Załącznik
do Formularza ofertowego
znak sprawy: 22/DI/PN/2013

.....
(oznaczenie wykonawcy

Specyfikacja techniczna oferowanego urządzenia - równoważnego

Urządzenie sterujące i zabezpieczające ruch danych aplikacji - równoważne, spełnia poniższe wymagania minimalne:
<u>liczba identycznych 2 kompletów</u>

Nazwa producenta i model:		**Deklaracja zgodności z opisem wymagań minimalnych (np. TAK / NIE)**
Lp.	**Opis wymagań minimalnych**	
1.	**Urządzenie(-a) muszą posiadać następujące parametry techniczne:**	
1.1.	Modularna budowa z możliwością rozbudowy do 4 blade'ów Parametry pojedynczego blade'a: Min. 16 GB RAM, min. 300 GB twardy dysk	
1.2.	Jeden blade cechuje się następującymi parametrami (w optymalnych warunkach) wydajność 18 Gbps przy 150 000 (cps) nowych połączeń na sekundę w warstwie 7 (1-1), obsługiwać 500 000 (rps) nowych requestów na sekundę w warstwie 7 (1-inf) oraz zapewnić obsługę 12 000 000 jednoczesnych połączeń.	
1.3.	Urządzenie musi posiadać wbudowany L2/L3 switch	
1.4.	Min. 8 portów 10Gbps slot SFP+ (dla pojedynczego blade'a)	
1.5.	Obsługa 50 000 nowych transakcji SSL na sek. (TPS) dla klucza 1K oraz obsługa minimum 2 500 000 jednoczesnych połączeń SSL dla pojedynczego blade'a	
1.6.	Możliwość kompresji ruchu http (minimum 200 Mbps) dla pojedynczego blade'a	
1.7.	Kit do montowania w szafie rack	

1.8.	Dwa redundantne zasilacze	
1.9.	Wysokość nie przekraczająca 4U	
1.10.	Liniowa skalowalnośc w przypadku dołożenia kolejnych blade'ów	
1.11.	Możliwość dołożenia/wyciągnięcia kolejnego blade'a podczas pracy urządzenia	
2.	**Urządzenie(-a) muszą umożliwiać**	
2.1.	VLAN, agregację połączeń i failover monitoring portów	
2.2.	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	
2.3.	Balansowanie ruchu dla serwerów polegające na tworzeniu wirtualnych adresów IP i ukrywania za nimi dowolnej liczby serwerów.	
2.4.	Pracę w architekturze wysokiej dostępności w postaci klastra failover (active/passive) przez port szeregowy oraz siec Ethernet	
2.5.	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.	
2.6.	Przejście określonego ruchu tą samą drogą bazując na dowolnej informacji z nagłówka i zawartości pakietu IP.	
2.7.	Wsparcie dla SSL Client Revocation List (CRL)	
2.8.	Brak ograniczeń dla ilości certyfikatów serwera	
2.9.	Metody podziału obciążenia typów: round robin, ratio, najszybsza odpowiedź lub najmniej połączeń oraz ich kombinacje	
2.10.	Bezpośredni odczyt wydajności obsługiwanej aplikacji z wykorzystaniem mechanizmu WMI	
2.11.	SDK SOAP/XML do zarządzania ruchem serwisów www i integracji z aplikacjami	
2.12.	Moduł uwierzytelniania użytkowników aplikacji webowych	
2.13.	Wsparcie dla IPv6	
2.14.	Możliwość uruchomienia 16 wirtualnych instancji urządzenia (wirtualizacja urządzenia)	

3.	**Urządzenie(-a) muszą posiadać funkcjonalność Web application 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	
3.9.	Możliwość definiowania polityk per URI aplikacji	
3.10.	Wsparcie dla technologii AJAX i JSON	
3.11.	Możliwość wykrywania połączeń pochodzących od botów	
3.12.	Możliwość zabezpieczenia aplikacji przed atakami DoS oraz DdoS na poziomie URI	
3.13.	Możliwość integracji urządzenia ze skanerem antywirusowym za pomocą protokołu ICAP	
3.14.	Możliwość blokowania użytkowniaków per kraj, z którego pochodzi atak (ip geolocation)	
3.15.	Możliwość integracji ze skanerami podatności aplikacji firm trzecich w celu budowy polityki	

UWAGA!
Należy wypełnić i załączyć do oferty tylko w przypadku oferowanego urządzenia równoważnego. Wypełnione muszą zostać wszystkie miejsca zaznaczone na niebiesko

..... dnia: ....., ...
Miejscowość podpis osoby uprawnionej