Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostarczenie przez Wykonawcę dla Zamawiającego subskrypcji licencji (przedłużenie wsparcia) na posiadane oprogramowanie. Uwaga! Każdorazowo, jeżeli w opisie przedmiotu zamówienia wskazana jest nazwa oprogramowania należy przez to rozumieć wskazane oprogramowanie lub oprogramowanie równoważne, zgodnie z zaoferowanym, spełniające wymagania wskazane w pkt 4, 8,10,12,16,18.

Przedmiot zamówienia podzielony jest na zamówienie podstawowe i zamówienie realizowane w ramach prawa opcji.

1. **Przedmiotem zamówienia podstawowego** jest zakup licencji na oprogramowanie Firewall aplikacyjny Fortinet – WAF (wersja wirtualna – FortiWeb-VM04 Supported), FortiADC-VM04 FortiCar Premium Support. Na rok 13.10.2024-12.10.2025
2. **Opcje** – jest zakup licencji na oprogramowanie Firewall aplikacyjny Fortinet – WAF (wersja wirtualna – FortiWeb-VM04 Supported), FortiADC-VM04 FortiCar Premium Support. Na rok 13.10.2025-12.10.2026

3. Opis przedmiotu zamówienia na zakup licencji na oprogramowanie Firewall aplikacyjny:

   Oryginalna nazwa: firmy Fortinet - FortiWeb - Web Aplication Firewall - virtual appliance for up to 4 x vCPU core – VM04 Supported - License 1 Years

   Szczegóły licencji:

Support Coverage			
Rodzaj wsparcia (Support Type)	Poziom Wsparcia (Support Level)	Data aktywacji (Activation Date)	Termin ważności (Expiration Date)
Firmware & General Updates	Web/Online	2024-10-13	2025-10-12
Enhanced Support	24x7	2024-10-13	2025-10-12
Advanced Malware Protection	Web/Online	2024-10-13	2025-10-12
FortiWeb Security Service	Web/Online	2024-10-13	2025-10-12
IP Reputation	Web/Online	2024-10-13	2025-10-12

4. Wymagania dla oprogramowania Firewall aplikacyjny firmy Fortinet - FortiWeb - Web Aplication Firewall - virtual appliance for up to 4 x vCPU core - oprogramowanie **równoważne musi spełniać następujące warunki:**

- wszystkie elementy systemu zabezpieczeń muszą być dostarczone przez jednego producenta w formie gotowych maszyn wirtualnych działających w środowisku ESX/ESXi
- system musi działać w następujących trybach pracy: Transparent Bridge (inline warstwa 2 ISO/OSI), Transparent Reverse Proxy – tj praca w trybie proxy nie wymagająca korzystania z nowych adresów IP, Reverse Proxy oraz Sniffing przy czym musi istnieć możliwość działania w trybie Transparent Bridge oraz Transparent Reverse Proxy w obrębie tych samych chronionych aplikacji
- moduły wykonawcze muszą mieć możliwość pracy w trybie High Availability (HA), powinny zawierać mechanizm ochrony typu Stateful Firewall oraz weryfikować zgodność komunikacji sieciowej ze standardem protokołu tcp/ip, opisanym w RFC
- system musi mieć wydajność analizy protokołu http/https na poziomie 500Mbps
- uwierzytelnianie użytkowników oferowanego rozwiązania musi być możliwe za pomocą integracji z Active Directory, LDAP w celu uzyskania dodatkowych informacji w logach na temat użytkownika. Obsługiwane muszą być nie mniej niż następujące metody uwierzytelnienia: formularze html, certyfikat cyfrowy, kerberos, NTLM
- całość konfiguracji oraz repozytorium logów musi być przechowywane na centralnym serwerze zarządzania
- system powinien na podstawie analizy obserwowanego ruchu zbudować odzwierciedlenie całej struktury aplikacji, składającej się z katalogów, URLi, metod dostępu, parametrów, typów wartości oraz długości ciągów znaków wprowadzanych przez użytkowników w poszczególnych formatkach a w szczególności powinien umożliwiać naukę formularzy, służących do logowania się użytkowników do aplikacji Web.
- system powinien zagwarantować wysoki poziom ochrony serwerów Web oraz serwerów aplikacyjnych (uwzględniając elementy XML oraz akcje SOAP) przed różnego typu atakami, a także powinien monitorować poprawne zachowanie chronionej aplikacji, a wszelkie próby wyjścia poza to poprawne zachowanie powinien blokować. Wymagane są sygnatury dla nie mniej niż : sieci, aplikacji Web, zapytań Web.
- monitorowanie i kontrolowanie w czasie rzeczywistym wszystkich operacji wykonywanych przez użytkowników. Rozwiązanie musi posiadać możliwość rejestrowania naruszeń bezpieczeństwa oraz udostępniać administratorom co najmniej następujące informacje o zdarzeniach: nazwa użytkownika aplikacyjnego (jeżeli klient zalogował się w systemie przez aplikację Web) ,

dodatkowe atrybuty użytkownika z zewnętrznych repozytoriów jak baza danych czy LDAP oraz zapytanie HTTP przesłane do serwera aplikacji Web

- musi istnieć możliwość rejestrowania kodu źródłowego strony zwracanej klientowi przez aplikację Web, dostępnego bezpośrednio z interfejsu GUI serwera zarządzającego
- system powinien posiadać GUI dostępne przez przeglądarkę internetową w celu zoptymalizowania pracy, eliminacji konieczności instalacji dodatkowego oprogramowania na stacji administratora a także scentralizować zarządzanie całością rozwiązania
- samoczynne uczenie się "normalnych" zachowań aplikacji umożliwiając przegląd zestawienia zachowań użytkowników z informacją o zagrożeniach
- kontrolowanie dostępu do danych wrażliwych występujących w aplikacjach, które system ma chronić
- przyśpieszenie procesów reagowania na incydenty naruszenia bezpieczeństwa oraz procesów śledczych dzięki zastosowaniu technik analitycznych
- automatyczne uczenie się struktury danej aplikacji webowej oraz zachowań użytkowników, profil aplikacji Web musi być budowany w sposób automatyczny poprzez analizę ruchu sieciowego. Musi istnieć możliwość automatycznej aktualizacji profilu w przypadku wystąpienia zmiany w strukturze aplikacji
- system musi posiadać możliwość sprawdzenia, które z wykorzystywanych pól aplikacji są typu „read-only” i nie mogą być zmieniane przez klientów
- wykrywanie ruchu sieciowego pochodzącego z potencjalnie niebezpiecznych źródeł w tym sieci TOR- ukrywania źródła ataku, szkodliwe adresy IP z których wielokrotnie zaatakowano inne strony Internetowe
- tworzenie wirtualnych poprawek dla aplikacji poprzez integrację ze skanerem podatności
- musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej bezpośrednio z centralnego serwera zarządzającego oraz możliwość cyklicznego wysyłania raportów wiadomością e-mail. Rozwiązanie musi posiadać funkcję wysyłania informacji o zdarzeniach: poprzez protokół SNMP. System musi posiadać możliwość wygenerowania gotowych raporty dotyczących: alarmów bezpieczeństwa, zdarzeń systemowych, zmian w profilach aplikacji, ostrzeżeń, ataków, prób włamań
- tworzenie tzw. "białej listy" akceptowanych zachowań użytkownika (profilowanie chronionych aplikacji), nie może dodawać do profilu informacji pochodzących z przeprowadzanych ataków

- automatyczne wykrywanie niepożądanych atrybutów, niezgodnych z protokołem http
- system powinien analizować słabe punkty zgłaszane przynajmniej przez Bugtraq, CVE, Snort
- powinien posiadać ochronę przed botami
- powinien posiadać możliwość geolokalizacji adresów IP – położenie geograficzne będące źródłem ataków i blokady dostępu
- system w przypadku ataku powinien umożliwić: blokowanie pakietu oraz źródła ataku w postaci adresu IP, nazwy użytkownika lub sesji (jeżeli użytkownik uwierzytelnił się w systemie)
- wykryć adresy z których wykonywane są krytyczne incydenty SQL Injection oraz Remote File Inclusion, anonimowe proxy maskujące tożsamość użytkowników oraz adresy IP znane ze spamowania na forach internetowych. Baza adresów IP musi być pogrupowana według zagrożeń a także automatycznie aktualizowana
- rozwiązanie musi posiadać reguły dotyczące identyfikacji incydentów typu web scraping poprzez zliczanie ilości odwołań do serwisu, oraz identyfikację ataków z sieci Bot dzięki wykorzystaniu skryptów java wykonywanych w przeglądarce klienta
- ochrona przed atakami CSRF bez modyfikacji ruchu http
- aktualizacja systemu musi być dostępna zarówno poprzez ręczne pobranie zawartości ze strony producenta jak i automatycznie, poprzez zdefiniowanie terminów wykonania procedury aktualizacji
- powinien posiadać możliwość integracji z systemem SIEM (syslog)
- tworzenie wirtualnych poprawek dla aplikacji poprzez integrację ze skanerami podatności

5. W przypadku dostarczenia oprogramowania równoważnego Wykonawca zobowiązany jest do przeniesienia wdrożonej u Zamawiającego konfiguracji (składającej się z ok. 200 serwisów WWW wraz ze wszystkimi regułami) w terminie 2 dni roboczych. Wykonawca zobowiązuje się, iż Oprogramowanie równoważne, nie będzie wymagało od Zamawiającego dokonywania żadnych zmian w posiadanej infrastrukturze informatycznej Zamawiającego i Oprogramowaniu, z którym ma współdziałać.

6. Infrastruktura techniczna

- wszystkie elementy systemu zabezpieczeń muszą być dostarczone przez jednego producenta w formie gotowych maszyn virtualnych działających w środowisku ESX/ESXi, kompatybilne z VMware 7.0.
- system musi działać w następujących trybach pracy: Transparent Bridge (inline warstwa 2 ISO/OSI), Transparent Reverse Proxy – tj praca w trybie

proxy nie wymagająca korzystania z nowych adresów IP, Reverse Proxy oraz Sniffing przy czym musi istnieć możliwość działania w trybie Transparent Bridge oraz Transparent Reverse Proxy w obrębie tych samych chronionych aplikacji.

- moduły wykonawcze muszą mieć możliwość pracy w trybie High Availability (HA), powinny zawierać mechanizm ochrony typu Stateful Firewall oraz weryfikować zgodność komunikacji sieciowej ze standardem protokołu tcp/ip, opisanym w RFC.
- system musi mieć wydajność analizy protokołu http/https na poziomie 500Mbps
  powinien posiadać możliwość integracji z systemem SIEM (syslog) - ManageEngine Eventlog Analyzer

7. Opis przedmiotu zamówienia na zakup licencji na oprogramowanie Firewall aplikacyjny:

Oryginalna nazwa: firmy Fortinet - FortiWeb - Web Aplication Firewall - virtual appliance for up to 4 x vCPU core - VM04 Supported - License 1 Years

Szczegóły licencji:

Support Coverage			
Rodzaj wsparcia (Support Type)	Poziom Wsparcia (Support Level)	Data aktywacji (Activation Date)	Termin ważności (Expiration Date)
Firmware & General Updates	Web/Online	2024-10-13	2025-10-12
Enhanced Support	24x7	2024-10-13	2025-10-12
Advanced Malware Protection	Web/Online	2024-10-13	2025-10-12
FortiWeb Security Service	Web/Online	2024-10-13	2025-10-12
IP Reputation	Web/Online	2024-10-13	2025-10-12

8. Oprogramowanie Firewall aplikacyjny firmy Fortinet - FortiWeb - Web Aplication Firewall - virtual appliance for up to 4 x vCPU core **oprogramowanie równoważne musi spełniać następujące warunki**:

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. Powinien zostać dostarczony w postaci komercyjnej platformy instalowanej w środowisku

wirtualnym: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure, Google Cloud, Oracle Cloud. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych w ww środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędny odpowiednio zabezpieczony systemem operacyjny.

Architektura systemu

1) Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2) Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie.
3) Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
4) Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web.
5) Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.
6) System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.

Parametry fizyczne systemu

1) System realizujący funkcje podstawowe musi obsługiwać minimum:
   - 4 interfejsy sieciowe
   - Ilość wirtualnych procesorów: 4
2) Obsługa powierzchni dyskowej - minimum 1 TB.

Parametry wydajnościowe

1) Przepustowość dla ruchu http - min 500 Mbps.

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1) Obsługa protokołów: - http 1.1, http 2.0, FTP.
2) Automatyczne tworzenie profili ochronnych aplikacji na bazie zaobserwowanego ruchu. Możliwość wyboru trybu wymuszania wyuczonego schematu bez konieczności akceptacji przez administratora.
3) Automatyczne tworzenie profilu ochrony przed botami na bazie zaobserwowanego ruchu użytkowników

4) Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:
   - Round Robin,
   - Weighted Round Robin,
   - Least Connection,
5) 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
6) Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3.
7) Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa.
8) 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.
9) Mechanizmy ochrony przed wyciekiem informacji poufnych.
10) Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację.
11) Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
12) Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego.

13) Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy.
14) Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only".
15) Content routing na bazie parametrów http oraz certyfikatów X.509.
16) Ochrona przed Web Scraping.
17) Wsparcie dla kompresji danych oraz cache.
18) Publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos).
19) Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3.
20) Ochrona przed atakami typu SLOW (Slowloris i podobne).
21) Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Dodanie wyjątków dla sygnatur na podstawie wielu parametrów:
    - Metoda HTTP.
    - IP klienta.
    - Host.
    - URI.
    - Cały URL.
    - Parametr.
    - Cookie.
    - http Header
    - JSON Elements
22) Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For".
23) Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
24) Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka.
25) Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload'u HTML.
26) Wsparcie dla walidacji OpenAPI, JSON i XML.
27) Blokowania „Illegal XML Format" oraz „Illegal JSON Format".
28) Możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy.
29) Przydzielanie różnych certyfikatów dla różnych nazw domenowych.
30) Ochrona przed atakami MiTB (Man-in-the-Browser) przynamniej dla Anti-keylogger, Obfuscate.
31) URL Encryption.

Wymagane funkcje dodatkowe

1) Kontrola antywirusowa dla komunikacji http realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną

platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

2) 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.
3) 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.
4) Dekodowanie Base64 oraz CSS.
5) Domyślne szablony ochrony dla Exchange, SharePoint i WordPress.
6) Uwierzytelnianie użytkowników w oparciu o protokół SAML.
7) Rozpoznawanie prawidłowo zalogowanych użytkowników do chronionej aplikacji.
8) Wsparcie dla CAPTCHA i Real Browser Enforcement do weryfikacji użytkowników.
9) Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla akcji: kwarantanna czasowa.
10) Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day.
11) Możliwość znakowania przez administratorów systemu za pomocą znaczników (flag) lub komentarza zdarzeń zalogowanych przez urządzenie w celu późniejszej ich analizy.
12) Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, intefejsu API - przy zastosowaniu funkcji biometrycznych.
13) Cross-Origin Resource Sharing (CORS) protection.
14) Integracja z Let's encrypt pozwalająca na automatyczne generowanie certyfikatów na potrzeby terminowania połączeń SSL.

Zarządzanie

1) Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.
2) Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture.
3) Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

4) Możliwość przechowywania lokalnie na urządzeniu do 10 plików konfiguracyjnych.

Logowanie i Raportowanie

1) System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2) Możliwość logowania do zewnętrznego serwera syslog i SIEM.
3) Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.
4) Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.

Certyfikaty

1) Z punktu widzenia jakości i skuteczności rozwiązania koniecznym jest przedstawienie wyników testów niezależnych organizacji, np. NSS Labs, ICSA Labs lub równoważnego z terminem realizacji do 2 dni roboczych liczonych od dnia zakończenia wdrożenia.

Sygnatury, subskrypcje

1) System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2) Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.
3) W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
    - Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres [12] miesięcy.

Gwarancja oraz wsparcie

1) System musi być objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla

bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

9. Opis przedmiotu zamówienia zakup licencji na oprogramowanie FortiADC Load Balancer:

Oryginalna nazwa: firmy Fortinet - FortiADC-VM04 - Application Delivery Controller – supported platforms - License 1 Years

Szczegóły licencji:

Support Coverage			
Rodzaj wsparcia (Support Type)	Poziom Wsparcia (Support Level)	Data aktywacji (Activation Date)	Termin ważności (Expiration Date)
Firmware & General Updates	Web/Online	2024-10-13	2025-10-12
Enhanced Support	24x7	2024-10-13	2025-10-12
Advanced Malware Protection	Web/Online	2024-10-13	2025-10-12
FortiWeb Security Service	Web/Online	2024-10-13	2025-10-12
IP Reputation	Web/Online	2024-10-13	2025-10-12

10. Oprogramowanie Firewall aplikacyjny firmy Fortinet - FortiWeb - Application Delivery Controller - virtual appliance for up to 4 x vCPU core **oprogramowanie równoważne musi spełniać następujące warunki:**

System podziału obciążenia dla ruchu przychodzącego i wychodzącego pracujący w warstwach 2,4,7. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Architektura systemu

1) Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest, aby system pracował w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2) 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) Powinna istnieć możliwość implementacji systemu w trybach: one-arm, reverse proxy, transparent proxy.
4) W zakresie sieciowym wymagana jest obsługa IEEE 802.3ad link aggregation.
5) Produkt nie powinien posiadać ograniczeń co do ilości obsługiwanych serwerów.
6) Powinna istnieć możliwość zdefiniowania co najmniej 2 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.

Wymagane mechanizmy High Availability

1) System musi mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive oraz Active-Active.
2) Klastrowanie N+1 bazujące na Stateful session failover zarówno w trybie Active-Passive jak i Active-Active.
3) Synchronizacja konfiguracji pomiędzy elementami klastra w czasie rzeczywistym.
4) Pływające adresy IP oraz grupy dla Stateful failover. Failover jest anonsowany dla sąsiednich urządzeń sieciowych używając Gratuitous ARP.
5) Wbudowane mechanizmy decyzji o failover w oparciu o: reboot systemu, niedostępność interfejsów, brak komunikacji Heartbeat, brak dostępności adresu IP.
6) Synchronizacja konfiguracji po przeładowaniu urządzenia jak i w czasie pracy.

Parametry fizyczne systemu

1) System realizujący funkcje podstawowe musi dysponować minimum:
   - 10 intefejsami wirtualnymi
2) Nielimitowana powierzchnia dyskowa.

Parametry wydajnościowe

1) Przepływność: nie mniej 4 Gbps w warstwie 4.
2) Ilość dostępnych procesorów wirtualnych – 4

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1) Podział obciążenia (loadbalancing) dla protokołów:
   - dns
   - ftp
   - http
   - https
   - ip
   - mysql
   - DIAMETER
   - radius
   - rdp
   - rtmp
   - rtsp
   - sip
   - smtp
   - tcp
   - udp
2) Mechanizmamy podziału obciążenia:
   - Round Robin,
   - Weighted Round Robin,
   - Least Connection,
   - Fastest Response
3) Wsparcie dla mechanizmów server persistence:
   - Source-IP
   - Source-IP Hash
   - Source-IP/Port Hash
   - Hash Header
   - Hash Request
   - Persistent Cookie
   - Rewrite Cookie

- Insert Cookie
- Hash Cookie
- Embedded Cookie
- RADIUS Attribute
- SSL Session ID
- RDP Cookie

4) Weryfikacja stanu pracy serwerów, co najmniej w oparciu o protokoły:
   - dns
   - ftp
   - http
   - https
   - icmp
   - imap4
   - l2-detection
   - mysql
   - DIAMETER
   - pop3
   - radacct
   - radius
   - rtsp
   - sip
   - sip-tcp
   - smtp
   - snmp
   - snmp-custom
   - ssh
   - tcp
   - tcp-echo
   - tcphalf
   - tcpssl
   - udp
   - LDAP
   - Oracle

5) Możliwość kontroli produkcyjnego przy uruchamianiu serwerów (warm up rate limiting) oraz przy ich konserwacji (session ramp down).
6) Content routing.
7) Funkcja podmiany zawartości - content rewriting.
8) Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For".
9) Obsługa języków skryptowych, umożliwiających manipulowanie żądaniami i odpowiedziami w transakcjach, z funkcją debugowania działania skryptów.
10) Podział obciążenia pomiędzy kilka łączy z funkcjami: health check oraz persistence, przy zastosowaniu metod rozkładania ruchu
11) Wyjściowy multi-homing Link Load Balancing używając funkcji virtual tunnel (enkapsulacja GRE) przy wielu łączach wychodzących przy zastosowaniu metod rozkładania obciążenia
12) Load balancing serwerów pomiędzy różnymi data center.
13) Global Load ballancing w oparciu o protokół DNS.
14) Obsługa DNSSEC z możliwością definiowania list kontroli dostępu.
15) Możliwość zdefiniowania co najmniej X interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
16) W zakresie routingu rozwiązanie powinno zapewniać obsługę protokołów dynamicznego routingu: OSPF oraz BGP.
17) System musi wspierać IPv4 oraz IPv6

Wymagane funkcje w zakresie SSL-offload:

1) Obsługa SSL Forward Proxy.
2) Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.
3) Bezpieczne dostarczanie aplikacji przy wsparciu szyfrowania SSL.
4) Wparcie formatów certyfikatów: .cer, .pem, and .pfx (PKCS12).
5) Backup i odtwarzanie certyfikatów oraz kluczy prywatnych na dysk lokalny za pośrednictwem interfejsu GUI.
6) Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
7) Możliwość generowania CSR (Certificate Signing Request), self-signed Certificate oraz klucza prywatnego dla określonego hosta.
8) Możliwość dostosowania komunikatów błędów dla zdarzeń SSL.
9) Przepisywanie nagłówka HTTP do HTTPS Host, Request URL, Referer oraz jego manipulację za pomocą skryptów.

10) Wsparcie SSL end-to-end, jako SSL Server i/lub jako SSL Client.

11) Weryfikacja certyfikatu klienta, CRL (HTTP, FTP, LDAP) przez http, SCEP oraz OSCP.

12) Wspierane algorytmy, co najmniej: Elliptic Curve Diffie-Helman, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-RC4-SHA, ECDHE-RSA-DES-CBC3-SHA.

13) Wsparcie rozszerzeń TLS SNI w połączeniach: client <-> ADC oraz ADC <-> server.

14) Wspiercie wersji SSL/TLS dla serwerów wirtualnych oraz rzeczywistych: TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3.

Wymagane funkcje w zakresie akceleracji aplikacji:

1) Optymalizacja wydajności przy użyciu TCP connection multiplexing oraz TCP buffering.
2) Obsługa w czasie rzeczywistym tzw. Dynamic Web Content Compression w celu redukcji obciążenia serwerów z opcją wyboru typu kontentu oraz URI.
3) Selektywna kompresja dla typów MIME, co najmniej: Text, HTML, XML, Java Scripts, CSS, Custom (images).
4) Zaawansowany i wydajny Web cache bazujący na pamięci RAM.
5) W zakresie HTTP cache'owanie obiektów statycznych oraz dynamicznych.
6) Konfiguracja reguł w oparciu o które działa cache. Powinny one uwzględniać co najmniej: max object size, TTL objects, refresh time interval.
7) Statystyki dostępu do cache bazujące na IP lub http hosts.
8) Obsługa Rate shaping oraz QoS dla: źródła, przeznaczenia i usług.

Wymagane funkcje w zakresie bezpieczeństwa aplikacji:

1) Ochrona przed atakami SYN flood oraz SYN Cookie.
2) Stateful firewall dla IPv4 oraz IPv6.
3) HTTP authentication.
4) Wsparcie Geo-IP dla ochrony przed DDoS.
5) Limitowanie połączeń w oparciu o polityki.
6) Pełna obsługa OWASP top 10
7) Ochrona przed podmianą strony WWW realizowana bezpośrednio na systemie podziału obciążenia lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcjonalność.
8) Skaner aplikacji WWW realizowany bezpośrednio na systemie podziału obciążenia lub zewnętrznym systemie. W ramach postępowania muszą

zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcjonalności.
9) Wsparcie dla walidacji OpenAPI, JSON i XML.

Wymagane funkcje dodatkowe

1) Uwierzytelnianie użytkowników w oparciu o: lokalną bazę, LDAP, RADIUS, Kerberos, SAML 2.0.
2) Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day
3) Możliwość przełączenia systemu w tryb inspekcji SSL, z możliwością uruchomienia kategoryzacji filtrowanych stron internetowych

Zarządzanie

1) Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, SNMP v1, v2c, v3.
2) Musi dostarczać w GUI informacji o zalogowanych administratorach.
3) Możliwość aktualizacji oprogramowania, backupu i odtwarzania konfiguracji z poziomu GUI.
4) Wsparcie dla REST API do integracji z innymi produktami.
5) Wbudowane narzędzie pozwalające na podgląd komunikacji sieciowej, np. Packet Capture.
6) System musi posiadać co najmniej dwie partycje, na których przechowywane jest oprogramowania i konfiguracja.

Logowanie i Raportowanie

1) System musi zapewniać lokalne logowanie oraz raportowanie.
2) Możliwość logowania do wielu zewnętrznych serwerów syslog z możliwością określenia facility.
3) Obsługa powiadomień o zdarzeniach systemowych mailem.
4) Powiadomienia o zdarzeniach systemowych za pośrednictwem trapów SNMP, w tym co najmniej zużycie: CPU, RAM, Dysku.

Gwarancja oraz wsparcie

1) System musi być objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski,

zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.znych repozytoriów jak baza danych czy LDAP oraz zapytanie HTTP przesłane do serwera aplikacji Web

- musi istnieć możliwość rejestrowania kodu źródłowego strony zwracanej klientowi przez aplikację Web, dostępnego bezpośrednio z interfejsu GUI serwera zarządzającego
- system powinien posiadać GUI dostępne przez przeglądarkę internetową w celu zoptymalizowania pracy, eliminacji konieczności instalacji dodatkowego oprogramowania na stacji administratora a także scentralizować zarządzanie całością rozwiązania
- samoczynne uczenie się "normalnych" zachowań aplikacji umożliwiając przegląd zestawienia zachowań użytkowników z informacją o zagrożeniach
- kontrolowanie dostępu do danych wrażliwych występujących w aplikacjach, które system ma chronić
- przyśpieszenie procesów reagowania na incydenty naruszenia bezpieczeństwa oraz procesów śledczych dzięki zastosowaniu technik analitycznych
- automatyczne uczenie się struktury danej aplikacji webowej oraz zachowań użytkowników, profil aplikacji Web musi być budowany w sposób automatyczny poprzez analizę ruchu sieciowego. Musi istnieć możliwość automatycznej aktualizacji profilu w przypadku wystąpienia zmiany w strukturze aplikacji
- system musi posiadać możliwość sprawdzenia, które z wykorzystywanych pól aplikacji są typu „read-only” i nie mogą być zmieniane przez klientów
- wykrywanie ruchu sieciowego pochodzącego z potencjalnie niebezpiecznych źródeł w tym sieci TOR- ukrywania źródła ataku, szkodliwe adresy IP z których wielokrotnie zaatakowano inne strony Internetowe
- tworzenie wirtualnych poprawek dla aplikacji poprzez integrację ze skanerem podatności
- musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej bezpośrednio z centralnego serwera zarządzającego oraz możliwość cyklicznego wysyłania raportów wiadomością e-mail. Rozwiązanie musi posiadać funkcję wysyłania informacji o zdarzeniach: poprzez protokół SNMP. System musi posiadać możliwość wygenerowania gotowych raporty dotyczących: alarmów bezpieczeństwa, zdarzeń systemowych, zmian w profilach aplikacji, ostrzeżeń, ataków, prób włamań

- tworzenie tzw. "białej listy" akceptowanych zachowań użytkownika (profilowanie chronionych aplikacji), nie może dodawać do profilu informacji pochodzących z przeprowadzanych ataków
- automatyczne wykrywanie niepożądanych atrybutów, niezgodnych z protokołem http
- system powinien analizować słabe punkty zgłaszane przynajmniej przez Bugtraq, CVE, Snort
- powinien posiadać ochronę przed botami
- powinien posiadać możliwość geolokalizacji adresów IP – położenie geograficzne będące źródłem ataków i blokady dostępu
- system w przypadku ataku powinien umożliwić: blokowanie pakietu oraz źródła ataku w postaci adresu IP, nazwy użytkownika lub sesji (jeżeli użytkownik uwierzytelnił się w systemie)
- wykryć adresy z których wykonywane są krytyczne incydenty SQL Injection oraz Remote File Inclusion, anonimowe proxy maskujące tożsamość użytkowników oraz adresy IP znane ze spamowania na forach internetowych. Baza adresów IP musi być pogrupowana według zagrożeń a także automatycznie aktualizowana
- rozwiązanie musi posiadać reguły dotyczące identyfikacji incydentów typu web scraping poprzez zliczanie ilości odwołań do serwisu, oraz identyfikację ataków z sieci Bot dzięki wykorzystaniu skryptów java wykonywanych w przeglądarce klienta
- ochrona przed atakami CSRF bez modyfikacji ruchu http
- aktualizacja systemu musi być dostępna zarówno poprzez ręczne pobranie zawartości ze strony producenta jak i automatycznie, poprzez zdefiniowanie terminów wykonania procedury aktualizacji
- powinien posiadać możliwość integracji z systemem SIEM (syslog)
- tworzenie wirtualnych poprawek dla aplikacji poprzez integrację ze skanerami podatności
-

11. Opis przedmiotu zamówienia na zakup drugiego oprogramowania Firewall aplikacyjnego:

Oryginalna nazwa: firmy Fortinet - FortiWeb - Web Aplication Firewall - virtual appliance for up to 4 x vCPU core – VM04 Supported - License 1 Years

Szczegóły licencji:

Support Coverage			
Rodzaj wsparcia (Support Type)	Poziom Wsparcia (Support Level)	Data aktywacji (Activation Date)	Termin ważności (Expiration Date)
Firmware & General Updates	Web/Online	2025-10-13	2026-10-12

Enhanced Support	24x7	2025-10-13	2026-10-12
Advanced Malware Protection	Web/Online	2025-10-13	2026-10-12
FortiWeb Security Service	Web/Online	2025-10-13	2026-10-12
IP Reputation	Web/Online	2025-10-13	2026-10-12

12. Oprogramowanie Firewall aplikacyjny firmy Fortinet - FortiWeb - Web Aplication Firewall - virtual appliance for up to 4 x vCPU core **oprogramowanie równoważne musi spełniać następujące warunki:**

- wszystkie elementy systemu zabezpieczeń muszą być dostarczone przez jednego producenta w formie gotowych maszyn wirtualnych działających w środowisku ESX/ESXi
- system musi działać w następujących trybach pracy: Transparent Bridge (inline warstwa 2 ISO/OSI), Transparent Reverse Proxy – tj praca w trybie proxy nie wymagająca korzystania z nowych adresów IP, Reverse Proxy oraz Sniffing przy czym musi istnieć możliwość działania w trybie Transparent Bridge oraz Transparent Reverse Proxy w obrębie tych samych chronionych aplikacji
- moduły wykonawcze muszą mieć możliwość pracy w trybie High Availability (HA), powinny zawierać mechanizm ochrony typu Stateful Firewall oraz weryfikować zgodność komunikacji sieciowej ze standardem protokołu tcp/ip, opisanym w RFC
- system musi mieć wydajność analizy protokołu http/https na poziomie 500Mbps
- uwierzytelnianie użytkowników oferowanego rozwiązania musi być możliwe za pomocą integracji z Active Directory, LDAP w celu uzyskania dodatkowych informacji w logach na temat użytkownika. Obsługiwane muszą być nie mniej niż następujące metody uwierzytelnienia: formularze html, certyfikat cyfrowy, kerberos, NTLM
- całość konfiguracji oraz repozytorium logów musi być przechowywane na centralnym serwerze zarządzania
- system powinien na podstawie analizy obserwowanego ruchu zbudować odzwierciedlenie całej struktury aplikacji, składającej się z katalogów, URLi, metod dostępu, parametrów, typów wartości oraz długości ciągów znaków wprowadzanych przez użytkowników w poszczególnych formatkach a w szczególności powinien umożliwiać naukę formularzy, służących do logowania się użytkowników do aplikacji Web.

- system powinien zagwarantować wysoki poziom ochrony serwerów Web oraz serwerów aplikacyjnych (uwzględniając elementy XML oraz akcje SOAP) przed różnego typu atakami, a także powinien monitorować poprawne zachowanie chronionej aplikacji, a wszelkie próby wyjścia poza to poprawne zachowanie powinien blokować. Wymagane są sygnatury dla nie mniej niż : sieci, aplikacji Web, zapytań Web.
- monitorowanie i kontrolowanie w czasie rzeczywistym wszystkich operacji wykonywanych przez użytkowników. Rozwiązanie musi posiadać możliwość rejestrowania naruszeń bezpieczeństwa oraz udostępniać administratorom co najmniej następujące informacje o zdarzeniach: nazwa użytkownika aplikacyjnego (jeżeli klient zalogował się w systemie przez aplikację Web) , dodatkowe atrybuty użytkownika z zewnętrznych repozytoriów jak baza danych czy LDAP oraz zapytanie HTTP przesłane do serwera aplikacji Web
- musi istnieć możliwość rejestrowania kodu źródłowego strony zwracanej klientowi przez aplikację Web, dostępnego bezpośrednio z interfejsu GUI serwera zarządzającego
- system powinien posiadać GUI dostępne przez przeglądarkę internetową w celu zoptymalizowania pracy, eliminacji konieczności instalacji dodatkowego oprogramowania na stacji administratora a także scentralizować zarządzanie całością rozwiązania
- samoczynne uczenie się "normalnych" zachowań aplikacji umożliwiając przegląd zestawienia zachowań użytkowników z informacją o zagrożeniach
- kontrolowanie dostępu do danych wrażliwych występujących w aplikacjach, które system ma chronić
- przyśpieszenie procesów reagowania na incydenty naruszenia bezpieczeństwa oraz procesów śledczych dzięki zastosowaniu technik analitycznych
- automatyczne uczenie się struktury danej aplikacji webowej oraz zachowań użytkowników, profil aplikacji Web musi być budowany w sposób automatyczny poprzez analizę ruchu sieciowego. Musi istnieć możliwość automatycznej aktualizacji profilu w przypadku wystąpienia zmiany w strukturze aplikacji
- system musi posiadać możliwość sprawdzenia, które z wykorzystywanych pól aplikacji są typu „read-only” i nie mogą być zmieniane przez klientów
- wykrywanie ruchu sieciowego pochodzącego z potencjalnie niebezpiecznych źródeł w tym sieci TOR- ukrywania źródła ataku, szkodliwe adresy IP z których wielokrotnie zaatakowano inne strony Internetowe
- tworzenie wirtualnych poprawek dla aplikacji poprzez integrację ze skanerem podatności
- musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej bezpośrednio z centralnego serwera

zarządzającego oraz możliwość cyklicznego wysyłania raportów wiadomością e-mail. Rozwiązanie musi posiadać funkcję wysyłania informacji o zdarzeniach: poprzez protokół SNMP. System musi posiadać możliwość wygenerowania gotowych raporty dotyczących: alarmów bezpieczeństwa, zdarzeń systemowych, zmian w profilach aplikacji, ostrzeżeń, ataków, prób włamań

- tworzenie tzw. "białej listy" akceptowanych zachowań użytkownika (profilowanie chronionych aplikacji), nie może dodawać do profilu informacji pochodzących z przeprowadzanych ataków
- automatyczne wykrywanie niepożądanych atrybutów, niezgodnych z protokołem http
- system powinien analizować słabe punkty zgłaszane przynajmniej przez Bugtraq, CVE, Snort
- powinien posiadać ochronę przed botami
- powinien posiadać możliwość geolokalizacji adresów IP – położenie geograficzne będące źródłem ataków i blokady dostępu
- system w przypadku ataku powinien umożliwić: blokowanie pakietu oraz źródła ataku w postaci adresu IP, nazwy użytkownika lub sesji (jeżeli użytkownik uwierzytelnił się w systemie)
- wykryć adresy z których wykonywane są krytyczne incydenty SQL Injection oraz Remote File Inclusion, anonimowe proxy maskujące tożsamość użytkowników oraz adresy IP znane ze spamowania na forach internetowych. Baza adresów IP musi być pogrupowana według zagrożeń a także automatycznie aktualizowana
- rozwiązanie musi posiadać reguły dotyczące identyfikacji incydentów typu web scraping poprzez zliczanie ilości odwołań do serwisu, oraz identyfikację ataków z sieci Bot dzięki wykorzystaniu skryptów java wykonywanych w przeglądarce klienta
- ochrona przed atakami CSRF bez modyfikacji ruchu http
- aktualizacja systemu musi być dostępna zarówno poprzez ręczne pobranie zawartości ze strony producenta jak i automatycznie, poprzez zdefiniowanie terminów wykonania procedury aktualizacji
- powinien posiadać możliwość integracji z systemem SIEM (syslog)
- tworzenie wirtualnych poprawek dla aplikacji poprzez integrację ze skanerami podatności

13. W przypadku dostarczenia oprogramowania równoważnego Wykonawca zobowiązany jest do przeniesienia wdrożonej u Zamawiającego konfiguracji (składającej się z ok. 200 serwisów WWW wraz ze wszystkimi regułami) w terminie 2 dni roboczych. Wykonawca zobowiązuje się, iż Oprogramowanie

równoważne, nie będzie wymagało od Zamawiającego dokonywania żadnych zmian w posiadanej infrastrukturze informatycznej Zamawiającego i Oprogramowaniu, z którym ma współdziałać.

14. Infrastruktura techniczna

- wszystkie elementy systemu zabezpieczeń muszą być dostarczone przez jednego producenta w formie gotowych maszyn virtualnych działających w środowisku ESX/ESXi, kompatybilne z VMware 7.0.
- system musi działać w następujących trybach pracy: Transparent Bridge (inline warstwa 2 ISO/OSI), Transparent Reverse Proxy – tj praca w trybie proxy nie wymagająca korzystania z nowych adresów IP, Reverse Proxy oraz Sniffing przy czym musi istnieć możliwość działania w trybie Transparent Bridge oraz Transparent Reverse Proxy w obrębie tych samych chronionych aplikacji.
- moduły wykonawcze muszą mieć możliwość pracy w trybie High Availability (HA), powinny zawierać mechanizm ochrony typu Stateful Firewall oraz weryfikować zgodność komunikacji sieciowej ze standardem protokołu tcp/ip, opisanym w RFC.
- system musi mieć wydajność analizy protokołu http/https na poziomie 500Mbps
  powinien posiadać możliwość integracji z systemem SIEM (syslog) - ManageEngine Eventlog Analyzer

15. Opis przedmiotu zamówienia jest zakup licencji na oprogramowanie Firewall aplikacyjny:

Oryginalna nazwa: firmy Fortinet - FortiWeb - Web Aplication Firewall - virtual appliance for up to 4 x vCPU core - VM04 Supported - License 1 Years

Szczegóły licencji:

Support Coverage			
Rodzaj wsparcia (Support Type)	Poziom Wsparcia (Support Level)	Data aktywacji (Activation Date)	Termin ważności (Expiration Date)
Firmware & General Updates	Web/Online	2025-10-13	2026-10-12
Enhanced Support	24x7	2025-10-13	2026-10-12
Advanced Malware Protection	Web/Online	2025-10-13	2026-10-12

FortiWeb Security Service	Web/Online	2025-10-13	2026-10-12
IP Reputation	Web/Online	2025-10-13	2026-10-12

16. Oprogramowanie Firewall aplikacyjny firmy Fortinet - FortiWeb - Web Aplication Firewall - virtual appliance for up to 4 x vCPU core **oprogramowanie równoważne musi spełniać następujące warunki:**

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. Powinien zostać dostarczony w postaci komercyjnej platformy instalowanej w środowisku wirtualnym: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure, Google Cloud, Oracle Cloud. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych w ww środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędny odpowiednio zabezpieczony systemem operacyjny.

Architektura systemu

1) Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2) Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie.
3) Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
4) Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web.
5) Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.
6) System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.

Parametry fizyczne systemu

1) System realizujący funkcje podstawowe musi obsługiwać minimum:
   - 4 interfejsy sieciowe
   - Ilość wirtualnych procesorów: 4
2) Obługa powierzchni dyskowej - minimum 1 TB.

Parametry wydajnościowe

1) Przepustowość dla ruchu http - min 500 Mbps.

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1) Obsługa protokołów: - http 1.1, http 2.0, FTP.
2) Automatyczne tworzenie profili ochronnych aplikacji na bazie zaobserwowanego ruchu. Możliwość wyboru trybu wymuszania wyuczonego schematu bez konieczności akceptacji przez administratora.
3) Automatyczne tworzenie profilu ochrony przed botami na bazie zaobserwowanego ruchu użytkowników
4) Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:
   - Round Robin,
   - Weighted Round Robin,
   - Least Connection,
5) 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
6) Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3.
7) Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa.
8) 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.

9) Mechanizmy ochrony przed wyciekiem informacji poufnych.
10) Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację.
11) Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
12) Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego.
13) Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy.
14) Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only".
15) Content routing na bazie parametrów http oraz certyfikatów X.509.
16) Ochrona przed Web Scraping.
17) Wsparcie dla kompresji danych oraz cache.
18) Publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos).
19) Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3.
20) Ochrona przed atakami typu SLOW (Slowloris i podobne).
21) Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Dodanie wyjątków dla sygnatur na podstawie wielu parametrów:
    - Metoda HTTP.
    - IP klienta.
    - Host.
    - URI.
    - Cały URL.
    - Parametr.
    - Cookie.
    - http Header
    - JSON Elements
22) Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For".
23) Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
24) Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka.
25) Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload'u HTML.
26) Wsparcie dla walidacji OpenAPI, JSON i XML.
27) Blokowania „Illegal XML Format" oraz „Illegal JSON Format".
28) Możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy.

29) Przydzielanie różnych certyfikatów dla różnych nazw domenowych.
30) Ochrona przed atakami MiTB (Man-in-the-Browser) przynamniej dla Anti-keylogger, Obfuscate.
31) URL Encryption.

Wymagane funkcje dodatkowe

1) Kontrola antywirusowa dla komunikacji http realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
2) 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.
3) 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.
4) Dekodowanie Base64 oraz CSS.
5) Domyślne szablony ochrony dla Exchange, SharePoint i WordPress.
6) Uwierzytelnianie użytkowników w oparciu o protokół SAML.
7) Rozpoznawanie prawidłowo zalogowanych użytkowników do chronionej aplikacji.
8) Wsparcie dla CAPTCHA i Real Browser Enforcement do weryfikacji użytkowników.
9) Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla akcji: kwarantanna czasowa.
10) Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day.
11) Możliwość znakowania przez administratorów systemu za pomocą znaczników (flag) lub komentarza zdarzeń zalogowanych przez urządzenie w celu późniejszej ich analizy.
12) Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, intefejsu API - przy zastosowaniu funkcji biometrycznych.
13) Cross-Origin Resource Sharing (CORS) protection.

14) Integracja z Let's encrypt pozwalająca na automatyczne generowanie certyfikatów na potrzeby terminowania połączeń SSL.

Zarządzanie

1) Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.
2) Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture.
3) Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
4) Możliwość przechowywania lokalnie na urządzeniu do 10 plików konfiguracyjnych.

Logowanie i Raportowanie

1) System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2) Możliwość logowania do zewnętrznego serwera syslog i SIEM.
3) Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.
4) Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.

Certyfikaty

1) Z punktu widzenia jakości i skuteczności rozwiązania koniecznym jest przedstawienie wyników testów niezależnych organizacji, np. NSS Labs, ICSA Labs lub równoważnego z terminem realizacji do 2 dni roboczych liczonych od dnia zakończenia wdrożenia.

Sygnatury, subskrypcje

1) System musi być dostarczony w modelu „na własność" tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
2) Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.
3) W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
    - Kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP na okres [12] miesięcy.

Gwarancja oraz wsparcie

1) System musi być objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy. W ramach tego serwisu producent musi zapewniać również

dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

17. Opis przedmiotu zamówienia na zakup licencji na oprogramowanie FortiADC Load Balancer:

Oryginalna nazwa: firmy Fortinet - FortiADC-VM04 - Application Delivery Controller – supported platforms - License 1 Years

Szczegóły licencji:

Support Coverage			
Rodzaj wsparcia (Support Type)	Poziom Wsparcia (Support Level)	Data aktywacji (Activation Date)	Termin ważności (Expiration Date)
Firmware & General Updates	Web/Online	2025-10-13	2026-10-12
Enhanced Support	24x7	2025-10-13	2026-10-12
Advanced Malware Protection	Web/Online	2025-10-13	2026-10-12
FortiWeb Security Service	Web/Online	2025-10-13	2026-10-12
IP Reputation	Web/Online	2025-10-13	2026-10-12

18. Oprogramowanie Firewall aplikacyjny firmy Fortinet - FortiWeb - Application Delivery Controller - virtual appliance for up to 4 x vCPU core **oprogramowanie równoważne musi spełniać następujące warunki:**

System podziału obciążenia dla ruchu przychodzącego i wychodzącego pracujący w warstwach 2,4,7. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Architektura systemu

1) Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest, aby system pracował w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2) 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) Powinna istnieć możliwość implementacji systemu w trybach: one-arm, reverse proxy, transparent proxy.
4) W zakresie sieciowym wymagana jest obsługa IEEE 802.3ad link aggregation.
5) Produkt nie powinien posiadać ograniczeń co do ilości obsługiwanych serwerów.
6) Powinna istnieć możliwość zdefiniowania co najmniej 2 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.

Wymagane mechanizmy High Availability

7) System musi mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive oraz Active-Active.
8) Klastrowanie N+1 bazujące na Stateful session failover zarówno w trybie Active-Passive jak i Active-Active.
9) Synchronizacja konfiguracji pomiędzy elementami klastra w czasie rzeczywistym.

10) Pływające adresy IP oraz grupy dla Stateful failover. Failover jest anonsowany dla sąsiednich urządzeń sieciowych używając Gratuitous ARP.

11) Wbudowane mechanizmy decyzji o failover w oparciu o: reboot systemu, niedostępność interfejsów, brak komunikacji Heartbeat, brak dostępności adresu IP.

12) Synchronizacja konfiguracji po przeładowaniu urządzenia jak i w czasie pracy.

Parametry fizyczne systemu

1) System realizujący funkcje podstawowe musi dysponować minimum:
   - 10 intefejsami wirtualnymi
2) Nielimitowana powierzchnia dyskowa.

Parametry wydajnościowe

1) Przepływność: nie mniej 4 Gbps w warstwie 4.
2) Ilość dostępnych procesorów wirtualnych – 4

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1) Podział obciążenia (loadbalancing) dla protokołów:
   - dns
   - ftp
   - http
   - https
   - ip
   - mysql
   - DIAMETER
   - radius
   - rdp
   - rtmp
   - rtsp
   - sip
   - smtp
   - tcp
   - udp
2) Mechanizmamy podziału obciążenia:
   - Round Robin,

- Weighted Round Robin,
- Least Connection,
- Fastest Response

3) Wsparcie dla mechanizmów server persistence:
   - Source-IP
   - Source-IP Hash
   - Source-IP/Port Hash
   - Hash Header
   - Hash Request
   - Persistent Cookie
   - Rewrite Cookie
   - Insert Cookie
   - Hash Cookie
   - Embedded Cookie
   - RADIUS Attribute
   - SSL Session ID
   - RDP Cookie
4) Weryfikacja stanu pracy serwerów, co najmniej w oparciu o protokoły:
   - dns
   - ftp
   - http
   - https
   - icmp
   - imap4
   - l2-detection
   - mysql
   - DIAMETER
   - pop3
   - radacct
   - radius
   - rtsp
   - sip
   - sip-tcp
   - smtp

- snmp
- snmp-custom
- ssh
- tcp
- tcp-echo
- tcphalf
- tcpssl
- udp
- LDAP
- Oracle

5) Możliwość kontroli produkcyjnego przy uruchamianiu serwerów (warm up rate limiting) oraz przy ich konserwacji (session ramp down).
6) Content routing.
7) Funkcja podmiany zawartości - content rewriting.
8) Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For".
9) Obsługa języków skryptowych, umożliwiających manipulowanie żądaniami i odpowiedziami w transakcjach, z funkcją debugowania działania skryptów.
10) Podział obciążenia pomiędzy kilka łączy z funkcjami: health check oraz persistence, przy zastosowaniu metod rozkładania ruchu
11) Wyjściowy multi-homing Link Load Balancing używając funkcji virtual tunnel (enkapsulacja GRE) przy wielu łączach wychodzących przy zastosowaniu metod rozkładania obciążenia
12) Load balancing serwerów pomiędzy różnymi data center.
13) Global Load ballancing w oparciu o protokół DNS.
14) Obsługa DNSSEC z możliwością definiowania list kontroli dostępu.
15) Możliwość zdefiniowania co najmniej X interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
16) W zakresie routingu rozwiązanie powinno zapewniać obsługę protokołów dynamicznego routingu: OSPF oraz BGP.
17) System musi wspierać IPv4 oraz IPv6

Wymagane funkcje w zakresie SSL-offload:

1) Obsługa SSL Forward Proxy.
2) Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.

3) Bezpieczne dostarczanie aplikacji przy wsparciu szyfrowania SSL.
4) Wparcie formatów certyfikatów: .cer, .pem, and .pfx (PKCS12).
5) Backup i odtwarzanie certyfikatów oraz kluczy prywatnych na dysk lokalny za pośrednictwem interfejsu GUI.
6) Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
7) Możliwość generowania CSR (Certificate Signing Request), self-signed Certificate oraz klucza prywatnego dla określonego hosta.
8) Możliwość dostosowania komunikatów błędów dla zdarzeń SSL.
9) Przepisywanie nagłówka HTTP do HTTPS Host, Request URL, Referer oraz jego manipulację za pomocą skryptów.
10) Wsparcie SSL end-to-end, jako SSL Server i/lub jako SSL Client.
11) Weryfikacja certyfikatu klienta, CRL (HTTP, FTP, LDAP) przez http, SCEP oraz OSCP.
12) Wspierane algorytmy, co najmniej: Elliptic Curve Diffie-Helman, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-RC4-SHA, ECDHE-RSA-DES-CBC3-SHA.
13) Wsparcie rozszerzeń TLS SNI w połączeniach: client <-> ADC oraz ADC <-> server.
14) Wspiercie wersji SSL/TLS dla serwerów wirtualnych oraz rzeczywistych: TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3.

Wymagane funkcje w zakresie akceleracji aplikacji:

9) Optymalizacja wydajności przy użyciu TCP connection multiplexing oraz TCP buffering.
10) Obsługa w czasie rzeczywistym tzw. Dynamic Web Content Compression w celu redukcji obciążenia serwerów z opcją wyboru typu kontentu oraz URI.
11) Selektywna kompresja dla typów MIME, co najmniej: Text, HTML, XML, Java Scripts, CSS, Custom (images).
12) Zaawansowany i wydajny Web cache bazujący na pamięci RAM.
13) W zakresie HTTP cache'owanie obiektów statycznych oraz dynamicznych.
14) Konfiguracja reguł w oparciu o które działa cache. Powinny one uwzględniać co najmniej: max object size, TTL objects, refresh time interval.
15) Statystyki dostępu do cache bazujące na IP lub http hosts.

16) Obsługa Rate shaping oraz QoS dla: źródła, przeznaczenia i usług.

Wymagane funkcje w zakresie bezpieczeństwa aplikacji:

1) Ochrona przed atakami SYN flood oraz SYN Cookie.
2) Stateful firewall dla IPv4 oraz IPv6.
3) HTTP authentication.
4) Wsparcie Geo-IP dla ochrony przed DDoS.
5) Limitowanie połączeń w oparciu o polityki.
6) Pełna obsługa OWASP top 10
7) Ochrona przed podmianą strony WWW realizowana bezpośrednio na systemie podziału obciążenia lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcjonalność.
8) Skaner aplikacji WWW realizowany bezpośrednio na systemie podziału obciążenia lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcjonalności.
9) Wsparcie dla walidacji OpenAPI, JSON i XML.

Wymagane funkcje dodatkowe

1) Uwierzytelnianie użytkowników w oparciu o: lokalną bazę, LDAP, RADIUS, Kerberos, SAML 2.0.
2) Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day
3) Możliwość przełączenia systemu w tryb inspekcji SSL, z możliwością uruchomienia kategoryzacji filtrowanych stron internetowych

Zarządzanie

1) Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, SNMP v1, v2c, v3.
2) Musi dostarczać w GUI informacji o zalogowanych administratorach.
3) Możliwość aktualizacji oprogramowania, backupu i odtwarzania konfiguracji z poziomu GUI.
4) Wsparcie dla REST API do integracji z innymi produktami.
5) Wbudowane narządzie pozwalające na podgląd komunikacji sieciowej, np. Packet Capture.
6) System musi posiadać co najmniej dwie partycje, na których przechowywane jest oprogramowania i konfiguracja.

Logowanie i Raportowanie

5) System musi zapewniać lokalne logowanie oraz raportowanie.
6) Możliwość logowania do wielu zewnętrznych serwerów syslog z możliwością określenia facility.
7) Obsługa powiadomień o zdarzeniach systemowych mailem.

8) Powiadomienia o zdarzeniach systemowych za pośrednictwem trapów SNMP, w tym co najmniej zużycie: CPU, RAM, Dysku.

Gwarancja oraz wsparcie

2) System musi być objęty serwisem gwarancyjnym producenta przez okres [12] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.znych repozytoriów jak baza danych czy LDAP oraz zapytanie HTTP przesłane do serwera aplikacji Web
- musi istnieć możliwość rejestrowania kodu źródłowego strony zwracanej klientowi przez aplikację Web, dostępnego bezpośrednio z interfejsu GUI serwera zarządzającego
- system powinien posiadać GUI dostępne przez przeglądarkę internetową w celu zoptymalizowania pracy, eliminacji konieczności instalacji dodatkowego oprogramowania na stacji administratora a także scentralizować zarządzanie całością rozwiązania
- samoczynne uczenie się "normalnych" zachowań aplikacji umożliwiając przegląd zestawienia zachowań użytkowników z informacją o zagrożeniach
- kontrolowanie dostępu do danych wrażliwych występujących w aplikacjach, które system ma chronić
- przyśpieszenie procesów reagowania na incydenty naruszenia bezpieczeństwa oraz procesów śledczych dzięki zastosowaniu technik analitycznych
- automatyczne uczenie się struktury danej aplikacji webowej oraz zachowań użytkowników, profil aplikacji Web musi być budowany w sposób automatyczny poprzez analizę ruchu sieciowego. Musi istnieć możliwość automatycznej aktualizacji profilu w przypadku wystąpienia zmiany w strukturze aplikacji

- system musi posiadać możliwość sprawdzenia, które z wykorzystywanych pól aplikacji są typu „read-only” i nie mogą być zmieniane przez klientów
- wykrywanie ruchu sieciowego pochodzącego z potencjalnie niebezpiecznych źródeł w tym sieci TOR- ukrywania źródła ataku, szkodliwe adresy IP z których wielokrotnie zaatakowano inne strony Internetowe
- tworzenie wirtualnych poprawek dla aplikacji poprzez integrację ze skanerem podatności
- musi istnieć możliwość tworzenia własnych raportów, zarówno w formie tekstowej jak i reprezentacji graficznej bezpośrednio z centralnego serwera zarządzającego oraz możliwość cyklicznego wysyłania raportów wiadomością e-mail. Rozwiązanie musi posiadać funkcję wysyłania informacji o zdarzeniach: poprzez protokół SNMP. System musi posiadać możliwość wygenerowania gotowych raporty dotyczących: alarmów bezpieczeństwa, zdarzeń systemowych, zmian w profilach aplikacji, ostrzeżeń, ataków, prób włamań
- tworzenie tzw. "białej listy" akceptowanych zachowań użytkownika (profilowanie chronionych aplikacji), nie może dodawać do profilu informacji pochodzących z przeprowadzanych ataków
- automatyczne wykrywanie niepożądanych atrybutów, niezgodnych z protokołem http
- system powinien analizować słabe punkty zgłaszane przynajmniej przez Bugtraq, CVE, Snort
- powinien posiadać ochronę przed botami
- powinien posiadać możliwość geolokalizacji adresów IP – położenie geograficzne będące źródłem ataków i blokady dostępu
- system w przypadku ataku powinien umożliwić: blokowanie pakietu oraz źródła ataku w postaci adresu IP, nazwy użytkownika lub sesji (jeżeli użytkownik uwierzytelnił się w systemie)
- wykryć adresy z których wykonywane są krytyczne incydenty SQL Injection oraz Remote File Inclusion, anonimowe proxy maskujące tożsamość użytkowników oraz adresy IP znane ze spamowania na forach internetowych. Baza adresów IP musi być pogrupowana według zagrożeń a także automatycznie aktualizowana
- rozwiązanie musi posiadać reguły dotyczące identyfikacji incydentów typu web scraping poprzez zliczanie ilości odwołań do serwisu, oraz identyfikację ataków z sieci Bot dzięki wykorzystaniu skryptów java wykonywanych w przeglądarce klienta
- ochrona przed atakami CSRF bez modyfikacji ruchu http
- aktualizacja systemu musi być dostępna zarówno poprzez ręczne pobranie zawartości ze strony producenta jak i automatycznie, poprzez zdefiniowanie terminów wykonania procedury aktualizacji
- powinien posiadać możliwość integracji z systemem SIEM (syslog)
- tworzenie wirtualnych poprawek dla aplikacji poprzez integrację ze skanerami podatności