Załącznik nr 18 do OPZ - WAF

# Specyfikacja urządzenia bezpieczeństwa i transmisji danych – WAF

## Obudowa i zasilanie

### Redundantne zasilanie 230 V 50 Hz.

### Montaż w stelażu/szafie RACK 19”.

### Wysokość maksymalna 2U.

## Architektura systemu

### System ochrony 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 inline 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, w tym system operacyjny i sprzęt pochodziły od jednego producenta.

### Nie dopuszcza się aby elementy funkcji ochronnych zastosowane w systemie były opracowane przez firmy trzecie.

## System operacyjny

### Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.

### **Parametry fizyczne**

### System musi dysponować minimum 2 portami Gigabit Ethernet RJ-45, 2 portami 10 Gigabit Ethernet z gniazdami SFP+.

### Powierzchnia dyskowa - minimum 2 TB.

### W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability)z trybem Active-Passive.

### **Funkcjonalności podstawowe i uzupełniające.**

* + 1. Tryb auto-uczenia – przyspieszający i ułatwiający implementację
    2. Podział obciążenia na kilkanaście serwerów (loadbalancing)
    3. Akcelerację SSL dla wybranych serwisów w centrum danych
    4. Możliwość analizy poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje)
    5. Firewall XML realizujący z możliwością routingu w oparciu o kontent, walidacją schematów XML oraz weryfikacją WDSL.
    6. Firewall aplikacji webowych chroniący przed takimi zagrożeniami jak:
       1. SQL and OS Command Injection
       2. Cross Site Scripting (XSS)
       3. Cross Site Request Forgery
       4. Outbound Data Leakage
       5. HTTP Request Smuggling
       6. Buffer Overflow
       7. Encoding Attacks
       8. Cookie Tampering/Poisoning
       9. Session Hijacking
       10. Broken Access Control
       11. Forceful Browsing /Directory Traversal

### Innymi podatnościami specyfikowanymi przez listę OWASP Top 10 2017

### **Parametry wydajnościowe**

* + 1. Przepustowość dla ruchu http - min 750 Mbps
    2. Min 40 tys. transakcji na sekundę

### **Sygnatury, subscrypcje**

### Aktualizacja baz sygnatur powinna być systematycznie aktualizowana zgodnie ze zdefiniowanych harmonogramem (Scheduler)

### **Zarządzanie**

### Lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS