Gmina Celestynów zaprasza do złożenia oferty cenowej dot. usługi polegającej na zakupie wraz dostawą, instalacją i konfiguracją zgodnie z zaleceniami Zamawiającego routera do Urzędu Gminy.

W celu wyliczenia oferty Wykonawca zobowiązany jest wypełnić formularz ofertowy zgodny z załącznikiem do wiadomości i przesłać w formie pisemnej do Urzędu Gminy w Celestynowie, ul. Regucka 3, 05-430 lub na nr fax. 22 789 70 11 w terminie do **23.04.2014 r. do godz. 12:00.**

Proszę również o wyznaczenie osoby do kontaktu wraz z podaniem telefonu.

W cenie realizacji zamówienia Wykonawca uwzględni dostawę i zakup routera do Urzędu Gminy w Celestynowie.

Termin wykonania zamówienia 14 dni od podpisania umowy.

FORMULARZ OFERTOWY

Nazwa Wykonawcy:. .....

.....

adres:

.....

.....

NIP ..... REGON .....

tel..... tel. kom .....

fax. ..... na który Zamawiający może przesyłać korespondencję. Osoba wyznaczona do kontaktów z Zamawiającym ….....

….....

OPIS PRZEDMIOTU ZAMÓWIENIA

System UTM o następujących cechach:

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

2. Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

a. System powinien być zaprojektowany w taki sposób aby możliwa była jego rozbudowa w celu wyeliminowania pojedynczego punktu awarii. W tym celu powinien zapewnić co najmniej możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.

b. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

c. Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.

d. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.

e. System realizujący funkcję Firewall powinien dysponować co najmniej następującymi interfejsami:

- 2 porty Ethernet 10/100/1000 Base-TX
- 6 portów 10/100 Base-TX
- gniazdem ExpressCard w celu umożliwienia rozbudowy o opcjonalny moduł GSM

f. 2.4 Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.

g. W zakresie Firewall'a obsługa nie mniej niż 65 tys jednoczesnych połączeń oraz 4 tys. nowych połączeń na sekundę

h. Przepustowość Firewall'a: nie mniej niż 300 Mbps

i. Wydajność szyfrowania 3DES: nie mniej niż 75 Mbps

3. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:

a. kontrola dostępu - zapora ogniowa klasy Stateful Inspection

b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar

c. poufność danych - IPSec VPN oraz SSL VPN

d. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]

e. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.

f. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)

g. kontrola pasma oraz ruchu [QoS, Traffic shaping]

h. Kontrola aplikacji oraz rozpoznawanie ruchu P2P

i. Możliwość analizy ruchu szyfrowanego SSL'em

j. Ochrona przed wyciekiem poufnej informacji (DLP)

4. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 45 Mbps

5. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 110 Mbps

6. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:

a. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site

b. Dostawca musi dostraczyć nielimitowanego klienta VPN współpracującego z propomownym rozwiązaniem.

c. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności

d. Praca w topologii Hub and Spoke oraz Mesh

e. Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF

f. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

7. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, 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.

8. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.

9. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.

10. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)

11. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ

12. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)

13. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 4000 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.

14. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP

15. Baza filtra WWW o wielkości co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.

16. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

17. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:

a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu

b. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP

c. haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych

d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Direktory bez konieczności instalowania jakiegokolwiek oprogramowania a kontrolerze domeny.

18. Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty ICSA dla funkcjonalności Firewall, IPS, Antywirus, SSL VPN

19. 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. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania, Dostawca winien przedłożyć dokument w j. polskim 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). Zamawiający wymaga od Oferenta dostarczenia oświadczenia autoryzowanego przedstawiciela producenta na terenie Polski, iż rozwiązania objęte oferowanymi usługami serwisowymi producenta, w przypadku korzystania z tych usług, zostaną przyjęte do naprawy w autoryzowanym punkcie serwisowym producenta na terenie Polski oraz, że pochodzą one z oficjalnego kanału sprzedaży na terenie Polski.

Wymaga się aby dostawa obejmowała również:

a. Minimum 12 miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu

a. Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 12 m-ce liczoną od dnia zakończenia wdrożenia całego systemu

b. 12 miesięczny Serwis logistyczny na terenie Polski z dostawą urządzenia zastępczego na drugi dzień roboczy / 8x5xNBD gwarantujący udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy w Następnym Dniu Roboczym.

Składam ofertę cenową na zakup wraz z dostawą, instalacją i konfiguracją routera do Urzędu Gminy w Celestynowie:

MODEL:

PRODUCENT:

Oferujemy/oferuję wykonanie ww. przedmiotu zamówienia zgodnie z warunkami zawartymi w zaproszeniu do składania ofert (opis przedmiotu zamówienia) za kwotę: ……

netto…….....% VAT, brutto…….……słownie (……..……..……).

Jednocześnie oświadczam, że podane ceny uwzględniają wszelkie koszty związane z wykonaniem zamówienia wraz z dostawą zamówienia do siedziby Zamawiającego.

W przypadku wyboru naszej oferty, zobowiązujemy się do podpisania umowy w terminie i miejscu wyznaczonym przez Zamawiającego.

W celu wykazania spełnienia przez Wykonawcę warunków udziału w postępowaniu Zamawiający żąda załączenia do oferty:

- aktualnego odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2 ustawy, wystawionego nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

....., dn. _ _ . _ _ .2014 r. .....

Podpis osób uprawnionych do składania oświadczeń woli w imieniu Wykonawcy oraz pieczątki.