Załącznik nr 6 do SIWZ – BZP.2410.9.2019.PM

Opis Przedmiotu Zamówienia

Spis treści

1. Wprowadzenie

Celem zakupu jest zwiększenie bezpieczeństwa sieci i urządzeń Zamawiającego poprzez dostawę urządzenia typu Next Generation Firewall – służącego do zabezpieczenia sieci komputerowej i serwerowej ze strony zagrożeń sieci Internet, filtrowaniem treści i filtrowaniem WWW oraz konsoli zarządzającej służącej do zarządzania, monitorowania i raportowania.

2. Firewall

Wymaganie	Opis
Ogólne	Sprzęt wymieniony w poniższej specyfikacji musi być fabrycznie nowy, aktualnie obecny w linii produktowej producenta w terminie minimum 6 miesięcy przed złożeniem oferty. Urządzenia muszą pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej. Producent rozwiązania musi być uwidoczniony w sekcji Leaders w raporcie Gartnera (Magic Quadrant) dla Enterprise Network Firewalls z 2018 roku lub uzyskać status „Recommended” w testach NSS Labs dla Next Generation Firewalls z lipca 2018 roku. Sprzęt musi mieć możliwość zainstalowania w standardowej szafie rack 19”. Wymagany jest zestaw montażowy do takiej instalacji. Każde z urządzeń musi być wyposażone w przestrzeń, do przechowywania logów i raportów, o pojemności nie mniejszej niż 2 TB (RAID 1). Każde z urządzeń musi być zasilane prądem zmiennym 230V i być wyposażone w redundantne zasilacze. Zasilacze muszą zapewnić poprawne działanie urządzenia przy jego pełnym obciążeniu w przypadku awarii połowy z nich. Urządzenia nie mogą znajdować się na liście „end-of-sale” oraz „end-of-support” producenta.
Liczba urządzeń	2 szt.
Klaster HA	Możliwość obudowy w oparciu o minimum dwa fizyczne urządzenia gotowe do pracy w konfiguracji odpornej na awarie (HA) 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.
Tryby pracy	Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy: • rutera (tzn. w warstwie 3 modelu OSI), • przełącznika (tzn. w warstwie 2 modelu OSI),

	• w trybie pasywnego nasłuchu (sniffer). 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.)
Polityki FW/Mechanizmy bezpieczeństwa	Musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji. Musi być dostarczone jako dedykowane urządzenia zabezpieczeń sieciowych. Nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej. 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 pasmem QoS. Musi umożliwiać zdefiniowanie nie mniej niż 20 000 reguł polityki bezpieczeństwa. 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 65 535 dostępnych portach. Wydajność kontroli firewalla stanowego i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż wskazano w wymaganiach wydajnościowych. Musi wykrywać co najmniej 2500 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, 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. 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. 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. 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. Musi zapewniać ochronę przed atakami typu „Drive-by-download". Musi umożliwiać uwierzytelnienie dwuskładnikowe (MFA - multi factor authentiaction) i zastosowanie tego mechanizmu w politykach. Polityki definiujące powinny umożliwiać wykorzystanie: • adresów źródłowych, • adresów docelowych, • użytkowników, • numerów portów usług, • kategorie URL. System musi obsługiwać co najmniej następujące mechanizmy uwierzytelnienia: • RADIUS, • Kerberos lub SAML 2.0, • LDAP.
NetFlow	Musi wspierać NetFlow minimum w wersji 9, minimum jednokierunkowy. Musi przetwarzać wszystkie pakiety na wszystkich interfejsach urządzenia. Musi posiadać możliwość konfiguracji eksportu danych do zewnętrznego kolektora. W przypadku używania specyficznych szablonów NetFlow przez urządzenie, muszą być one możliwe do pobrania ze strony producenta.
Filtracja WWW/Web Filtering	Musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering/Web Filtering wraz z aktualizacją w okresie wsparcia serwisowego. Baza adresów 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. 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 nie wymaga jej dostarczenia w chwili zakupu urządzenia.
Intrusion Prevention System (IPS)	Musi posiadać możliwość rozbudowy o funkcjonalność Intrusion Prevention System (IPS). System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania 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). Musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to Zamawiający nie wymaga jej dostarczenia w chwili zakupu urządzenia.
Antivirus (AV)	Musi posiadać możliwość rozbudowy o funkcjonalność Antywirus (AV). Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak HTTP, SMTP, IMAP, POP3, FTP, SMB. Baza sygnatur AV musi być przechowywania 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. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to Zamawiający nie wymaga jej dostarczenia w chwili zakupu urządzenia.
Antymalware/Antyspyware	Musi posiadać możliwość rozbudowy o 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 antyspyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik antyspyware musi być uruchamiany per reguła polityki bezpieczeństwa. 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. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to Zamawiający nie wymaga jej dostarczenia w chwili zakupu urządzenia.
Sandboxing	Musi posiadać możliwość rozbudowy o funkcjonalność ochrony przed atakami 0-day i współpracy z sandboxem producenta. Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu sandbox plików różnych typów (np. exe, dll, pdf, MS Office, Java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu 0-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 nie wymaga jej dostarczenia w chwili zakupu urządzenia.
Listy dynamiczne	Musi umożliwiać zastosowanie zewnętrznych dynamicznych list w procesie realizacji, co najmniej następujących funkcji: filtrowanie adresów URL, filtrowanie adresów IP, filtrowanie nazw domenowych.
Blokowanie DNS	Musi posiadać możliwość rozbudowy o 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). Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to Zamawiający nie wymaga jej dostarczenia w chwili zakupu urządzenia.
Detekcja BotNet	Musi posiadać możliwość rozbudowy o funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej. Jeżeli funkcja ta wymaga zakupu dodatkowej licencji to Zamawiający nie wymaga jej dostarczenia w chwili zakupu urządzenia.
VLAN	Musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q z obsługą minimum 4094 znaczników. Podinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
LAG	Musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad.
IPv6	Musi zapewniać obsługę dla IPv6.
NAT	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. 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. Musi umożliwiać wysyłanie logów z informacjami o sesjach w ramach NAT do zewnętrznych systemów Syslog.
DoS	Musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
IPSec/IKE VPN	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). W przypadku gdy funkcjonalność jest oferowana jako subskrypcja czasowa, Zamawiający wymaga dostarczenia subskrypcji na min. 12 miesięcy lub jeśli funkcjonalność oferowana jest na liczbę aktywnych tuneli VPN należy przyjąć co najmniej 10 tuneli.
SSL-VPN	Musi realizować funkcję SSL VPN dla użytkowników zdalnych z możliwością wskazania zarówno sieci, do których dostęp ma odbywać się przez VPN jak i wykluczenia sieci, do których ruch nie będzie realizowany za pośrednictwem kanału VPN. Musi także oferować możliwość kompletnego zablokowania dostępu do sieci lokalnej użytkownika zalogowanego do VPN. Musi oferować możliwość sprawdzania hosta, który dokonuje podłączenia do SSL-VPN, pod względem danych z systemu operacyjnego, m.in. statusów i parametrów: • aktualizacji systemu operacyjnego • firewalla, • ochrony antywirusowej, • ochrony antispyware, • szyfrowania dysku, i możliwości wykorzystania tych danych do ograniczania dostępu do usługi SSL-VPN lub poszczególnych usług zdefiniowanych w ramach połączenia SSL-VPN. W przypadku gdy funkcjonalność jest oferowana jako subskrypcja czasowa, Zamawiający wymaga dostarczenia subskrypcji na min. 12 miesięcy lub jeśli funkcjonalność oferowana jest na liczbę aktywnych kont należy przyjąć co najmniej 2000 kont.
QoS	Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej: • oznaczania pakietów znacznikami DiffServ, • ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego,

	• utworzenia co najmniej 8 klas ruchu sieciowego, • kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników, • kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP, • przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
Routing	Musi obsługiwać protokoły routingu dynamicznego, nie mniej niż: RIP, BGP i OSPF (IPv4 i IPv6). Musi wspierać mechanizm PBR (policy based routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu. Musi wspierać protokół BFD (bidirectional forwarding detection).
Zarządzanie	Urządzenie musi być wyposażone dedykowany port konsoli/zarządzania. Port ten musi być wydzielony co najmniej logicznie i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. W przypadku gdy system pozwala na jednoczesną pracę dwu lub więcej administratorów musi istnieć wbudowany w system mechanizm umożliwiający jednemu z administratorów uzyskanie wyłączności na wprowadzanie zmian. W tym czasie pozostali zalogowani użytkownicy nie mogą być w stanie dokonać żadnych zmian w konfiguracji. Zarządzanie musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Każda metoda zarządzania systemem musi uwzględniać uwierzytelnienie, szyfrowanie i audyt operacji wykonywanych przez administratora. System musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI. System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach Musi umożliwiać uwierzytelnianie administratorów za pomocą: • bazy lokalnej, • LDAP, • RADIUS. Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS)

	Musi umożliwiać przesyłanie logów do kilku zdefiniowanych serwerów Syslog. Interfejs administracyjny urządzeń musi być w języku polskim lub angielskim. 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). Musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. 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.
Inspekcja ruchu szyfrowanego	System 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 Zamawiającego. Oferowany sprzęt 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 anty-spyware), filtracja plików, danych i URL. Musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. Musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
Wirtualne routery/systemy	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 dwukrotnie 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) Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych firewalli/systemów/domen/kontekstów i posiadać możliwość rozbudowy do 20 takich systemów. Każdy firewall wirtualny musi mieć możliwość konfiguracji indywidualnych, niezależnych i odrębnych: • tablic routingu (przy czym system musi umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń, lub zapewnić odpowiednio więcej systemów wirtualnych), • polityk bezpieczeństwa obejmujących o system IPS, o system ochrony antymalware/antyspyware, o system ochrony antywirus, • koncentratorów VPN dla zdalnego dostępu.
Wydajność	Każde z urządzeń musi spełniać co najmniej następujące parametry wydajnościowe: • minimum 20 Gbps dla Firewall/kontroli aplikacji, • minimum 9 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji, • minimum 8 Gbps dla ruchu IPSec VPN, • minimum 150 tys. nowych połączeń na sekundę, • minimum 4.000.000 równoległych sesji, • minimum 2 000 tuneli SSL VPN z wykorzystaniem klienta VPN.
Uwierzytelnianie/ustalanie tożsamości	Musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: • Active Directory, • LDAP, • Terminal Services. Nie jest dopuszczalna instalacja dodatkowych agentów na kontrolerach domeny lub zmiana schematu usługi Active Directory, w celu realizacji funkcji powiązania adresów IP do użytkowników oraz odczytu przynależności użytkowników do grup Active Directory. 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. Musi posiadać 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. 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" logowania użytkowników.
Akcesoria, okablowanie	Należy dostarczyć komplet okablowania i akcesoriów, wymaganego do redundantnego podłączenia sprzętu oraz do pełnego podłączenia urządzeń jako klaster. Każde z urządzeń musi posiadać minimum: • 2 interfejsy 100/1000 Ethernet (RJ45), • 16 interfejsów 1/10GE SFP/SFP+ (8 interfejsów obsadzonych modułami 10G SFP+ SR), • 4 interfejsy 40GE QSFP+.
Wsparcie techniczne	Min. 12 miesięcy serwisu realizowanego przez producenta sprzętu w zaoferowanym okresie gwarancji z gwarantowanym czasem usunięcia awarii w ciągu 24 godzin, z dostępem do nowych wersji oprogramowania wydawanych przez producenta, bazy wiedzy, instrukcji konfiguracyjnych jak i narzędzi diagnostycznych.
Wdrożenie	Montaż i uruchomienie urządzenia w miejscu dostawy.

3. Konsola zarządzania

Wymaganie	Opis
Ogólne	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. System musi pracować w trybie kolektora logów zbierającego jedynie dane z systemów bezpieczeństwa lub w trybie pełnej analizy w celu optymalizacji procesu zbierania logów. System zarządzania, logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku VMWare posiadanego przez Zamawiającego. System zarządzania, logowania i raportowania musi: • obsługiwać nie mniej niż 10 firewalli fizycznych, • obsługiwać nie mniej niż 100 firewalli wirtualnych,

	• zapewnić obsługę przestrzeni dyskowej o pojemności nie mniejszej niż 16 TB, • posiadać możliwość rozbudowy o dodatkową przestrzeń dyskową przeznaczoną na logowanie (dopuszcza się rozbudowę poprzez dokupienie dodatkowej licencji). 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. Musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
Analiza danych	Musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej umożliwiać: • tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych, • tworzenie statycznych raportów dopasowanych do aktualnych potrzeb, • 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. • tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do aktualnych potrzeb z funkcjonalnością „drill-down”.

Zarządzanie	Musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi w tym co najmniej:
	• 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),
	• 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),
	• pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń,
	• umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium,
	• umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i

	obiektów w nich użytych, • umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi. Musi umożliwiać centralne narzędzia inwentury i audytu oraz zarządzania konfiguracjami w tym co najmniej: • umożliwiać dystrybucję i zdalną instalację nowych wersji systemu, • umożliwiać tworzenie kopii zapasowych zarządzanych firewalli, • umożliwiać dystrybucję i zdalną instalację nowych sygnatur, • umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem, • pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów, • umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone, • informować o zmianach konfiguracji systemu. Musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów. Musi umożliwiać uwierzytelnianie administratorów za pomocą: • bazy lokalnej, • LDAP, • RADIUS.
Wsparcie techniczne	Min. 12 miesięcy serwisu realizowanego przez producenta w zaoferowanym okresie gwarancji, z dostępem do nowych wersji oprogramowania wydawanych przez producenta, bazy wiedzy, instrukcji konfiguracyjnych jak i narzędzi diagnostycznych.