ZAŁĄCZNIK B

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa dwóch urządzeń klasy UTM wraz z implementacją w sieci komputerowej Powiatowego Urzędu Pracy w Opolu”

Cel:

Budowa systemu bezpieczeństwa do kompleksowej ochrony sieci i aplikacji przy jednoczesnym zachowaniu:

- niskich kosztów eksploatacji i utrzymania systemu,
- wysokiej wydajności i niezawodności systemu oraz
- ograniczeniu kosztów rozbudowy istniejącego systemu IT i jego złożoności

Dla spełnienia w/w celu i założeń system musi spełniać następujące wymagania:

1. Założenie funkcyjne - system musi posiadać zintegrowaną architekturę bezpieczeństwa, tzn. w jednym urządzeniu umożliwia realizacje następujących funkcji:
    a. Firewall klasy *Stateful Inspection*
    b. Antywirus
    c. System detekcji i prewencji włamań (IDP)
    d. VPN, zgodny z IPSec, PPTP i L2TP z możliwością rozbudowy do SSL-VPN
    e. Antyspam
    f. Filtracja stron www
    g. Kontrola pasma (Traffic Management)
2. Wszystkie funkcje muszą być realizowane w oparciu w technologie i podzespoły jednego producenta.
3. System powinien pracować bez użycia dysków obrotowych, w oparci o pamięci FLASH.
4. Funkcjonalność antywirusa powinna być zaimplementowana w oparciu o sprzętowy akcelerator (ASIC).
5. Firewall powinien obsługiwać NAT traversal dla protokołów SIP i H323.
6. Firewall powinien umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS lub LDAP.
7. Antywirus powinien skanować protokoły HTTP, FTP, POP3, IMAP i SMTP.
8. Antywirus powinien móc transferować częściowo przeskanowany plik do klienta w celu zapobieżenia przekroczeniu dopuszczalnego czasu oczekiwania (timeout).
9. Antywirus powinien skanować zarówno na bazie sygnatur jak i heurystycznie.
10. Urządzenie powinno obsługiwać NAT Traversal dla VPN.
11. Producent powinien móc dostarczyć klienta VPN własnej produkcji wyposażonego dodatkowo w moduł firewall i antywirusowy.
12. Urządzenie powinno móc być klientem usług dynamicznego DNS’u.
13. Zawarty moduł antyspamowy powinien pracować w obrębie protokołów SMTP, POP3 i IMAP.
14. Antyspam powinien bazować na wielu czynnikach, takich jak:
    a. sprawdzenie zdefiniowanych przez administratora adresów IP przez które przechodził mail,
    b. sprawdzenie zdefiniowanych przez administratora adresów pocztowych,
    c. RBL, ORDBL
    d. Sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych
15. Oprócz powyższego mechanizm antyspamowy powinien umożliwiać skorzystanie z zewnętrznej, wieloczynnikowej bazy spamu.
16. Moduł filtracji stron www powinien mieć możliwość filtracji:
    a. Na bazie białej i czarnej listy URL
    b. W oparciu o zawarte w stronie słowa kluczowe
    c. Javy, cookies i ActiveX

17. Oprócz powyższego moduł filtracji powinien umożliwiać kategoryzację w oparciu o bazę przynajmniej 25 mln stron www pogrupowanych w 56 kategorii.
18. Wszystkie moduły programowe i funkcje powinny pochodzić od jednego producenta.
19. Urządzenie powinno dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej lub jako bridge warstwy drugiej.
20. Urządzenie powinno wspierać konfigurację wysokiej dostępności w klastrach do 32 nodów zarówno w trybie Active-Active jak i Active-Standby w obu trybach.
21. Urządzenie powinno wspierać routing statyczny i dynamiczny w oparciu o protokoły RIP i OSPF.
22. Urządzenie powinno wpierać policy routing w oparciu o adres źródła, porty, interface wejściowy.
23. Urządzenie powinno wspierać różne poziomy i domeny uprawnień dla administratorów.
24. Dla urządzenia powinno być dostępne zewnętrzne sprzętowe urządzenie logujące pochodzące od tego samego producenta.
25. Dla urządzenia powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
26. Urządzenie powinno posiadać certyfikaty iCALabs Firewall, AntiVirus, SSL-TLS, IPs.

System powinien ponadto spełniać następujące minimalne parametry techniczne:

1. Minimalna liczba niezależnych portów Ethernet 10/100 powinna wynosić cztery (4).
2. Minimalna przepustowość Firewall-a powinna wynosić 70 Mbps.
3. Minimalna przepustowość przy szyfrowaniu 3DES powinna wynosić 20 Mbps.
4. Minimalna liczba tuneli VPN nie powinna być mniejsza niż 40.
5. Minimalna liczba polityk bezpieczeństwa Firewall’a nie powinna być mniejsza niż 500.
6. Minimalna liczba wpisów w tablicy routingu nie powinna być mniejsza niż 32.
7. Minimalna liczba równoczesnych sesji nie powinna być mniejsza niż 50 000.