Oznaczenie sprawy: I.DZP.23110.Pn-8.2018

Załącznik nr 2b do SIWZ

Specyfikacja techniczna i informacja dotycząca Części nr 2 zamówienia

I. Uwagi ogólne:

1. Występujące w tabelach parametry należy traktować jako minimalne.
2. Wykonawca nie może złożyć oferty proponując sprzęt o parametrach (chociażby jednym z parametrów), gorszych niż wskazane w niniejszej informacji.
3. Dopuszcza się składanie ofert na urządzenie/towar lepsze (tj. o parametrach lepszych np. większej ilości pamięci, szybszej szyny pamięci, większej ilości portów we/wy urządzenia).
4. Opisane w niniejszej informacji minimalne parametry techniczne stanowią dolną granicę równoważności produktu tj. Zamawiający uzna za produkt równoważny każdy produkt spełniający każdy z minimalnych parametrów wskazanych w niniejszym dokumencie. Zamawiający uzna za produkt równoważny produkt oferujący parametry wyższe/lepsze niż wskazane jako minimalne z zastrzeżeniem punktu 2 niniejszej informacji.
5. Wykonawca, który powołuje się na rozwiązania równoważne obowiązany jest wykazać, że oferowane przez niego urządzenie/towar spełnia wymagania określone przez Zamawiającego w szczególności przedstawiając przetłumaczoną na język polski kartę katalogową oferowanego produktu a jeśli w karcie katalogowej produktu nie znajduje się pełna informacja o produkcie (udawadniająca zaoferowania produktu nie gorszego pod względem każdego wymaganego przez Zamawiającego parametru) to Wykonawca dostarczy przetłumaczone na język polski i podpisane przez osobę uprawnioną oświadczenie producenta sprzętu ze wskazaniem brakującego parametru.
6. Wykonawca udziela gwarancji jakości i rozszerzonej rękojmi na dostarczony sprzęt na okres wskazany w formularzu oferty, nie mniejszy niż 1 rok.
7. Oferowany sprzęt musi być fabrycznie nowy ,wyprodukowany nie wcześniej niż 12 miesięcy przed datą dostawy.
8. Oferowany sprzęt nie może być powystawowy/testowy.
9. Oferowany sprzęt musi pochodzić z legalnego źródła- od dystrybutora sprzętu na rynek polski.
10. Oferowany sprzęt musi posiadać instrukcję obsługi w języku polskim.

II. Tabele parametrów technicznych:

Pozycja nr 1 (produkt nr 1 w ramach Części nr 2 zamówienia)

Nazwa produktu:
Zapora aplikacji webowych z instalacją, konfiguracją i szkoleniem

Ilość sztuk wymagana przez Zamawiającego: 1

Lp.	Konfiguracja	Parametry techniczne/funkcjonalność/ wymagania
1	**Rodzaj urządzenia**	Zapora aplikacji webowych (urządzenie sprzętowe)
2	Wymagania ogólne	Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowane w systemie były opracowane przez firmy trzecie.
3	Tryb pracy zapory	Zapora powinna mieć możliwość pracy w trybach : inline reverse proxy oraz transparent.

Oznaczenie sprawy: I.DZP.23110.Pn-8.2018

4	Ilość chronionych aplikacji	Zapora nie powinien posiadać ograniczeń co do ilości chronionych aplikacji web.
5	Wysoka dostępność (High Availability)	Zapora powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive.
6	Parametry fizyczne	Ilość portów Gigabit Ethernet RJ45 >=4 Powierzchnia dyskowa >=16 GB Zasilanie z sieci 230V/50Hz
7	Parametry wydajnościowe	Przepustowość dla ruch http >=25Mbps
8	Podstawowe funkcje	Zapora musi realizować poniższe funkcje: 1. Tryb auto-uczenia – przyspieszający i ułatwiający implementację. 2. Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia: • Round Robin, • Weighted Round Robin, • Least Connection, • Source IP Hash, 3. Wsparcie dla mechanizmów session persistence: • Source IP • HTTP Header • URL parameter • Insert Cookie • Rewrite Cookie • Persistent Cookie • Embedded Cookie • ASP Session ID • PHP Session ID • JSP Session ID • SSL Session ID 4. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla SSL 3.0, TLS 1.1, TLS 1.2. 5. Możliwość analizy poszczególnych rodzajów ruchu w oparciu o polityki bezpieczeństwa (polityka to obiekt określający zbiór ustawień zabezpieczających aplikacje). 6. Kontrola komunikacji XML z możliwością routingu w oparciu o kontent, walidacją schematu XML.

Oznaczenie sprawy: I.DZP.23110.Pn-8.2018

		7. Ochrona aplikacji www 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. • Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP. • DoS w warstwie aplikacji. • Ochrona przed atakami typu Brute force. • Ochrona przed atakami clickjacking. • Ochrona przed credential stuffing. 8. Mechanizmy ochrony przed wyciekiem informacji poufnych. 9. Definiowanie polityk w oparciu o geo-lokalizację. 10. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania. 11. Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego. 12. Wsparcie dla ochrony http 2 natywnego oraz offload do http 1.1 w trybie pracy reverse proxy. 13. Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only”. 14. Content routing na bazie parametrów http oraz certyfikatów X.509. 15. Ochrona przed Web Scraping. 16. Wsparcie dla kompresji danych oraz cache. 17. Publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos). 18. Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF. 19. Ochrona przed atakami typu SLOW (Slowloris i podobne).

Oznaczenie sprawy: I.DZP.23110.Pn-8.2018

		20. Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Wyłączanie konkretnych sygnatur na podstawie wielu parametrów: profil bezpieczeństwa: • Metoda HTTP. • IP klienta. • Host. • URI. • Cały URL. • Parametr. • Cookie. 21. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For". 22. Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej. 23. Możliwość konfigurowania własnych stron z informacjami o błędzie. 24. Ustawienie wymaganej sekwencji otwieranych stron. 25. Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload'u HTML. 26. Detekcja XML w body żądań typu http POST w celu skutecznego użycia sygnatur do ochrony aplikacji web. 27. Detekcja JSON w żądaniach http w celu skutecznego użycia sygnatur do ochrony aplikacji web. 28. Blokowania „Illegal XML Format" oraz „Illegal JSON Format".
9	Funkcje dodatkowe	Zapora musi realizować poniższe funkcje: 1. Skaner aplikacji WWW realizowany bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. 2. Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. 3. Domyślne szablony ochrony dla Exchange, SharePoint i WordPress. 4. Uwierzytelnianie użytkowników w oparciu o protokół SAML. 5. Rozpoznawanie użytkowników logujących się bezpośrednio do chronionej aplikacji bez udziału WAF. 6. Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu

Oznaczenie sprawy: I.DZP.23110.Pn-8.2018

		od użytkowników generujących ataki z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa.
10	Zarządzanie	Zapora musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów: HTTPS, SSH, API.
11	Logowanie i Raportowanie	Zapora musi realizować poniższe funkcje 1. Możliwość logowania oraz raportowania - w oparciu o zestaw predefiniowanych wzorców raportów. 2. Możliwość logowania do zewnętrznego serwera syslog. 3. Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem. 4. Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP
12	Certyfikaty	Z punktu widzenia jakości i skuteczności rozwiązania koniecznym jest przedstawienie wyników testów niezależnych organizacji, np. NSS Labs, ICSA Labs lub równoważnego.
13	Sygnatury, subskrypcje	1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem. 2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować: Uwaga: Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres 12 miesięcy.
14	Instalacja, konfiguracja	Wykonawca zainstaluje oraz skonfiguruje zaporę aplikacji webowych w środowisku produkcyjnym Zamawiającego według jego wymagań oraz przeprowadzi testy poprawności działania zapory.
15	Szkolenie	Wykonawca przeprowadzi 1 dniowe szkolenie dla 2 osób z zakresu konfiguracji i zarzadzania zaporą w siedzibie Zamawiającego. Zakres szkolenia: Identyfikacja najważniejszych ataków na aplikacje webowe Podstawowe informacje oraz funkcjonalności dostępne na urządzeniu Podstawowa konfiguracja i zarzadzanie urządzeniem Definicja polityk bezpieczeństwa Load Balancing Ochrona aplikacji webowych przed atakami DoS Diagnostyka poprawności działania urządzenia Obsługa komunikatów, w szczególności reagowanie na sygnały o awarii i incydenty bezpieczeństwa.