SI-II.2601.43.2018 Olsztyn, 22 czerwca 2018 r.

ZAPYTANIE OFERTOWE

Departament Społeczeństwa Informacyjnego Urzędu Marszałkowskiego Województwa Warmińsko-Mazurskiego w Olsztynie, ul. Głowackiego 17, 10-447 Olsztyn, zaprasza do przedłożenia oferty cenowej na **dostawę urządzenia klasy UTM – 1 szt..**

1. Opis przedmiotu zamówienia:

Przedmiotem zamówienia jest dostawa 1 (jednego) urządzenia klasy UTM, spełniającego poniższe wymagania :

1. System pełniący funkcję Firewall'a, IPSec VPN'a oraz routera musi być zaprojektowany w taki sposób, aby możliwa była jego rozbudowa w celu wyeliminowania pojedynczego punktu awarii. W tym celu musi zapewnić co najmniej:
   a. Możliwość łączenia w klaster Active-Active lub Active-Passive w przypadku systemu Firewall oraz IPSec VPN
   b. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   c. Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów w realizowanej strukturze zgodnie z trasą definiowaną przez protokół OSPF.
2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z dwóch trybów: router z funkcją NAT lub transparentnym.
3. System realizujący funkcję Firewall musi dysponować minimum:
   a. potem USB
   b. portem konsolowym
   c. dedykowanym portem 1Gbps RJ45 DMZ
   d. dedykowanym portem RJ45 do zarządzania
   e. dedykowanymi minimum 2 portami 1Gbps RJ45 typu WAN
   f. dedykowanymi minimum 16 portami 1Gbps RJ45 typu internal switch (przełącznik wbudowany) w tym minimum 2 porty tupu COMBO mogącymi pracować na wkładkach SFP
   g. wbudowaną przestrzenią dyskową (od 400 do 500 GB) do przechowywania informacji, generowanych przez urządzenie, przestrzeń dyskowa musi opierać się o technologię SSD
4. Możliwość tworzenia interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.

5. W zakresie Firewall'a obsługa nie mniej niż 1,8 miliona jednoczesnych sesji oraz minimum 28 tys. nowych sesji na sekundę.
6. Przepustowość Firewall'a: nie mniej niż 6Mpps lub 7Gbps (dla pakietów 1518 bajtów UDP).
7. Możliwość utrzymania nie mniej niż 280 równoczesnych sesji SSL VPN
8. 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, FITTP, FTP, HTTPS,
   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, witryn typu proxy avoidance oraz 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.
   j. Kontrola wysyłania plików z możliwością zablokowania ich wysyłania
9. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Statefull Firewall, Antivirus, WebFilter – min 350 Mbps.
10. W zakresie kontroli treści WWW musi istnieć możliwość współpracy z zewnętrznymi systemami cache'a dla ruchu HTTP.
11. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 1,8 Gbps. System IPS musi umożliwiać włączenie dowolnych sygnatur sprawdzających niezależnie dla określonych par interfejsów, VLAN'ów lub adresów IP.
12. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    a. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site.
    b. Wykonawca musi dostarczyć klienta VPN współpracującego z proponowanym 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 routingu, np. OSPF.
    f. Obsługa mechanizmów: IPSec NATTraversal, uwierzytelniania dla połączeń.
13. Rozwiązanie musi zapewniać: obsługę routingu statycznego i dynamicznego w oparciu o protokoły OSPF i BGP Protokół OSPF musi funkcjonować w ramach terminowanych na urządzeniu połączeń IPSec VPN.
14. Możliwość budowy min 10 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, FirewalTa, Antywirus'a, IPS'a, Web Filteringu.
15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
16. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
17. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
18. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
19. Ochrona IPS musi opierać się co najmniej na analizie protokołów i sygnatur. Ponadto

administrator systemu musi mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo musi być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS.

20. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
21. Baza filtra WWW adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, proxy avoidance, spam URL). W przypadku ograniczeń wewnętrznych rozwiązania istnieje możliwość zastosowania dodatkowego system do URL Filteringu. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
22. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
23. 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) w oparciu o zewnętrzne bazy danych,
    d. rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On dla funkcjonalności Firewall oraz Web Filtering w środowisku Microsoft Active Directory.
24. Funkcje bezpieczeństwa systemu muszą posiadać certyfikaty:
    a. ICSA dla funkcjonalności IPSec VPN, IPS, Antywirus,
    b. ICSA lub EAL4 dla funkcjonalności Firewall.
25. Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) lub 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.
26. Deklaracja zgodności CE na dostarczony sprzęt (wraz z dostawą).
27. Pełna integracja z rozwiązaniami FortiAnalyzer i FortiManager (dla wersji oprogramowania 5.4) firmy Fortinet posiadanymi przez zamawiającego.
28. Urządzenie musi posiadać wsparcie producenta urządzenia w okresie 5 lat od zakupu w trybie serwisowym - 8 godzin dziennie przez 5 dni w tygodniu. Wsparcie musi obejmować:
    a. wymianę urządzenia w przypadku jego fizycznej awarii
    b. możliwość aktualizacji oprogramowania urządzenia (firmware)
    c. możliwość aktualizacji komponentów składowych takich jak: filtrowanie stron oraz ich typów, szczepionki antywirusa, baza aplikacji oraz ich typów, filtrów antyspamu, definicji sieci botnetowych, IPS, oraz innych wbudowanych funkcji.
29. Urządzenie powinno być fabrycznie nowe i dostarczone w fabrycznym, niezniszczonym opakowaniu producenta urządzenia.

2. Opis kryterium wykonawcy:

Kryterium wyboru wykonawcy jest cena 100%. Cena powinna być podana w złotych w kwocie netto + VAT.

3. Warunki realizacji zamówienia:

Dostarczenie przedmiotu zamówienia w terminie 14 dni od dnia otrzymania zamówienia przez Wykonawcę. Przedmiot zamówienia należy dostarczyć do: Departament Społeczeństwa Informacyjnego Urzędu Marszałkowskiego Województwa Warmińsko-Mazurskiego w Olsztynie, ul. Głowackiego 17, 10-477 Olsztyn.

4. Termin i sposób złożenia oferty przez wykonawcę:

Ofertę proszę złożyć do 02 lipca 2018 r. do godz. 12:00 wyłącznie na adres mailowy: zakupy.dsi@warmia.mazury.pl. Proszę o wpisanie w tytule wiadomości: SI-II.2601.43.2018

5. Płatność

Płatność nastąpi w terminie 14 dni po dostarczeniu ww. przedmiotu zamówienia zgodnie z opisem przedmiotu zamówienia oraz prawidłowo wystawioną fakturą VAT.

Dane do faktury:
Nabywca: Województwo Warmińsko-Mazurskie, ul. Emilii Plater 1, 10-562 Olsztyn, NIP: 739-38-90-447
Odbiorca: Urząd Marszałkowski Województwa Warmińsko-Mazurskiego w Olsztynie, ul. Emilii Plater 1, 10-562 Olsztyn

6. Warunki ogólne:

- Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez podania przyczyny.
- Oferent może wprowadzić zmiany w złożonej ofercie lub ją wycofać, pod warunkiem, że uczyni to przed upływem terminu składania ofert. Zarówno zmiana jak i wycofanie oferty wymagają zachowania formy pisemnej.
- Zamawiający zastrzega sobie prawo sprawdzania w toku oceny ofert wiarygodności przedstawionych przez Oferentów informacji.
- Zamawiający wykluczy z postępowania Oferentów, co do których wskutek sprawdzenia wiarygodności oferty poweźmie informację o zawarciu w złożonej ofercie danych niezgodnych z prawdą.
- Ofertę Oferenta wykluczonego z postępowania uznaje się za odrzuconą.
- Oferty złożone po terminie nie zostaną rozpatrzone.
- Oferenci uczestniczą w postępowaniu ofertowym na własne ryzyko i koszt, nie przysługują im żadne roszczenia z tytułu odstąpienia przez Zamawiającego od realizacji postępowania ofertowego.
- Zamawiający bierze pod uwagę wyłącznie oferty przesłane na adres mailowy wskazany w zapytaniu ofertowym.
- Zamawiający zastrzega sobie możliwość wyboru kolejnej wśród najkorzystniejszych ofert, jeżeli oferent, którego oferta zostanie wybrana jako najkorzystniejsza, uchyli się od umowy o realizację przedmiotu niniejszego zamówienia.

7. Osoby do kontaktów

W sprawach technicznych: Marek Konopiński, tel. 89 521 94 07, e-mail: m.konopinski@warmia.mazury.pl
W sprawach realizacji zamówienia: Jakub Jakimczuk, tel. 89 521 94 38, e-mail: j.jakimczuk@warmia.mazury.pl