POWIATOWY URZĄD PRACY W ROPCZYCACH
ul. Najświętszej Marii Panny 2, 39-100 Ropczyce, tel. 17 2218172, fax 17 2227569
rzro@praca.gov.pl www.pup-ropczyce.pl

WA. 2510.1.70.2017.AK **Ropczyce, 2017-05-16**

Zaproszenie do składania ofert

Powiatowy Urząd Pracy w Ropczycach zaprasza do składania ofert cenowych na dostawę urządzenia sieciowego klasy UTM
dla Powiatowego Urzędu Pracy w Ropczycach

Postępowanie prowadzone jest z pominięciem procedur określonych w ustawie Prawo zamówień publicznych na podstawie art. 4 pkt 8 (do 30 000euro) wymienionej ustawy, w oparciu o Zarządzenie Nr 9/2015 z dnia 9.03.2015r. Dyrektora Powiatowego Urzędu Pracy w Ropczycach.

1. Zamawiający:

Powiatowy Urząd Pracy w Ropczycach
Ul. Najświętszej Marii Panny 2
39 – 100 Ropczyce

Osobami ze strony Zamawiającego upoważnionymi do kontaktowania się z Wykonawcami są:
1. Witold Cesarz tel. 17 22 31 684 e-mail wcesarz@pup-ropczyce.pl
2. Aneta Kubik tel. 17 22-31-661 e-mail akubik@pup-ropczyce.pl

2. Opis przedmiotu zamówienia:

2.1 Dostawa urządzenia sieciowego klasy UTM – 1 szt.
kategoria wg Wspólnego Słownika Zamówień (CPV) – **32420000-3,**

2.2. Wykonawca dostarczy Zamawiającemu urządzenie sieciowe klasy UTM Fortigate 100E lub równoważne, spełniające poniższe kryteria:

1. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji:
   - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
   - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
   - Obsługa połączeń szyfrowanych IPSec VPN oraz SSL VPN
   - Ochrona przed atakami - Intrusion Prevention System
   - Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
   - Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP
   - Kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma
   - Kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet
   - Możliwość analizy ruchu szyfrowanego protokołem SSL
   - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
2. Możliwość łączenia w klaster Active-Active lub Active-Passive dla urządzenia pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS
3. Monitoring stanu realizowanych połączeń VPN.

4. Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. Firewall powinien dysponować minimum 16 portami Ethernet 10/100/1000 Base-TX
6. System powinien umożliwiać zdefiniowanie co najmniej 250 interfejsów wirtualnych - definiowanych jako VLAN w oparciu o standard 802.1Q.
7. W zakresie Firewall obsługa nie mniej niż 2 milionów jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę
8. Przepustowość Firewall: nie mniej niż 7 Gbps
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 4 Gbps
10. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń. W ramach dostarczonej licencji usługa nie musi być aktywna.
11. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Dostawa powinna obejmować min. 2 tokeny programowe.
12. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) – minimum 1,5 Gbps
13. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 250 Mbps
14. W zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    - 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
15. W ramach funkcji IPSec VPN, SSL VPN – producent powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
16. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
17. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
18. Translacja adresów NAT adresu źródłowego i docelowego.
19. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
20. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
21. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
22. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 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.
23. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
24. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych 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 lub tworzenia wyjątków i reguł omijania filtra WWW.
25. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
26. System zabezpieczeń musi umożliwiać weryfikację 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

27. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    - ICSA lub EAL4 dla funkcji Firewall
    - ICSA lub NSS Labs dla funkcji IPS
    - ICSA dla funkcji: SSL VPN, IPSec VPN
28. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania.
29. W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 12 miesięcy z możliwością przedłużenia.
30. Gwarancja: system powinien być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Naprawa lub wymiana powinna zostać przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący **ma posiadać** certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię.
    Oferent winien przedłożyć dokumenty:
    - oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej;
    - certyfikat ISO 9001 podmiotu serwisującego.

3. Warunki udziału w postępowaniu i wykaz dokumentów na potwierdzenie ich spełnienia.

Zamawiający nie precyzuje warunków udziału w postępowaniu.

4. Termin i miejsce składania ofert:

do 29.05.2017r. godz. 12.00

Oferty należy składać na adres Zamawiającego:

POWIATOWY URZĄD PRACY w ROPCZYCACH
39-100 Ropczyce
ul. Najświętszej Marii Panny 2
I piętro pok. nr 12 – kancelaria

5. Termin wykonania zamówienia:

Termin realizacji zamówienia: **21 dni od podpisania umowy z Wykonawcą**.

6. Opis sposobu przygotowania oferty:

6.1 Zaleca się złożenie oferty na formularzu ofertowym przygotowanym przez Zamawiającego – wg wzoru stanowiącego załączniki nr **1 do zaproszenia.** W przypadku przygotowania oferty na innym formularzu Wykonawca umieści w nim wszelkie informacje i oświadczenia zawarte w formularzu ofertowym przygotowanym przez Zamawiającego.

6.2 Wykonawca zamieści ofertę w zamkniętej nieprzeźroczystej kopercie z napisem:

Oferta na dostawę urządzenia sieciowego
dla Powiatowego Urzędu Pracy w Ropczycach

nie otwierać przed dniem 29 maja 2017 r. – godz. 12^{15} WA.2510.1.70.2017.AK

6.3 Oferta powinna być czytelna i złożona w języku polskim.
Wszelkie zmiany w tekście oferty (przekreślenia, poprawki dopiski) powinny być podpisane lub parafowane przez Wykonawcę, w przeciwnym wypadku nie będą uwzględniane.

6.4 Ofertę podpisuje osoba lub osoby uprawnione do reprezentowania i składania oświadczeń woli w imieniu Wykonawcy. Jeżeli ofertę w imieniu Wykonawcy podpisuje pełnomocnik Wykonawcy, do oferty należy dołączyć **pełnomocnictwo**.

6.5 Oferta nie podpisana zostanie odrzucona w postępowaniu.

6.6 Na ofertę składają się następujące dokumenty:

6.6.1. Wypełniony formularz ofertowy – zgodnie z załącznikiem **nr 1**.

6.6.2. Pełnomocnictwo – jeżeli dotyczy.

6.6.3. Dokumenty wymagane w pkt 2.2 ppkt 30 (oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej, certyfikat ISO 9001 podmiotu serwisującego)

6.7 Termin związania ofertą wynosi 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

6.8 Wszelkie koszty związane przygotowaniem i złożeniem oferty ponosi Wykonawca.

6.9 **Zamawiający nie dopuszcza składania ofert częściowych.**

6.10 Zamawiający nie dopuszcza składania ofert wariantowych.

7. Otwarcie ofert nastąpi w dniu 29.05.2017r godzina 12.15.

8. Opis sposobu obliczenia ceny oferty:

8.1 Cena podana w ofercie musi obejmować wszystkie koszty związane z wykonaniem zamówienia w pełnym zakresie.

8.2 Rozliczenia pomiędzy Zamawiającym a Wykonawcą dokonywane będą w walucie „złoty polski".

8.3 Wykonawcy zobowiązani są podać cenę oferty brutto, netto, VAT w PLN.

9. Kryteria oceny ofert:

CENA – 100 %

9.1 Ocenie podlegają wyłącznie oferty spełniające wymagania określone przez Zamawiającego w niniejszym zaproszeniu.

9.2 O wyborze najkorzystniejszej oferty zadecyduje największa ilość punktów uzyskanych przez Wykonawcę w kryterium „cena" po zastosowaniu nw. wzoru:

PUNKTACJA WG WZORU: $Z = (C_n : C_o) \times 100$

gdzie:

C_n – cena najniższa wśród ofert

C_o – cena danego Wykonawcy

Obliczenia zostaną dokonane z dokładnością do dwóch miejsc po przecinku.

9.3 Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że zostały złożone dwie lub więcej ofert o takiej samej cenie, Zamawiający wezwie

Wykonawców, którzy złożyli te oferty, do złożenia, w wyznaczonym terminie, ofert dodatkowych. Zamawiający zastrzega, że Wykonawcy, składający oferty, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach. Złożenie oferty dodatkowej zawierającej wyższą ceną skutkować będzie odrzuceniem oferty z postępowania.

10. Odrzucenie oferty.

10.1 Złożenie oferty niezgodnej z opisem przedmiotu zamówienia określonym przez Zamawiającego skutkuje odrzuceniem oferty z postępowania. Za niezgodną z przedmiotem zamówienia uznaje się w szczególności ofertę, która nie uwzględnia pełnego zakresu przedmiotu zamówienia, lub ofertę zawierającą przedmiot zamówienia niezgodny z warunkami niniejszego zaproszenia.

11. Zawarcie umowy.

11.1 Zawarcie umowy nastąpi w terminie wyznaczonym przez Zamawiającego. Przed podpisaniem umowy Zamawiający może żądać od Wykonawcy przedstawienia aktualnego odpisu z właściwego rejestru (KRS) lub centralnej ewidencji i informacji o działalności gospodarczej, a w przypadku Wykonawców ubiegających się wspólnie o udzielenie zamówienia, przedłożenia umowy regulującej współpracę tych Wykonawców.

12. Unieważnienie postępowania:

12.1 Zamawiający unieważni postępowanie o udzielenie zamówienia publicznego, jeżeli:

- nie złożono żadnej oferty niepodlegającej odrzuceniu,
- cena najkorzystniejszej oferty przewyższa kwotę, którą zamawiający może przeznaczyć na sfinansowanie zamówienia, chyba, że Zamawiający może zwiększyć tę kwotę do kwoty oferty najkorzystniejszej;
- wystąpiła istotna zmiana okoliczności powodująca, że prowadzone postępowanie lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć,
- postępowanie obarczone jest wadą uniemożliwiającą zawarcie ważnej umowy w sprawie zamówienia,
- z ważnych przyczyn, których nie można było wcześniej przewidzieć.

13. Ogłoszenie wyników prowadzonego postępowania

Zamawiający powiadomi e-mailowo lub faksem Wykonawców biorących udział w postępowaniu o wynikach oraz zamieści stosowną informacje na swojej stronie internetowej.

Załączniki:
1. Formularz ofertowy.

DYREKTOR
Powiatowego Urzędu Pracy
w Kępczycach
mgr Ryszard Świętoń