Załącznik Nr 1b do SIWZ
jednocześnie Załącznik nr 1 do Umowy

Opis przedmiotu zamówienia - Część II

Zawiera minimalne wymagania dla poszczególnych urządzeń

Całość rozwiązania musi pochodzić i być zarządzana centralnym systemem jednego (tego samego) producenta.

1. Wymagania ogólne wspólne urządzeń typu Firewall.

Nr	Wymagania minimalne
1	Urządzenia typu Firewall muszą być dostarczone jako dedykowane urządzenie (tzw. appliance). Całość rozwiązania musi pochodzić i być zarządzana centralnym systemem jednego (tego samego) producenta.
2	Urządzenie musi być wyposażone w dedykowany szeregowy port konsoli RJ45, port konsolowy micro USB, port USB do konfiguracji wstępnej za pomocą tzw. USB pen-drive.
3	Urządzenie musi być wyposażone dedykowany port zarządzania IP Ethernet 10/100/1000. Port ten musi być wydzielony co najmniej logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji (tzw. Out of band management).
4	Urządzenie musi umożliwiać równoległe działanie co najmniej w 4 trybach pracy a. rutera (tzn. w warstwie 3 modelu OSI), b. przełącznika (tzn. w warstwie 2 modelu OSI), c. w trybie pasywnego nasłuchu (tzw. TAP interface). d. w trybie transparentnym (całkowicie przeźroczyste - urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny rozgłoszeniowe w sensie Ethernet/CSMA)
5	Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.)
6	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.
7	Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.
8	Urządzenie musi umożliwiać zestawianie 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).

9	Jeżeli wykorzystanie funkcji IPSEC VPN (site-to-site) wymaga zakupu dodatkowych licencji, lub jeżeli oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności.
10	Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach. a. Polityki definiujące powinny umożliwiać wykorzystanie i. adresów źródłowych, ii. adresów docelowych, iii. użytkowników, iv. numerów portów usług, v. kategorie URL. b. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia i. RADIUS lub TACACS+, ii. LDAP, iii. Kerberos lub SAML 2.0.
11	Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej: a) oznaczania pakietów znacznikami DiffServ, b) ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. c) utworzenia co najmniej 8 klas ruchu sieciowego. d) kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników. e) kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. f) przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego
12	Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
13	Urządzenie musi obsługiwać funkcję wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych).
14	Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.
15	Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.
16	Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.
17	Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie QoS.

18	Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. 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 65535 dostępnych portach. Wydajność kontroli firewalla stanowego i kontroli aplikacji całego ruchu nie może być mniejsza niż wskazano w wymaganiach wydajnościowych urządzeń. Urządzenie musi wykrywać co najmniej 2900 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
19	Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.
20	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
21	Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia
22	Urządzenie musi pozwalać na 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
23	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download"
24	Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL, który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
25	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH
26	Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory, b) usługi katalogowe LDAP, c) serwery Terminal Services.
27	Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
28	Urządzenie musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż tylko MS Windows (np. Linux lub Unix)

	w celu łączenia nazw użytkowników z adresami IP hostów, z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. Dopuszcza się zastosowanie innego mechanizmu wbudowanego w urządzenie, który technicznie pozwoli na uzyskanie równoważnej funkcjonalności dotyczącej „śledzenia" logowań użytkowników.
29	Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa) Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.
30	Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb, http2. Baza sygnatur AV musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV musi być uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).
31	Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania.
32	Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę 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).

33	Urządzenie musi posiadać funkcjonalność URL Flitering. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to Zamawiający wymaga jej dostarczenia w chwili zakupu urządzenia.
34	Urządzenie musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk, elf,) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) 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. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to Zamawiający wymaga jej dostarczenia w chwili zakupu urządzenia.
35	Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
36	System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą a. bazy lokalnej, b. serwera LDAP, c. RADIUS lub TACACS+ Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS)
37	Urządzenie musi zapewniać interfejs API (JSON, REST, XML lub inny) będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI). Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to Zamawiający wymaga jej dostarczenia w chwili zakupu urządzenia.
38	Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia.

39	Urządzenie musi zapewniać możliwość zatwierdzania zmian per pojedynczy system/firewall/kontekst wirtualny. Zmiany zatwierdzane w pojedynczym firewallu wirtualnym nie mogą być w jakikolwiek sposób widoczne w innych systemach wirtualnych, w szczególności niedopuszczalne jest aby zatwierdzenie zmian w pojedynczym systemie/kontekście wpływało w jakikolwiek sposób na ciągłość komunikacji/filtrację/reguły/polityki etc. w innych systemach wirtualnych
40	Urządzenie musi umożliwiać wysyłanie logów do zewnętrznych serwerów SYSLOG jako UDP, TCP i SSL.

2. Wymagania dla urządzeń Firewall Typu 1 – 2 szt. (1 para HA)

Nr	Wymagania minimalne
1	Urządzenie musi być wyposażone w - 4 interfejsy 100M/1GE/10GE Ethernet (RJ45) - 16 interfejsów Ethernet 1Gbps (SFP) oraz 16 interfejsów 10Gbps (SFP+), lub 16 interfejsów elastycznych obsługujących tryb 1G/10G akceptujących odpowiednio SFP/SFP+, które można wykorzystać w trybie 1Gbps lub 10Gbps. - 4 interfejsy 40GE Ethernet (QSFP+). - 1 dedykowany port HA minimum 40GE Ethernet (QSPF+).
2	Urządzenie musi być wyposażone w system dyskowy do przechowywania logów sieciowych o pojemności nie mniejszej niż 2 TB (RAID 1), oraz w redundantny elektroniczny nośnik danych lub 2 dyski SSD wielkości minimum 200 GB (RAID 1) na potrzeby systemu operacyjnego i logów systemowych.
3	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 20 Gbps dla NG Firewall z rozpoznawaniem i kontrolą aplikacji, Minimum 9 Gbps dla funkcji NG Firewall z rozpoznawaniem i kontrolą aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antymalware, Antyspyware, kontrola typów plików. Minimum 150 000 nowych sesji na sekundę. Minimum 4 000 000 równoległych sesji
4	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 7 Gbps dla IPSEC VPN Minimum 10 000 tuneli IPSEC VPN (site-to-site)
5	Urządzenie musi obsługiwać nie mniej niż 20 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Zamawiający dopuszcza rozwiązania, gdzie system urządzenia wymaga, aby tablica routingu była powiązana z wirtualnym systemem w relacji 1:1 wówczas należy przewidzieć w ofercie trzykrotnie większą liczbę wirtualnych firewalli obsługiwanych przez urządzenie aniżeli wymagana w pozostałych wymaganiach dla urządzenia oraz odpowiednio większą instalację systemu zarządzania (dotyczy liczby zarządzanych firewalli logicznych)
6	Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych instancji (firewalli/systemów/domen/kontekstów) i posiadać możliwość rozbudowy do 20 takich instancji. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych:

	a. tablic routingu (przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń, lub zapewnić odpowiednio więcej systemów wirtualnych) b. Polityk bezpieczeństwa obejmujących i. System IPS ii. System ochrony antymalware/antyspyware iii. System ochrony antywirus, kontrola typów plików
7	Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 30 000 reguł polityki bezpieczeństwa
8	Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
9	Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie, każdy maksymalnie 1500W.
10	Urządzenie musi być przeznaczone do montażu w szafie Rack 19” z maksymalnym rozmiarem 3RU.
11	Wraz z każdym urządzeniem muszą być dostarczone następujące kable i wkładki: a) Wkładka optyczna MultiMode Ethernet 10Gb/s SFP+ SR zasięg 300m – sztuk 4 b) Wkładka optyczna MultiMode Ethernet 40Gb/s QSFP+ BiDi zasięg 150 m – sztuk 4 c) Kabel typu DAC 10Gb/s SFP+ - SFP+ o długości minimum 5m - sztuk 2 d) Zestaw okablowania pozwalający zestawić klaster HA w trybie active/active z maksymalną oferowaną przez urządzenie prędkością długość min. 3 metry – jeden zestaw okablowania na parę urządzeń. e) Przewód zasilający 230V AC - sztuk 2

3. Wymagania dla urządzeń Firewall Typu 2 – 2 szt. (1 para HA).

Nr	Wymagania minimalne
1	Urządzenie musi być wyposażone w 12 interfejsów 10/100/1000 Mbps Ethernet (RJ45), 4 interfejsy 1Gbps typu SFP, oraz minimum 4 interfejsy 10Gbps typu SFP+
2	Urządzenie musi być wyposażone w elektroniczny nośnik danych lub dysk SSD wielkości minimum 200 GB. Dyski obrotowe nie są akceptowalne.
3	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 4,4 Gbps dla NG Firewall z rozpoznawaniem i kontrolą aplikacji, Minimum 2,2 Gbps dla funkcji NG Firewall z rozpoznawaniem i kontrolą aplikacji przy włączonych funkcjach bezpieczeństwa: IPS, Antywirus, Antymalware, Antyspyware, kontrola typów plików. Minimum 55000 nowych połączeń na sekundę. Minimum 900 000 równoległych sesji
4	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 2,2 Gbps dla IPSEC VPN Minimum 4000 tuneli IPSEC VPN (site-to-site)
5	Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.

6	Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 9000 reguł polityki bezpieczeństwa
7	Urządzenie musi być wyposażone w redundantne zasilacze AC 230V, każdy maksymalnie 800W.
8	Urządzenie musi być przeznaczone do montażu w szafie Rack 19” z maksymalnym rozmiarem 2RU.
9	Wraz z każdym urządzeniem muszą być dostarczone następujące kable i wkładki: a. Wkładka optyczna MultiMode Ethernet 10Gb/s SFP+ SR zasięg 300m – sztuk 4 b. Wkładka optyczna MultiMode Ethernet 1Gb/s SFP+ SR zasięg 300m – sztuk 4 c. Zestaw okablowania pozwalający zestawić klaster HA w trybie active/active z maksymalną oferowaną przez urządzenie prędkością długość min. 3 metry – jeden zestaw okablowania na parę urządzeń. d. Przewód zasilający 230V AC - sztuk 2

4. Wymagania dla centralnego system zarządzania urządzeniami Firewall.

Nr	Wymagania minimalne
1	Wraz z urządzeniami Firewall konieczne jest dostarczenie centralnego systemu zarządzania. Zamawiający dopuszcza budowę systemu w oparciu o kilka komponentów zarządzania oferowanych przez producenta firewalli i systemu zarządzania pod warunkiem, iż będą one pochodziły od jednego producenta i będą przez niego w całości serwisowane. Zamawiający wymaga jednocześnie, aby wymagania dotyczące liczby zarządzanych firewalli, pojemności przestrzeni dyskowej oraz możliwości rozbudowy były spełnione przez każdy z komponentów tworzących system zarządzania. System musi umożliwiać pracę w trybie kolektora logów zbierającego jedynie dane z systemów bezpieczeństwa lub w trybie pełnej analizy w celu optymalizacji procesu zbierania logów.
2	System zarządzania, logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku VMWare.
3	a) System zarządzania, logowania i raportowania musi spełnić następujące wymagania minimalne b) obsługa nie mniej niż 10 firewalli fizycznych c) obsługa nie mniej niż 15 firewalli wirtualnych (w rozumieniu wirtualny kontekst/domena/system uruchomiony na dostarczanym firewallu) d) zapewnienie obsługi przestrzeni dyskowej o pojemności nie mniejszej niż 6 TB. e) Możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczonej na logowanie (dopuszcza się rozbudowę poprzez dokupienie dodatkowej licencji)
4	System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW. System musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
5	a) System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej

	b) umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych. c) tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. d) zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. e) tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”
6	a) System zarządzania, logowania i raportowania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym co najmniej: b) budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla). Globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli). c) umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery lub logiczne grupy urządzeń umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów). d) Pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń e) umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium. f) umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych. g) umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.
7	System zarządzania, logowania i raportowania musi umożliwiać centralne narzędzia inwentury i audytu oraz zarządzania konfiguracjami w tym co najmniej musi a) umożliwiać dystrybucję i zdalną instalację nowych wersji systemu b) umożliwiać tworzenie kopii zapasowych zarządzanych firewalli. c) umożliwiać dystrybucję i zdalną instalację nowych sygnatur. d) umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem. e) pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów. f) umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone g) informować o zmianach konfiguracji systemu
8	System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.
9	Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej korelując zdarzenia z wielu urządzeń Firewall.

Usługa wsparcia technicznego - gwarancja

Wymagane jest dostarczenie wsparcia producenta na okres 36 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7.