OGŁOSZENIE O ZAMÓWIENIU
Usługi /dostawy/ roboty budowlane

Zamieszczenia: obowiązkowe.
Ogłoszenie dotyczy: zamówienia publicznego

SEKCJA I: ZAMAWIAJĄCY - PREZYDENT MIASTA PIŁY
I. 1)NAZWA I ADRES: Plac Staszica 10 , 64-920 Piła
I.2) RODZAJ ZAMAWIAJĄCEGO: Administracja samorządowa

SEKCJA II: PRZEDMIOT ZAMÓWIENIA
II.1) OPIS
II.1.1) Nazwa nadana zamówieniu przez zamawiającego : Dostawa sprzętu komputerowego - gate defendera wraz z 35 licencjami
II.1.2) Rodzaj zamówienia : dostawa
II.1.3) Określenie przedmiotu oraz wielkość lub zakresu zamówienia: 1. Przedmiot zamówienia

Przedmiotem zamówienia jest: dostawa date defendera wraz z 35 licencjami

Ogólna charakterystyka przedmiotu zamówienia

- Urządzenie powinno być zarządzane poprzez konsolę web za pomocą przeglądarki www.
- Dostęp do konsoli powinien być zabezpieczony poprzez zastosowanie szyfrowanego protokołu HTTPS.
- Urządzenie powinno posiadać dwa tryby pracy: transparent bridge oraz router.
- Urządzenie powinno być wyposażone w minimum 8 interfejsów sieciowych, które można skonfigurować tak by pracowały z szybkością tylko 10Mbps, tylko 100Mbps, tylko 1Gbps lub by wybierały prędkość przez autonegocjację
- Interfejsy sieciowe muszą mieć możliwość ustawienia trybu halfduplex / fullduplex
- Urządzenie powinno umożliwiać import i eksport do pliku wszystkich ustawień.
- Urządzenie powinno mieć możliwość pobrania z Internetu aktualizacji oprogramowania (na życzenie) oraz co 1,5 godziny aktualizacje baz sygnatur wirusów (automatycznie), baz sygnatur spamu i baz sygnatur kategorii stron internetowych oraz pliki reguł dla IPS. Powinna być również możliwość wymuszenia aktualizacji sygnatur na życzenie.
- Urządzenie powinno skanować następujące protokoły: HTTP (także Java oraz ActiveX), FTP, SMTP, POP3, IMAP4 oraz NNTP.
- Urządzenie powinno być wyposażone w system WatchDog (układ elektroniczny monitorujący pracę systemu. Zapobiega on sytuacjom, w których urządzenie zawiesza się i nie funkcjonuje poprawnie przez określony czas. System WatchDog otrzymuje od systemu ciągłe sygnały o jego pracy. Gdy komunikacja ta z jakiegoś powodu zostaje zatrzymana, WatchDog resetuje urządzenie, przywracając normalny tryb pracy.
- Administrator powinien mieć możliwość definiowania numerów portów na których urządzenie nasłuchuje na połączenia, które mają być przechwycone przez filtry antywirusowe i antyspamowe działające na protokołach: HTTP, FTP, SMTP, POP3, IMAP4 oraz NNTP.
- Rozwiązanie powinno natywnie wspierać pracę takich samych urządzeń w klastrze – tworząc klastry wydajnościowe bądź klastry niezawodnościowe.
- Urządzenia pracujące w klastrze powinny synchronizować między sobą konfigurację przez szyfrowany protokół.
- W jednym urządzeniu powinna być zapewniona ochrona antywirusowa, anty-spamowa, ochrona przed niepożądanymi treściami www, filtr zawartości dla HTTP, FTP i SMTP, POP3 i IMAP4, Firewall, VPN oraz IPS.

- Urządzenie powinno pełnić podstawowe funkcje routera.
- Powinna być możliwość skonfigurowania strefy DMZ.
- Dla firewalla powinna być możliwość zdefiniowania harmonogramu działania dla poszczególnych reguł.
- W module firewall powinna być możliwość logowania zdarzeń dla wybranych reguł i dla całego ruchu sieciowego.
- Firewall zastosowany w urządzeniu powinien być wyposażony w filtr statyczny i dynamiczny.
- Filtr dynamiczny firewalla powinien wykorzystywać m.in. analizę pełnostanową w FTP, PPTP, L2TP, IPSEC, status połączeń, timeouts, nawiązane połączenia.
- Filtr dynamiczny powinien wykorzystywać również Wnikliwą Analizę Pakietów tzw. Deep Packet Inspection.
- W module firewall powinna być możliwość konfigurowania dla poszczególnych interfejsów różnych reguł filtrowania pakietów.
- W module firewall powinna być możliwość ustawienia reguł na podstawie protokołów IP, ICMP, TCP i UDP.
- W module firewall powinna być możliwość określenia maksymalnej liczby jednoczesnych połączeń dla każdej z zdefiniowanych reguł.
- Urządzenie z aktywnym modułem firewall powinno oferować przepustowość conajmniej 870 Mbps.
- Moduł IPS zaimplementowany w urządzeniu powinien działać w oparciu o sieciowy system wykrywania ataków – SNORT.
- System IPS powinien skanować następujące protokoły: IP, ICMP, TCP i UDP.
- System IPS powinien wykrywać przynajmniej 4000 ataków sieciowych.
- Moduł VPN powinien umożliwiać tworzenie tuneli host-host, host-sieć, sieć-sieć.
- Moduł VPN powinien wspierać protokoły: IPSec, SSL, L2TP i PPTP.
- W przypadku modułu VPN liczba tuneli powinna być nieograniczona.
- Moduł VPN powinien wykorzystywać następujące standardy szyfrowania: 3DES, AES 128, AES 192, AES 256, Blowfish, Twofish 128, Twofish 192, Twofish 256, Serpent 128, Serpent 192, Serpent 256.
- Moduł VPN powinien mieć możliwość integracji z zewnętrznym serwerem autoryzacji RADIUS.
- Urządzenie z aktywnym modułem VPN powinno oferować przepustowość conajmniej 75 Mbps
- Urządzenie oprócz wirusów, robaków, koni trojańskich i programów szpiegowskich powinno eliminować również inne zagrożenia z Internetu takie jak: dialery, phishing, programy typu jokes, narzędzia hakerskie.
- Urządzenie powinno skanować pocztę zarówno wchodzącą jak i wychodzącą w poszukiwaniu wirusów i innych zagrożeń.
- Powinna być możliwość konfigurowania tekstu powiadomień w przypadku znalezienia wirusa.
- Powinna być możliwość wysyłania powiadomień o zdarzeniach na adres e-mail wskazany przez administratora.
- W przypadku ochrony antywirusowej powinien być zaimplementowany mechanizm analizy heurystycznej.
- W przypadku ochrony antywirusowej powinna być możliwość konfigurowania listy zaufanych stron internetowych, domen z których informacje nie będą skanowane w celu wykrywania zagrożeń internetowych.
- W przypadku ochrony antywirusowej powinien być dostępny konfigurowalny filtr zawartości plików pobieranych po protokołach HTTP i FTP, umożliwiający m.in.

określenie czy urządzenie ma przepuszczać pliki potencjalnie niebezpieczne spełniające określone założenia np.:
   1. określenie maksymalnego rozmiaru pobieranego pliku,
   2. określenie maksymalnej ilości „spakowań" pojedynczego pliku,
   3. określenie czy mają być przepuszczane pliki z makrami,
   4. określenie czy mają być przepuszczane pliki z podwójnym rozszerzeniem,
   5. określenie czy mają być przepuszczane pliki mające niezgodności typu MIME,
- W przypadku ochrony antywirusowej powinien być dostępny konfigurowalny filtr zawartości plików pobieranych po protokołach SMTP, POP3, IMAP4, umożliwiający m.in. określenie czy urządzenie ma przepuszczać pliki potencjalnie niebezpieczne spełniające określone założenia np.:
   1. określenie maksymalnego rozmiaru pobieranego pliku,
   2. określenie maksymalnej ilości „spakowań" pojedynczego pliku,
   3. określenie czy mają być przepuszczane pliki z makrami,
   4. określenie czy mają być przepuszczane pliki z podwójnym rozszerzeniem,
   5. określenie czy mają być przepuszczane pliki mające niezgodności typu MIME,
- W przypadku ochrony antyspamowej powinna być możliwość konfigurowania białej listy adresów e-mailowych, adresów IP, domen, od których wiadomości e-mail nie będą traktowane jako spam.
- W przypadku ochrony antyspamowej powinna być możliwość konfigurowania czarnej listy adresów e-mailowych, adresów IP, domen od których wiadomości e-mail będą traktowane jako spam.
- W przypadku ochrony antyspamowej w razie zakwalifikowania wiadomości jako spam powinny być opcje do wyboru co ma się z tą wiadomością stać, mianowicie: wiadomość może być automatycznie usunięta, przekierowana na wskazany adres e-mail lub do tematu wiadomości ma być dodany np. wyraz SPAM, który po ustawieniu reguł w programie pocztowym będzie automatycznie przerzucał wiadomość do osobnego katalogu.
- W przypadku filtru niepożądanych treści www powinna być możliwość wyboru kategorii tematyk jakie administrator może wytypować jako niepożądane, niepotrzebne lub niebezpieczne.
- W przypadku filtru niepożądanych treści www powinna być możliwość konfigurowania białej listy stron internetowych jakie urządzenie zawsze zakwalifikuje jako pożądane.
- W przypadku filtru niepożądanych treści www powinna być możliwość konfigurowania czarnej listy stron internetowych jakie urządzenie zawsze zakwalifikuje jako niepożądane.
- W przypadku filtru niepożądanych treści www powinna być możliwość konfigurowania listy użytkowników (po numerze IP i masce podsieci), którzy mieliby dostęp do wszystkich zasobów sieci Internet.
- Powinna być możliwość przygotowywania raportów zdarzeń jakie były wykonywane przez poszczególne moduły (anty-wirusowy, anty-spamowy, filtr zawartości (content filter) filtr zawartości stron internetowych (web content filter), firewall, IPS, VPN). Raporty powinny zawierać m.in. informacje o ilości przeskanowanych plików, wiadomości, wykrytych wirusów. Raporty powinny zawierać również informacje o tym, który komputer (adres IP) próbował pobrać zainfekowany plik lub próbował otworzyć stronę o „zabronionej" kategorii. Powinna być również podana lokalizacja, z której użytkownik próbował ściągnąć zawirusowany plik.
- Możliwość logowania wszystkich zdarzeń z urządzenia do zewnętrznego serwera Syslog.
- Możliwość monitorowania pracy urządzenia przez komunikaty SNMP v1/v2c
- Producent powinien zapewniać pomoc techniczną online oraz telefoniczną w języku polskim.
- ***Rozwiązanie powinno być dostępne z subskrypcją 1-roczną, 2-letnią lub 3letnią.***

- Licencje na 35 stanowisk na wykorzystanie usług oferowanych przez urzadzenie sprzętowe w nastepujacym zakresie:

  a/ Firewall

  b/Usługa VPN

  c/System zapobiegania włamaniom

  d/Moduł antywirusowy

  e/Filtr zawartości

  f/Moduł antyspamowy

  g/Filtr stron internetowych

II.1.4) Wspólny Słownik zamówień (CPV): 301
II.1.5) Czy dopuszcza się złożenie oferty częściowej: Nie
II.1.6) Czy dopuszcza się złożenie oferty wariantowej: Nie
II.2) CZAS TRWANIA ZAMÓWIENIA LUB TERMIN WYKONANIA: 20 grudzień 2007r
SEKCJA III: **INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM**
III.1) WARUNKI DOTYCZĄCE ZAMÓWIENIAI

Informacja na temat wadium: ***Zamawiający nie przewiduje wadium***

III.2) WARUNKI UDZIAŁU

Informacja o oświadczeniach i dokumentach, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełnienia warunków udziału w postępowaniu:

1) **Ofertę** na formularzu ofertowym o treści zgodnej z określoną we wzorze stanowiącym załącznik Nr 1
2) **Oświadczenia oraz dokumenty potwierdzające spełnianie warunków:**

a) Oświadczenie o treści określonej w **art. 22 ust.1** ustawy – Prawo zamówień publicznych - wg wzoru określonego w załączniku Nr 2

b) **aktualny** (wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert) **odpis** z właściwego rejestru albo aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej

3. **Parafowany wzór umowy** jako akceptacja jej treści i warunków załącznika nr 3

SEKCJA IV: PROCEDURA
IV.1) TRYB UDZIELENIA ZAMÓWIENIA
IV.1.1) Tryb udzielenia zamówienia: przetarg nieograniczony
IV.2) KRYTERIA OCENY OFERT
IV>2.1) Kryteria oceny ofert : cena 100

IV.2.2) Wykorzystana będzie aukcja elektroniczna: Nie
IV.3) INFORMACJE ADMINISTRACYJNE

IV.3.1) Adres strony internetowej, na której dostępna jest specyfikacja istotnych warunków zamówienia: www.bip.um.pila.pl
Specyfikację istotnych warunków zamówienia można uzyskać pod adresem:Urząd Miasta Piły, 64-920 Piła Plac Staszica 10 pok. 13
IV.3.2) Opis potrzeb i wymagań zamawiającego określonych w sposób umożliwiający przygotowanie się wykonawcy do udziału w dialogu konkurencyjnym lub informacja o sposobie uzyskania tego opisu: tekst
IV.3.3) Informacja o wysokości nagród dla wykonawców, którzy podczas dialogu konkurencyjnego przedstawili rozwiązania stanowiące podstawę do składania ofert, jeżeli zamawiający przewiduje nagrody: tekst
IV.3.4). Termin składania wniosków o dopuszczenie do udziału w postępowaniu lub ofert: 7.12.2007r godzina 12.00 miejsce: siedziba Zamawiającego, pok. 233
IV.3.5) Termin związania ofertą: okres w dniach **30** (od ostatecznego terminu składania ofert)
I**V.3.6) Informacje dodatkowe, w tym dotyczące finansowania projektu/programu ze środków Unii Europejskiej**: tekst