Załącznik nr 2 do SIWZ

SPECYFIKACJA TECHNICZNA

CZĘŚĆ II PRZEDMIOTU ZAMÓWIENIA
[Urządzenie zarządzające (sterujące) i zabezpieczające ruch aplikacji]

OBLIGATORYJNE WYMAGANIA TECHNICZNE

I. Urządzenie zarządzające (sterujące) i zabezpieczające ruch aplikacji

Produkt	Opis wymagań minimalnych	Liczba sztuk
F5-BIG-LTM-3600-AS-R lub równoważny	**BIG-IP 3600 Local Traffic Manager, Application Security Edition (4 GB Memory) z dodatkowym redundantnym zasilaczem**	**1**

lub urządzenie(-a) równoważne, spełniające poniżej wymagania minimalne:

Lp.	Opis wymagań minimalnych
1	**Urządzenie(-a) muszą posiadać następujące parametry techniczne:**
1.1	Min. 8 GB pamięci Flash z systemem operacyjnym oraz min. 4 GB RAM, min. 300 GB twardy dysk
1.2	Urządzenie musi w optymalnych warunkach zapewniać wydajność 1,5 Gbps przy 15 000 (cps) nowych połączeń na sekundę w warstwie 7 (1-1), obsługiwać 65 000 (rps) nowych requestów na sekundę w warstwie 7 (1-inf) oraz zapewnić obsługę 3 800 000 jednoczesnych połączeń.
1.3	Urządzenie musi posiadać wbudowany L2/L3 switch
1.4	Min. 8 portów 10/100/1000, 2x1Gbps slot SFP
1.5	Obsługa 10 000 nowych transakcji SSL na sek. (TPS) oraz obsługa minimum 1 000 000 jednoczesnych połączeń SSL.
1.6	Możliwość kompresji ruchu http (minimum 50 Mbps)
1.7	Kit do montowania w szafie rack
1.8	Dwa redundantne zasilacze

2	**Urządzenie(-a) muszą umożliwiać**
2.1	IP Packet Filtering, NAT, Secure NAT, Load ballancing
2.2	VLAN, agregację połączeń i failover monitoring portów
2.3	Zarządzanie przez Web (https), CLI. Odrębny podsystem (z odrębnym adresem IP) pozwalający na zdalny dostęp SSH do urządzenia i możliwość przeprowadzenia prostego maintanance'u (reboot, reset) nawet w przypadku braku dostępu do głównego systemu
2.4	Balansowanie ruchu dla serwerów polegające na tworzeniu wirtualnych adresów IP i ukrywania za nimi dowolnej liczby serwerów.
2.5	Pracę w architekturze wysokiej dostępności w postaci klastra failover (active/passive) przez port szeregowy oraz siec Ethernet
2.6	Możliwość ręcznego programowania reguł kierowania i filtrowania ruchu, w oparciu o dowolny parametr nagłówka i pakietu IP (warstwy od 4 do 7 OSI), w oparciu o język TCL. Możliwość modyfikacji nagłówka w pakietach IP za pomocą ręcznego programowania w oparciu o język TCL.
2.7	Przejście określonego ruchu tą samą drogą bazując na dowolnej informacji z nagłówka i zawartości pakietu IP.
2.8	Wsparcie dla SSL Client Revocation List (CRL)
2.9	Brak ograniczeń dla ilości certyfikatów serwera
2.10	Metody podziału obciążenia typów: round robin, ratio, najszybsza odpowiedź lub najmniej połączeń oraz ich kombinacje
2.11	Bezpośredni odczyt wydajności obsługiwanej aplikacji z wykorzystaniem mechanizmu WMI
2.12	SDK SOAP/XML do zarządzania ruchem serwisów www i integracji z aplikacjami
2.13	Moduł uwierzytelniania użytkowników aplikacji webowych
2.14	Wsparcie dla IPv6
3	**Urządzenie(-a) muszą posiadać funkcjonalność Web firewall w zakresie:**
3.1	Dowolna ilość chronionych aplikacji
3.2	Obsługa dwóch modelów polityk (Whitelist i Blacklist)
3.3	Możliwość aktualizacji sygnatur ataków
3.4	Możliwość definiowania typów obiektów i nazw obiektów
3.5	Możliwość definiowania nazw parametrów i oczekiwanych wartości parametrów
3.6	Możliwość definiowania oczekiwanej kolejności występowania obiektów po sobie

3.7	Możliwość wykrywania i blokowania ataków typu „brute force” na hasła użytkowników.
3.8	Wsparcie dla XML: • Walidacja Schema/WSDL • Wybór dozwolonych metod SOAP • Sygnatury ataków XML • Pełne logowanie requestów XML
4.	**Pakiet serwisowy**
4.1	Urządzenie musi posiadać pakiet serwisowy producenta, który umożliwia Zamawiającemu pobieranie z serwera WWW lub ftp producenta sprzętu najnowszego oprogramowania systemu operacyjnego urządzenia i jego instalację - najnowsze wersje oprogramowania w ramach tej samej funkcjonalności udostępnione przez producenta w okresie trwania gwarancji.

Zakres prac po stronie Wykonawcy:

1. Montaż urządzenia w szafie
2. Konfiguracja sieciowa
3. Konfiguracja wirtualnych serwerów
4. Przypisanie klas ruchu do wirtualnych serwerów
5. Włączenie ochrony sygnatur
6. Włączenie urządzenia w tryb uczenia
7. Sprawdzenie płynącego ruchu
8. Modyfikacja i akceptacja polityki
9. Przełączenie urządzenia w tryb ochrony
10. Wykonanie dokumentacji powdrożeniowej
11. Wykonanie szkolenia przystanowiskowego w zakresie podstawowej obsługi i konfiguracji urządzenia dla 3 osób.