Krakowskie Pogotowie Ratunkowe
Dział Informatyki i Łączności
31-530 Kraków, ul. św. Łazarza 14
tel. 12 42-44-222, fax 12 42-44-300

pieczęć zamawiającego

Załącznik nr 4 do regulaminu
udzielania zamówień do 130 000 zł netto

Nr sprawy : XXI-042-1-24-2021
Data 06.05.2021

ZAPYTANIE CENOWE - OFERTA

Zamawiający – Krakowskie Pogotowie Ratunkowe zaprasza do złożenia oferty na :

1. Przedmiot zamówienia (opis): **Dostawa i wdrożenie urządzenia Firewall – NGFW, (Router klasy UTM)** o parametrach szczegółowo opisanych w załączniku nr 1 do niniejszego zapytania
2. Inne parametry: **Opisane szczegółowo w załączniku nr 1 do niniejszego zapytania**
3. Warunki płatności : **Płatne przelewem, 21 dni od daty otrzymania faktury.**
4. Osoba upoważniona do kontaktu z wykonawcami: **Przemysław Woźniczka**
   Tel. **124333935** e-mail **przemysław.wozniczka@kpr.med.pl**
5. Miejsce złożenia oferty: **filip.banas@kpr.med.pl**
   (~~*w formie **pisemnej***~~ / ***elektronicznej(e-mailem)*** **- niepotrzebne skreślić*
6. Termin złożenia oferty: data **12.05.2021** r, godzina: **14:00**
7. Ofertę należy przygotować w języku polskim.
8. Treść oferty musi zawierać co najmniej :
   1) nazwa wykonawcy;……..
   2) adres wykonawcy;……
   3) NIP;……..
   4) telefon,…… e-mail;…….
   5) termin realizacji zamówienia;
   6) okres gwarancji ; **Opisane szczegółowo w załączniku nr 1 do niniejszego zapytania**
   7) Oświadczenie ofertowe Wykonawcy:
   8) Oferuję wykonanie przedmiotu zamówienia za :
      Cenę netto …….. (za całość przedmiotu zamówienia)
      Podatek VAT …… (za całość przedmiotu zamówienia)
      Cenę brutto …… (za całość przedmiotu zamówienia)
   9) Wyrażam zgodę na warunki płatności określone w zapytaniu cenowym.

Z-ca Dyrektora
ds. Ekonomiczno-Administracyjnych
Marek Kobierz

…….
Podpis Zamawiającego

…….
podpis Wykonawcy

Kierownik
Działu Informatyki i Łączności
mgr inż. Filip Banaś

Formularz ofertowy

Załącznik nr 1

Opis przedmiotu zamówienia:

1. Przedmiot zamówienia:

Dostawa i wdrożenie urządzenia Firewall – NGFW (Router klasy UTM)

2. Szczegółowe parametry przedmiotu zamówienia:

Lp.	Parametry przedmiotu zamówienia	*Wpisać **TAK** lub **NIE**
	Urządzenie musi być dostarczone jako samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.	
	Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.	
	Urządzenie nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.	
	Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.	
	Urządzenie musi być wyposażone w dedykowany port zarządzania out-of-band.	
	Urządzenie musi zapewniać obsługę dla IPv6.	
	Urządzenie musi zapewnić możliwość statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.	
	Reguły zabezpieczeń firewall muszą być tworzone zgodnie z ustaloną polityką opartą o profile oraz obiekty.	
	Polityka zabezpieczeń firewall musi uwzględniać adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.	
	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.	
	Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.	
	Urządzenie musi działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (w warstwie 2 modelu OSI), w trybie transparentnym oraz trybie pasywnego nasłuchu. Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.	
	Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, 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.).	

	Zarządzanie systemem zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.	
	Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.	
	Urządzenie 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, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.	
	Urządzenie musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.	
	Urządzenie musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.	
	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.	
	Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.	
	Urządzenie musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym:	
	Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami.	
	Możliwość blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.	
	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.	
	Urządzenie musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.	
	Urządzenie musi posiadać możliwość automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.	
	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontunuowania lub zaniechania pobrania.	

	Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.	
	Urządzenie musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule YouTube, FaceBook itp.	
	Urządzenie musi zapewnić możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.	
	System zabezpieczeń firewall 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 wyłącznie na podstawie rozszerzenia.	
	Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.	
	Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.	
	Urządzenie 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 są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną).	
	Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN dla platform Windows, Mac oraz Android.	
	Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.	
	Urządzenie musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.	
	Urządzenie musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.	
	Urządzenie musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Raporty powinny być wbudowane w interfejs użytkownika i w pełni konfigurowalne. Generowane na podstawie zbieranych logów z możliwością dowolnego sortowania i grupowania oraz filtrowania wg dowolnych warunków np. użytkownik, IP, aplikacja itp. Urządzenie powinno pozwalać na generowanie raportów na podstawie wbudowanych szablonów. Możliwość skonfigurowania automatycznego wysyłania raportów na maile. Zbierane dane	

	powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.	
	Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.	
	Urządzenie musi być rozwiązaniem o uznanej na rynku pozycji i musi znajdować się w kwadracie „Leaders" lub „Challengers" raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls" w raportach opublikowanych w przeciągu 2 ostatnich lat.	
	Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.	
	Urządzenie musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.	
	Urządzenie nie może znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.	
	Serwis dostępu do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres **36** miesięcy.	
	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.	
	Rozwiązanie musi posiadać możliwość podłączenia urządzeń firewall pod scentralizowany system zarządzania pochodzący od tego samego producenta.	
	Urządzenie musi być dostarczone w konfiguracji z minimum 4 portami Ethernet 1Gb/s Rj45 10/100/1000, 4 portami typu SFP 1G i 4 portami SFP+.	
	Urządzenie musi posiadać redundantne zasilanie.	
	Urządzenie musi posiadać przepustowość w ruchu nie mniej niż 2 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 1,2 Gbps.	
	Urządzenie musi obsłużyć minimum 190 000 jednoczesnych sesji oraz 12 000 nowych połączeń na sekundę.	
	Urządzenie musi zapewniać wydajność przynajmniej 1,5 Gbps dla ruchu IPSec VPN.	
	Urządzenie musi umożliwiać zestawienie przynajmniej 2 000 równoczesnych tuneli site-to-site.	
	Urządzenie 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 firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention) i innego złośliwego kodu (wirusy, spyware, malware), filtracja plików, danych i URL.	
	Urządzenie musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia **na okres 36 miesięcy**	

	Urządzenie musi posiadać funkcjonalność definiowana i przydzielania różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia **na okres 36 miesięcy**	
	Urządzenie musi zapewniać zestawienie przynajmniej 200 sesji SSL VPN.	
	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów.	
	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność sterowania zachowaniem binarnego klienta VPN z poziomu systemu - połączenie automatyczne bądź ręczne przez użytkownika a także umożliwiać sprawdzenie czy klient posiada zainstalowane oprogramowanie antywirusowe.	
	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN.	
	Urządzenie musi posiadać funkcjonalność wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia **na okres 36 miesięcy.**	
	Urządzenie musi posiadać funkcjonalność uruchomienia inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia **na okres 36 miesięcy.**	
	Urządzenie musi posiadać funkcjonalność filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza przypisania URL do kategorii musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia **na okres 36 miesięcy.**	
	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.	
	Urządzenie musi posiadać moduł z sygnaturami DNS wykrywającymi blokującymi ruch do domen uznanych za złośliwe.	
	Urządzenie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików (przynajmniej exe, dll, pdf, jar, apk, pliki MS Office, ELF, BAT, JS, VBS, PS1, shell script, HTA, linki w wiadomościach e-mail) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Informacja zwrotna na temat wykrytego złośliwego oprogramowania musi zostać dostarczona na firewall w czasie nie dłuższym jak 5 minut. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików. Jeżeli funkcjonalność wymaga wykupienia dodatkowej licencji wtedy Zamawiający wymaga jej dostarczenia **na**	

	okres 36 miesięcy.	
	Urządzenie musi mieć możliwość przekierowania ruchu (PBR - policy based routing) dla wybranych aplikacji i konkretnych użytkowników z pominięciem tablicy routingu.	
	Urządzenie musi posiadać interfejs API który musi być jego integralną częścią i umożliwiać konfigurowanie i sprawdzanie stanu urządzenia bez użycia konsoli do zarządzania lub linii poleceń (CLI).	
	Urządzenie musi mieć możliwość wyboru sposobu blokowania ruchu w politykach bezpieczeństwa. Powinna istnieć możliwość ustawienia cichego blokowania ruchu bez wysyłania RST, blokowanie z wysłaniem RST tylko do klienta, blokowanie z wysłaniem RST tylko do serwera, blokowanie z wysłaniem RST do klienta i serwera jednocześnie.	
	Urządzenie 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 lub TACACS+, LDAP, Kerberos lub SAML 2.0	
	Rozwiązanie musi umożliwiać wykrywanie domen DGA i ruchu tunelowanego przez DNS. Jeżeli funkcjonalność ta wymaga dodatkowej licencji wtedy Zamawiający wymaga subskrypcji tej usługi na okres 36 miesięcy	
	Zezwolenie dostępu dla aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).	
	Urządzenie musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń.	
	Urządzenie 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.	
	Urządzenie musi posiadać funkcjonalność definiowania i przydzielania dla ruchu webowego odmiennych profili kontrolujących transfer różnych rodzajów plików lub profili ochrony typu AV, IPS, AS ze względu na kategorię URL.	
	Urządzenie 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.	
	Urządzenie musi posiadać funkcjonalność definiowania i przydzielania dla ruchu webowego odmiennych profili kontrolujących transfer różnych rodzajów plików lub profili ochrony typu AV, IPS, AS ze względu na kategorię URL.	
	Moduł filtrowania stron WWW musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.	
	Urządzanie musi umożliwiać zdefiniowanie stron WWW i serwisów do których	

	użytkownicy mogą wysyłać swoje poświadczenia Active Directory. W przypadku próby wysłania poświadczeń Active Directory do niezaufanej strony lub serwisu administrator może zdefiniować odpowiednią politykę blokującą dla takiego zdarzenia.	
	Urządzenie musi mieć możliwość tworzenia dynamicznych obiektów adresowych do których, na podstawie zdefiniowanych etykiet, można w automatyczny sposób przypisywać adresy IP. Powinna istnieć możliwość ręcznego tworzenia etykiet bezpośrednio na urządzeniu lub automatycznego pobierania ich z zewnętrznych systemów np. VMware vCenter lub ESX(i) oraz skojarzonych z tymi etykietami adresów IP. Powinna istnieć możliwość wykorzystania tak zbudowanych obiektów adresowych w politykach bezpieczeństwa.	
	Administrator urządzenia musi mieć możliwość zdefiniowania, dla każdej reguły bezpieczeństwa, innego serwera Syslog.	
	Zezwolenie dostępu dla aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).	

3. Kryteria wyboru oferty i testy:

Zamawiający będzie weryfikował parametry urządzeń na podstawie dokumentacji producenta przedstawionej przez Wykonawcę. Zamawiający zastrzega sobie także prawo do weryfikacji parametrów urządzeń na podstawie testów (decyzja o przeprowadzeniu testów zostanie podjęta podczas analizy otrzymanych ofert). Wszelkie testy będą przeprowadzone przez Wykonawcę na jego koszt i ryzyko. Każdy z wezwanych Wykonawców będzie miał możliwość okazania oferowanych urządzeń tylko jeden raz w terminie wyznaczonym przez Zamawiającego.
Zamawiający wymaga gotowości oferenta do przeprowadzenia testów w terminie nie dłuższym niż 14 dni kalendarzowych liczonym od dnia otwarcia ofert.
W przypadku podjęcia decyzji o przeprowadzeniu testów będą się one składały z dwóch części: funkcjonalnej oraz wydajnościowej z wykorzystaniem dedykowanego urządzenia typu appliance (generator ruchu) umożliwiającego wytworzenie ruchu o wymaganej charakterystyce i wolumenie (dokładne informacje zostaną podane na etapie wezwania do testów jeżeli będzie taka decyzja). Dodatkowo, Zamawiający zastrzega sobie prawo do zweryfikowania, że zaproponowane rozwiązanie spełnia minimalne wymagania funkcjonalne oraz opcjonalne właściwości zadeklarowane przez Wykonawcę.
Wykonawca w terminie wykonania testów musi dostarczyć kompletne środowisko testowe, w szczególności urządzenia i oprogramowanie składające się na oferowany system oraz wszelkie inne elementy konieczne do przeprowadzenia testów. Po wykonaniu testów Wykonawca zabierze dostarczone przez siebie na czas testów urządzenia.

4. Zakres usług wdrożeniowych:

W ramach wdrożenia wykonawca powinien wykonać:

1. Instalacje fizyczną sprzętu
2. Konfiguracje ustawień administracyjnych
3. Konfiguracje interfejsów, routingu, translacji NAT, stref bezpieczeństwa
4. Konfiguracje polityk bezpieczeństwa

5. Konfiguracje profili bezpieczeństwa (AV, URL filtering, IPS, sandbox, anti-spyware, kontrola przesyłania plików)
6. Integracje z AD
7. Konfiguracje tuneli VPN

Czynności powyższe powinny być wykonywane przy ścisłej współpracy z administratorami zamawiającego w taki sposób, aby zapewniły pełną obsługę sieci zamawiającego.

5. Terminy dostawy i harmonogram wdrożenia

Wykonawca dostarczy przedmiot umowy na własny koszt i ryzyko do siedziby Krakowskiego Pogotowia Ratunkowego, 31-530 Kraków ul. Łazarza 14, w terminie **do 60 dni kalendarzowych od daty podpisania umowy**. Wdrożenie powinno być zaplanowane i uzgodnione z zamawiającym i przeprowadzone **do 30 dni kalendarzowych od daty dostawy sprzętu**.

Plan wdrożenia musi obejmować:

a) przygotowanie wstępne,
b) okno serwisowe na wdrożenie poza godzinami pracy administracji,
c) 48 godzin okresu stabilizacji i pielęgnacji z całodobowym suportem wykonawcy,
d) 5 dni roboczych na obserwacje i odbiór konfiguracji przez zamawiającego.

Podpisanie protokołu końcowego nastąpi po pozytywnym zakończeniu wszystkich etapów wdrożenia.

Wszystkie prace wdrożeniowe skutkujące niedostępnością sieci w budynku przy ulicy Łazarza 14 w Krakowie muszą być wykonywane po zakończeniu pracy administracji KPR (tj. poza godzinami 7:00 - 14:35).

W okresie **48 godzin od zakończenia wdrożenia** tj. w okresie stabilizacji i pielęgnacji nowej konfiguracji, wykonawca zapewnieni **support 24h/dobę** w usuwaniu awarii krytyczny związanych z działaniem usług zdefiniowanych wcześniej przez Zamawiającego.

6. Kary umowne:

a) Za niedotrzymanie terminu dostawy zamawiający może naliczyć kary umowne w wysokości 0,5% wartości umowy za każdy rozpoczęty dzień zwłoki licząc od następnego dnia po terminie, w którym miała być dokonana dostawa.
b) Za zwłokę w usunięciu awarii lub uszkodzenia, za każdy rozpoczęty dzień zwłoki w wysokości 0,5 % wartości jednostkowej brutto przedmiotu zamówienia.
c) w przypadku odstąpienia od umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy karę w wysokości 10% ceny (zawierającej podatek VAT) przedmiotu umowy.

7. Gwarancja i warunki Serwisu;

1. Wykonawca zapewni 40h konsultacji zdalnych w okresie 12 miesięcy od zakończenia wdrożenia w dniach roboczych od poniedziałku do piątku.

2. Gwarancja i wsparcie producenta powinna być świadczone przez autoryzowany serwis producenta w Polsce lub bez[pośrednio przez producenta **przez okres 36 miesięcy.**
    a. Zgłaszanie problemów w dni robocze (8:00-17:00)
    b. Zgłaszanie problemów krytycznych również w dni wolne od pracy i po godzinach pracy
    c. Czasy obsługi zgłoszeń:
        i. Krytyczny do 1 godziny
        ii. Wysoki do 2 godzin w dni i godziny robocze
        iii. Średni do 4 godzin w dni i godziny robocze
        iv. Niski do 8 godzin w dni i godziny robocze
    d. Wymiana uszkodzonego sprzętu w następnym dniu roboczym pod warunkiem przyjęcia zgłoszenie do godziny 14:00
    e. Dostęp do bazy wiedzy producenta

Oświadczam, że zaoferowany przedmiot zamówienia spełnia wszystkie wymagania przedstawione w niniejszym formularzu ofertowym.

.....
podpis Wykonawcy

Kierownik
Działu Informatyki i Łączności
mgr inż. Filip Banaś