Załącznik nr 2
do warunków technicznych

Parametry techniczne i warunki dostawy sprzętu

I. Dostawa sprzętu

1. Wykonawca dostarczy 2 (dwa) urządzenia Firewall oraz 2 (dwa) urządzenia UPS wraz z wymaganymi akcesoriami i oprogramowaniem, spełniające wymagania określone w Tabeli 1;
2. Dostarczony przez Wykonawcę sprzęt musi być fabrycznie nowy i oryginalnie zapakowany oraz mieć gwarancję producenta przez minimum 12 miesięcy. Wraz ze sprzętem Wykonawca musi dostarczyć dokumenty gwarancyjne.
3. Wykonawca dostarczy urządzenia do siedziby Zamawiającego: Główny Urząd Geodezji i Kartografii, Centrum Zarządzające ASG-EUPOS w Katowicach, ul. Graniczna 29, 40-017 Katowice.

Tabela 1 Wymagane parametry techniczne sprzętu

Lp.	Parametr techniczny	Parametry minimalne
Urządzenie Firewall – 2 szt.		
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 IP Minimum 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: i. Active/Active dla trybu pracy L3, ii. 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.		
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 .

II. Warunki gwarancji i serwisu

1. Wykonawca zapewni, że dostarczony sprzęt będzie posiadał świadczenia gwarancyjne oparte na oficjalnej gwarancji producenta sprzętu. Z dostawą sprzętu Wykonawca zobowiązuje się dostarczyć dokument wydany przez producenta lub jego polskiego przedstawiciela, że sprzęt pochodzi z oficjalnego kanału dystrybucji i objęty jest wsparciem serwisowym producenta przez wymagany okres gwarancji.
2. Wykonawca udzieli pisemnej gwarancji na dostarczony sprzęt i wyposażenie dodatkowe na okres gwarancji, liczony od daty podpisania protokołu odbioru ostatecznego
3. Niezależnie od uprawnień wynikających z udzielonej gwarancji, Zamawiającemu przysługują uprawnienia z tytułu rękojmi za ukryte wady fizyczne sprzętu.
4. W trakcie trwania okresu gwarancji Wykonawca będzie nieodpłatnie dostarczał oprogramowanie wewnętrzne do dostarczonego sprzętu w przypadku pojawiania się nowszych wersji tego oprogramowania.
5. Serwis gwarancyjny wykonywany będzie w miejscu zainstalowania sprzętu. W przypadku braku możliwości naprawy sprzętu w miejscu używania, dopuszcza się wykonanie czynności serwisowych u Wykonawcy, przy czym koszty związane z dostarczeniem sprzętu do i z serwisu obciążają Wykonawcę.
6. Wykonawca zapewni w przypadku awarii któregokolwiek ze składników dostarczonego sprzętu:
   1) usunięcie zgłoszonej awarii w przeciągu dwóch dni roboczych od daty zgłoszenia;
   2) w przypadku braku możliwości usunięcia zgłoszonej awarii, dostarczenie zastępczego sprzętu (modułu) w przeciągu następnego dnia roboczego od zgłoszenia awarii oraz naprawę uszkodzonego sprzętu (modułu) w przeciągu 21 dni od dnia zgłoszenia
   3) w przypadku niemożności naprawy uszkodzonego sprzętu w terminie 21 dni, za usunięcie awarii uznaje się dostarczenie sprzętu zastępczego (modułu), o ile jego parametry techniczne nie są gorsze od sprzętu (modułu) uszkodzonego.
10. Zgłaszanie awarii może odbywać się faksem lub e-mailem, przy czym przyjęcie zgłoszenia będzie niezwłocznie potwierdzone przez Wykonawcę faksem lub e-mailem.
12. Wykonawca będzie zobowiązany wymienić dany egzemplarz sprzętu na wolny od wad w przypadku, gdy po trzech naprawach tego samego modułu sprzęt nie będzie w pełni sprawny.