Polska Agencja
Inwestycji i Handlu
Grupa PFR

Warszawa, dnia ...06.07.2018...r.

ZAPYTANIE OFERTOWE

Polska Agencja Inwestycji i Handlu Spółka Akcyjna (adres: ul. Bagatela 12, 00-585 Warszawa) zwraca się z prośbą o przygotowanie oferty cenowej na

Zakup urządzeń typu UTM poprawiających bezpieczeństwo sieci wewnętrznej oraz stabilność dostępu do sieci Internet wraz z licencjami do programów i systemów obsługujących urządzenia oraz aktualizacją oprogramowania na okres 36 miesięcy na potrzeby Polskiej Agencji Inwestycji i Handlu S.A.

Niniejszy wydatek jest realizowany i finansowany ze środków własnych.

I. ZAMAWIAJĄCY

Polska Agencja Inwestycji i Handlu S.A.
Warszawa, 00-585, ul. Bagatela 12
tel. (22) 334-98-00; fax (22) 334-99-99
e-mail: post@paiz.gov.pl, strona internetowa: www.paih.gov.pl

NIP: 526-030-01-67, kapitał zakładowy: 137.718.000,00 zł, wpłacony w całości KRS 0000109815 Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego.

II. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest zakup 2 urządzeń typu UTM poprawiających bezpieczeństwo sieci wewnętrznej oraz stabilność dostępu do sieci Internet, działających w klastrze wysokiej dostępności „HA" wraz z konfiguracją i ***licencjami do programów i systemów obsługujących urządzenia oraz aktualizacją oprogramowania na okres 36 miesięcy***.

Wymagania dotyczące urządzeń

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 8 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
- 18 portami Gigabit Ethernet RJ-45.
- 4 gniazdami SFP 1 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.
5. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 135.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 9 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.5 Gbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 9 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 6 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.

8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem nie słabszym niż AES128-SHA256) dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.

- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
4. System musi dysponować sygnaturami do ochrony urządzeń mobilnych.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikacje

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.
- ICSA lub NSS Labs dla funkcji IPS.
- ICSA dla funkcji IPSec VPN.
- ICSA dla funkcji SSL VPN.

Serwisy i licencje
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:
b) Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering, Sandbox, ochrona systemów mobilnych na okres 36 miesięcy.

Gwarancja oraz wsparcie
System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania, wsparcie techniczne w trybie 8x5 tzn. możliwość przedłużenia gwarancji oraz dodatkowo ewentualnej wymiany urządzenia na kolejny model, a także aktualizację wewnętrznego oprogramowania.

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Zamawiający nie dopuszcza składania ofert częściowych.

III. MIEJSCE I TERMIN REALIZACJI USŁUGI

Termin realizacji zamówienia:
1) dostawa urządzeń nastąpić winna w terminie do 14 dni roboczych od dnia podpisania Umowy z wybranym Wykonawcą na okres serwisu i wsparcia wynoszący 36 miesięcy od daty dostarczenia i konfiguracji urządzeń.
Miejsce realizacji umowy: Miejscem świadczenia Usługi i dostawy jest siedziba Zamawiającego ul. Bagatela 12 (lub inne miejsce, które będzie nową siedzibą) w Warszawie, zwana dalej „Miejscem Usługi"

IV. WARUNKI PODMIOTOWE

O zamówienie nie mogą ubiegać się podmioty pozostające z Zamawiającym w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze Wykonawcy zamówienia, w szczególności o zamówienie nie mogą ubiegać się podmioty powiązane kapitałowo lub osobowo z Zamawiającym.

Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru wykonawcy a wykonawcą, polegające w szczególności na:

a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,

b) posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez IZ PO,

c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,

d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia

V. INORMACJE DODATKOWE

1. Wykonawca ponosi wszelkie koszty związane z dzierżawą, obsługą eksploatacyjną urządzeń i serwisowaniem sprzętu.
2. Za terminowe i należyte wykonanie Umowy Zamawiający wypłaci Wykonawcy wynagrodzenie, przelewem w ciągu 14 dni od daty dostarczenia faktury VAT do siedziby PAIiH S.A. Ustalone wynagrodzenie Wykonawcy obejmuje wszelkie koszty, jakie Wykonawca poniesie w związku z wykonaniem przedmiotu umowy i jest wynagrodzeniem ryczałtowym i nie podlega zmianom. Płatności będą realizowane w polskich złotych, przelewem na rachunek bankowy wskazany na fakturze, na podstawie faktury VAT wystawionej przez Wykonawcę. Wzór umowy stanowi załącznik Nr 3 do niniejszego zapytania.
3. Zamawiający zastrzega sobie możliwość negocjacji z wybranymi Wykonawcami, którzy złożyli oferty, w zakresie szczegółów wykonania usługi oraz ewentualnie wysokości ceny w zakresie jej zmniejszenia. Zamawiający zastrzega sobie prawo do wezwania Wykonawców do wyjaśnienia treści złożonej oferty.
4. Zamawiający zastrzega sobie prawo do niedokonania rozstrzygnięcia postępowania i nie dokonania wyboru oferty bez podawania przyczyny i zwrotu ewentualnych kosztów sporządzenia oferty.

Zamawiający oczekuje od Wykonawcy na całym etapie realizowania Zamówienia, należytej staranności, wysokiej jakości świadczonych usług oraz profesjonalnego podejścia do jego wykonania.

VI. KRYTERIA OCENY OFERTY

1. Ocenie podlega wyłącznie oferta przygotowana wg wzoru stanowiącego Załącznik nr 1 do zapytania ofertowego.
2. Do oferty należy załączyć:

- kopię aktualnego odpisu z właściwego rejestru **(KRS lub CEiIDG etc.)**, jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawionego nie wcześniej niż 3 miesięcy przed upływem terminu składania ofert;
- Aktualne zaświadczenie właściwego naczelnika Urzędu Skarbowego potwierdzające, że Wykonawca nie zalega z opłacaniem podatków, lub zaświadczenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu w postaci oryginału lub kopii poświadczonej podpisem oraz pieczęcią wykonawcy – wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
- Specyfikację techniczną proponowanych urządzeń

3. Oferty złożone bez wymienionych załączników nie będą podlegały ocenie.
4. Kryterium oceny ofert:

KRYTERIUM: CENA – WAGA 100 %

W trakcie oceny ofert kolejno ocenianym ofertom zostaną przyznane punkty według następującego wzoru:

$$C = \frac{\text{Najniższa cena brutto za realizację zamówienia}}{\text{Cena brutto badanej oferty za realizację zamówienia}} \times 100 \text{ pkt}$$

Za najkorzystniejszą ofertę zostanie uznana oferta spełniająca wymagania Zamawiającego, która uzyskała najwyższą liczbę punktów wg podanego kryterium.

VI. TERMIN I MIEJSCE SKŁADANIA OFERT

Termin złożenia ofert – .....11.07.a.....2018 r. (decyduje **data wpływu oferty do PAIiH**). Oferty złożone po terminie zostaną odrzucone.

Ofertę należy złożyć na formularzu załączonym do niniejszego zapytania pod adresem: Polska Agencja Inwestycji i Handlu S.A., ul. Bagatela 12, 00-585 Warszawa z dopiskiem: ***„Zakup urządzeń typu UTM poprawiających bezpieczeństwo sieci wewnętrznej oraz stabilność dostępu do sieci Internet wraz z licencjami do programów i systemów obsługujących urządzenia oraz usługą aktualizacji oprogramowania na okres 36 miesięcy na potrzeby Polskiej Agencji Inwestycji i Handlu S.A.”.***

Dopuszczalne jest również przesłanie skanów wszystkich wymaganych dokumentów na adres mailowy: **utm@paih.gov.pl** w wyznaczonym terminie.

PROKURENT
Małgorzata Przymus

Krzysztof Senger
Członek Zarządu

Mariola Dąbrowska
RADCA PRAWNY
WA2490

DYREKTOR
Biura ds. Finansów i Logistyki
Małgorzata Przymus

wniosku nr 6/2018-04-04
K. ogólne

Polska Agencja
Inwestycji i Handlu
Grupa PFR

Załącznik nr 1 do zapytania ofertowego

Miejsce ..... data.....

Pieczęć Wykonawcy

Formularz ofertowy

Nazwa i adres Wykonawcy:
.....
.....
.....
Tel. ..... Faks .....
Odpowiadając na zaproszenie do składania ofert na *Zakup urządzeń typu UTM poprawiających bezpieczeństwo sieci wewnętrznej oraz stabilność dostępu do sieci Internet wraz z usługą aktualizacji oprogramowania na okres 36 miesięcy na potrzeby Polskiej Agencji Inwestycji i Handlu S.A.* oferujemy:

Nazwa / Usługa	Typ/Model	Wartość netto	Wartość brutto
Urządzenie – 2 szt.			
Usługa instalacji, konfiguracji i aktualizacji oprogramowania na okres 36 miesięcy			
	Łącznie		

Oświadczamy, że :
Wykonawca nie pozostaje z Zamawiającym w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze Wykonawcy zamówienia, w szczególności nie:
a) uczestniczy w spółce jako wspólnik spółki cywilnej lub spółki osobowej z Zamawiającym ,
b) posiada co najmniej 10% udziałów lub akcji Zamawiającego ,
c) pełnieni funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika Zamawiającego,
d) pozostaje w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia nie pełni wobec Zamawiającego funkcji członka organu nadzorczego lub Zapoznaliśmy się z treścią zapytania ofertowego i akceptujemy bez zastrzeżeń jego postanowienia;

- Akceptujemy wzór Umowy, stanowiący Załącznik Nr 3 do niniejszego Zapytania Ofertowego,

- Akceptujemy wzór protokołu instalacji, stanowiący Załącznik nr 4 do wzoru umowy;
- Uważamy się za związanych ofertą **przez okres 30 dni od upływu terminu składania ofert;**

Zobowiązujemy się do wykonania usługi zgodnie z wytycznymi wyszczególnionymi w niniejszym Zapytaniu Ofertowym w sposób należyty.

Załącznikiem do niniejszej oferty są;

- ✓ kopia aktualnego odpisu z właściwego rejestru **(KRS lub CEiIDG)**, jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawionego nie wcześniej niż 3 miesięcy przed upływem terminu składania ofert;
- ✓ Specyfikacja techniczna proponowanych urządzeń
- ✓ Oświadczenia.

.....

podpis Wykonawcy

Załącznik nr 2 do Zapytania ofertowego

UMOWA

(wzór)

z dnia .....2018 roku w Warszawie

zawarta pomiędzy:

Polską Agencją Inwestycji i Handlu S.A. z siedzibą w Warszawie przy ul. Bagatela 12 (00-585 Warszawa), wpisaną do rejestru przedsiębiorców prowadzonym przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000109815, o kapitale zakładowym w wysokości 121.818.000,00 zł opłaconym w całości, zgodnie z wpisem dokonanym w rejestrze przedsiębiorców KRS, o nr NIP: 526-030-01-67, reprezentowaną przez:

.....

.....

zwaną dalej „**Zamawiającym**"

a

.....

.....,

reprezentowaną przez:

.....

zwaną/ym dalej „**Wykonawcą**",

dalej zwanymi również łącznie „**Stronami**".

Odpis z rejestru KRS Wykonawcy stanowi Załącznik Nr 1 do Umowy.

Umowa została zawarta bez zastosowania przepisów ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (tekst jedn. Dz.U. z 2017 r. poz. 1579 z poź.zm.), na podstawie art. 4 pkt 8 tejże ustawy, po przeprowadzeniu postępowania zgodnie z trybem udzielenia zamówienia określonym w Regulaminie udzielania zamówień publicznych do 30.000 Euro, przyjętym Uchwałą Zarządu PAIiH S.A. z dnia 07 lutego 2017 r.

§ 1

1. Na warunkach określonych w Umowie, Zapytaniu Ofertowym, stanowiącym załącznik Nr 3 do Umowy, Wykonawca zobowiązuje się do dostarczenia 2 szt. urządzeń typu UTM wraz z usługą wsparcia.
2. Wykonawca zobowiązuje się dostarczyć, uruchomić i wdrożyć zakupiony sprzęt, w siedzibie Zamawiającego w terminie 14 dni od podpisania umowy
3. Dostawca przeprowadzi szkolenie z konfiguracji i administracji sprzętem w terminie 14 dni od dostarczenia, wdrożenia i uruchomienia dostarczonego sprzętu potwierdzonego protokołem instalacji (Załącznik nr 3 do umowy).
4. Dostarczone rozwiązanie pochodzić będzie z oficjalnych kanałów dystrybucyjnych producenta obejmujących również rynek Unii Europejskiej, zapewniających w szczególności realizację uprawnień gwarancyjnych.
5. Dostawca świadczyć będzie usługę aktualizacji oprogramowania urządzeń przez okres 36 miesięcy, płynący od momentu podpisana protokołu instalacji, co oznacza, iż Wykonawca powiadomi oraz udostępni możliwość pobrania nowych wersji oprogramowania. .
6. Osoby upoważnione do podpisu protokołu instalacji:
   Ze strony Wykonawcy:
   Imię i nazwisko, mail, telefon
   ……..
   ze strony Zamawiającego:
   Imię i nazwisko, mail, telefon
   ……..
7. Zamawiający zobowiązuje się do terminowej zapłaty za wykonaną Usługę.

§ 2

Miejscem świadczenia Usługi i dostawy jest siedziba Zamawiającego ul. Bagatela 12 lub inne miejsce w Warszawie, zwana dalej „Miejscem Usługi". Nowe miejsce usługi w Warszawie zostanie wskazane Wykonawcy z 7 dniowym wyprzedzeniem.

§ 3

1. Umowa zawarta jest na czas określony - 36 miesięcy od dnia dostawy i instalacji urządzeń do siedziby Zamawiającego.
2. Dostarczone rozwiązania wraz z oprogramowaniem objęte są 36 miesięczną gwarancją producenta liczoną od dnia podpisania protokołu instalacji. Ewentualne wady urządzeń i oprogramowania będą zgłaszane na wskazany adres e-mail …….. Wykonawca zobowiązuje się wady usunąć w okresie 2 dni roboczych od chwili zgłoszenia, a w przypadku braku możliwości usunięcia wady w tym terminie do dostarczenia urządzenia zastępczego o tożsamych parametrach.
3. Wykonawca wraz ze sprzętem dostarcza Licencje do oprogramowania/systemów serwisów na korzystanie z dostarczonego oprogramowania udzielone przez producenta oprogramowania oraz dokument gwarancji na dostarczony sprzęt.

4. W wyniku zawarcia umowy Kupujący nie nabywa majątkowych praw autorskich do oprogramowania komputerowego w rozumieniu przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, ale wyłącznie egzemplarz programu komputerowego wraz z licencją do użytkowania programu na warunkach określonych w umowie licencyjnej, bez prawa do udzielania sublicencji. Licencja obejmuje w szczególności prawo do eksploatacji tego programu poprzez przechowywanie go w pamięci komputera oraz na nośnikach zewnętrznych i wykorzystanie go zgodnie z warunkami licencji. Szczegółowe warunki korzystania z programu określa umowa licencyjna.
5. Dane użytkownika końcowego podlegają zarejestrowaniu w bazie danych Dostawcy oraz w bazie dystrybutora i producenta.

§ 5

1. Zamawiający zobowiązuje się do zapłaty na rzecz Wykonawcy wynagrodzenia z tytułu realizacji przedmiotu zamówienia, zgodnie z ofertą, stanowiącą Załącznik Nr 4 do Umowy w terminie 14 dni od dostarczenia do siedziby Zamawiającego faktury, tj ..... zł netto (słownie ..... złotych) powiększoną o wartość podatku VAT ..... zł dające łączną cenę brutto ..... zł (słownie ..... złotych), wystawionej prawidłowo po podpisaniu przez Zamawiającego protokołu odbioru sprzętu wraz z oprogramowanie.

2. Wynagrodzenie zostanie wypłacone na rachunek bankowy Wykonawcy wskazany w fakturze w terminie 14 dni od daty otrzymania faktury.

3. Za dzień zapłaty uznaje się datę obciążenia rachunku bankowego Zamawiającego kwotą należnego Wykonawcy wynagrodzenia.

§ 6

1. Wykonawca ponosi odpowiedzialność z tytułu niewykonania lub nienależytego wykonania Umowy zgodnie z przepisami Kodeksu Cywilnego
2. Wszystkie oświadczenia przekazywane zgodnie z niniejszą Umową wymagają zachowania formy pisemnej i uznaje się je za skutecznie doręczone z chwilą :
   - ich doręczenia na wskazanym poniżej adres ,
   - ich doręczenia na wskazany poniżej adres za pośrednictwem kuriera,
   - ich doręczenia listem poleconym na wskazany poniżej adres ,

   dla Wykonawcy:
   .....
   .....
   dla Zamawiającego:
   Polska Agencja Inwestycji i Handlu S.A.
   00-585 Warszawa ul. Bagatela 12

§ 7

Kary umowne:

1. Za rozwiązanie umowy z przyczyn niezależnych od Zamawiającego Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wynagrodzenia brutto określonego w par.5 ust.1 umowy.
2. Wykonawca wyraża zgodę na dokonanie przez Zamawiającego potrącenia naliczonych przez Zamawiającego kar umownych z należności wynikających z faktury VAT wystawionej przez Wykonawcę.
3. Zapłata kary umownej nie wyłącza możliwości dochodzenia przekraczającego jej wysokość odszkodowania na zasadach ogólnych.
4. W sprawach nieuregulowanych Umową znajdują zastosowanie przepisy Kodeksu cywilnego.
5. Wszelkie zmiany niniejszej Umowy, a szczególnie wypowiedzenie Umowy, oświadczenie o rozwiązaniu lub odstąpieniu od Umowy wymagają formy pisemnej pod rygorem nieważności.
6. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO",

- administratorem danych osobowych wskazanych przez Wykonawcę w toku postępowania, w tym w ofercie i niniejszej umowie jest Zamawiający - Polska Agencja Inwestycji i Handlu SA z siedzibą w Warszawie (adres: 00-585 Warszawa, ul. Bagatela 12),
- inspektorem ochrony danych osobowych jest wyznaczona przez Zamawiającego osoba z którą można skontaktować się pod adresem: ……..: *adres e-mail, telefon/* *;
- przekazane dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b RODO w celu związanym z postępowaniem o udzielenie zamówienia ***Zakup urządzeń typu UTM poprawiających bezpieczeństwo sieci wewnętrznej oraz stabilność dostępu do sieci Internet wraz z licencjami do programów i systemów obsługujących urządzenia oraz usługą aktualizacji oprogramowania na okres 36 miesięcy na potrzeby Polskiej Agencji Inwestycji i Handlu S.A.*** i wykonaniem niniejszej umowy oraz w celach archiwizacyjnych będących realizacją naszego prawnie uzasadnionego interesu zabezpieczenia informacji na wypadek prawnej potrzeby wykazania faktów dotyczących złożonej przez Wykonawcę oferty (podstawa z art. 6 ust. 1 lit. f RODO) i w celu ewentualnego ustalenia, dochodzenia lub obrony przed roszczeniami będącego realizacją naszego prawnie uzasadnionego w tym interesu (podstawa z art. 6 ust. 1 lit. f RODO)

- przekazane dane osobowe będą przechowywane przez cały czas trwania umowy, a po tym okresie dla celów archiwizacyjnych i oraz dla potrzeb obrony interesów Zamawiającego, w tym dochodzenia roszczeń przez okres 5 lat;
- w odniesieniu do przekazanych danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- osoby wskazane przez Wykonawcę posiadają :

- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
- na podstawie art. 16 RODO prawo do sprostowania danych osobowych ;
- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie danych osobowych narusza przepisy RODO;

▪ osobom wskazanym przez Wykonawcę nie przysługuje :
- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

7. Umowa została sporządzona w czterech jednobrzmiących egzemplarzach po dwa dla każdej ze Stron.
8. Umowa zawiera następujące załączniki stanowiące jej integralną część:

Załączniki:
Załącznik nr 1 – odpis KRS Wykonawcy,
Załącznik nr 2 – kopia Zapytania Ofertowego,
Załącznik nr 3 – Protokół Instalacji
Załącznik nr 4 – Oferta z załącznikiem

Zamawiający	**Wykonawca**
....	....
pieczęć i podpis	pieczęć i podpis
....	....
pieczęć i podpis	pieczęć i podpis

wniosek nr 6/2018-04-04
k. ogólne

Załącznik nr 3 do umowy

PROTOKÓŁ INSTALACJI

wzór

Protokół sporządzono dnia: .....

pomiędzy

Polską Agencją Informacji i Inwestycji S.A.

a

.....

Strony potwierdzają dostarczenie i instalację sprzętu zgodnie z Załącznikiem nr 1 do Zapytania ofertowego.

Uwagi Zamawiającego/Wykonawcy:

.....

.....

Odbioru dokonali:

1. W imieniu Zamawiającego:

.....

2. W imieniu Wykonawcy:

.....

Niniejszy protokół stanowi podstawę do rozpoczęcia świadczenia usług.

Zamawiający Wykonawca