Nr sprawy : XXI-042-1-31/2022 Data: 23-06-2022r.

ZAPYTANIE CENOWE

Zamawiający – Krakowskie Pogotowie Ratunkowe zaprasza do złożenia oferty na :

1. Przedmiot zamówienia (opis) : **Zakup 11 sztuk Routerów/Firewall klasy NGFW do oddziałów.**

2. Inne wymogi szczególne:

Urządzenie PaloAlto PA-440 lub równoważne w pełni kompatybilne z urządzeniem PaloAlto PA-850 zainstalowanym w siedzibie głównej, spełniające następujące parametry:

Lp.	Opis wymaganego parametru
1	Zamawiający wymaga, aby zaoferowane urządzenia były uznanymi rozwiązaniami na świecie – producent zaoferowanego rozwiązania musi być notowany w raportach Gartnera dla rozwiązań Enterprise Network Firewall nie starszych niż 2 lata przed złożeniem oferty. Jako równoważny dla raportu Gartnera Zamawiający dopuści również inny raport udostępniany publicznie, powszechnie akceptowany, mający charakter zewnętrznego i obiektywnego raportu standaryzacyjnego, który zapewnia analizę, wgląd w kierunek oraz dojrzałość uczestników rynku w rozwiązaniach typu Network Firewall, aktualizowany co roku od min. 20 lat.
2	Klasa urządzenia: specjalizowane urządzenia sieciowe (tzw. appliance) mogące pracować jako pojedyncze urządzenie oraz jako klaster wysokiej dostępności (HA) w trybie Active/Standby.
3	Całość sprzętu i oprogramowania musi być dostarczona i wspierana przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat.
4	Urządzenia muszą umożliwiać działanie w następujących trybach pracy: a. rutera (tzn. w warstwie 3 modelu OSI), b. mostu (tzn. w warstwie 2 modelu OSI), c. w trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych; Musi pracować w trybie przezroczystego łączenia interfejsów w pary.). d. w trybie pasywnego nasłuchu (sniffer/tap).
5	System musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu.
6	Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 oraz w co najmniej jeden dedykowany port ethernet 10/100/1000 na cele zarządzania out-of-band.
7	Urządzenia firewall muszą posiadać logiczną separację zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
8	Urządzenia firewall muszą posiadać dedykowane zasoby procesora (CPU) do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania urządzeniem.
9	Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.
10.	Urządzenia firewall muszą wspierać protokół LACP.
11.	Urządzenia firewall muszą zgodnie z ustaloną polityką prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
12.	Urządzenia firewall muszą działać zgodnie z zasadą bezpieczeństwa najmniejszego możliwego przywileju. Musi blokować wszystkie aplikacje i ruch sieciowy, poza tymi które w regułach polityki bezpieczeństwa skonfigurowanych na firewall są wskazane jako dozwolone.
13.	Polityka zabezpieczeń firewall musi uwzględniać a. adresy IP źródłowe i docelowe, b. protokoły i usługi sieciowe, c. aplikacje, d. kategorie URL,

	e. użytkowników aplikacji i grupy, f. reakcje zabezpieczeń, g. logowanie zdarzeń (początek i koniec sesji) h. strefa wejściowa i wyjściowa
14.	Urządzenia firewall muszą automatycznie identyfikować aplikacje bez względu na numery portów (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Urządzenie musi wykrywać co najmniej 3300 predefiniowanych aplikacji wspieranych przez producenta wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. Muszą pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na GUI urządzenia (bez użycia zewnętrznych narzędzi).
15.	Urządzenia firewall muszą pozwalać na blokowanie transmisji plików, nie mniej niż: .pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk, szyfrowany MS Office, szyfrowany RAR, szyfrowany ZIP. Rozpoznawanie pliku musi odbywać się na podstawie zawartości i metadanych pliku.
16.	Urządzenia firewall muszą zarządzane z linii poleceń (CLI) oraz graficznej konsoli Web GUI. Nie jest dopuszczalne, aby istniała konieczność instalacji dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.
17.	Urządzenia firewall muszą być wyposażone w interfejs API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
18.	Dostęp do urządzeń i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
19.	Urządzenia firewall muszą umożliwiać uwierzytelnianie administratorów za pomocą nie mniej niż: baza lokalna, serwer Radius, serwer TACACS+, serwer AD/LDAP. Dla dostępu administracyjnego SSH musi być wspierane uwierzytelnianie za pomocą kluczy SSH a dla dostępu GUI za pomocą certyfikatów kryptograficznych.
20.	Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie z systemami: a. Active Directory, b. Terminal Services c. Syslog
21.	Polityka kontroli dostępu (urządzeń firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym mających wspólny adres IP źródłowy, ustalanie tożsamości musi odbywać się również transparentnie.
22.	Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL.
23.	Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.
24.	Urządzenia firewall muszą umożliwiać tworzenie dynamicznych grup użytkowników. Przynależność do grupy musi bazować na etykietach a proces oznaczania etykietami musi pozwalać na użycie: a. reakcji na zdarzenie/log (np. wystąpienie zagrożenia) b. API
25.	Urządzenia firewall muszą posiadać funkcję dynamicznego pobierania i odświeżania informacji o zasobach VM i ich adresach IP i etykietach (tagi) dla środowiska VMWare vCenter. Tak pobierane adresy IP muszą pozwalać na budowanie dynamicznych obiektów, które można potem wykorzystywać w polityce bezpieczeństwa urządzeń.
26	Urządzenia firewall muszą obsługiwać protokoły routingu dynamicznego, minimum: BGP i OSPF dla IPv4 i IPv6.
27.	Urządzenia firewall muszą obsługiwać 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.
28.	Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
29.	Wykonywanie operacji translacji adresów NAT musi być odnotowywane w logach ruchu sieciowego za pomocą dedykowanego pola lub flagi oraz odpowiednich kolumn ze szczegółami NAT.
30.	Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju.

31.	Urządzenia firewall muszą obsługiwać możliwość deszyfrowania ruchu użytkowników w celu inspekcji dla protokołów HTTP/2, SSL, TLS 1.2, TLS 1.3.
32.	Urządzenia firewall muszą posiadać możliwość zdefiniowania ruchu SSL/TLS, który należy poddać lub wykluczyć z operacji deszyfrowania i inspekcji rozdzielny od polityk bezpieczeństwa.
33.	Wykonywanie operacji deszyfrowanie ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji. Musi zawierać informacje ułatwiające diagnostykę m.in. informacje o błędach, typ i rozmiar klucza, wersja TLS. Musi istnieć mechanizm automatycznego wykluczania z szyfrowania problematycznych stron na bazie tego logu.
34.	Wykonywanie operacji deszyfrowania ruchu musi umożliwiać wykorzystanie mechanizmów filtrowania URL.
35.	Urządzenia firewall muszą posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
36.	Urządzenia firewall muszą wspierać zarządzanie pasmem (QoS) i ustawiania dla aplikacji priorytetu oraz pasma.
37.	Urządzenia firewall muszą 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 trasowania (tzw. routing-based VPN).
38.	Dla IKE wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
39.	Dla IPsec wymagane jest wsparcie AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, grupy Diffie-Hellman 14,19,20.
40.	Urządzenia firewall muszą zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell).
41.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję wykrywania i blokowania ataków/intruzów w warstwie 7 modelu OSI (IPS). Baza sygnatur takiego modułu musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. W obecnym postepowaniu licencja nie jest wymagana.
42.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję inspekcji antywirusowej uruchamianą per aplikacja/polityka oraz wybrany protokół minimum: http, http2, smtp, imap, pop3, ftp, smb. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż raz na 24 godziny i pochodzić od tego samego producenta co firewall. W obecnym postepowaniu licencja nie jest wymagana.
43.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję anty-spyware. Baza sygnatur musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co systemu firewall. W obecnym postepowaniu licencja nie jest wymagana.
44.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję filtrowania URL w oparciu o kategorie związane z treścią oraz poziomem ryzyka. Baza kategorii URL musi pochodzić od tego samego producenta. W obecnym postepowaniu licencja nie jest wymagana.
45.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o funkcję przechwytywania i przesyłania do zewnętrznego systemu sandbox plików wykonywalnych PE, DLL, ELF oraz JAR przechodzących przez firewall. Systemy sandbox, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików, adresów IP, DNS i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik. W obecnym postepowaniu licencja nie jest wymagana.
46.	Urządzenia firewall muszą mieć możliwość licencyjnego rozszerzenia o ochronę DNS w zakresie: a. możliwości skonfigurowania fałszowania odpowiedzi na zapytania DNS zaklasyfikowane jako niebezpieczne (tzw. DNS sinkholing), b. wykrywania domen generowanych dynamicznie przez złośliwe oprogramowanie w celu uniknięcia wykrycia kanałów komunikacyjnych (tzw. domeny DGA), c. wykrywanie domen dynamicznych Dynamic DNS, d. wykrywania nadużyć protokołu DNS w celu infiltracji i eksfiltracji danych. W obecnym postepowaniu licencja nie jest wymagana.
47.	Urządzenia firewall muszą obsługiwać funkcjonalność zdalnego dostępu VPN dla użytkowników (tzw. Remote Access VPN). Funkcja ta musi być realizowana na bazie technologii SSL VPN oraz IPSec. Jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz co najmniej dla 1000 użytkowników. Oprogramowanie klienta Remote Access VPN musi pochodzić od tego samego producenta i być objęte wsparciem technicznym producenta w takim samym okresie jak okres wsparcia technicznego, którym będzie objęty firewall.
48.	Funkcjonalność zdalnego dostępu VPN musi integrować się z funkcją rozpoznawania użytkowników.
49.	W przypadku gdy jakakolwiek funkcjonalność (włącznie z klientem Remote Access VPN) lub parametr ilościowy wymagają licencji, Zamawiający wymaga ich dostarczenia w celu zapewnienia pełni wymaganych właściwości przez okres 12 miesięcy od daty odbioru sprzętu.

50.	Wsparcie serwisowe (techniczne) i gwarancja dla systemu (zwana dalej wsparciem) będzie świadczone przez producenta lub autoryzowane przez producenta centrum serwisowe, niezależne od Wykonawcy, realizowane we współpracy z producentem, przez okres 12 miesięcy od daty odbioru sprzętu.
51.	Urządzenie musi być wyposażone w minimum: a. 8 wbudowanych interfejsów 10/100/1000 Ethernet (RJ45)
52.	Urządzenie musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 120 GB na potrzeby systemu operacyjnego, logów i nagrywania pakietów.
53.	Urządzenie musi być wyposażone w co najmniej dwa zasilacze AC.
54.	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: a. Minimum 2,4 Gbps dla rozpoznawania i kontroli aplikacji, b. Minimum 1 Gbps dla rozpoznawania kontroli aplikacji przy włączonych co najmniej następujących funkcjach bezpieczeństwa: IPS, Anty-wirus, Anty-spyware, blokowanie typów plików i z włączonym logowaniem na dysk urządzenia. Funkcje bezpieczeństwa muszą być skonfigurowane w trybie gwarantującym najwyższy poziom ochrony (włączone wszystkie sygnatury IPS i wszystkie sygnatury AV) c. Minimum 39 000 nowych sesji na sekundę. d. Minimum 200 000 równoległych sesji
55.	Urządzenie musi obsługiwać nie mniej niż 3 wirtualne routery 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.
56.	Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 2000 reguł polityki bezpieczeństwa.

3. Warunki płatności : **Przelew 14 dni od daty dostarczenia faktury**
4. Osoba upoważniona do kontaktu z wykonawcami : **Filip Banaś**

   Tel. **607744909** e-mail: **filip.banas@kpr.med.pl**
5. Sposób/Miejsce złożenia oferty: **Ofertę należy przesłać mailem na adres filip.banas@kpr.med.pl. *(Skan podpisanego dokumentu w pdf lub oferta w pdf opatrzona podpisem kwalifikowanym lub podpisem zaufanym)***
6. Do oferty należy załączyć:
   a. **Formularz ofertowy**
   b. **Oświadczenie sankcyjne.**
7. Termin złożenia oferty: **najpóźniej dnia: 30.06.2022, do godziny: 12:00**
8. Ofertę należy przygotować w języku polskim.
9. Złożone oferty mogą podlegać dodatkowo negocjacjom.
10. Z wybranym wykonawcom zostanie podpisana Umowa.

Załączniki:
Załącznik nr 1 – formularz ofertowy
Załącznik nr 2 – oświadczenie sankcyjne

Dyrektora
ds. Ekonomiczno-Administracyjnych
Piotr Wüsterz

.....
Podpis Zamawiającego

Kierownik
Działu Informatyki i Łączności
mgr inż. Filip Banaś