Załącznik nr 1 do SIWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Minimalne parametry techniczno-jakościowe Przedmiotu zamówienia:

1. System zabezpieczeń sieciowych – 2 urządzenia wraz z licencjami

L.p.	Opis wymagań technicznych
1	System zabezpieczeń sieciowych musi być dedykowanym urządzeniem zabezpieczeń sieciowych (tzw. appliance).
2	Całość sprzętu i oprogramowania musi być wspierana przez jednego producenta.
3	1) Urządzenia zabezpieczeń sieciowych muszą być zaoferowane wraz z niezbędnymi do instalacji w szafie szynami montażowymi lub uchwytami. 2) Urządzenia muszą charakteryzujących się takimi samymi parametrami technicznymi. 3) Urządzenia muszą zapewniać taką samą względem siebie funkcjonalność.
4	1) Wysokość każdego z urządzeń zabezpieczeń sieciowych nie może być większa niż 2U (jednostka wysokości szafy montażowej). 2) Musi istnieć możliwość montażu w standardowej szafie typu rack 19” dowolnego producenta.
5	1)Każde z oferowanych urządzeń zabezpieczeń sieciowych musi posiadać przepływność nie mniejszą niż 2 Gb/s dla kontroli firewall z włączona funkcją kontroli aplikacji. 2)Każde z oferowanych urządzeń zabezpieczeń sieciowych musi posiadać przepływność nie mniejszą niż 1 Gb/s dla kontroli zawartości z włączoną funkcją kontroli AV, IPS i URL Filtering. Funkcja kontroli AV, IPS i URL Filtering musi być realizowana w ramach kontroli zawartości. 3)Każde z oferowanych urządzeń zabezpieczeń sieciowych musi posiadać przepływność nie mniejszą niż 400 Mb/s dla ruchu VPN.
6	Każde z oferowanych urządzeń zabezpieczeń sieciowych musi obsługiwać nie mniej niż 250 000 jednoczesnych sesji.
7	Każde z oferowanych urządzeń zabezpieczeń sieciowych musi obsługiwać nie mniej niż 50 000 nowych sesji na sekundę.
8	Urządzenia zabezpieczeń sieciowych muszą być wyposażone w co najmniej 8 interfejsów Ethernet 10/100/1000 każde (interfejsy zarządzające nie są wliczane). Musi istnieć możliwość agregacji co najmniej 8 interfejsów sieciowych zgodnej z IEEE 802.3ad.
9	1)Urządzenia zabezpieczeń sieciowych muszą być wyposażone w co najmniej 8 interfejsów optycznych (SFP) każde, w tym co najmniej 2 interfejsy w każdym urządzeniu obsadzone wkładkami SFP. 2)Musi być możliwość połączenia urządzeń w klaster przy

	wykorzystaniu interfejsów obsadzonych wkładkami SFP, o których mowa w ppkt 1).
10	Każde z oferowanych urządzeń zabezpieczeń sieciowych musi posiadać wbudowany twardy dysk o pojemności minimum 120 GB (HDD lub SSD).
11	System zabezpieczeń sieciowych musi działać co najmniej w następujących trybach łącznie: a) w trybie router/NAT (tzn. w warstwie 3 modelu OSI), b) w trybie transparentnym. Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych.
12	W trybie router/NAT musi istnieć możliwość konfiguracji interfejsów w trybie: a) przełącznika (tzn. w warstwie 2 modelu OSI), b) pasywnego nasłuchu (sniffer). Tryb pracy interfejsów musi być ustalany w konfiguracji interfejsów. Musi istnieć możliwość jednoczesnej konfiguracji poszczególnych interfejsów w różnych trybach.
13	1) Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. 2) Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
14	Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu.
15	Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP, OSPF i routing statyczny.
16	Musi istnieć możliwość podłączenia do urządzenia co najmniej dwóch łączy WAN (routing statyczny). Równoważenie łączy powinno odbywać się za pomocą adresu źródłowego, docelowego oraz portu, na którym jest zestawiana sesja. Musi być zapewniony mechanizm failover dla łączy co najmniej w przypadku, gdy do każdego urządzenia podłączone są dwa w/w łącza WAN.
17	System zabezpieczeń musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy: a) sieciowej (IP), b) transportowej (TCP, UDP), c) aplikacji.
18	1) System zabezpieczeń sieciowych, zgodnie z ustaloną polityką, musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa. 2) System musi umożliwiać utworzenie minimum 20 stref bezpieczeństwa. 3) System musi umożliwiać utworzenie minimum 2000 polityk zabezpieczeń firewall.
19	Polityka zabezpieczeń musi uwzględniać co najmniej: a) strefy bezpieczeństwa, b) adresy IP, c) protokoły i usługi sieciowe, d) aplikacje, e) użytkowników aplikacji, f) reakcje zabezpieczeń, g) rejestrowanie zdarzeń i alarmowanie, h) zarządzanie pasma sieci (minimum priorytet, pasmo

	gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
20	System zabezpieczeń sieciowych musi umożliwiać filtrację zdarzeń według co najmniej następujących kryteriów: data, godzina, adres IP źródłowy, adres IP docelowy, użytkownik, strefa bezpieczeństwa źródłowa, strefa bezpieczeństwa docelowa, interfejs źródłowy, interfejs docelowy, port, protokół (TCP/UDP), aplikacja, polityka zabezpieczeń, akcja (allow/deny). Wszystkie moduły monitorowania, analizy logów i raportowania muszą być dostępne zarówno lokalnie w systemie jak i w zaoferowanym systemie analizy zdarzeń.
21	System zabezpieczeń sieciowych musi umożliwiać odnotowywanie w dzienniku systemowym działań użytkowników lub obiektów systemowych polegających na dostępie do: a) systemu z uprawnieniami administracyjnymi, b) konfiguracji systemu, w tym konfiguracji zabezpieczeń, c) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa. System zabezpieczeń sieciowych musi umożliwiać przechowywanie ww. informacji przez wskazany okres.
22	System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego (np. komunikacji użytkowników do Internetu) oraz ruchu przychodzącego. System musi mieć możliwość deszyfracji 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 adresów URL.
23	System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P, Instant Messaging, Remote Access). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
24	System zabezpieczeń musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
25	System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa są wskazane jako dozwolone.
26	System zabezpieczeń musi identyfikować co najmniej 1000 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS, nie mniej niż: Skype, Gadu-Gadu, Tor, BitTorrent, eMule, TeamViewer.
27	System zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN).
28	Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii IPSec VPN oraz SSL VPN. Oferowany system zabezpieczeń musi umożliwiać uwierzytelnianie użytkowników VPN zintegrowane z Active Directory.
29	Oferowany system zabezpieczeń musi zapewniać bezpieczny zdalny dostęp do chronionych zasobów w oparciu o standard IPSec VPN oraz SSL VPN, z następujących systemów operacyjnych: Windows - 7/8/10, Android - 4.1.x/4.2.x/4.3/5.x/6.x, Mac OS X 10.9.x i nowsze, Apple iPhone OS/iOS - 9.x i nowsze, bez konieczności dokupowania

	jakichkolwiek komponentów, poza subskrypcją. Zdalny dostęp musi być możliwy dla minimum 500 jednoczesnych sesji.
30	Oferowany system zabezpieczeń musi zapewniać możliwość kontroli urządzeń uzyskujących dostęp do sieci Zamawiającego przez VPN co najmniej w zakresie aktualności sygnatur ochrony antywirusowej.
31	System zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych polityk priorytetu, pasma maksymalnego i gwarantowanego.
32	System zabezpieczeń musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, exe, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, cab, rar, zip, tar, gzip, hta, pdf, text/html, tiff, torrent. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
33	System zabezpieczeń musi umożliwiać ochronę przed atakami typu „Drive-by-download".
34	System zabezpieczeń musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS) bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków musi zawierać co najmniej 6000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur.
35	System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej, kontrolującego przynajmniej pocztę elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP i HTTPS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny.
36	System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza URL Filtering musi być regularnie aktualizowana w sposób automatyczny. Baza URL Filtering o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie treści. W ramach filtrowania musi istnieć możliwość blokowania przez kategorie stron zawierających co najmniej następujące treści: spyware, malware, spam, proxy.
37	System zabezpieczeń musi posiadać funkcję wykrywania Botnet na podstawie analizy behawioralnej lub aktualizowanej automatycznie, dostarczanej przez producenta bazy adresów IP serwerów C&C.
38	System zabezpieczeń musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
39	System zabezpieczeń musi transparentnie ustalać tożsamość użytkowników sieci (integracja z Active Directory, LDAP). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
40	Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli dostępnej przez aplikację lub przeglądarkę

	internetową. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie minimum 3 administratorów o różnych poziomach uprawnień. Interfejs do zarządzania musi być w języku angielskim.
41	System zabezpieczeń 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 pod jednym lub wieloma publicznymi adresami IP.
42	System zabezpieczeń sieciowych nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
43	System zabezpieczeń musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu muszą być takie same zarówno podczas pracy w sieci lokalnej jak i przy połączeniu do Internetu poza siecią lokalną).
44	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.
45	Wymagane jest udzielenie gwarancji na warunkach określonych w Umowie, na oba urządzenia przeznaczone do pracy w klastrze niezawodnościowym HA (w trybie Active-Passive lub Active-Active) na okres 60 miesięcy.
46	Wymagane jest zaoferowanie rozwiązania wraz z licencjami, uprawniającymi do korzystania z wszystkich funkcjonalności określonych przez Zamawiającego w wymaganiach minimalnych, w tym w szczególności do: a)aktualizacji bazy ataków IPS, b)aktualizacji aplikacji, c)definicji wirusów, d)bazy kategorii stron WWW, e)zdalnego dostępu VPN ze stacji roboczych (komputerów, laptopów) i telefonów/tabletów dla minimum 500 jednoczesnych sesji, f)korzystania z funkcji kontroli urządzeń uzyskujących dostęp do sieci co najmniej w zakresie posiadania aktualnych sygnatur ochrony antywirusowej, na oba urządzenia przeznaczone do pracy w klastrze niezawodnościowym HA (w trybie Active-Passive lub Active-Active). Wymagane jest zapewnienie dla oferowanych licencji prawa do subskrypcji na warunkach określonych w Umowie przez okres 60 miesięcy.
47	Wymagane jest, aby oferowane rozwiązanie spełniało wszystkie określone przez Zamawiającego wymagania minimalne, bez konieczności dokupowania dodatkowych elementów (np. urządzeń, modułów, licencji, itp.) nie będących przedmiotem zamówienia. Zamawiający nie dopuszcza zaoferowania dodatkowych urządzeń, w

	celu spełnienia wymagań minimalnych określonych przez Zamawiającego.
48	Oferowany sprzęt musi być zaprojektowany i wyprodukowany zgodnie z normą jakościową ISO 9001:2008 oraz normą środowiskową ISO 14001:2004. Oferowany sprzęt musi spełniać wymagania dyrektyw Unii Europejskiej: 2006/95/WE (bezpieczeństwo elektryczne), 2004/108/WE (kompatybilność elektromagnetyczna).

2. System analizy zdarzeń z systemu zabezpieczeń sieciowych - 1 licencja

1	Musi być możliwość instalacji systemu analizy logów na maszynie wirtualnej VMWare ESXi 6.0.
2	System analizy logów musi obsługiwać dzienny rozmiar logów na poziomie 5 GB.
3	System analizy logów musi umożliwiać przechowywanie logów o łącznym rozmiarze nie mniejszym niż 2TB.
4	System analizy logów musi pochodzić od tego samego producenta, co zaoferowane urządzenia systemu zabezpieczeń sieciowych.
5	System analizy logów musi obsługiwać zaoferowane urządzenia systemu zabezpieczeń sieciowych.
6	System analizy zdarzeń musi umożliwiać podgląd logowanych zdarzeń w czasie rzeczywistym.
7	Wszystkie moduły monitorowania, analizy logów i raportowania muszą być dostępne lokalnie w systemie.
8	System analizy zdarzeń musi umożliwiać filtrację zdarzeń oraz generowanie raportów w oparciu co najmniej o następujące kryteria: data, godzina, adres IP źródłowy, adres IP docelowy, użytkownik, strefa bezpieczeństwa źródłowa, strefa bezpieczeństwa docelowa, interfejs źródłowy, interfejs docelowy, port, protokół (TCP/UDP), aplikacja, polityka zabezpieczeń, akcja (allow/deny).
9	System analizy zdarzeń musi umożliwiać odnotowywanie w dzienniku systemowym działań użytkowników lub obiektów systemowych polegających na dostępie do: a) systemu z uprawnieniami administracyjnymi, b) konfiguracji systemu, w tym konfiguracji zabezpieczeń, przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa. System analizy zdarzeń musi umożliwiać przechowywanie ww. informacji przez wskazany okres.
10	System musi umożliwiać generowanie raportów na żądanie oraz cyklicznie, według zdefiniowanych kryteriów, co najmniej w formacie pliku pdf.
11	System analizy logów musi mieć graficzny interfejs użytkownika.
12	Zarządzanie systemem analizy zdarzeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli dostępnej przez aplikację lub przeglądarkę internetową.
13	System analizy zdarzeń musi posiadać konfigurowalne opcje powiadamiania o zdarzeniach, jak e-mail, SNMP
14	Wymagane jest zaoferowanie rozwiązania wraz z licencjami, uprawniającymi do korzystania z wszystkich funkcjonalności w zakresie monitorowania, analizy zdarzeń i raportowania, bez

	konieczności dokupowania dodatkowych zewnętrznych urządzeń, oprogramowania ani licencji. Wymagane jest zapewnienie dla oferowanych licencji prawa do subskrypcji przez okres 60 miesięcy liczonych od dnia podpisania bez zastrzeżeń Protokołu Odbioru. System, jeżeli wymagane, musi być zaoferowany wraz z licencją na system operacyjny, na którym zostanie zainstalowany.
15	Wymagane jest udzielenie gwarancji na warunkach określonych w Umowie na zaoferowany system analizy zdarzeń na okres 60 miesięcy liczonych od dnia podpisania bez zastrzeżeń Protokołu Odbioru.