Załącznik Nr 2 do SIWZ- Szczegółowa specyfikacja techniczno-cenowa zamówienia (UWAGA: po wypełnieniu przez Wykonawcę staje się formularzem cenowym oferty i Załącznikiem Nr 1 do Umowy).

Szczegółowa specyfikacja techniczno-cenowa zamówienia część II

Uwaga: Nie można edytować kolumn o numerach I, II i III niniejszego formularza. W kolumnach IV, V, VI należy wpisać wartości. W kolumnie VII należy wypełnić odpowiednie wiersze poprzez wpisanie w wykropkowane miejsca danych charakteryzujących oferowany przedmiot zamówienia oraz odpowiednie skreślenie pozycji oznaczonych TAK/NIE* na zasadzie spełnia lub nie spełnia

Lp.		Opis minimalnych parametrów technicznych i funkcjonalnych	Liczba	Cena jednostkowa netto	Cena jednostkowa brutto	Łączna cena ofertowa brutto (ilość x cena jednostkowa brutto)		Opis parametrów technicznych i funkcjonalnych sprzętu oferowanego przez Wykonawcę.
			szt.	zł	zł	zł		
I		II	III	IV	V	VI		VII
1		**Urządzenia zabezpieczeń sieci z obsługą VPN**						**Producent:** ..... **Model:** ..... **Nr konfiguracji (*jeżeli występuje*):** .....
	1	Montaż w szafie 19" rack. System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19''.					1	TAK / NIE *
	2	System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.					2	TAK / NIE *
	3	System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.					3	TAK / NIE *
	4	Parametry wydajności urządzenia: 1. Obsługa nie mniej niż 1 miliona jednoczesnych połączeń i 20 000 nowych połączeń na sekundę. 2. Przepustowość: a) nie mniejsza niż 2 Gb/s dla ruchu nieszyfrowanego, b) nie mniejsza niż 500 Mb/s dla IPsec VPN (AES256).					4	TAK / NIE *
	5	Urządzenie zabezpieczeń musi być wyposażone w co najmniej 8 portów GbE RJ45 (w tym co najmniej 2 dedykowane porty WAN) oraz port USB z możliwością obsługi modemów 3G/4G).					5	TAK / NIE *
	6	Urządzenie zabezpieczeń musi obsługiwać redundancje połączeń WAN w trybie co najmniej: 1. Automatycznego przełączanie na sprawne łącze WAN, przy czym musi istnieć również możliwość używania jako łącza zapasowego modemu podłączonego przez wbudowany port USB. 2. Loadbalancing (rozkładanie obciążenia) na łącza WAN (fizyczne porty WAN oraz port USB z możliwością obsługi modemów 3G/4G.					6	TAK / NIE *
	7	System zabezpieczeń musi działać w trybie co najmniej: 1. Routera (tzn. w warstwie 3 modelu OSI). 2. Transparentnym, przy czym tryb przezroczysty musi umożliwiać wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.					7	TAK / NIE *
	8	System musi obsługiwać statyczną i dynamiczna translacja adresów (NAT). Translacja NAPT.					8	TAK / NIE *
	9	System ochrony musi zapewniać obsługę w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę ogniową klasy Stateful Inspection, • poufność danych - IPSec VPN oraz SSL VPN.					9	TAK / NIE *
	10	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).					10	TAK / NIE *
	11	Urządzenie musi umożliwiać wykrywanie i blokowanie technik i ataków (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. Możliwość wykrywania anomalii protokołów i ruchu.					11	TAK / NIE *
	12	System musi zapewniać obsługę: 1. Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. 2. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.					12	TAK / NIE *
	13	Wymaga się, aby urządzenie w zakresie połączeń VPN realizowało co najmniej: • Tworzenie połączeń w topologii Site-to-site oraz Client-to-site, Hub & Spoke (gwiazdy). • klient VPN własnej produkcji. • 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.	15				13	TAK / NIE *
	14	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 musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory bez dodatkowych opłat licencyjnych.					14	TAK / NIE *
	15	System musi posiadać 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 bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.					15	TAK / NIE *
	16	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym: • Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej. • Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości. • Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia. • Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia. • Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM). • Zapis i zdalne wykonywanie skryptów na urządzeniach.					16	TAK / NIE *
	17	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.					17	TAK / NIE *
	18	System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive oraz w trybie Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.					18	TAK / NIE *

19	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym. Dostawca musi na etapie odbioru sprzętu okazać zaświadczenie informujące o możliwości przyjęcia uszkodzonego urządzenia objętego serwisem do naprawy u dystrybutora na terenie polski.					19	TAK / NIE *
20	Zasilanie z sieci 230V/50Hz.					20	TAK / NIE *
21	Uszkodzony dysk: hdd/ssd (jeżeli występuje i nie jest integralną - nierozłączalną częścią urządzenia) pozostaje u Zamawiającego.					21	TAK / NIE *
22	Urządzenie nie może być urządzeniem wycofanym ze sprzedaży lub nie posiadającym wsparcia producenta.					22	TAK / NIE *
23	Co najmniej 36 miesięcy bezpłatnej gwarancji (części i robocizna) od daty obustronnego podpisania Końcowego Protokołu Zdawczo-Odbiorczego Dostawy, na miejscu u Zamawiającego.					23	TAK / NIE *
24	Zamawiający wymaga dostępu do aktualizacji oprogramowania wewnętrznego (firmware) przez co najmniej 36 miesięcy od daty obustronnego podpisania Końcowego Protokołu Zdawczo-Odbiorczego Dostawy. Dostęp do akualizacji oprogramowania wewnętrznego musi być realizowany co najmniej poprzez stronę internetową producenta dostarczonego urządzenia.					24	TAK / NIE *
25	Maksymalny czas usunięcia awarii do następnego dnia roboczego (poniedziałek-piątek) od dnia zgłoszenia lub w przypadku braku możliwości usunięcia awarii w w/w terminie podstawienie sprzętu zastępczego o parametrach technicznych niegorszych niż sprzęt oferowany.					25	TAK / NIE *
Dodatkowe kryteria oceny spełnienie wszystkich wymagań daje dodatkowe 40 pkt. do oceny końcowej zgodnie z kryteriami oceny.							
26	System ochrony obsługuje w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę ogniową klasy Stateful Inspection, • poufność danych - IPSec VPN oraz SSL VPN, • ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, SMTPS, POP3S, IMAPS, HTTPS), • ochronę przed atakami - Intrusion Prevention System [IPS/IDS], oraz funkcjonalności uzupełniających: • kontrolę treści – Web Filter [WF], • kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP, SMTPS, POP3S, IMAPS), • kontrolę pasma oraz ruchu [QoS i Traffic shaping], • kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P), • zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Preention), • inspekcje SSL z możliwością pełniej analizy szyfrowanej komunikacji.					26	TAK / NIE *
27	Posiada możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 5 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny.					27	TAK / NIE *
28	System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w sieci Internet) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona AntiVirus i AntiSpyware), filtracja plików, danych i URL.					28	TAK / NIE *
29	System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.					29	TAK / NIE *
30	System zabezpieczeń musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.					30	TAK / NIE *
31	Zamawiający **nie wymaga** dostarczenia licencji dla modułów bezpieczeństwa (antywirus, wykrywanie włamań, kontrola aplikacji i webfiltering) jednak wymaga, aby zakup tego typu licencji był możliwy w momencie dostawy urządzania oraz przez co najmniej 1 rok od daty obustronnego podpisania Końcowego Protokołu Zdawczo-Odbiorczego Dostawy.					31	TAK / NIE *
32	Wykonawca przeszkoli wyznaczone przez Zamawiającego osoby (nie więcej niż 3) w formie jedno dniowych warsztatów (co najmniej 6 godzin zegarowych) w siedzibie u Zamawiającego z zakresu: 1. Konfiguracji routingu BGP, OSPF. 2. Konfiguracji wysokiej dostępności w trybach Active/Pasive, Active/Active. 3. Zaawansowanej konfiguracji IPsec VPN. 4. Monitorowania statystyki dla kontroli ruchu, IPsec, BGP, OSPF.					32	TAK / NIE *
33	Potwierdzeniem wysokiej skuteczności systemów bezpieczeństwa są posiadane przez producenta certyfikaty. Producent musi posiadać co najmniej certyfikaty: ISO 9001, UTM NSS Approved, EAL4+, ICSA Labs dla funkcji: Firewall, IPSec, Network IPS, Antywirus.					33	TAK / NIE *
Łączna wartość ofertowa brutto zamówienia:							

.....
(pieczęć i podpis Wykonawcy