ZAPYTANIE OFERTOWE

z dnia 16.06.2025 r., l.dz. 01_06_2025_FEWiM_VM

wersja 1

Spis treści:

A. Informacje podstawowe - część metrykalna

A.1. Informacje o projekcie

Zamówienie jest realizowane w ramach projektu: System informacji przestrzennej do zarządzania infrastrukturą, nr wniosku o dofinansowanie: FEWM.01.12-IP.02-0026/24, program: Fundusze Europejskie dla Warmii i Mazur.

A.2. Oznaczenie zamówienia we wspólnym słowniku CPV

32420000-3 Urządzenia sieciowe
48219100-7 Pakiety oprogramowania bramowego
48732000-8 Pakiety oprogramowania do zabezpieczania danych

A.3. Zamawiający

VIMAP Sp. z o.o.
ul. Dworcowa 3, 10-413 Olsztyn
NIP 8733256604

A.4. Sposób komunikacji

Zgodnie z wytycznymi, głównym kanałem komunikacji między Zamawiającym a Wykonawcami jest Baza Konkurencyjności 2021 (BK2021). Ogłoszenie zapytań ofertowych, składanie ofert, pytania i odpowiedzi, wymiana informacji oraz przekazywanie dokumentów i oświadczeń do czasu zakończenia postępowania, odbywa się wyłącznie za pomocą tej platformy, chyba, że platforma nie posiada funkcjonalności/możliwości technicznych w tym zakresie. Wówczas dopuszcza się tradycyjne formy komunikacji: e-mail, poczta, zgodne ze wskazanymi przez Wykonawcę w Formularzu ofertowym.

A.5. Miejsce i termin złożenia oferty

1. Ofertę można złożyć wyłącznie za pośrednictwem platformy Baza konkurencyjności 2021.
2. Ostateczny termin składania ofert upływa:
   25.06.2025 r., godz. 12.00.

A.6. Wykaz i zakres zmian

Nie dotyczy. Wersja 1 postępowania.

A.7. Podstawa i tryb postępowania

Wytyczne dotyczące kwalifikowalności wydatków na lata 2021-2027, Zasada konkurencyjności,
https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/dokumenty/wytyczne-dotyczace-kwalifikowalnosci-2021-2027

B. Opis przedmiotu zamówienia

B.1. Nazwa nadana zamówieniu

Dostawa infrastruktury sieciowej w postaci firewall wraz z systemem ochrony aplikacji webowych oraz API.

B.2. Rodzaj zamówienia

Dostawa.

B.3. Przedmiot zamówienia (charakterystyka, specyfikacja, funkcjonalności, ilości)

Przedmiotem zamówienia jest dostawa infrastruktury sieciowej w postaci firewall wraz z systemem ochrony aplikacji webowych oraz API, zwana w dalszej części również „przedmiotem zamówienia" lub „infrastrukturą sieciową" lub „systemem" według następującej specyfikacji:

1. Zakres dostawy obejmuje firewall i system ochrony aplikacji webowych oraz API. Oba systemy muszą mieć wspólną platformę logowania oraz wspólną platformę raportowania dla przyjmowania nie mniej niż 500mb logów dziennie. Dostarczona platforma ma być w postaci maszyny wirtualnej.
   Urządzenia muszą być nowe. Nie dopuszcza się rozwiązań powystawowych, demonstracyjnych lub po naprawach.
2. **Wymagania, funkcjonalności i specyfikacja dla firewall:**

2.1. Wymagania Ogólne:
   1) System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
   2) System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.
   3) System wspiera protokoły IPv4 oraz IPv6 w zakresie:
      a) Firewall.
      b) Ochrony w warstwie aplikacji.

2.2. Redundancja:
   1) System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

2.3. Interfejsy, Dysk, Zasilanie:
   1) System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
      a) 10 portami Gigabit Ethernet RJ-45.
      b) 8 gniazdami SFP 1 Gbps.
      c) 4 gniazdami SFP+ 10 Gbps.
   2) System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.
   3) System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
   4) System jest wyposażony w zasilanie AC.

2.4. Parametry wydajnościowe:
   1) W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.
   2) Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B.
   3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
   4) Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 33 Gbps.
   5) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla

środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 5 Gbps.

2.5. Funkcje Systemu Bezpieczeństwa:

1) W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
   a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
   b) Kontrola Aplikacji.
   c) Ochrona przed atakami - Intrusion Prevention System.
   d) Kontrola stron WWW.
   e) Zarządzanie pasmem (QoS, Traffic shaping).
   f) Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.

2.6. Polityki Firewall:

1) Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2) System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   a) Translację jeden do jeden oraz jeden do wielu.
   b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3) Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

2.7. Połączenia VPN:

1) System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   a) Wsparcie dla IKE v1 oraz v2.
   b) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   c) Obsługa protokołu Diffie-Hellman grup 19, 20.
   d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
   e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.

2.8. Routing i obsługa łączy WAN:

1) W zakresie routingu rozwiązanie zapewnia obsługę:
   a) Routingu statycznego.
   b) Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego).
   c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
   d) Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
   e) ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
   f) BFD (Bidirectional Forwarding Detection).
   g) Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

2.9. Funkcje SD-WAN:

1) System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2) SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

2.10. Zarządzanie pasmem:
1) System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2) System daje możliwość określania pasma dla poszczególnych aplikacji.
3) System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4) System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

2.11. Ochrona przed malware:
1) Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2) Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.

2.12. Ochrona przed atakami:
1) Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2) System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3) Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

2.13. Kontrola aplikacji:
1) Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2) Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

2.14. Kontrola WWW:
1) Moduł kontroli WWW korzysta z bazy adresów URL pogrupowanych w kategorie tematyczne.
2) Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
3) Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).

2.15. Zarządzanie:
1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2) Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.

3. Wymagania, funkcjonalności i specyfikacja dla systemu ochrony aplikacji webowych oraz API:

3.1. Architektura systemu:

1) Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi, Amazon AWS, Citrix XenServer, Google Cloud Platform, Linux KVM, Microsoft Azure, Microsoft Hyper-V Server, Nutanix AHV, OpenSource XenServer, Oracle Private Cloud.
2) Dla zapewnienia bezpieczeństwa ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie.
3) Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
4) Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web.
5) Powinna istnieć możliwość zdefiniowania co najmniej 64 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami systemu.
6) System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.

3.2. Wirtualne zasoby sprzętowe:

1) System musi obsługiwać co najmniej: 4 interfejsy sieciowe, 2 wirtualne procesory oraz 8 GB pamięci RAM.

3.3. Parametry wydajnościowe

1) Przepustowość dla ruchu http - min 100 Mbps.

3.4. Wymagane podstawowe funkcje systemu:

1) Obsługa protokołów: HTTP 1.1, HTTP 2.0, FTP.
2) Wsparcie dla mechanizmów session persistence:
   a) Source IP
   b) HTTP Header
   c) URL parameter
   d) Insert Cookie
   e) Rewrite Cookie
   f) Persistent Cookie
   g) Embedded Cookie
   h) ASP Session ID
   i) PHP Session ID
   j) JSP Session ID
   k) SSL Session ID
3) Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3.
4) Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa.
5) Ochrona aplikacji www przed takimi zagrożeniami jak:
   a) SQL and OS Command Injection.
   b) Cross Site Scripting (XSS).

c) Cross Site Request Forgery.
d) DoS w warstwie aplikacji.
e) Ochrona przed atakami typu Brute force.

6) Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację.
7) Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
8) Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy.
9) Wsparcie dla kompresji danych oraz cache.
10) Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3.
11) Ochrona przed atakami typu SLOW (Slowloris i podobne).
12) Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For".
13) Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload'u HTML.
14) Wsparcie dla walidacji OpenAPI, JSON i XML.
15) Blokowania „Illegal XML Format" oraz „Illegal JSON Format".
16) Ochrona przed atakami MiTB (Man-in-the-Browser) przynamniej dla Anti-keylogger, Obfuscate.
17) System musi posiadać możliwość automatycznego uczenia się działania aplikacji w zakresie:
    a) Obserwacji i budowania profilu dla URL, parametrów, metod HTTP, sesji HTTPS. Obserwacje powinny uczyć model matematyczny normalnych zachowań, który następnie umożliwi wykrywanie anomalii.
    b) Wyuczony model matematyczny wykrywa odstępstwa od normy w obserwowanych elementach.
    c) System automatycznie wykrywa zmiany po stronie aplikacji lub zachowania użytkowników i ponawia proces uczenia.
    d) Możliwe jest zdefiniowanie wyjątków, które nie będą brały udziału w uczeniu modelu matematycznego.
    e) Musi istnieć możliwość strojenia czułości modelu wykrywającego anomalie przez administratora systemu. Poziom czułości musi być ustawiany globalnie dla aplikacji jak i na poziomie pojedynczych parametrów.
18) System ochrony aplikacji musi być wyposażony w mechanizm wykrywania komunikacji pochodzącej od internetowych bot'ów. Wykrywanie musi być oparte co najmniej o następujące mechanizmy:
    a) Reputacja adresów IP.
    b) Sygnatury.
    c) Wartości progowe generowanego ruchu.
    d) Monitorowanie biometryczne – obserwowanie zdarzeń związanych z ruchem myszy, klikiem myszy, zdarzeń klawiatury, przewijania, sterowania dotykiem.
    e) Uczenie maszynowe: powinno działać w trybie nauki modelu matematycznego standardowego zachowania użytkowników. Po zebraniu informacji system powinien przejść do trybu ochrony, gdzie wykrycie zachowania odbiegającego od normy powinno skutkować uznaniem źródła za automat.

3.5. Wymagane dodatkowe funkcje systemu:

1) Kontrola antywirusowa dla komunikacji HTTP realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół ICAP. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze w celu rozpoznawania nieznanych dotąd zagrożeń.
2) System ochrony musi posiadać własny, wbudowany skaner podatności aplikacji www. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje, support) niezbędne do uruchomienia tej funkcjonalności. Zakres skanowania musi obejmować co najmniej:
3) Podatności związane z typowymi atakami jak na przykład Blind SQL Injection; BufferOverflow Attack; CORS Origin; CSRF, Cross Site Scripting, SQL Injection.
4) Ataki Brute Force co najmniej dla uwierzytelnienia podstawowego oraz w postaci formularza HTML.
5) W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji dla nielimitowanej ilości skanowanych aplikacji.
6) Dekodowanie Base64 oraz CSS.
7) Rozpoznawanie i możliwość śledzenia prawidłowo zalogowanych użytkowników do chronionej aplikacji (User Tracking).
8) Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, intefejsu API - przy zastosowaniu funkcji biometrycznych.
9) Cross-Origin Resource Sharing (CORS) protection.

3.6. Zarządzanie:

1) Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.

B.4. Składanie ofert częściowych

Zamawiający nie przewiduje możliwości składania ofert częściowych.

B.5. Podział zamówienia na części (informacja o pozostałych postępowaniach)

Przedmiotowe postępowanie obejmuje część zamówienia. Pozostałe części, zamawiane odrębnym/i postępowaniem/i, dotyczą dostawy: **Oprogramowanie moduł paszportyzacji, Infrastruktura sieciowa – serwer, macierz dyskowa. Zamówienie planowane do przeprowadzenia w 2025 roku. Zamówienia przekraczające wartość 80 tyś. zł netto będą publikowane w Bazie konkurencyjności.**

B.6. Składanie ofert wariantowych

Zamawiający nie przewiduje możliwości składania ofert wariantowych.

C. Wymagania związane z jego realizacją zamówienia oraz projektowane postanowienia umowy (tzw. OWH/OWD)

C.1. Dodatkowe obowiązki Wykonawcy

1. Jeżeli dla uzyskania i korzystania z jakiekolwiek funkcjonalności wskazanej w opisie przedmiotu zamówienia wymagane jest posiadanie przez Zamawiającego licencji (w tym

licencji od podmiotów trzecich), Wykonawca zobowiązany jest wraz z dostawą przekazać wymagane licencje, bez dodatkowego wynagrodzenia (winny być ujęte w cenie dostawy).
2. Zakres dostawy po stronie Wykonawcy obejmuje również:
    1) Instalację przedmiotu zamówienia u Zamawiającego
    2) Instruktaż z obsługi, na miejscu u Zamawiającego, min. 3 dni po 8 godzin (1h = 45 minut)

C.2. Obowiązki Zamawiającego

1. Nie dotyczy.

C.3. Miejsce dostawy/realizacji

Adres: ul. Dworcowa 3, 10-413 Olsztyn , woj. warm.-maz., Polska.

C.4. Termin realizacji zamówienia i odbiory

1. Do 4 tygodni. Termin liczony jest w pełnych tygodniach liczonych od pierwszego poniedziałku po podpisaniu Umowy.
2. Umowa winna być podpisana w terminie do 7 dni roboczych od daty wyboru oferty.
3. Za termin wykonywania zamówienia uznaje się datę podpisania protokołu zdawczo-odbiorczego.
4. W przypadku opóźnienia w dostarczeniu przedmiotu zamówienia powyżej 30 dni, Zamawiający ma prawo rozwiązać umowę z zachowaniem jednomiesięcznego terminu wypowiedzenia. Wówczas Wykonawca zobowiązany jest do zwrotu otrzymanej zaliczki, zwrot w terminie do 14 dni od daty wezwania do zwrotu.
5. W przypadku opóźnień w płatnościach z winy Zamawiającego, Wykonawca ma prawo wydłużyć termin dostawy, adekwatnie do opóźnień w płatnościach.

C.5. Warunki płatności

Nie przewiduje się płatności zaliczkowych.
Płatność po dostawie, na podstawie dostarczonych Zamawiającemu prawidłowo wystawionych dokumentów księgowych (faktura lub inny równoważny) z terminem płatności do 21 dni.

C.6. Okres i warunki gwarancji oraz serwisu

1. Na dostarczany przedmiot zamówienia wymagana jest gwarancja producenta udzielona na okres minimum 36 miesięcy, obejmująca naprawę lub wymianę przedmiotu zamówienia w przypadku jego wadliwości.
2. Naprawa lub wymiana winna zostać zrealizowana w terminie do 30 dni od daty zgłoszenia reklamacji przez Zamawiającego.
3. W okresie gwarancji Zamawiający ma prawo, bez dodatkowego wynagrodzenia lub opłat, do wszystkich aktualizacji oprogramowania wprowadzanych przez producenta, które bezpośrednio dotyczą przedmiotu zamówienia.

C.7. Kary umowne

1. Nie przewiduje się.

C.8. Zasady podwykonawstwa

Zamawiający nie zastrzega, że Wykonawca ma obowiązek osobistego wykonania kluczowych części zamówienia. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy.

Za działania i zaniechania podwykonawców Wykonawca odpowiada jak za własne.

C.9. Wymagania dotyczące zabezpieczenia należytego wykonania umowy

Nie przewiduje się.

C.10. Dopuszczone warunki zmian umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego

1. Zamawiający przewiduje możliwość dokonania istotnych zmian postanowień zawartej umowy w zakresie:
   a) przesunięcia terminów, zmian sposobu lub zakresów wykonania przedmiotu zamówienia, umożliwiające dalsze prawidłowe wykonanie umowy, w uzasadnionym przypadkach wynikających z:
      - siły wyższej uniemożliwiającej wykonanie przedmiotu zamówienia (za siłę wyższą uznawane będą zdarzenia takie jak wojna, atak terrorystyczny, katastrofa, stan klęski żywiołowej, zamieszki, strajki, pożar, epidemie, na które Strony nie mają wpływu),
      - zmian powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację Umowy,
      - działań organów administracyjnych,

      w zakresie adekwatnym i proporcjonalnym do okoliczności,
   b) przesunięcia terminów realizacji przedmiotu umowy, przy czym zmiana spowodowana może być okolicznościami leżącymi wyłącznie po stronie Zamawiającego, takimi jak: awaria sprzętu, na którym instalowane będą systemy, konieczność dostosowania parametrów technicznych posiadanego sprzętu, awaria posiadanych systemów/urządzeń i lub baz danych, z którymi wdrażane systemy będą integrowane, powiązane, lub przenoszone, odpowiednio do powstałego opóźnienia,
   c) pojęć, definicji, użytych określeń, które przyczynią się do powstania rozbieżności lub niejasności w rozumieniu pojęć użytych w Umowie, których nie będzie można usunąć w inny sposób, a zmiana będzie umożliwiać usunięcie rozbieżności i doprecyzowanie Umowy w celu jednoznacznej interpretacji jej postanowień przez Strony,
   d) zmian sposobu lub zakresów wykonania przedmiotu zamówienia, wyłącznie za zgodą Zamawiającego, jeżeli dotyczą one możliwych do wykonania proponowanych przez Wykonawcę rozwiązań alternatywnych, które charakteryzują się lepszymi parametrami lub funkcjonalności względem pierwotnie określonych w zamówieniu lub są konieczne z przyczyn technicznych do prawidłowego wykonania przedmiotu zamówienia (np. zmiana technologii, kompatybilność z urządzeniami technicznymi, dostosowanie do nowszych wersji środowisk programistycznych i użytkowych); zmiana taka uzasadnia również wydłużenie terminu realizacji, adekwatnie do czasu niezbędnego do zrealizowania uaktualnionego zamówienia;
   e) zmiany osoby lub osób wskazanych przez Wykonawcę w ofercie, jako osoby wskazane przy warunkach dostępu, pod warunkiem, że nowe wskazane osoby, będą spełniały warunki, o których mowa w kryterium dostępu,

f) oznaczenia danych dotyczących Zamawiającego i/lub Wykonawcy,
g) dodatkowych dostaw, usług lub robót budowlanych, nieobjętych zamówieniem podstawowym, o ile stały się niezbędne (i niemożliwe do przewidzenia przez Wykonawcę na etapie ofertowania – w innym przypadku patrz: zasady ustalenia ceny i wynagrodzenia ryczałtowego), o ile zostały spełnione łącznie następujące warunki:
   - zmiana Wykonawcy nie może zostać dokonana z powodów ekonomicznych lub technicznych, w szczególności dotyczących zamienności lub interoperacyjności sprzętu, usług lub instalacji, zamówionych w ramach zamówienia podstawowego,
   - zmiana wykonawcy spowodowałaby istotną niedogodność lub znaczne zwiększenie kosztów dla Zamawiającego,
   - wartość zmian nie przekracza 50% wartości zamówienia określonej pierwotnie w umowie.

2. Wprowadzenie zmiany postanowień umowy wymaga zatwierdzenia obu Stron i zachowania formy pisemnej pod rygorem nieważności.

D. Wykluczenia i warunki udziału w postępowaniu

D.1. Informacje na temat zakresu wykluczenia i zakaz konfliktu interesów

1. Zamówienia nie mogą być udzielane podmiotom powiązanym osobowo lub kapitałowo. Powyższe należy rozumieć jako brak istnienia albo brak wpływu powiązań osobowych lub kapitałowych między Zamawiającym (w tym osobami zaangażowanymi w czynności związane z przygotowaniem oraz przeprowadzeniem postępowania) a Wykonawcą, które mogłyby wpłynąć na bezstronność postępowania, a polegających na:
   a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej, posiadaniu co najmniej 10% udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa), pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
   b) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związaniu z tytułu przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia,
   c) pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.
2. Wykonawcą zamówienia nie może być Wykonawca wykluczony na mocy art. 1 pkt 23 rozporządzenia 2022/576 do rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1), zakazuje się udzielania lub dalszego wykonywania wszelkich zamówień publicznych lub koncesji objętych zakresem dyrektyw w sprawie zamówień publicznych, a także zakresem art. 10 ust. 1, 3, ust. 6 lit. a)–e), ust. 8, 9 i 10, art. 11, 12, 13 i 14 dyrektywy 2014/23/UE, art. 7 i 8, art. 10 lit. b)–f) i lit. h)–j) dyrektywy 2014/24/UE, art. 18, art. 21 lit. b)–e) i lit. g)–i), art. 29 i 30 dyrektywy 2014/25/UE oraz art. 13 lit. a)–d), lit. f)–h) i lit. j) dyrektywy 2009/81/WE na rzecz lub z udziałem:

a) obywateli rosyjskich lub osób fizycznych lub prawnych, podmiotów lub organów z siedzibą w Rosji;
b) osób prawnych, podmiotów lub organów, do których prawa własności bezpośrednio lub pośrednio w
c) ponad 50 % należą do podmiotu, o którym mowa w lit. a) niniejszego ustępu; lub
d) osób fizycznych lub prawnych, podmiotów lub organów działających w imieniu lub pod kierunkiem podmiotu, o którym mowa w lit. a) lub b) niniejszego ustępu, w tym podwykonawców, dostawców lub podmiotów, na których zdolności polega się w rozumieniu dyrektyw w sprawie zamówień publicznych, w przypadku gdy przypada na nich ponad 10 % wartości zamówienia.

3. Weryfikacja braku podstaw do wykluczenia Wykonawcy z postępowania, w tym braku konfliktu interesów, odbywa się na podstawie Oświadczenia o braku podstaw do wykluczenia – Załącznik nr 2 do niniejszego zapytania ofertowego.

D.2. Warunki udziału w postępowaniu (tzw. kryteria dostępu)

O udzielenie zamówienia publicznego ubiegać się mogą Wykonawcy, którzy posiadają niezbędną wiedzę i doświadczenie do wykonania zamówienia.
Wykonawca musi spełniać następujące warunki:

1. **W zakresie wiedzy i doświadczenia:**
   - w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, zrealizował w sposób należyty **min. 2 zamówienia (dostawy) urządzeń typu firmewall wraz z Systemem ochrony aplikacji webowych o wartości minimum 80 000,00 zł netto każda** (dla dostaw realizowanych w walutach obcych, bierze się wartość dostawy przeliczaną po średnim kursie NBP z dnia sprzedaży).

D.3. Zasady spełnienia i weryfikacji warunków udziału

1. Ocena spełniania ww. warunków dokonana zostanie w oparciu o informacje zawarte w przedkładanych wymaganych dokumentach i oświadczeniach.
2. Z treści załączonych dokumentów i oświadczeń musi wynikać jednoznacznie, iż ww. warunki Wykonawca spełnił.
3. Na potwierdzenie spełniania opisanych warunków udziału w postępowaniu, Wykonawca jest zobowiązany złożyć niżej wymienione oświadczenia i dokumenty:
   1) Wykaz zrealizowanych zamówień, wykonanych w okresie ostatnich 3 lat przed upływem terminu składania ofert a jeżeli okres prowadzenia działalności jest krótszy w tym okresie, z podaniem zakresu, wartości, dat i podmiotów, na rzecz których zamówienia były realizowane wraz z załączeniem dowodów określających, czy zostały one wykonane w sposób należyty - **Załącznik nr 4** do niniejszego zapytania ofertowego,

   Dowodami, o których mowa powyżej, są:
   a) poświadczenie,
   b) inne dokumenty – jeżeli z uzasadnionych przyczyn o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać poświadczenia.
4. Ocena spełniania warunków wymaganych od Wykonawcy zostanie dokonana według formuły: spełnia – nie spełnia.

5. Warunek nr 1, tj. w zakresie wiedzy i doświadczenia, nie będzie podlegał sumowaniu. Oznacza to, że spełnieniem ww. warunku musi wykazać się albo wykonawca składający ofertę, albo co najmniej jeden z uczestników konsorcjum (jeżeli dotyczy). Warunek ten nie będzie spełniony, jeżeli wszyscy uczestnicy konsorcjum w sumie wykażą spełnienie ww. warunku, ale żaden z nich nie spełni go samodzielnie. Jeżeli do realizacji zostanie wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego umowy regulującej współpracę tych wykonawców.

E. Ocena punktowa - kryteria, sposób przyznawania punktów

E.1. Kryteria wyboru

Przy wyborze oferty Zamawiający będzie się kierował następującym kryteriami i ich waga:

Cena ofertowa – 100%

Razem - 100%.

E.2.Zasady oceny i wyboru

Sposób obliczania wartości punktowej ocenianego kryterium:
Kryterium nr 1 – CENA
W kryterium kolejno ocenianym ofertom zostaną przyznane punkty według następującego wzoru:

P=(Cn/Cb) x 100% x 100 punktów

gdzie: P – liczba punktów przyznanych rozpatrywanej ofercie w ramach kryterium, Cn – łączna cena brutto najtańszej oferty; Cb – łączna cena brutto badanej oferty

Przy czym w sytuacji gdy w trakcie oceny ofert Zamawiający uzna, że ma do czynienia z ofertą zawierającą cenę rażąco niską w stosunku do przedmiotu zamówienia:

- wzywania Wykonawcę do wyjaśnienia ceny oferty,
- termin na dokonanie wyjaśnień wynosi do 3 dni roboczych od daty wezwania, przy czym dla uznania spełnienia terminu liczy się data wpływu wyjaśnień do Zamawiającego,
- jeżeli Wykonawca nie złoży wyjaśnień w wyznaczonym terminie lub jeżeli dokonana ocena wyjaśnień wraz z dostarczonymi dowodami potwierdzi, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia, Zamawiający może odrzucić ofertę Wykonawcy.

Podsumowanie:
Za ofertę najkorzystniejszą zostanie uznana oferta niepodlegająca odrzuceniu, złożona przez niewykluczonego z postępowania Wykonawcę, która uzyska największą ilość punktów.

Kryteria weryfikowane będą na podstawie informacji zawartych w Formularzu ofertowym – Załącznik nr 1.

E.3.Postępowanie w sytuacji wystąpienia rażąco niskiej ceny/kosztu

Jeżeli zaoferowana cena lub koszt wydają się rażąco niskie w stosunku do przedmiotu zamówienia, tj. różnią się o więcej niż 30% od średniej arytmetycznej cen wszystkich ważnych ofert niepodlegających odrzuceniu, lub budzą wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w zapytaniu ofertowym lub wynikającymi z odrębnych przepisów, wówczas Zamawiający żąda od Wykonawcy złożenia w wyznaczonym terminie (3 dni roboczych od daty wezwania, przy czym dla uznania spełnienia terminu liczy się data wpływu wyjaśnień do Zamawiającego) wyjaśnień, w tym złożenia dowodów w zakresie wyliczenia ceny lub kosztu. Zamawiający ocenia te wyjaśnienia w konsultacji z Wykonawcą i może odrzucić tę ofertę w przypadku, gdy złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej ceny lub kosztu w tej ofercie.

F. Sposób ustalenia ceny, przygotowania i złożenia oferty

F.1. Opis sposobu ustalenia ceny

1. Cena podana w ofercie jest ceną ryczałtową, musi uwzględniać wszystkie wymagania związane z zamówieniem oraz obejmować wszystkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia i nie może ulec zmianie przez cały okres obowiązywania umowy.
2. Wszelkie koszty dodatkowe, które wystąpią w okresie realizacji zamówienia, a które Wykonawca mógł przewidzieć na etapie składania oferty, a nie zawarł ich w cenie oferty, będą ponoszone w ramach wynagrodzenia Wykonawcy, co oznacza, iż Wykonawcy nie przysługuje roszczenie o zwrot tego rodzaju kosztów dodatkowych przewyższających wynagrodzenie Wykonawcy.
3. Cenę oferty podaje się za wykonanie całości przedmiotu zamówienia.
4. W formularzu ofertowym należy podać cenę netto oraz jako osobną pozycję – należny podatek VAT i cenę brutto.
5. Cenę należy podać w polskich złotych z dokładnością do dwóch miejsc po przecinku (c**enę oferty można podać wyłącznie w polskich złotych**).
6. Dla całości zamówienia należy zastosować stawkę podatku VAT w wysokości 23%.
7. Zamawiający nie dopuszcza przedstawienia ceny ofertowej w kilku wariantach.

F.2. Opis sposobu przygotowania oferty

1. Wykonawcy mają obowiązek zapoznać się dokładnie z treścią zapytania ofertowego wraz z załącznikami.
2. Wykonawcy przygotują i przedstawią swoje oferty zgodnie z wymaganiami zapytania ofertowego wraz z załącznikami.
3. Załączone przez Wykonawcę do oferty oświadczenia, deklaracje, formularze muszą odpowiadać swoją treścią treści zaproponowanych przez Zamawiającego wzorów tychże dokumentów będących załącznikami do niniejszego zapytania ofertowego.
4. Oferta powinna być sporządzona w języku polskim w sposób czytelny (dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę).
5. Wykonawca może złożyć tylko jedną ofertę w niniejszym postępowaniu.
6. Oferta nie powinna zawierać żadnych nieczytelnych lub nieautoryzowanych poprawek i skreśleń. Ewentualne poprawki lub korekty błędów należy nanieść czytelnie oraz zaopatrzyć podpisem co najmniej jednej z osób podpisujących ofertę.

7. Składana oferta wraz załącznikami w postaci oświadczeń musi być złożona w formie oryginału. Inne dokumenty mogą być złożone jako kopie potwierdzone przez Wykonawcę za zgodność z oryginałem.
8. Oferta (oraz załączniki do niej) musi być podpisana przez Wykonawcę zgodnie z zasadami reprezentacji określonymi w dokumencie rejestrowym Wykonawcy lub przez osobę upoważnioną do składania oświadczeń woli w jego imieniu.
9. W przypadku pełnomocnictwa – do reprezentowania Wykonawcy w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia – powinno być ono załączone do oferty w formie oryginału lub kserokopii poświadczonej za zgodność z oryginałem przez notariusza lub mocodawcę.
10. Dopuszcza się następujące formy podpisywania ofert:
    a) podpis elektroniczny kwalifikowany,
    b) w przypadku braku dysponowania podpisem elektronicznym kwalifikowanym, papierową wersję oferty wraz z załącznikami należy czytelnie podpisać (lub podpis z pieczątką imienną) zgodnie z wymaganiami przedstawionymi powyżej, wykonać skan i zamieścić go, jako oferta w Bazie konkurencyjności 2021. W przypadku tej formy ofertowania, Wykonawca, którego oferta zostanie wybrana do realizacji, przed podpisaniem umowy, zostanie poproszony o przekazanie oryginału złożonej oferty wraz z załącznikami lub potwierdzenia za zgodność z oryginałem wydrukowanej z Bazy konkurencyjności 2021 kopii złożonej oferty wraz z załącznikami (przez osobę upoważnioną do reprezentowania Wykonawcy). Jeżeli Wykonawca będzie uchylał się od przedstawienia oryginału oferty lub potwierdzenia jej kopii, Zamawiający może odrzucić ofertę Wykonawcy.
11. Zamawiający nie zwraca Wykonawcom dokumentów zawartych w ofercie (jeżeli dotyczy).
12. Koszty przygotowania oferty ponosi Wykonawca.
13. Ofertę należy złożyć za pomocą opcji składania ofert dostępnej na portalu Baza Konkurencyjności 2021, zgodnie z obowiązującymi na dzień składania oferty Instrukcjami korzystania z bazy konkurencyjności dostępnymi m.in. https://archiwum-bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/info/web_instruction
14. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia, zgodnie z obowiązującymi na dany moment instrukcjami i funkcjonalnościami Bazy konkurencyjności 2021, instrukcja dostępna m.in. pod linkiem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/pomoc/52-wycofanie-i-edycja-oferty.

F.3. Wymagania dotyczące wadium

Nie przewiduje się.

F.4. Termin związania ofertą

Wykonawca jest związany ofertą przez okres 30 dni.
Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

G. Pozostałe informacje

1. Procedura wynikająca z „Zasady konkurencyjności” nie przewiduje środków odwoławczych.
2. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego. Zamawiający dołoży staranności, aby udzielić wyjaśnień niezwłocznie,

jednak nie później niż na 2 dni przed terminem składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści Zapytania ofertowego wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.

3. Dokonywane i publikowane przez Zamawiającego zmiany treści Zapytania ofertowego, a także publikowane odpowiedzi na zadane pytania stają się integralną częścią Zapytania ofertowego.
4. Zamawiający zastrzega sobie prawo do unieważnienia postępowania, na każdym jego etapie bez podania przyczyny, a także do pozostawienia postępowania bez wyboru oferty.
5. O zamówienie mogą ubiegać się Wykonawcy, którzy zaoferują przedmiot zamówienia zgodny z wymogami Zamawiającego określonymi w niniejszym zapytaniu ofertowym.
6. W przypadku oczywistych omyłek, braku podpisu, braku załącznika innego niż formularz ofertowy, Zamawiający może wezwać Wykonawcę do uzupełnienia braków. Wezwanie dokonywane jest za pośrednictwem platformy Baza konkurencyjności 2021, o ile platforma umożliwia taką formę komunikacji, a jeżeli nie, wezwanie wysyłane jest w formie e-mail na adres wskazany w formularzu ofertowym. Za czytelne i prawidłowe wskazanie adresu kontaktowego e-mail odpowiada Wykonawca. Wykonawca ma możliwość uzupełnienia wskazanych braków w terminie do 3 dni roboczych od daty wysłania wezwania. Dla spełnienia terminu liczy się data wpływu uzupełnień do Wnioskodawcy. Jeżeli korespondencja z przyczyn technicznych prowadzona jest poza Bazą konkurencyjności 2021, w przypadku nadania uzupełnień listem (lub paczką), termin uznaje się za zachowany, jeżeli zostanie on nadany w polskiej placówce pocztowej operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Poczta Polska S.A) nie później niż w dniu zakończenia przyjmowania uzupełnień – decyduje data nadania. W przypadku braku uzupełnień, oferta zostanie odrzucona bez dalszego rozpatrzenia.
7. Oferty niespełniające któregokolwiek z wymagań zostaną odrzucone.
8. Zamawiający zastrzega sobie prawo do podjęcia negocjacji cenowych z Wykonawcą, który złożył w oparciu o przyjęte kryteria najkorzystniejszą ofertę. Negocjacje cenowe zostaną podjęte w szczególności w przypadku, gdy zaoferowana cena będzie wyższa od założonej przez Zamawiającego.
9. W przypadku wystąpienia Wykonawcy w formule konsorcjum, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego ponoszą solidarną odpowiedzialność za wykonanie umowy. Wynika z tego, że Zamawiający może żądać całości lub części realizacji umowy od wszystkich partnerów konsorcjum łącznie, od kilku z nich lub od każdego z osobna, a zaspokojenie zamawiającego przez któregokolwiek z konsorcjantów zwalnia pozostałych. Ponadto, wszyscy konsorcjanci pozostają zobowiązani, aż do zupełnego zaspokojenia zamawiającego w zakresie obowiązków wynikających z umowy w sprawie zamówienia publicznego. Wykonawca ma prawo wglądu w Umowę konsorcjum.
10. Informacja o wynikach postępowania zostanie zamieszczona na portalu https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/.
11. Składając ofertę należy być świadomym, że mogą znajdować się w niej dane osób fizycznych, np. osób wskazywanych do kontaktu. Pozyskane oferty, a wraz z nimi ewentualne dane osobowe, służą Zamawiającemu wyłącznie do realizacji zamówienia zgodnie z obowiązującymi Wytycznymi kwalifikowalności wydatków, a następnie ich

rozliczeniu i archiwizacji, zgodnie z umową o dofinansowanie projektu unijnego, w ramach którego finansowane jest zamówienie. Oznacza to, że dostęp do złożonych ofert mogą mieć inni potencjalni Wykonawcy, Instytucje finansujące projekt oraz uprawnione Instytucje kontrolujące projekt. Informacje dotyczące ofert publikowane są, zgodnie z ww. Wytycznymi, na stronach internetowych, na których publikowane było zapytanie ofertowe. Ponadto oferty mogą być przekazywane do Instytucji zaangażowanych w obsługę projektu za pomocą systemu SL. Administratorem ww. portali i systemów nie jest Zamawiający, a Instytucje publiczne zaangażowane we wdrażanie funduszy europejskich w Polsce. Złożenie oferty jest równoznaczne z tym, że Wykonawca jest świadomy powyższych uwarunkowań i je akceptuje.

H. Załączniki

Załącznik nr 1 - Formularz ofertowy
Załącznik nr 2 - Oświadczenie o braku podstaw do wykluczenia
Załącznik nr 3 – Klauzula informacyjna o przetwarzaniu danych osobowych
Załącznik nr 4 – Wykaz doświadczenia