompletna instrukcja użytkownika . |  |
| **Urządzenie UPS w wersji TOWER (2 szt.) – typ** …………………………………….. **/ model** …………………………………………… |
| 1 | Moc pozorna | 1000 VA |  |
| 2 | Moc rzeczywista | 700 W |  |
| 3 | Nominalne napięcie wyjściowe | 230V |  |
| 4 | Architektura  | Line-interactive |  |
| 5 | Liczba i rodzaj gniazd z podtrzymaniem zasilania | Co najmniej 8 gniazd IEC 320 C13 |  |
| 6 | Typ gniazda wejściowego | IEC320 C14  |  |
| 7 | Zakres napięcia wejściowego dla normalnej pracy | Co najmniej 160-294 V |  |
| 8 | Zakres częstotliwości wejściowej | 47-53Hz dla 50Hz |  |
| 9 | Baterie | Baterie wewnętrzne, które mogą być wymieniane w trakcie pracy urządzenia. Możliwość uruchomienia UPS bez zasilania sieciowego. |  |
| 10 | Obudowa | Typu TOWER. Nie dopuszcza się rozwiązania typu RACK z podstawkami. |  |
| 11 | Zdalne zarządzanie | Za pomocą wbudowanej karty sieciowej RJ-45 10/100 Base-T |  |
| 12 | Obsługiwane protokoły | HTTP, SNMP |  |
| 13 | Ciężar | Poniżej 25 kg |  |
| 14 | Szerokość |  Nie więcej niż 230 mm |  |
| 15 | Wysokość | Nie więcej niż 175 mm |  |
| 16 | Głębokość | Nie więcej niż 440 mm |  |
| 17 | Kabel zasilający | O długości minimum 2 m z wtykiem DIN 49441 |  |
| 18 | Gwarancja  | Minimum 24 miesiące gwarancji w miejscu używania urządzenia na terenie kraju. |  |
| 19 | Dokumentacja | Kompletna instrukcja użytkownika . |  |