STAROSTWO POWIATOWE
W GOŁDAPI
19-500 Gołdap; ul. Krótka 1

Gołdap, 29 września 2016 r.

Znak sprawy: OR.272.2.3.2016

ZAPROSZENIE DO SKŁADANIA OFERT

1. Zamawiający:

Starostwo Powiatowe w Gołdapi
ul. Krótka 1, 19-500 Gołdap, NIP 847-14-62-135
zaprasza do złożenia oferty na: **dostawę urządzenia UTM do Starostwa Powiatowego w Gołdapi.**

2. Opis przedmiotu zamówienia:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Dla elementów systemu bezpieczeństwa obsługujących Zamawiającego, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.

3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
6. System realizujący funkcję Firewall powinien dysponować minimum 16 portami Ethernet 10/100/1000 Base-TX
7. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
8. W zakresie Firewall'a obsługa nie mniej niż 1,5 miliony jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę
9. Przepustowość Firewall'a: nie mniej niż 2 Gbps
10. Wydajność szyfrowania VPN IPSec: nie mniej niż 120 Mbps
11. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 16 GB. System powinien 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 platformy sprzętowej lub programowej.
12. System realizujący funkcję kontroli przed złośliwym oprogramowaniem musi mieć możliwość współpracy z platformą lub usługą typu Sandbox w celu eliminowania nieznanych dotąd zagrożeń.

13. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    - Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
    - Poufność transmisji danych - połączenia szyfrowane 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 (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów)
    - Możliwość analizy ruchu szyfrowanego protokołem SSL
    - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
    - System powinien realizować kontrolę sieci botnet również w oparciu o bazy reputacyjne sdresów IP oraz domen.
    - W ramach systemu powinna zostać dostarczona funkcja analizy behawioralnej plików (Sandbox) realizowana lokalnie lub w postaci usługi w chmurze.
    - Dostarczone rozwiązanie powinno być wyposażone w mechanizmy analizy złośliwego kodu dla urządzeń mobilnych. W ramach postępowania koniecznym jest dostarczenie licencji niezbędnych do aktualizacji sygnatur niezbędnych do takiej analizy.
14. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 900 Mbps
15. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 200 Mbps
16. 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
17. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
18. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
19. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.
20. Translacja adresów NAT adresu źródłowego i docelowego.

21. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
22. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
23. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) oraz powinien umożliwiać skanowanie archiwów typu zip, RAR.
24. 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.
25. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
26. Baza filtra WWW 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.
27. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
28. 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
29. 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
30. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
31. Serwisy i licencje
    - W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres co najmniej 36 miesięcy.
32. System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.

33. Zamawiający przewiduje możliwość wymiany dotychczas posiadanego UTM FortiGate 80C na model spełniający ww. wymagania
34. Wykonawca przez rok powinien zapewnić wsparcie Zamawiającemu w zakresie:
    - uruchomienia nowego urządzenia
    - wstępnej konfiguracji urządzenia w zakresie: konfiguracji łącza internetowego, konfiguracji stref bezpieczeństwa, konfiguracji VPN
    - rozwiązywania bieżących problemów zgłaszanych przez Zamawiającego
    - wsparcie będzie świadczone telefonicznie, pocztą elektroniczną lub za pomocą narzędzi do zdalnej pomocy
35. Wykonawca w ramach wdrożenia urządzenia UTM przeprowadzi szkolenie z zaawansowanej konfiguracji i obsługi oferowanego urządzenia dla 1 pracownika Zamawiającego;
    - Szkolenie w formie warsztatów,
    - Tematyka szkolenia musi obejmować min.:
        - ✓ ustawienia routingu na zakupionym urządzeniu,
        - ✓ kontrolę urządzeń,
        - ✓ konfigurację polityk bezpieczeństwa w oparciu o adresy, użytkowników urządzenia,
        - ✓ konfigurację VPN,
        - ✓ konfigurację wirtualnych domen,
        - ✓ raportowanie
    - Szkolenie zostanie przeprowadzone w miejscu wskazanym przez Wykonawcę przy czym szkolenie nie może odbyć się dalej niż 320 km od siedziby Zamawiającego,
    - Prowadzący powinien posiadać certyfikat producenta urządzenia poświadczający posiadanie odpowiednich umiejętności z zakresu zagadnień poruszonych na szkoleniu,
    - Szkolenie musi się odbyć w ciągu 12 miesięcy od podpisania umowy,
    - W przypadku szkolenia kilkudniowego poza siedzibą Zamawiającego, Wykonawca zapewnia nocleg dla pracownika Zamawiającego.

3. Termin realizacji zamówienia: 14 dni roboczych od dnia podpisania umowy.

4. Warunki płatności: na podstawie poprawnie faktury wystawionej po podpisaniu protokołu dostawy urządzenia z terminem płatności 14 dni

5. Kryteria wyboru ofert: Cena – 80%. Cena zamówienia musi zawierać wszystkie koszty niezbędne do realizacji zamówienia np.: opakowanie, transport, itp.

Dodatkowy okres upoważniający do pobierania aktualizacji baz zabezpieczeń (co najmniej 12 miesięcy) – 20%

6. Sposób przygotowania oferty:

Ofertę należy sporządzić wg wzoru Formularza ofertowego załączonego do niniejszego zaproszenia, w języku polskim.

Przy wyliczaniu wartości poszczególnych elementów, należy ograniczyć się do dwóch miejsc po przecinku w PLN.

7. Miejsce i termin składania ofert:

Ofertę należy przesłać drogą emailową na adres: informatyk@powiatgoldap.pl do Starostwa Powiatowego, ul. Krótka 1, 19-500 Gołdap do dnia 3 października 2016 roku godzina 11.00

Osoba upoważniona do kontaktów z Wykonawcami: Łukasz Dębowski, email: informatyk@powiatgoldap.pl Tel. 87 615 44 05

Uwaga!

1. Zamawiający zastrzega sobie prawo do:
   - poproszenia Wykonawcę o dodatkowe informacje dotyczące zgodności oferowanego przedmiotu z opisem przedmiotu zamówienia.
   - unieważnienia postępowania bez podania przyczyny.
2. Termin związania ofertą wynosi 14 dni.
3. Wykonawca ma obowiązek zachowania tajemnicy w zakresie infrastruktury bezpieczeństwa Zamawiającego

WICESTAROSTA
Grażyna Barbara Senda

(Data i podpis Kierownika Zamawiającego)

STAROSTWO POWIATOWE
W GOŁDAPI
19-500 Gołdap; ul. Krótka 1

UMOWA OR.272.2.3.2016 (WZÓR)

zawarta w Gołdapi, dnia ..... 2016 r. pomiędzy Starostwem Powiatowym w Gołdapi, 19 – 500 Gołdap, ul. Krótka 1, NIP: 847 14 62 135, zwanym w dalszej części umowy „**Zamawiającym**" reprezentowanym przez:
Andrzeja Ciołka – Starostę Gołdapskiego,
przy kontrasygnacie Bożeny Radzewicz - Skarbnika Powiatu,
a firmą:
....., NIP: ....., reprezentowaną przez: ....., zwaną dalej „**Wykonawcą**".

W nawiązaniu do rozpoznania cenowego w sprawie udzielenia zamówienia publicznego o wartości szacunkowej powyżej 4000 euro netto, a których wartość nie przekracza kwoty 10.000 euro netto OR.272.2.2.2016 z dnia ... września 2016 r. na dostawę urządzenia UTM do Starostwa Powiatowego w Gołdapi została zawarta umowa następującej treści:

§1

1. Wykonawca zobowiązuje się dostarczyć do Starostwa Powiatowego w Gołdapi przedmiot zamówienia zgodnie z ofertą złożoną dnia .....

§2

Wykonawca zobowiązuje się wykonać zamówienie w ciągu czternastu dni roboczych od daty podpisania niniejszej umowy.

§3

1. Zapłatę za dostarczenie przedmiotu umowy ustala się na kwotę ..... zł brutto (słownie .....).
2. Wynagrodzenie, o którym mowa w ust. 1 płatne będzie po wykonaniu ww. przedmiotu umowy.
3. Podstawą do wystawienia faktury jest: protokół odbioru, podpisany przez Zamawiającego oraz Wykonawcę.
4. Wynagrodzenie płatne będzie przelewem na rachunek bankowy Wykonawcy, w terminie 14 dni od daty doręczenia prawidłowo wystawionej przez Wykonawcę faktury VAT.
5. Faktura powinna być adresowana na Starostwo Powiatowe w Gołdapi, ul. Krótka 1, 19-500 Gołdap, NIP 847-14-62-135.
6. Wynagrodzenie brutto nie ulega zmianie przez okres trwania umowy. Zamawiający nie przewiduje możliwości zmiany wynagrodzenia brutto w przypadku zmiany stawki VAT określonej przepisami ustawy o podatku VAT.

§4

Wszystkie zmiany i uzupełnienia niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§5

W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu Cywilnego.

§6

Spory wynikłe na tle niniejszej umowy rozstrzygane będą przez Sąd właściwy dla siedziby Zamawiającego.

§7

Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Wykonawca

Zamawiający