



Warszawa, 10.03.2011 r.

## Załącznik nr 1 Załącznik techniczny przedmiotu zamówienia nr 1.3/2011 – zakup urządzenia firewall/router wraz z dostawą do siedziby Zamawiającego

Przedmiotem zamówienia jest zakup dwóch urządzeń firewall/router, działających w klastrze High Availability, posiadających zintegrowaną architekturę bezpieczeństwa.

Specyfikacja techniczna firewall/router:

### ZAPORA KORPORACYJNA (Firewall)

1. Urządzenie powinno obsługiwać translacje adresów NAT, PAT, 1-PAT.
2. Administrator powinien mieć możliwość zdefiniowania harmonogramu dla minimum 10 różnych zestawów reguł na firewall'u określający dzień tygodnia, godzinę w jakich nastąpi automatyczne uruchomienie konkretnego zestawu.
3. Oprogramowanie dostarczone przez producenta powinno posiadać graficzny edytor konfiguracji harmonogramu reguł na firewall'u.
4. Urządzenie powinno dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej lub jako bridge warstwy drugiej lub hybrydowo (część jako router a część jako bridge).
5. Edytor reguł na firewall'u powinien posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).
6. Firewall powinien umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS lub LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows NT4.0 (NTLM) i Windows 2k (Kerberos).

### INTRUSION PREVENTION SYSTEM (IPS)

7. System detekcji i prewencji włamań (IPS) powinien być zaimplementowany w jądrze systemu i wykrywać włamanie oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
8. Administrator powinien mieć możliwość wyłączenia analizy protokołów oraz analizy w oparciu o sygnatury kontekstowe dla wybranych połączeń.
9. IPS powinien być konfigurowalny na poziomie reguł dla firewall'a. Cecha ta ma umożliwiać wykorzystanie harmonogramu dla firewall'a w celu użycia tego samego harmonogramu dla IPS.
10. Dla ustawień IPS możliwe jest skonfigurowanie co najmniej 4 profili ustawień. Przy czym w domyślnej konfiguracji jeden profil jest ustawiony automatycznie dla połączeń wychodzących, a drugi dla połączeń przychodzących.

*Dla rozwoju Mazowsza*



#### KSZTAŁTOWANIE PASMA (Traffic Shapping)

11. Urządzenie powinno mieć możliwość kształtowania pasma w oparciu o priorytyzację oraz o minimalną i maksymalną wartość dostępnego pasma.

#### OCHRONA ANTYWIRUSOWA

12. Rozwiązanie pozwala na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
13. Co najmniej jeden z dwóch skanerów antywirusowych powinien być dostarczany w ramach podstawowej licencji.
14. Skaner antywirusowy powinien skanować ruch poprzez mechanizm Proxy. Skanowane są protokoły HTTP, POP3, SMTP.

#### OCHRONA ANTYSZPAM

15. Producent powinien udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM) w oparciu o białe/czarne listy, DNS RBL, Moduł analizy heurystycznej

#### WIRTUALNE SIECI PRYWANE (VPN)

16. Urządzenie powinno posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
17. Odpowiednio kanały VPN można budować w oparciu o PPTP VPN, IPSec VPN, SSL VPN.

#### FILTR ADRESÓW URL

18. Filtr URL powinien działać w oparciu o klasyfikacje adresów URL dostarczoną przez producenta, klasyfikacje adresów stworzoną przez administratora oraz klasyfikacje firmy trzeciej (opcjonalnie)

#### UWIERZYTELNIANIE

19. Urządzenie powinno pozwalać na uruchomienie systemu uwierzytelniania w oparciu o:
  - a. lokalną bazę użytkowników (wewnętrzny LDAP),
  - b. zewnętrzną bazę użytkowników (zewnętrzny LDAP) ,
  - c. integrację z serwerem Microsoft Active Directory.
20. Rozwiązanie powinno pozwalać na uruchomienie specjalnego portalu, który umożliwia autoryzację w oparciu o protokoły SSL, Radius, NTLM, Kerberos.
21. Autoryzacja może zostać włączona na:
  - a. Zewnętrznym interfejsie (od strony sieci Internet)
  - b. Wewnętrznym interfejsie (od strony sieci LAN)
  - c. Jednocześnie na wewnętrznym jak i zewnętrznym interfejsie.

*Dla rozwoju Mazowsza*



## ADMINISTRACJA ŁĄCZAMI OD DOSTAWCÓW USŁUG INTERNETOWYCH (ISP).

22. Urządzenie musi posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
23. Mechanizm równoważenia obciążenia łącza internetowego powinien działać w oparciu o równoważenie względem adresu źródłowego oraz względem adresu docelowego.
24. Urządzenie posiada możliwość definiowania przynajmniej 4 rodzajów połączeń typu Dial-up włączając w to: PPPoE, PPTP, PPP, L2TP.

## ADMINISTRACJA URZĄDZENIEM

25. Producent powinien dostarczać w podstawowej licencji oprogramowania narzędziowe, które umożliwia:
  - a. lokalną oraz zdalną konfigurację i administrację,
  - b. lokalny oraz zdalny podgląd pracy urządzenia (tzw. monitoring w trybie rzeczywistym),
  - c. umożliwiającą zarządzanie, analizę i prostą interpretację logów,
  - d. zarządzanie więcej niż jednym urządzeniem (centralna administracja).
26. Urządzenie powinno być dostarczane z oprogramowaniem do generowania kompleksowych raportów z jego działania. Program generujący raporty powinien tworzyć pliki HTML oraz mieć możliwość stworzenia pliku index.html zawierającego łącza do wszystkich dotychczas stworzonych raportów. Powinien również mieć możliwość składowania raportu lokalnie na dysku twardym, wysyłania przy użyciu poczty elektronicznej lub przesłania na serwer FTP.

## POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA

27. System operacyjny urządzenia powinien być oparty o jeden ze znanych systemów operacyjnych (preferowany system operacyjny z rodziny BSD).
28. Restart urządzenia może być zabezpieczony poprzez zastosowanie fizycznego tokena USB.
29. Urządzenie oferuje możliwość skonfigurowania usługi dynamicznego DNS dzięki czemu klienci z dynamicznym adresem IP mogą korzystać ze stałej nazwy hosta/domeny.

## PARAMETRY SPRZĘTOWE

30. Urządzenie powinno być wyposażone w dysk twardy o pojemności co najmniej 70 GB. Dysk powinien być podzielony na co najmniej 3 partycje. W tym dwie systemowe (umożliwiając tym samym start urządzenia z jednej z dwóch partycji) oraz jedną przeznaczoną na logi.
31. Liczba portów Ethernet 10/100/1000 – min. 6
32. Przepustowość Firewall-a wraz z włączonym systemem IPS wynosi min. 700 Mbps.
33. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 160 Mbps.
34. Maksymalna liczba tuneli VPN IPsec nie powinna być mniejsza niż 500.
35. Możliwość zdefiniowania co najmniej 6 500 reguł filtrujących
36. Obsługa min. 128 VLAN-ów
37. Maksymalna liczba równoczesnych sesji wynosi 200 000.

*Dla rozwoju Mazowsza*



38. Maksymalna liczba tuneli SSL VPN nie powinna być mniejsza niż 256.

#### LICENCJE

39. Licencja do urządzenia zapewnia przez okres 3 lat:

- aktualizacje do wszystkich modułów urządzenia
- funkcjonalność SSL VPN (256 tuneli) w podstawowej cenie urządzenia

#### GWARANCJA

Gwarancja 3 letnia. Dostarczony sprzęt musi być fabrycznie nowy, musi pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski. Urządzenia muszą być objęte gwarancją producenta, potwierdzoną przez oryginalne karty gwarancyjne.

- wsparcie techniczne od poniedziałku do piątku od 8.00 do 18.00
- wymiana urządzenia na nowe w przypadku awarii na następny dzień roboczy

Oferent zobowiązany jest dostarczyć wraz z ofertą, szczegółową specyfikację techniczną oferowanego sprzętu.

*Dla rozwoju Mazowsza*