Szczecin, dnia 25 października 2012 r.

OGŁOSZENIE

o rozpoczęciu przetargu nieograniczonego o wartości zamówienia poniżej 125 000 euro

Wojewódzka Stacja Sanitarno - Epidemiologiczna w Szczecinie
ul. Spedytorska 6/7, 70-632 Szczecin, ogłasza przetarg nieograniczony
na:
„zakup i dostawę do Wojewódzkiej Stacji Sanitarno-Epidemiologicznej w Szczecinie routera wraz z systemem centralnego logowania i raportowania"

W ramach kodów CPV:

32420000-3	Urządzenie sieciowe
32413100-2	Routery sieciowe

wg „Wspólnego słownika zamówień".

Bezpłatną Specyfikację Istotnych Warunków Zamówienia można:

- pobrać ze strony internetowej: http://www.wsse.szczecin.pl
- odebrać w siedzibie przy ul. Spedytorskiej 6/7, pok. Nr 15 w godzinach od 7:25 do 15:00
- przesłać pocztą na wniosek Wykonawcy, przesłany na numer fax.: 091/462-40-60 wew. 151.

I. .Przedmiotem zamówienia jest zakup wraz z dostawą do siedziby Wojewódzkiej Stacji Sanitarno Epidemiologicznej w Szczecinie przy ul. Spedytorskiej 6/7 routera wraz z systemem centralnego logowania i raportowania **;**

II Określenie wielkości i zakresu zamówienia **(wymagania ogólne)**

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza. Elementy wchodzące w skład systemu ochrony muszą być zrealizowane w postaci zamkniętej platformy sprzętowej. Nie dopuszcza się komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. Dla elementów systemu bezpieczeństwa Wykonawca zapewni wszystkie poniższe funkcjonalności – w ofercie należy podać model i producenta oferowanego rozwiązania wraz z podaniem wszystkich oferowanych parametrów technicznych:

Nazwa producenta.....
Oferowany model.....

Lp.	Wymagania techniczne
1.	Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
2.	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3.	Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.
4.	System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
5.	System realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/1000 Base-TX.
6.	Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
7.	W zakresie Firewall'a obsługa nie mniej niż 1,8 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
8.	Przepustowość Firewall'a: nie mniej niż 8 Gbps. Wydajność szyfrowania AES lub 3DES: nie mniej niż 40 Gbps.
9.	System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 32 GB do celów logowania, cache itp.

10.	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych: • kontrola dostępu - zapora ogniowa klasy Stateful Inspection, • ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). W celu zapewnienia wysokiej skuteczności mechanizmu antywirusowego wymaga się aby mechanizm skanowania działał w oparciu o technologię proxy, która umożliwia analizę dowolnego typu załączników, • poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN, • ochrona przed atakami - Intrusion Prevention System [IPS], • kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM, • kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP), • kontrola pasma oraz ruchu [QoS, Traffic shaping] • Kontrola aplikacji oraz rozpoznawanie ruchu P2P, • Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji na lokalnym dysku,
11.	Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 1,3 Gbps.
12.	Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Antivirus, min. 500 Mbps.
13.	W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż: • Tworzenie połączeń w topologii Site-To-Site oraz Client-To-Site, • Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem, • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, • Praca w topologii Hub and Spoke oraz Mesh, • Możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF • Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth,
14.	Rozwiązanie powinno zapewniać: obsługę Policy Routing, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.
15.	Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
16.	Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
17.	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
18.	Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
19.	Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
20.	Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.

21.	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
22.	Baza filtra WWW powinna być pogrupowana w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
23.	Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
24.	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: • 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, • Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny,
25.	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać minimalnie następujące certyfikaty: • ICSA dla funkcjonalności SSLVPN, IPS, Antywirus • ICSA lub EAL4 dla funkcjonalności Firewall
26.	Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami wchodzącymi w skład systemu. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
27.	Serwisy i licencje: • Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres nie mniejszy niż 12 miesięcy., z możliwością rozszerzenia gwarancji w przyszłości przez okres co najmniej 3 lat od daty dostawy
28.	Gwarancja oraz wsparcie: a) System powinien być objęty serwisem gwarancyjnym producenta przez okres nie mniejszy niż 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia. Na czas naprawy wykonawca zapewni urządzenie zastępcze, w terminie na następny dzień roboczy licząc od dnia zgłoszenia usterki / 8x5xNBD. W przypadku gdy producent nie posiada na terenie Rzeczpospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć do oferty dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej. b) W przypadku istnienia wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć do oferty dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Rzeczypospolitej Polskiej, 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. c) Oferent winien przedłożyć do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Rzeczypospolitej Polskiej, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych. d) Oferent winien przedłożyć do oferty oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Rzeczypospolitej Polskiej, iż oferowany sprzęt będzie zakupiony w autoryzowanym kanale sprzedaży producenta na terenie Rzeczypospolitej Polskiej. Oświadczenie ma zawierać numer postępowania oraz odbiorcę końcowego.

2. System centralnego logowania i raportowania współpracujący poprawnie z oferowanym systemem bezpieczeństwa - w ofercie należy podać model i producenta oferowanego rozwiązania wraz z podaniem wszystkich oferowanych parametrów technicznych:
Nazwa producenta.....
Oferowany model.....

Lp.	Parametr	Wymagania techniczne
1.	Architektura systemu ochrony	System logowania i raportowania powinien stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta oraz musi w pełni współpracować z urządzeniem zaoferowanym systemem bezpieczeństwa (routerem)
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.
3.	Parametry fizyczne systemu	Nie mniej niż 1 port Ethernet 10/100 Nie mniej niż 2 porty Ethernet 10/100/1000 Powierzchnia dyskowa - minimum 1 TB
4.	Funkcjonalności podstawowe i uzupełniające	System musi zapewniać: • Składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników i inne określone przez administratora, • Możliwość gromadzenia zawartości przesyłanych za pośrednictwem protokołów Web, FTP, email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci • Kwarantannę dla współpracujących z nim urządzeń. Kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki. • Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących, • Wyświetlanie nowych logów w czasie rzeczywistym, • Analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy, • Analizę podatności stacji roboczych w sieci wraz z możliwością raportowania wykrytych luk, • Export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych),
5.	Parametry wydajnościowe	Urządzenie musi obsługiwać: • Do 100 urządzeń sieciowych, • Do 100 urządzeń klienckich /VPN-client/,
6.	Zarządzanie	System udostępnia: • Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH i konsolę szeregową,
7.	Zasilanie	Zasilanie z sieci 230V/50Hz.
8.	Instalacja i konfiguracja	Instalacja i konfiguracja systemu powinna być przeprowadzona przez uprawnionego inżyniera posiadającego aktualny certyfikat producenta zaoferowanego rozwiązania.
9.	Serwisy, szkolenia i usługi	Wymaga się aby dostawa obejmowała również: • Roczną gwarancję producenta sprzętu, • Serwis producenta na okres: nie mniejszy niż 12 miesięcy, • Serwis logistyczny na terenie Rzeczypospolitej Polskiej z dostawą urządzenia zastępczego: na następny dzień roboczy licząc od dnia zgłoszenia usterki / 8x5xNBD przez okres nie mniejszy niż 12 miesięcy.

III. W zakres dostawy wchodzi również transport do siedziby Wojewódzkiej Stacji Sanitarno- Epidemiologicznej w Szczecinie na koszt Wykonawcy.

IV. Zamawiający dopuszcza możliwość składania ofert częściowych : nie

V. Zamawiający rozstrzygnie postępowanie, gdy wpłynie co najmniej jedna niepodlegająca odrzuceniu oferta.

VI. Zamawiający dopuszcza możliwości składania ofert wariantowych - nie

VII. Wymagany termin realizacji umowy:
- termin dostawy: do 21 dni od daty podpisania umowy.

VIII. O udzielenia zamówienia mogą się ubiegać Wykonawcy, którzy:
- posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
- posiadają wiedzę i doświadczenie oraz dysponują odpowiednim potencjałem technicznym i osobami zdolnymi do wykonywania zamówienia,
- znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,
- nie podlegają wykluczeniu z postępowania o udzielenie zamówienia.

W celu potwierdzenia spełnienia warunków udziału w postępowaniu do oferty należy dołączyć:

1. Oświadczenie Wykonawcy, o spełnianiu warunków określonych w art. 22 ust. 1 pkt 1- 4 i art. 24 ust. 1 i 2 ustawy Prawo zamówień publicznych, według wzoru, stanowiącego załącznik nr 2 do niniejszej SIWZ.
   W przypadku składania oferty wspólnej ww. oświadczenie składa każdy z Wykonawców składających ofertę wspólną.
2. Aktualny odpis z właściwego rejestru (jeżeli odrębne przepisy wymagają wpisu do rejestru w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy), wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
   W przypadku składania oferty wspólnej ww. dokument składa każdy z wykonawców składających ofertę wspólną.
   Jeżeli wykonawca jest osobą fizyczną prowadzącą działalność gospodarczą – składa oświadczenie w zakresie art. 24 ust. 1 pkt 2 ustawy.
3. Aktualne zaświadczenie właściwego Naczelnika Urzędu Skarbowego oraz właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzających odpowiednio, że Wykonawca nie zalega z opłacaniem podatków, opłat oraz składek na ubezpieczenie zdrowotne i społeczne lub zaświadczenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymane w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
4. W przypadku składania oferty przez podmioty występujące wspólnie – Zamawiający może żądać, przez zawarciem umowy w sprawie zamówienia publicznego, umowy regulującej współpracę tych Wykonawców. W przypadku Wykonawców prowadzących działalność w formie spółki cywilnej - Zamawiający może żądać umowy spółki cywilnej po wybraniu ich oferty, a przed zawarciem umowy.
5. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w ust. 1 i ust. 3.
   1) składa dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
   a) nie otwarto jego likwidacji ani nie ogłoszono upadłości,
   b) nie zalega z uiszczeniem podatków, opłat, składek na ubezpieczenia społeczne i zdrowotne, z wyjątkiem przypadków gdy uzyskał on przewidziane prawem zwolnienie, odroczenie, rozłożenie na raty zaległych płatności lub wstrzymanie w całości decyzji właściwego organu,
   c) nie orzeczono wobec niego zakazu ubiegania się o zamówienia,
   oraz :
   2) składa zaświadczenie właściwego organu sadowego lub administracyjnego miejsca zamieszkania albo zamieszkania osoby, której dokumenty dotyczą, w zakresie określonym w art. 24 ust. 1 pkt 4 – 8 ustawy.
6. Dokumenty, o których mowa w ust. 5 pkt 1 lit. a i c oraz pkt 2, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
   Dokument, o którym mowa w ust. 5 pkt. 1 lit. b, powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
   Jeżeli w miejscu zamieszkania osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 5 zastępuje się je dokumentami zawierającymi oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio miejsca zamieszkania lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania. Przepisy pkt. 5 stosuje się odpowiednio.

Niespełnienie powyższych warunków, bądź niedołączenie do oferty dokumentów i oświadczeń potwierdzających ich spełnienie spowoduje wykluczenie Wykonawcy z postępowania, z zastrzeżeniem postanowień art. 26 ust. 3 ustawy Prawo zamówień publicznych.

VIII. Ponadto do oferty należy dołączyć ofertę cenową sporządzoną według formularza oferty stanowiącego załącznik Nr 1 do SIWZ.

IX. Kryterium oceny ofert: najniższa cena

X. Zamawiający nie przewiduje udzielenie zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 7 ustawy Prawo zamówień publicznych.

XI. Zamawiający nie żąda wniesienia wadium.

XII. Oferty w zamkniętych kopertach należy składać do dnia 06.11. **2012** roku do godz. 9^{00} w siedzibie Wojewódzkiej Stacji Sanitarno-Epidemiologicznej w Szczecinie przy ul. Spedytorskiej 6/7 pokój nr 15.
Otwarcie ofert nastąpi dnia 06.11. **2012** roku o godz. 10^{00} w siedzibie WSSE w Szczecinie przy ul. Spedytorskiej 6/7 pokój nr 13b.

XIII. Termin związania ofertą – **30 dni (od ostatniego terminu składania ofert)**

XIV. Zamawiający nie zamierza zawierać umowy ramowej.

XV. Zamawiający nie zamierza ustanawiać dynamicznego systemu zakupów.

XVI. Zamawiający nie przewiduje zastosowania aukcji elektronicznej.

ZATWIERDZAM

DYREKTOR
Wojewódzkiej Stacji
Sanitarno-Epidemiologicznej
w Szczecinie
lek. med. Jerzy Jakubek