Krajowe Centrum
Monitorowania
Ratownictwa Medycznego

Załącznik do SIWZ

Opis Przedmiotu Zamówienia

Dostawa 4 szt. urządzeń typu FireWall do centrów przetwarzania danych Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM) w związku z budową Podsystemu Zintegrowanej Łączności SWD PRM – Zadanie 2

Lotnicze Pogotowie Ratunkowe

ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

1. Słowniki i skróty

Dla potrzeb niniejszego opracowania przyjmuje się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Informacje	Należy przez to rozumieć informacje, o których mowa w art. 78 ust. 3 ustawy z dnia 16 lipca 2004 r., Prawo telekomunikacyjne (t. j. Dz. U. z2019 r., poz.2460 z późn. zm.).
Lokalizacja/ Lokalizacje	Oznacza wskazane przez Zamawiającego lokalizacje na terenie RP określone w przedmiocie niniejszego zamówienia. Zamówienie będzie realizowane w dwóch Ośrodkach Przetwarzania Danych w Warszawie oraz w Radomiu. Bliższe dane adresowe zostaną przekazane na etapie podpisywania umowy.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Urządzenia	Sprzęt teleinformatyczny wraz z niezbędnym wyposażeniem i odnoszącą się do niego dokumentacją techniczną producenta, w tym również okablowanie strukturalne, będące przedmiotem niniejszego zamówienia.
Usługa Serwisu Gwarancyjnego	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Urządzeń oraz ich poszczególnych komponentów, w szczególności usuwanie błędów.
Wykonawca/Dostawca	Podmiot realizujący zamówienie.
Zamawiający/LPR	Lotnicze Pogotowie Ratunkowe.

2. Przedmiot zamówienia

Celem Zamawiającego jest budowa systemu ochrony sieciowej. W skład całościowego systemu bezpieczeństwa będą wchodziły cztery urządzenia pracujące w trybie 2 klastrów niezawodnościowych będące przedmiotem zamówienia.

Celem Zamawiającego jest zarządzanie wszystkimi urządzeniami z centralnej konsoli umożliwiającej scentralizowane zarządzanie.

Zamawiający wymaga, aby oferowane rozwiązanie firewall było sprawdzone w praktyce rynkowej, co oznacza, że oferowany produkt musiał być dostępny na rynku co najmniej 6 miesięcy przed terminem składania ofert. Przez „*dostępność produktu na rynku*" Zamawiający rozumie, iż produkt w postaci konkretnego modelu urządzenia firewall oraz produkt w postaci wskazanej oferowanej wersji firmware musiał być dostępny w terminie 6 miesięcy przed złożeniem oferty.

Jednocześnie Zamawiający wymaga, aby w przypadku oprogramowania zainstalowanego na urządzeniu oraz oprogramowania do zarządzania firewallami było dostępne oprogramowanie objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowania np. w wersji Beta), a za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania firewall. W przypadku rozwiązania sprzętowego Zamawiający wymaga dostępności konkretnego modelu urządzenia firewall. Niedopuszczalne jest wskazanie innego urządzenia z typoszeregu czy urządzenia z innej „*rodziny*".

Usługa wsparcia technicznego:

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, aktualizację baz sygnatur aplikacyjnych, aktualizację baz sygnatur IPS, AV, AntySpyware oraz aktualizację baz kategorii URL, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24h x 7 dni.

3. Urządzenia bezpieczeństwa

Zamawiający wymaga dostarczenia urządzeń (po dwie sztuki do danej lokalizacji) oraz oprogramowania zarządzającego dostarczanymi urządzeniami. Zamawiający informuje, iż posiada obecnie dwa urządzenia Paloalto Network, które również muszą zostać objęte scentralizowanym zarządzaniem. Wymagania dla urządzeń i oprogramowania przedstawiono w tabeli poniżej:

Lp.	Part Number	Description	Ilość
1.	PAN-PA-3220	Palo Alto Networks PA-3220 with redundant AC power supplies	4
2.	PAN-PA-3220-GP-3YR-HA2	GlobalProtect subscription 3 year prepaid for device in an HA pair, PA-3220	4
3.	PAN-PA-3220-TP-3YR-HA2	Threat prevention subscription 3 year prepaid for device in an HA pair, PA-3220	4
4.	PAN-SVC-BKLN-3220-3YR	Partner enabled premium support 3-year prepaid, PA-3220	4
5.	PAN-PRA-25	Panorama central management software, 25 devices	1
6.	PAN-SVC-BKLN-PRA-25-3YR	Partner enabled premium support 3 year prepaid, Panorama 25 devices	1

lub dostarczenie urządzeń równoważnych spełniających poniższe wymagania.

4. Wymagania równoważne

(Zamawiający dopuszcza również zastosowanie urządzeń równoważnych pod warunkiem spełnienia poniższych wymagań)

1. Każde z urządzeń Firewall posiada łącznie następujące cechy sprzętowe:
   1) musi posiadać 12 interfejsów 10/100/1000 (RJ45);
   2) musi posiadać 4 interfejsy 1GE SFP+;
   3) musi posiadać 4 interfejsy 1/10GE SFP+ obsadzone dwoma modułami 10GE SFP+ SR i dwoma modułami 10GE SFP+ LR. Zamawiający dopuszcza by urządzenie zamiennie dla czterech interfejsów 1/10GE było wyposażone w 4 (cztery) interfejsy 10GE i 4 (cztery) interfejsy 1GE;
   4) musi posiadać dedykowany port zarządzania. Port ten musi być wydzielony i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji;
   5) musi być wyposażony w moduł klasy Lights Out Management (LOM) lub odpowiednik pozwalający na wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie fizycznym lub sprzętowym (wówczas urządzenie musi zapewniać dedykowane procesory i pamięć dla realizacji modułu zarządzania);
   6) musi być wyposażony w dysk HDD lub SSD do przechowywania logów i raportów o pojemności nie mniejszej niż 200GB.

2. Parametry wydajnościowe:
   1) Minimum 4,5 Gbps dla Firewall/kontroli aplikacji;
   2) Minimum 2,2 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware;
   3) Minimum 50 tys. nowych połączeń na sekundę;
   4) Minimum 1.000.000 równoległych sesji;
   5) Minimum 2 Gbps dla IPSEC VPN;
   6) Minimum 1 000 tuneli IPSEC VPN (site-to-site);
   7) Minimum 1 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN.
3. Każde z urządzeń Firewall posiada łącznie następujące cechy związane z obsługą ruchu sieciowego:
   1) musi umożliwiać działanie co najmniej w trzech trybach pracy. Tryb musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych poniżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu:
      a) rutera (tzn. w warstwie 3 modelu OSI),
      b) przełącznika (tzn. w warstwie 2 modelu OSI),
      c) w trybie pasywnego nasłuchu (sniffer);
   2) 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;
   3) musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP;
   4) 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;
   5) musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP;
   6) musi wspierać mechanizm PBR (Policy Base Routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu;
   7) 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). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN (dla Windows, Android, iOS) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 1000 jednoczesnych użytkowników;
   8) 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.
4. Firewall wspiera następujące mechanizmy związane z zarządzaniem pasmem w sieci (QoS) w zakresie co najmniej:
   1) oznaczanie pakietów znacznikami DiffServ;

2) utworzenie co najmniej 8 klas ruchu sieciowego;
3) kształtowanie ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP.

5. Firewall wspiera następujące mechanizmy związane z rozpoznawaniem i uwierzytelnieniem użytkowników:
   1) musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:
      a) Microsoft Active Directory,
      b) usługi katalogowe LDAP,
      c) serwery Terminal Services,
      d) logi z syslog;
   2) Polityka kontroli dostępu firewalla musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP;
   3) w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się transparentnie.
6. Firewall musi wspierać następujące mechanizmy związane z konfiguracją polityk bezpieczeństwa i mechanizmami inspekcyjnymi:
   1) 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. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 10 000 reguł polityki bezpieczeństwa oraz obsługę minimum 100 stref bezpieczeństwa;
   2) Firewall 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;
   3) Firewall musi wykrywać co najmniej 3000 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;
   4) Firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie;
   5) Firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tiff. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia;
   6) Firewall 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;

7) Firewall musi zapewniać ochronę przed atakami typu „Drive-by-download";
8) Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet;
9) Firewall musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć
z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa;
10) Firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH;
11) Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji.
12) 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;
13) 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);
14) Musi być zapewniona możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi lub z poziomu centralnej konsoli zarządzania i monitorowania.

7. Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji:
   a) Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb,
   b) 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.

   Zamawiający dopuszcza zastosowanie zamiennie do modułu antywirus silnika antymalware opisanego jako funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem.
8. Firewall musi posiadać rozbudowy o funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem.
   a) Firewall musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus/IPS (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,
   b) Zamawiający NIE wymaga dostarczenia licencji na współpracę z sandboxem lokalnym i sandboxem chmurowym w chwili zakupu urządzenia jednakże licencja na współpracę z sandboxem lokalnym i sandboxem chmurowym jest wymagana, jeżeli zaoferowane rozwiązanie nie posiada dedykowanego silnika antywirusowego.
9. 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.

a) Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń,
b) 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),
c) Musi być zapewniona możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta lub zapewniona z poziomu centralnej konsoli zarządzania i monitorowania.

10. 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).
11. Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering.
    a) Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL,
    b) 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),
    c) 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. Dopuszcza się, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania,
    d) Zamawiający NIE wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia.
12. Narzędzia konfiguracji i zarzadzania firewallem:
    1) Zarządzanie firewallem 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).
    2) Firewall musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności musi mieć zdefiniowane w systemie co najmniej dwa konta typu:
        a) Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu,
        b) Operator, który ma możliwość tylko odczytu konfiguracji;
    3) Firewall musi umożliwiać uwierzytelnianie administratorów za pomocą:
        a) bazy lokalnej,
        b) serwera LDAP,
        c) RADIUS lub TACACS+
        d) SAML 2.0;
    4) Firewall musi zapewniać możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
    5) Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej. Realizacja tego wymagania musi opierać się o samo urządzenie – nie dopuszcza się realizacji koncepcji kandydackiej z wykorzystaniem centralnej konsoli zarządzania. Funkcja ta musi być dostępna również w przypadku utraty komunikacji

z centralną konsolą zarządzania. Funkcja ta musi być realizowana co najmniej przez graficzny interfejs zarządzania firewallem (GUI).

6) Firewall musi zapewniać interfejs API (JSON lub REST lub XML lub inny) będący jego integralną częścią, i za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
7) Firewall musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia.
8) Firewall musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.

13. Firewall musi być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej.
14. Obudowa firewalla może mieć rozmiar maksymalnie 3RU (rack unit), musi być przeznaczona do montażu w szafie rackowej 19”.

Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

5. Wyjaśnienia dotyczące wydajności urządzenia

1. Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.
2. Jako scenariusz Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus i antyspyware.

6. Dostawa systemu centralnego zarządzania urządzeniami bezpieczeństwa

Zamawiający dopuszcza również zastosowanie równoważnego systemu zarządzania po warunkiem spełnienia poniższych wymagań:

1. System zarządzający realizuje następujące grupy funkcjonalne:
   1) Kolektor logów;
   2) Zarządzanie uprawnieniami administratorów;
   3) Zarządzanie firewallami jako infrastrukturą;
   4) Generowanie raportów.
2. Cechy ogólne systemu:
   1) musi być realizowany jako pojedynczy system - nie dopuszcza się oferowania systemu zarządzania składającego się z kilku komponentów;
   2) może zostać dostarczony w postaci maszyny wirtualnej pracującej w środowisku VMWare;
   3) może zostać dostarczony jako rozwiązanie sprzętowe po następującymi warunkami:
      a) musi być oferowane i serwisowane jako całość wraz z systemem zarządzania przez jednego producenta,
      b) musi zapewniać docelowe wielkości przestrzeni dyskowej,
      c) należy przewidzieć pełną redundancję sprzętową (również dla samych urządzeń). Zamawiający przyjmuje, iż system wirtualizacyjny zapewnia odpowiedni poziom redundancji/dostępności rozwiązania w postaci maszyny wirtualnej.
3. Parametry wydajnościowe:
   1) obsługa nie mniej niż 20 firewalli fizycznych;
   2) obsługa nie mniej niż 100 firewalli wirtualnych (w rozumieniu wirtualny kontekst/domena/system uruchomiony na dostarczanym firewallu);
   3) obsługa co najmniej 10 000 logów/zdarzeń na sekundę;

4) obsługa przestrzeni dyskowej na logi o pojemności nie mniejszej niż 3 TB jako przestrzeni użytecznej na logi. W przypadku zastosowania dedykowanych urządzeń zarządzania przestrzeń ta musi być dostarczona jako realizowana w RAID-1 lub RAID-6.

4. Wymagania dotyczące kolektora logów:
   1) musi umożliwiać zbieranie logów zdarzeń z urządzeń firewall;
   2) zbierane dane powinny zawierać informacje co najmniej o:
      a) ruchu sieciowym,
      b) użytkownikach,
      c) aplikacjach,
      d) zagrożeniach,
      e) filtrowanych stronach WWW;
   3) musi umożliwiać korelację logów zdarzeń z wielu zarządzanych firewalli.
5. Wymagania dotyczące analizy i filtracji informacji:
   1) musi umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych
   2) musi umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych.
   3) Musi pozwalać na tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego.
   4) Musi umożliwiać 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.
   5) Musi pozwalać na tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down"
6. Wymagania dotyczące zarządzania firewall'ami i inwentury:
   1) System zarządzania musi umożliwiać centralne zarządzanie wieloma firewallami fizycznymi i logicznymi;
   2) musi pozwalać na budowanie i dystrybucję polityk bezpieczeństwa:
      a) Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla),
      b) globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli);
   3) musi 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);
   4) musi pozwalać na tworzenie raportów na podstawie zbudowanych kontenerów lub grup urządzeń;
   5) musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium;
   6) musi umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych;

7) musi umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi;
8) musi umożliwiać dystrybucję i zdalną instalację nowych wersji systemu do zarządzanych firewalli;
9) musi umożliwiać tworzenie kopii zapasowych zarządzanych firewalli;
10) musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur aplikacyjnych i IPS;
11) musi umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem;
12) musi pozwalać na zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów;
13) musi umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby system zarządzania, logowania i raportowania zrozumiał, iż nowe urządzenie zastępuje urządzenie uszkodzone;
14) musi informować o zmianach konfiguracji systemu.

7. Wymagania dotyczące administratorów - musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.

Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

7. Wymagania gwarancyjne i serwisowe

1. Wykonawca wraz z dostawą urządzeń przekaże warunki gwarancyjne i serwisowe, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta.
2. Wymagania gwarancyjne:
   1) Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu:
      a) prawo do pobierania nowych wersji i aktualizacji oprogramowania przez okres minimum 36 miesięcy od podpisania protokołu odbioru produktu,
      b) przyjmowanie zgłoszeń Zamawiającego przez Wykonawcę 24 godziny na dobę (dla sprzętu objętego serwisem NBD, zgłoszenia zamawiającego dokonane po godz. 15:35 i w dni wolne od pracy będą traktowane jako zgłoszenia dokonane następnego dnia roboczego),
      c) wymianę sprzętu w przypadku zdiagnozowania awarii urządzenia,
      d) dostarczenie sprawnego urządzenia lub jego elementu podlegającego wymianie do miejsca zainstalowania urządzenia uszkodzonego,
      e) możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania,
      f) dostęp do pomocy technicznej producenta,
      g) dostęp do poprawek i nowych wersji oprogramowania;
   2) gwarancją producenta muszą zostać objęte wszystkie dostarczone urządzenia przez okres minimum 36 miesięcy, przy czym bieg okresu gwarancji rozpocznie się z chwilą podpisania bez zastrzeżeń protokołu odbioru produktu. Do dostarczonych urządzeń będą dołączone karty gwarancyjne zawierające numery seryjne produktu, numery seryjne oprogramowania, termin i warunki ważności gwarancji (zgodnie z umową), adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
3. Do przedmiotu zamówienia muszą zostać dostarczone procedury zgłaszania awarii w formie edytowalnych dokumentów w wersji elektronicznej.
4. Do kontaktów/zgłoszeń Wykonawca udostępnia:
   1) numer telefonu – _____ (infolinia bezpłatna), _____ (dla telefonów komórkowych i z zagranicy);
   2) numer faksu - _____;
   3) e-mail - _____
5. Wykonawca zobowiązuje się do świadczenia usług gwarancyjnych w trybie NBD (następny dzień roboczy).
6. Ilekroć w treści niniejszego dokumentu jest mowa o awarii rozumie się taki stan sprzętu i oprogramowania, który uniemożliwia korzystanie z dostarczonego sprzętu.
7. Zamawiający wymaga, aby awaria została usunięta następnego dnia roboczego od chwili jej zgłoszenia, dotyczy serwisu NBD.
8. W przypadku braku możliwości wykonania naprawy w terminie podanym wyżej, Wykonawca na okres przedłużającej się naprawy bądź usuwania awarii, dostarczy Zamawiającemu sprzęt zastępczy, równoważny funkcjonalnie. Po zakończeniu naprawy sprzęt zastępczy zostanie zwrócony Wykonawcy z wyłączeniem nośników danych.
9. Uszkodzone elementy sprzętu będą wymienione przez Wykonawcę na nowe, wolne od wad i o parametrach nie gorszych od uszkodzonych.

10. W okresie gwarancji, w przypadku awarii dysku twardego lub innego nośnika danych, będzie on wymieniony przez gwaranta na nowy bez konieczności zwrotu uszkodzonego dysku twardego lub innego nośnika danych przez Zamawiającego i dokonywania ekspertyzy dysku poza siedzibą Zamawiającego.
11. Przez usunięcie awarii należy rozumieć przywrócenie pierwotnej funkcjonalności sprzętu i systemu operacyjnego sprzed wystąpienia awarii.
12. Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.
13. Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.
14. Dla oprogramowania obowiązują prawa gwarancyjne producenta.
15. Zamawiający wymaga elastyczności w rozbudowie, aby była możliwość bez konieczności uzyskania zgody Wykonawcy czy Producenta, rozbudowy posiadanych urządzeń o kolejne moduły rozszerzeń. Rozbudowa nie może powodować utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego urządzenia.
16. Zamawiający zastrzega sobie prawo do dodawania nowych modułów dowolnych producentów oraz wymiany zainstalowanych modułów samodzielnie lub z pomocą Wykonawcy, w zakresie przewidzianym przez producenta Urządzenia, bez utraty gwarancji na zakupione Urządzenia. Zamawiający będzie dokonywał wymiany modułów samodzielnie po wcześniejszym uzgodnieniu z Wykonawcą.

8. Zasady ogólne

1. Wykonawca zobowiązany jest wykonać przedmiot zamówienia wraz ze wszystkimi wymaganymi, nie później niż w ciągu 4 tygodni od dnia podpisania Umowy.
2. Odbiór przedmiotu zamówienia zostanie przeprowadzony w m.st. Warszawa i Radomiu.
3. Odbiór przedmiotu zamówienia zostanie potwierdzony podpisaniem przez wyznaczonych przedstawicieli Zamawiającego i Wykonawcy Protokołu odbioru przedmiotu zamówienia.
4. Wszelkie pozostałe kwestie i szczegółowe postanowienia w zakresie realizacji przedmiotu zamówienia regulować będzie umowa zawarta pomiędzy Zamawiającym a Wykonawcą.

Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl