DOTYCZY: **Dostawy systemu ochrony aplikacji webowych**

Opis Przedmiotu Zamówienia

Lp.	Parametr	Wymagania minimalne
	Wymagania ogólne	Zamawiający obecnie posiada urządzenie FortiWeb-400C produkcji Fortinet bez aktualnego wsparcia Zamawiający wymaga aby dostarczone środowisko zostało skonfigurowane zgodnie z obecnie zastosowanymi politykami . Zamawiający dopuszcza dostawę zarówno rozwiązania sprzętowego jak i w postaci środowiska wirtualnego
1	Architektura systemu	wykrywanie i blokowanie ataków celujących w aplikacje webowe i informowanie operatora w przypadku wystąpienia określonych zdarzeń.
2	Wsparcie dla infrastruktury	wsparcie przynajmniej dla systemów wirtualizacyjnych tj. dla: VMware, Microsoft Hyper-V, Citrix XenServer, VirtualBox, KVM, AWS, Microsoft Azure, Oracle Cloud
3	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie/system musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.
4	Funkcjonalności	System powinien posiadać minimum następujące funkcjonalności: 1. definiowanie oddzielnych polityk ochrony dla aplikacji webowych umieszczonych na tym samym serwerze Zamawiającego (witryn/virtual hostów znajdujących się pod tym samym adresem IP). 2. ochrona danej witryny przed dostępem z puli adresów przypisanych dla danego kraju(ów). 3. zablokowanie danej witryny przed dostępem z określonych adresów IP. 4. analiza poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje). 5. podział obciążenia ruchu HTTP na kilkanaście serwerów (load balancing). 6.ustanowienie limitu żądań HTTP w ciągu sekundy dla danego adresu IP. 7. Sprzętowa akceleracja protokołów SSL/TLS zaimplementowanych do ochrony wybranych serwisów webowych umieszczonych w centrum danych Zamawiającego. 8.Funkcjonalność konfigurowania na tym samym adresie IP urządzenia, dostępu do witryn HTTPS posiadających różne certyfikaty SSL (mechanizm SNI). 9. Funkcjonalność konfigurowania dostępu użytkownika do danej witryny po przez mechanizm PKI. 10. Przeglądanie sesji ustanowionych przez komputery klienckie z uwzględnieniem adresu serwera do którego ruch jest przekazywany.

		11. Firewall aplikacji webowych chroniący przed minimum następującymi zagrożeniami : - SQL Injection 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, - Inne podatności specyfikowane przez listę OWASP Top 10. 12. Uruchomienie trybu auto-uczenia przyspieszającego i ułatwiającego implementację systemu. 13. Funkcjonalność konfigurowania przekierowań - URL rewirting. 14. ochrona witryny przed atakami typu „Brute force". 15. Funkcjonalność przekazywania ruchu dla danej witryny internetowej do kilku serwerów www.
5	Licencjonowanie	Licencjonowanie bez limitu chronionych serwerów, domen (licencja na urządzenie/system).
6	Tryb działania	Możliwość implementacji systemu w trybach Reverse-Proxy lub Transparentnym.
7	Parametry wydajnościowe	Obsługa przepustowości dla ruchu HTTP – co najmniej 100 Mbps
	vCPU	Obsługa minimum 2 wirtualnych procesorów
8	Ilość portów do obsługi ruchu HTTP/HTTPS	Nie mniej niż 4 interfejsy typu 10/100/1000 Mbps wirtualne lub RJ45
9	Powierzchnia dyskowa	Nie mniej niż 40GB z możliwością powiększenie do 2TB
10	Tryb wysokiej dostępności	W celu zwiększenia niezawodności system należy skonfigurować do pracy w konfiguracji HA (High Availability) z trybem Active-Passive
11	Logowanie i raportowanie	1. lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów. 2. Funkcjonalność wysyłania logów z urządzenia do serwera typu rsyslog. 3. Funkcjonalność wysyłania logów z urządzenia do systemu FortiAnalyzer (produkcji Fortinet) będącego w posiadaniu Zamawiającego.
12	Zarządzanie	1. Interfejs zarządzający dostępny poprzez protokół HTTPS. 2.Dostęp do panelu administratora tylko dla zaufanych adresów IP. 3. Fukcjonalność wykonywania kopii bezpieczeństwa konfiguracji urządzenia na zdalny serwer.
13	Wdrożenie	Zamawiający wymaga aby Dostawca posiadał/zatrudniał do realizacji niniejszego zadania personel posiadający aktualne certyfikaty techniczne producenta w zakresie zarządzania i konfiguracji dostarczanego rozwiązania.

14	Szkolenia	Zamawiający wymaga przeszkolenia minimum 2 pracowników z dostarczonego rozwiązania przez wykwalifikowany personel Wykonawcy potwierdzone certyfikatem.
15	Gwarancja	Wykonawca udzieli gwarancji na dostarczony przedmiot zamówienia na okres 3 lat od daty podpisania protokołu końcowego odbioru W ramach gwarancji Wykonawca zapewni: • Asystę techniczną producenta • Wsparcie techniczne
		Warunki świadczenia Asysty technicznej producenta: • świadczona w trybie 24/7 (24 godziny przez 7 dni w tygodniu) • świadczona w języku polskim • zapewnienie kontaktu telefonicznego z pomocą techniczną • czat internetowy w celu uzyskania szybkich odpowiedzi • portal wsparcia do tworzenia zgłoszeń • Czasy reakcji na zgłaszane błędy: czas reakcji w przypadku błędu krytycznego 1 godzina od momentu zgłoszenia błędu przez Zamawiającego czas reakcji w przypadku pozostałych błędów 1 dzień od momentu zgłoszenia błędu przez Zamawiającego • czasy usunięcia błędów: dla błędu krytycznego - 4 godziny od momentu zgłoszenia błędu przez Zamawiającego dla błędów pozostałych - 2 dni od momentu zgłoszenia błędu przez Zamawiającego • dostęp do aktualizacji oprogramowania błąd krytyczny – błąd uniemożliwiający użytkowanie dostarczonego rozwiązania (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika i prowadzący do zatrzymania jego eksploatacji pozostałe błędy – błędy nie będące błędami krytycznymi. Stan mający wpływ na poprawne funkcjonowanie dostarczonego rozwiązania lub jego składowych, odbiegający od założeń, niezakłócający rutynowej eksploatacji rozwiązania.

16	Wsparcie techniczne Wykonawcy	Wsparcie techniczne Wykonawcy obejmuje: - Udzielanie pomocy dotyczącej obsługi, konfiguracji, optymalizacji i administracji dostarczonym rozwiązaniem - Udzielanie pomocy dotyczącej bieżącej obsługi dostarczonego rozwiązania - diagnozowanie problemów dotyczących funkcjonowania dostarczonego rozwiązania Wsparcie techniczne świadczone : telefonicznie, za pośrednictwem e-mail lub w siedzibie Zamawiającego. w godzinach pracy Zamawiającego (od 7:00 do 15:00) przez 5 dni w tygodniu. Czas uzyskania pomocy – 1 dzień roboczy od momentu zgłoszenia przez Zamawiającego