Załącznik nr 1 do SIWZ
Znak sprawy: KA-2/097/2016

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA:

Wirtualna platforma Web Application Firewall

Lp.	Parametr	Wymagania techniczne
1.	Architektura systemu	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. Wymaga się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci komercyjnych aplikacji instalowanych w środowisku wirtualnym. Całość systemu musi mieć możliwość uruchomienia w środowisku VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Citrix XenServer 6.2, Open Source Xen 4.2. System powinien umożliwiać ochronę aplikacji webowych oraz Firewall XML - którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System powinien umożliwiać lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów. Powinna istnieć możliwość implementacji systemu online w trybach Reverse Proxy lub Transparentnym, jak również implementacji w trybie nasłuchu. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta.
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.
3.	Parametry fizyczne systemu	Wsparcie dla minimum 4 interfejsów sieciowych oraz 2 wirtualnych CPU. Obsługa powierzchni dyskowej - minimum 2 TB W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability)z trybem Active-Passive
4.	Funkcjonalności podstawowe i uzupełniające	System powinien realizować co najmniej poniższe funkcjonalności: • Tryb auto-uczenia – przyspieszający i ułatwiający implementację • Podział obciążenia na kilkanaście serwerów (loadbalancing) • Akceleracją i terminowanie SSL dla wybranych serwisów w centrum danych • Możliwość analizy poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje) • Firewall XML realizujący z możliwością routingu w oparciu o kontent, walidacją schematów XML oraz formatowania JSON • Wsparcie dla SNI (Server Name Indication), co w połączeniu z funkcją routingu treści (content routing) ma pozwalać na kierowanie ruchem z jednego IP terminującego ruch SSL, do wielu serwerów logicznych (występujących pod różnymi adresami IP). Każda domena ma się przedstawiać swoim certyfikatem i w oparciu tę informację ma być podejmowana decyzja o routingu • Firewall aplikacji webowych chroniący przed takimi zagrożeniami jak:

		○ SQL and OS Command Injection ○ Cross Site Scripting (XSS) ○ Cross Site Request Forgery ○ Outbound Data Leakage ○ HTTP Request Smuggling ○ Buffer Overflow ○ Encoding Attacks ○ Cookie Tampering / Poisoning ○ Session Hijacking ○ Broken Access Control ○ Forceful Browsing /Directory Traversal oraz ○ Innymi podatnościami specyfikowanymi przez listę OWASP Top 10 • Monitorowanie aktywności użytkowników (sesji) w logach związanych z ruchem sieciowym i atakami • Integrację z rozwiązaniami FortiGate przy wykorzystaniu protokołu WCCP, celem inspekcji i analizy ruchu sieciowego który jest z nich przekierowywany
5.	Parametry wydajnościowe	Urządzenie musi obsługiwać: • Przepustowość dla ruchu http - min 100 Mbps • Min 8 tyś transakcji HTTP na sekundę • Min 4 tys. transakcji HTTPS na sekundę
6.	Sygnatury, subskrypcje	• Aktualizacja baz sygnatur powinna być systematycznie aktualizowana zgodnie ze zdefiniowanych harmonogramem (Scheduler)
7.	Zarządzanie	System udostępnia: • Graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS • Linia poleceń - CLI • Wymagany jest dedykowany system centralnego zarządzania rozwiązaniem opisanym w poprzednich punktach, pochodzący od tego samego producenta, pozwalający na: ○ konfigurację obiektów ○ konfigurację polityk bezpieczeństwa, w tym ich szablonów ○ stworzenie centralnego repozytorium konfiguracji ○ aktualizację oprogramowania poszczególnych systemów bezpieczeństwa ○ uruchomienie go na platformie wirtualnej (VMWare, Hyper-V)
8.	Serwisy, szkolenia i usługi	Wymaga się aby dostawa obejmowała również: • Serwis i wsparcie w systemie min. 8 godzin x 5 dni, przez okres: 36 miesięcy • Subskrypcje funkcji bezpieczeństwa na okres: 36 miesięcy