Załącznik Nr 1
do Zapytania Ofertowego
ZP. 271.A.26.2012
z dnia 8 maja 2012 r.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

System ochrony sieci komputerowej i informacji.
(lista minimalnych wymagań, tzn.: „nie gorszych niż...")

Cel: Budowa skutecznego systemu ochrony sieci komputerowej i aplikacji przed zagrożeniami.

1. Założenie funkcyjne.
   System musi posiadać zintegrowaną architekturę bezpieczeństwa – w jednym urządzeniu realizuje następujące funkcje:
   1) [FW] Zapora Ogniowa / Firewall Stateful Inspection
   2) [AV] Antywirus
   3) [IDP] System detekcji i prewencji włamań (IPS+IDS)
   4) [VPN] Szyfracji danych: IPSec z rozbudową do SSL
   5) [AS] Filtrację SPAMu (Antyspam)
   6) [WF] Filtrację stron www (Web Filter)
   7) [TS] Kontrolę pasma (Traffic Shaping)
   8) IM/P2P Kontrola komunikatorów (IM) i aplikacji P2P
   9) [DLP] Ochrona przed wypływem informacji z wewnątrz instytucji
   10) Kontrola aplikacji oparta na sygnaturach charakterystyki ruchu (min.1000 zdefiniowanych aplikacji)
2. Wszystkie funkcje muszą być realizowane w oparciu o technologie i podzespoły jednego producenta.
3. System musi pracować bez użycia dysków twardych, jedynie w oparciu o pamięci FLASH.
4. Funkcjonalność antywirusa musi być zaimplementowana w oparciu o sprzętowy akcelerator (ASIC).
5. Firewall musi obsługiwać NAT traversal dla protokołów SIP i H323.
6. Firewall musi umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer Windows AD, RADIUS lub LDAP.
7. Możliwość podłączenia modemu 3G na złączu PCExpress.
8. Antywirus musi skanować protokoły HTTP, HTTPS FTP, POP3, POP3S, IMAP, IMAPS i SMTP, SMTPS, IM, NNTP.
9. Antywirus musi transferować częściowo przeskanowany plik do klienta w celu zapobieżenia przekroczeniu dopuszczalnego czasu oczekiwania (timeout).
10. Antywirus musi skanować zarówno na bazie sygnatur jak i heurystycznie.
11. Urządzenie musi obsługiwać NAT Traversal dla VPN.
12. Producent musi dostarczyć klienta VPN dla systemu Windows 2000 / XP / XP 64 Bit / Vista / Vista 64 Bit / Seven / Seven 64Bit / Server / Server 64 Bit / Mobile / Symbian, własnej produkcji wyposażonego dodatkowo w moduł firewall wraz z filtrem antywirusowym, antyspamowym oraz filtracji kategorii treści WWW.
13. Urządzenie musi być klientem usług dynamicznego DNS'u.
14. Zawarty moduł antyspamowy musi pracować w obrębie protokołów SMTP, POP3 i IMAP.
15. Antyspam musi bazować na wielu czynnikach, takich jak:
    1) Sprawdzenie zdefiniowanych przez administratora adresów IP przez które przechodził mail,

2) Sprawdzenie zdefiniowanych przez administratora adresów pocztowych,
3) RBL, ORDBL
4) Sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych.

16. Oprócz powyższego mechanizm antyspamowy musi umożliwiać skorzystanie z zewnętrznej, wieloczynnikowej bazy spamu.
17. Moduł filtracji stron www musi mieć możliwość filtracji:
    1) na bazie białej i czarnej listy URL,
    2) w oparciu o zawarte w stronie słowa kluczowe z możliwością określania wag,
    3) javy, cookies i ActiveX.
18. Oprócz powyższego moduł filtracji musi umożliwiać kategoryzację w oparciu o gotową bazę przynajmniej 54 mln już skategoryzowanych stron www, pogrupowanych w 77 kategorii, 6 klas treści oraz umożliwiać kategoryzację ręczną.
19. Wszystkie moduły programowe i funkcje muszą pochodzić od jednego producenta.
20. Urządzenie musi dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej lub jako bridge warstwy drugiej.
21. Urządzenie musi wspierać konfigurację wysokiej dostępności w klastrach do 32 nodów zarówno w trybie Active-Active jak i Active-Standby w obu trybach (p. 19).
22. Urządzenie musi wspierać routing statyczny i dynamiczny w oparciu o protokoły RIP, OSPF, BGP4, PIM.
23. Urządzenie musi wspierać policy routing w oparciu o adres źródła, porty, interface wejściowy.
24. Urządzenie musi wspierać różne poziomy i domeny uprawnień dla administratorów
25. Dla urządzenia musi być dostępne zewnętrzne sprzętowe urządzenie logujące pochodzące od tego samego producenta.
26. Dla urządzenia musi być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
27. System musi umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z dowolnej pamięci USB.
28. System musi ponadto spełniać następujące minimalne parametry techniczne:
    1) minimalna liczba niezależnych portów Ethernet 10/100 musi wynosić – 6,
    2) minimalna liczba niezależnych portów Ethernet 10/100/1000 musi wynosić – 2,
    3) minimalna przepustowość Firewall-a musi wynosić – 350,00 Mbps,
    4) minimalna przepustowość przy szyfrowaniu 3DES musi wynosić – 80 Mbps,
    5) minimalna liczba tuneli VPN nie może być mniejsza niż – 200,
    6) minimalna liczba nowych sesji na sekundę nie może być mniejsza niż – 5 000,
    7) minimalna liczba równoczesnych sesji nie może być mniejsza niż – 100.000,
    8) możliwość podłączenia dedykowanego urządzenia zewnętrznego do rejestracji logów długoterminowych o minimalnej pojemności pamięci – 750GB,
    9) elementy umożliwiające montaż w szafie rack 19’’.

29. Założenia dodatkowe – serwis i szkolenia, gwarancja:
    1) gwarancja producenta na okres 12 miesięcy,
    2) subskrypcje oprogramowania i serwisu na okres 24 miesięcy,
    3) w przypadku stwierdzenia uszkodzenia urządzenia w okresie gwarancyjnym Wykonawca dostarczy i zainstaluje na czas naprawy identyczne urządzenie zastępcze w następnym dniu roboczym. Zgłoszenia serwisowe przyjmowane będą w trybie 8x5. Wykonawca zapewnia pierwszą linię wsparcia technicznego telefonicznie w języku polskim (w godzinach 8:00 – 16:00, od poniedziałku do piątku),
    4) Wykonawca przeprowadzi na własny koszt szkolenie w języku polskim w autoryzowanym centrum szkoleniowym producenta, wyznaczonego przez Zamawiającego pracownika, z zakresu obsługi i konfiguracji systemu, potwierdzone stosownym certyfikatem,
    5) w zakres zamówienia wchodzi oprócz dostawy wyspecyfikowanych urządzeń, także ich wdrożenie na miejscu u Zamawiającego przez certyfikowanego inżyniera (certyfikat do umowy poświadczający zdanie egzaminów i znajomość konfiguracji dostarczanego systemu bezpieczeństwa na poziomie min. II producenta oferowanego rozwiązania),
    6) Wykonawca musi posiadać co najmniej dwóch certyfikowanych inżynierów w zakresie obsługi oferowanego sprzętu (kserokopie certyfikatów dostarczone do umowy),
    7) w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania, Wykonawca winien przedłożyć dokument 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.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych. Wymagane dokumenty należy przedłożyć przed zawarciem umowy.