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 I

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	**Przedmiotem zamówienia jest rozbudowa istniejącego systemu zabezpieczeń sieci złożonego z urządzenia Palo Alto Networks model PA-3020 o dodatkowe (1 sztuka) urządzenie Palo Alto Networks model PA-3020 wraz z subskrypcjami: Threat prevention, Bright cloud URL filtering, WildFire oraz gwarancją producenta na okres 24 miesięcy od daty obustronnego podpisania Końcowego Protokołu Zdawczo-Odbiorczego Dostawy, na miejscu u Zamawiającego lub dostarczenie rozwiązania równoważnego (złożonego z dwóch urządzeń umożliwiających pracę w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active) spełniającego poniższe wymagania:**	1				**Producent:** …… **Model:** …… **Nr konfiguracji (*jeżeli występuje*):** ……	
	1 Urządzenie zabezpieczeń sieciowych musi być dostarczone jako dedykowane rozwiązanie (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.					1	TAK / NIE *
	2 Urządzenie zabezpieczeń sieciowych musi posiadać przepływność w ruchu full-duplex nie mniejszą niż 2 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniejszą niż 1 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirusowa, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 250 000 jednoczesnych połączeń.					2	TAK / NIE *
	3 Urządzenie zabezpieczeń sieciowych musi być wyposażone w co najmniej 8 portów Ethernet 10/100/1000.					3	TAK / NIE *
	4 Urządzenie zabezpieczeń sieciowych musi działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym, urządzenie nie musi posiadać skonfigurowanych adresów IP na interfejsach sieciowych.					4	TAK / NIE *
	5 Urządzenie zabezpieczeń sieciowych musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.					5	TAK / NIE *
	6 Urządzenie musi obsługiwać protokoły routingu dynamicznego, co najmniej: BGP, RIP i OSPF.					6	TAK / NIE *
	7 Urządzenie zabezpieczeń sieciowych musi zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji.					7	TAK / NIE *
	8 Polityka zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).					8	TAK / NIE *
	9 Urządzenie zabezpieczeń sieciowych musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.					9	TAK / NIE *
	10 Urządzenie zabezpieczeń sieciowych musi automatycznie 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.					10	TAK / NIE *
	11 Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli aplikacji musi wynosić w ruchu full-duplex nie mniej niż 2 Gbit/s.					11	TAK / NIE *
	12 Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.					12	TAK / NIE *
	13 Urządzenie zabezpieczeń sieciowych musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.					13	TAK / NIE *
	14 Urządzenie zabezpieczeń sieciowych musi posiadać możliwość definiowania i przydzielania różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi istnieć możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.					14	TAK / NIE *
	15 Urządzenie zabezpieczeń sieciowych musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.					15	TAK / NIE *
	16 Urządzenie zabezpieczeń sieciowych musi umożliwiać analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.					16	TAK / NIE *
	17 Urządzenie zabezpieczeń sieciowych musi umożliwiać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.					17	TAK / NIE *
	18 Urządzenie zabezpieczeń sieciowych musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów wewnętrznych. 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 anty-wirus i any-spyware), filtracja plików, danych i URL.					18	TAK / NIE *
	19 Urządzenie zabezpieczeń sieciowych musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.					19	TAK / NIE *
	20 Urządzenie zabezpieczeń sieciowych musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.					20	TAK / NIE *
	21 Urządzenie zabezpieczeń sieciowych musi mieć możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, LDAP). Polityka kontroli dostępu powinna precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.					21	TAK / NIE *
	22 Urządzenie zabezpieczeń sieciowych musi mieć możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia.					22	TAK / NIE *
	23 Urządzenie zabezpieczeń sieciowych musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 15 milionów rekordów URL.					23	TAK / NIE *
	24 Urządzenie zabezpieczeń sieciowych musi umożliwiać uruchomienie modułu filtrowania stron WWW per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).	1				24	TAK / NIE *
	25 Urządzenie zabezpieczeń sieciowych musi posiadać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.					25	TAK / NIE *
	26 Urządzenie zabezpieczeń sieciowych musi umożliwiać uruchomienie modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).					26	TAK / NIE *
	27 Urządzenie zabezpieczeń sieciowych musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.					27	TAK / NIE *
	28 Urządzenie zabezpieczeń sieciowych musi umożliwiać uruchomienie modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).					28	TAK / NIE *
	29 Urządzenie zabezpieczeń sieciowych musi posiadać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.					29	TAK / NIE *
	30 Urządzenie zabezpieczeń sieciowych musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.					30	TAK / NIE *
	31 Urządzenie zabezpieczeń sieciowych musi umożliwiać uruchomienie modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).					31	TAK / NIE *
	32 Urządzenie zabezpieczeń sieciowych musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.					32	TAK / NIE *
	33 Urządzenie zabezpieczeń sieciowych musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.					33	TAK / NIE *
	34 Urządzenie zabezpieczeń sieciowych musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirusa czyli nie mniej niż 1 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.					34	TAK / NIE *
	35 Urządzenie zabezpieczeń sieciowych musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.					35	TAK / NIE *
	36 Urządzenie zabezpieczeń sieciowych musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.					36	TAK / NIE *
	37 Urządzenie zabezpieczeń sieciowych musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.					37	TAK / NIE *
	38 Urządzenie zabezpieczeń sieciowych musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN.					38	TAK / NIE *
	39 Urządzenie zabezpieczeń sieciowych musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 4 klas dla różnego rodzaju ruchu sieciowego.					39	TAK / NIE *
	40 Urządzenie zabezpieczeń sieciowych musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.					40	TAK / NIE *
	41 Urządzenie zabezpieczeń sieciowych musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.					41	TAK / NIE *

42	Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli.					42	TAK / NIE *
43	Dostęp do urządzenia i zarządzanie z sieci musi być zabezpieczony kryptograficznie (poprzez szyfrowanie komunikacji). Urządzenie musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.					43	TAK / NIE *
44	Urządzenie zabezpieczeń sieciowych musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS i Kerberos.					44	TAK / NIE *
45	Platforma sprzętowa musi posiadać wbudowany twardy dysk lub pamięć flash do przechowywania logów i raportów o pojemności nie mniejszej niż 80 GB.					45	TAK / NIE *
46	Urządzenie zabezpieczeń sieciowych musi umożliwiać usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.					46	TAK / NIE *
47	Urządzenie zabezpieczeń sieciowych musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.					47	TAK / NIE *
48	Urządzenie zabezpieczeń sieciowych musi mieć możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.					48	TAK / NIE *
49	Urządzenie zabezpieczeń sieciowych musi mieć możliwość stworzenia raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.					49	TAK / NIE *
50	Urządzenie zabezpieczeń sieciowych musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.					50	TAK / NIE *
51	Urządzenie zabezpieczeń sieciowych musi posiadać aktywne (w okresie trwania gwarancji na dostarczone urządzenie) wsparcie techniczne producenta dla posiadanych funkcjonalności.					51	TAK / NIE *
52	Co najmniej 24 miesięcy bezpłatnej gwarancji (części i robocizna) od daty obustronnego podpisania Końcowego Protokołu Zdawczo-Odbiorczego Dostawy, na miejscu u Zamawiającego.					52	TAK / NIE *
53	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.					53	TAK / NIE *
Dodatkowe kryteria oceny spełnienie wszystkich wymagań daje dodatkowe 40 pkt. do oceny końcowej zgodnie z kryteriami oceny							
54	Urządzenie zabezpieczeń sieciowych wyposażone jest w co najmniej 8 portów Ethernet 10/100/1000, z możliwością zamontowania 8 interfejsów optycznych (SFP).					54	TAK / NIE *
55	Tryb pracy urządzenia ustalany w konfiguracji interfejsu sieciowego, a system umożliwia pracę we wszystkich wymienionych trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).					55	TAK / NIE *
56	Urządzenie zabezpieczeń sieciowych obsługuje nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwia uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.					56	TAK / NIE *
57	Zezwolenie dostępu do aplikacji odbywa się w regułach polityki firewall (tzn. reguła firewall posiada oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe. Nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile).					57	TAK / NIE *
58	Urządzenie nie dokonuje kontroli aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).					58	TAK / NIE *
59	Urządzenie nie dokonuje kontroli aplikacji wykorzystując moduł IPS, sygnatury IPS ani dekodery protokołu IPS.					59	TAK / NIE *
60	Urządzenie zabezpieczeń sieciowych wykrywa co najmniej 1500 różnych aplikacji (takich jak np. Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.					60	TAK / NIE *
61	Urządzenie zabezpieczeń sieciowych odczytuje oryginalne adresy IP stacji końcowych z nagłówka X-Forwarded-For i wykrywa na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesję, w przypadku, gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.					61	TAK / NIE *
62	Urządzenie zabezpieczeń sieciowych posiada moduł inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolujący ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją.					62	TAK / NIE *
63	Baza sygnatur anty-wirus jest przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzi od tego samego producenta co producent systemu zabezpieczeń.					63	TAK / NIE *
64	Urządzenie zabezpieczeń sieciowych posiada sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.					64	TAK / NIE *
65	Urządzenie zabezpieczeń sieciowych posiada funkcjonalność podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).					65	TAK / NIE *
66	Integracja z zewnętrznymi systemami typu "Sand-Box" pozwala administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".					66	TAK / NIE *
67	Administrator ma możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box".					67	TAK / NIE *
68	Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.					68	TAK / NIE *
69	Urządzenie zabezpieczeń sieciowych posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.					69	TAK / NIE *
70	Urządzenie zabezpieczeń sieciowych pozwala na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.					70	TAK / NIE *
71	Wszystkie narzędzia monitorowania, analizy logów i raportowania są dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.					71	TAK / NIE *
72	Urządzenie zabezpieczeń sieciowych umożliwiają sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.					72	TAK / NIE *
73	Urządzenie zabezpieczeń sieciowych posiada możliwość konfigurowania różnych serwerów Syslog per polityka bezpieczeństwa.					73	TAK / NIE *
Łączna wartość ofertowa brutto zamówienia:							

.....
(pieczęć i podpis Wykonawcy