ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI V

I. Nazwa zamówienia

Dostawa 8 wirtualnych appliance (klasy Load Balancer z funkcjonalnością terminacji SSL/TLS i WAF) wraz z usługami wsparcia na okres 36 miesięcy

I.1 Kody CPV

32420000-3 Urządzenia sieciowe.
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.

II. Przedmiot zamówienia

(1) Przedmiotem zamówienia jest dostawa licencji na wirtualny Load Balancer z funkcjonalnością terminacji SSL/TLS i modułem ochrony aplikacji webowych klasy WAF (ang. Web Application Firewall – System ochrony aplikacji webowych), **zwane dalej „System LB"** (ang. Load Balancer), opisany w pkt III.1., a następnie świadczenie Godzin eksperckich, opisanych w pkt III.2 oraz usług wsparcia techicznego w pkt. III.3.

(2) Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Dzień Roboczy	oznacza dzień od poniedziałku do piątku nie będący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Godziny ekspercie	usługi konsultacji (tzw. ang. *Professional Services*), których przedmiotem będą miedzy innymi zagadnienia wskazane w OPZ, dotyczące obsługi, konfiguracji I eksploatacji Systemu LB, bieżących problemów dotyczących funkcjonowania Systemu LB, jego konfiguracji, wyjaśniania wątpliwości lub rozwiązania zagadnień z tego zakresu przedstawianych przez Zamawiającego, związanych z obsługą Systemu LB, świadczone w miejscu zainstalowania Systemu LB lub zdalnie, na warunkach wskazanych w OPZ, w terminach uzgodnionych zgodnie z postanowieniami Umowy również poza Dniami Roboczymi oraz poza Godzinami Roboczymi.
Godziny Robocze	oznacza godziny od 09:00 do 17:00 w dni od poniedziałku do piątku, nie będące dniami ustawowo wolnymi od pracy na terenie Rzeczypospolitej Polskiej.
Wsparcie producenta	Oznacza oferowane przez producenta Systemu LB aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla Systemu LB przez zdefiniowany okres czasu, zgodnie z pkt III.3 OPZ.
Roboczogodzina	jedna godzina pracy jednego członka personelu Wykonawcy.

WAF	*ang.* Web Application Firewall oznacza moduł ochrony ruchu webowego.
SSL/TLS	*ang.* Secure Socket Layer / Transport Layer Security oznacza protokół szyfrowania komunikacji sieciowej. (ze wsparciem co najmniej w wersji TLS 1.2 lub TLS 1.3)
Wirtualny Appliance	ang. Virtual Appliance oznacza system, do którego Producent dostarcza oprogramowanie i wsparcie techniczne.

(3) Przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, a Zamawiający dopuszcza rozwiązania równoważne opisywanym i takim odniesieniom towarzyszą wyrazy "lub równoważne".

(4) W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp., Zamawiający nie odrzuci oferty tylko dlatego, że oferowane dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp., że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

(5) W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp., zamawiający nie odrzuci oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107, że dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.

(6) W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przyapdkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.

(7) Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.

(8) Wykonawca zobowiązany jest posiadać status partnera producenta Systemu LB z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby Wykonawca posiadał nie niższy niż drugi w kolejności poziom partnerstwa licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu poprzedzającym.

(9) Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji ul. Królewska 27, 00-060 Warszawa.

(10) Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z oprogramowania w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją chmury prywatnej na rzecz Ministra Cyfryzacji.

III. Specyfikacja wymagań

III.1 Dostawa Licencji

(1) Przedmiotem zamówienia jest dostawa 8 Systemów LB.

(2) System LB musi spełniać wymagania opisane w pkt. III.1.1.

(3) Termin dostawy 8 Systemów LB wynosi do 5 Dni Roboczych od dnia zawarcia umowy;

Szczegółowe warunki dostawy określone są w Rozdziale III SIWZ – Projektowanych postanowieniach umowy

III.1.1 Wymagania dla Systemu LB

Wymagania dla Systemu LB		
LP.	**Opis wymagania**	**Parametry minimalne**
1.	Ogólne	1.1. Obsługiwane funkcjonalności: 1.1.1. Zaawansowany system klasy Load Balancer 1.1.2. Terminacja SSL/TLS 1.1.3. Zaawansowany system klasy WAF w ramach jednego Wirtualnego Appliance. 1.2. System LB nie może znajdować się na liście (typu „end-of-life” oraz „end-of-support”), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025. 1.3. Klucze prywatne zapisane na dysku muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.

2.	Wsparcie dla platform wirtualizacyjnych	2.1. System LB musi działać w co najmniej jednym z następujących środowisk: 2.1.1. VMware lub 2.1.2. KVM.
3.	Przepustowość	3.1. Minimum 1 Gbps (z włączonym modułem WAF i terminacją SSL/TLS) z możliwością zwiększenia poprzez dokupienie licencji.
4.	Protokoły IP	4.1. Musi zapewniać obsługę IPv4 I IPv6.
5.	Tryb proxy	5.1. System LB musi umożliwić pracę w trybie proxy. 5.2. Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.
6.	Funkcje Load Balancera - ogólne	6.1. System LB musi świadczyć, co najmniej następujące usługi w warstwach 4-7: 6.1.1. Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http 6.1.2. Ukrywanie zasobów 6.1.3. Zmiana odpowiedzi serwera 6.1.4. Przepisywanie odpowiedzi (response rewriting) 6.1.5. Multipleksowanie połączeń http 6.2. System LB musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. 6.3. Musi zapewniać selektywny http caching. 6.4. Musi zapewniać selektywną kompresja danych. 6.5. System LB musi zapewniać funkcjonalność stanowej zapory sieciowej umożliwiającej kontrolę ruchu sieciowego w warstwie 3 i 4 ISO/OSI, przy spełnieniu następujących wymagań: 6.5.1. Zarządzanie regułami bezpieczeństwa musi być realizowane za pomocą wbudowanego w System LB interfejsu graficznego. 6.5.2. Reguły definiujące ruch muszą zawierać oprócz adresu, adresów IP również możliwość wskazanie lokalizacji (w ruchu źródłowym oraz ruchu docelowym) tzw. geolokalizacja 6.5.3. System LB musi chronić przed atakami typu flood, sweep, teardrop oraz smurf. 6.5.4. System LB powinien umożliwiać uruchomienie proxy SSH, które umożliwia np. blokowanie ściągania lub wgrywania plików po SCP lub SFTP, ustawienie czy użytkownik ma dostęp do shella.[1]

[1] Stanowi kryterium oceny ofert

		6.5.5. System LB musi wykrywać nieprawidłowe protokoły przechodzące przez otwarte porty (np. otwarty port 80 dla ruchu http, gdy na tym porcie odbywa się ruch ssh). 6.5.6. System LB musi posiadać wsparcie obsługi protokołów routingu statycznych i dynamicznych: BGP/BGP-4, OSPF, RIP/RIPv2. 6.6. System musi wspierać mechanizm pojedynczego logowania SSO (ang. Single Sign-On) oraz mieć możliwość uruchomienie usługi dostawcy tożsamości (Identity Provider).
7.	Funkcje Load Balancera - równoważenie obciążenia DNS	7.1. Rozwiązanie musi zapewniać globalne, inteligentne sterowanie ruchem wykorzystując usługę DNS jako mechanizm rozdziału ruchu (Global Solution Load Balancing), w ramach którego zapewni: 7.1.1. Monitorowanie stanu pracy usług korzystając z monitorów działających w warstwie sieci, transportowej oraz aplikacji modelu ISO/OSI 7.1.2. Rozdzielanie ruchu korzystając co najmniej z metod: 7.1.2.1. Cykliczna 7.1.2.2. Ważona 7.1.2.3. Na podstawie adresów IP klienta usługi (topologii) 7.1.2.4. Obciążenia serwera 7.1.2.5. Najmniejszej liczby połączeń. 7.1.3. Mechanizmy utrzymywania sesji polegające na kierowaniu zapytań z lokalnego serwera DNS klienta aplikacji zawsze do tego samego centrum danych i serwera aplikacji 7.1.4. Wbudowany w system operacyjny język skryptowy, umożliwiający analizę i zmianę parametrów w protokole DNS 7.1.5. Ochronę serwerów DNS z wykorzystanie DNSSEC, a także na zastosowaniu list kontroli dostępu umożliwiających filtrowanie ruchu DNS bazując na typie rekordu 7.1.6. Możliwość pracy jako serwer DNS, obsługujący następujące rekordy: A, NS, CNAME, SOA, PTR, MX, TXT, KEY, AAAA, SRV, NAPTR, CERT, DNAME, OPT, DS, IPSECKEY, RRSIG, NSEC, DNSKEY, DHCID, NSEC3, TKEY, TSIG, ANY, DLV 7.1.7. Konwersja rekordów między IPv4 i IPv6

		7.1.8. Wsparcie dla usług geolokacji, możliwość przekierowania ruchu do najbliższej geograficznie lokalizacji 7.1.9. Wybór lokalizacji na podstawie ilości urządzeń pośredniczących oraz ilości przetwarzanych danych 7.1.10. Możliwość wysyłania zapytań dotyczących obciążenia do urządzeń firm trzecich 7.2. Możliwość bezpośredniego odpytywania serwerów o obciążenie 7.2.1. Możliwość przekierowania ruchu do innej lokalizacji po przekroczeniu zdefiniowanego progu ilości sesji.
8.	Funkcje Load Balancera - metody równoważenia obciążenia	8.1. Musi zapewnić rozkład ruchu pomiędzy serwerami aplikacji Web. 8.2. Musi zapewniać metody równoważenia obciążenia: 8.2.1. Cykliczna 8.2.2. Ważona 8.2.3. Najmniejsza liczba połączeń 8.2.4. Najszybsza odpowiedź serwera 8.2.5. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera 8.2.6. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie 8.2.7. Dynamicznie ważona oparta na SNMP/WMI 8.2.8. Definiowana na podstawie grupy priorytetów dla serwerów 8.3. Buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera. 8.4. Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL/TLS, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, SIP, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług. 8.5. Obsługiwane mechanizmy przywiązywania sesji: cookie, adres źródłowy, adres docelowy, SSL/TLS ID, RDP login name, JSESSIONID, SIP call ID. 8.6. Wsparcie dla usług warstw 4-7 modelu OSI: inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera,

		zaszyfrowane cookies, przepisywanie odpowiedzi, multipleksacja zapytań HTTP, kompresja i cache'owanie HTTP. 8.7. System LB musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.
9.	Funkcje LB - optymalizacja i akceleracja aplikacji	9.1. System LB musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci: 9.1.1. LAN 9.1.2. WAN 9.1.3. Urządzenia mobilne 9.1.4. System LB powinien mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control).[2] 9.1.5. System LB musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP. 9.1.6. System LB powinien umożliwiać kompresję zwracanej zawartości http. 9.1.7. Użycie kompresji zwracanej zawartości http w systemie LB powinno być zależne od: 9.1.7.1. Listy dozwolonych URI 9.1.7.2. Listy wykluczonych URI 9.1.7.3. Listy kompresowalnych Content-Type 9.1.7.4. Listy wykluczonych Content-Type[3] 9.2. System LB musi posiadać funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu co najmniej następujących atrybutów: 9.2.1. Cookie 9.2.2. Adres źródła 9.2.3. SIP call ID 9.2.4. Identyfikator sesji SSL/TLS 9.2.5. Microsoft Terminal Services (RDP) – nazwa użytkownika 9.2.6. Adres docelowy 9.2.7. Tworzone przez administratora Systemu LB przy wykorzystaniu języka skryptowego z punktu 10.

[2] Stanowi kryterium oceny ofert.
[3] Stanowi kryterium oceny ofert.

10.	Możliwości programowania w Systemie LB	10.1. Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy: 10.1.1. Analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów. 10.1.2. Obsługa protokołów: http, tcp, xml, rtsp, sip. 10.1.3. Musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS. 10.1.4. Język skryptowy musi bazować na języku programowania TCL (ang. Tool Command Language). 10.1.5. Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego. 10.1.6. System LB musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji.
11.	Tryb pracy WAF	11.1. System LB musi wspierać następujące tryby pracy: 11.1.1. Tryb wykrywania, logowania i blokowania ataków 11.1.2. Tryb wykrywania i logowania ataków bez blokowania 11.1.3. Tryb uczenia się bez blokowania 11.1.4. Tryb uczenia się z blokowaniem i logowaniem
12.	Funkcje WAF	12.1. WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. 12.2. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej: 12.2.1. wystąpienie URL, długość URL, zabezpieczenie przed tzw.clickjackiem dla danego URL. 12.2.2. typ serwlet-u występujący pod danym url-em – format komunikacji (http form, JSON, XML) 12.2.3. dopuszczalne metody http 12.2.4. dopuszczalne cookie 12.2.5. dopuszczalne parametry w polityce 12.2.6. parametry dynamiczne 12.2.7. typ/format parametrów (np. alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML) 12.2.8. dopuszczalne parametry w danym serwlet 12.2.9. długość zapytań

		12.2.10. wystąpień i długość parametrów (per każdy parametr) 12.2.11. wystąpień i długości nagłówków 12.2.12. wystąpień i długości cookies 12.2.13. oczekiwanych typów znaków per każdy parametr 12.2.14. typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku 12.2.15. URL podatnych na CSRF[4] 12.3. Profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego. 12.4. Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń). 12.5. Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego. 12.5.1. W szczególności na podstawie publicznego ruchu produkcyjnego. 12.6. Powinna być możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa WAF będzie akceptować wszystkie zachowania jako prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa.[5] 12.7. Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr. 12.8. Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa. 12.9. Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http. 12.10. WAF musi posiadać mechanizmy ochrony przed atakami: 12.10.1. SQL Injection 12.10.2. Cross-Site Scripting 12.10.3. Cross-Site Request Forgery 12.10.4. Session hijacking 12.10.5. Command Injection 12.10.6. Cookie/Session Poisoning 12.10.7. Parameter/Form Tampering

[4] Stanowi kryterium oceny ofert
[5] Stanowi kryterium oceny ofert

		12.10.8. Forceful Browsing 12.10.9. Brute Force Login 12.10.10. Web Scraping 12.10.11. Cookie manipulation/poisoning 12.10.12. Dynamic Parameter tampering 12.10.13. Buffer Overflow 12.10.14. Stealth Commanding 12.10.15. Unused HTTP Methods 12.10.16. Malicious File Uploads 12.10.17. Hidden Field Manipulation 12.11. Mechanizm zabezpieczenia przed Cross-Site Request Forgery powinien dodawać losowy token do odpowiedzi http zawierających odwołania do chronionego zasobu (servleta).[6] 12.12. WAF musi posiadać mechanizmy ochrony przed atakami DDoS lub DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http). 12.13. WAF musi blokować ataki typu Slow Loris. 12.14. WAF powinien rozróżniać rzeczywistych użytkowników od automatów podczas ataku DDoS lub DoS poprzez: 12.14.1. Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania 12.14.2. Mechanizmu browser fingerprinting, w celu wykrycia tzw. headless browser 12.14.3. Sygnatury botów 12.14.4. Wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik).[7] 12.14.5. WAF powinien posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania dużej ilości incydentów wykonywanych w zdefiniowanym czasie przez tego użytkownika.[8] 12.15. WAF powinien: 12.15.1. umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania.

[6] Stanowi kryterium oceny ofert.
[7] Stanowi kryterium oceny ofert.
[8] Stanowi kryterium oceny ofert.

		12.15.2. umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack'iem.[9] 12.16. WAF powinien umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności WAF.[10] 12.17. W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP. 12.18. WAF musi posiadać wsparcie dla aplikacji działających w technologiach AJAX oraz JSON. 12.19. WAF powinien wyświetlać strony blokowania (błędu) w technologiach AJAX i JSON.[11] 12.20. WAF musi posiadać wsparcie dla Google Web Toolkit. 12.21. WAF musi posiadać możliwość ochrony komunikacji XML poprzez: 12.21.1. walidację Schema/WSDL 12.21.2. wybór dozwolonych metod SOAP 12.21.3. Definiowanie możliwości użycia załączników wiadomości SOAP 12.21.4. Walidację SOAPAction Header 12.21.5. Włączanie/wyłączanie możliwości użycia DTD 12.21.6. Włączanie/wyłączanie możliwości użycia zewnętrznych referencji 12.21.7. Włączanie/wyłączanie możliwości użycia CDATA 12.21.8. Ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace 12.21.9. Definicję dopuszczalnych znaków 12.21.10. Definicję sygnatur 12.22. WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. 12.23. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach wsparcia, zapewnionego razem z Systemem LB, opisanego w OPZ.[12] 12.24. WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać, conajmniej: 12.24.1. Directory traversal 12.24.2. Kodowanie typu % 12.24.3. Kodowanie typu IIS backslash 12.24.4. IIS Unicode codepoints 12.24.5. Bare byte decoding

[9] Stanowi kryterium oceny ofert.
[10] Stanowi kryterium oceny ofert.
[11] Stanowi kryterium oceny ofert.
[12] Stanowi kryterium oceny ofert.

		12.24.6. Apache whitespace 12.24.7. Bad unescape 12.24.8. Wstrzykiwanie komentarzy (np. <!-- -->) 12.25. WAF musi umożliwiać integracje z systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach. 12.26. WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolne inne ciągi znaków zdefiniowany poprzez PCRE wyrażenia regularne. 12.27. System LB powinien umożliwiać proaktywne wykrywanie i blokowanie botów (j.w.), zanim wywołają atak DDoS lub DOS, web scraping lub brute force.[13] 12.28. System LB musi mieć możliwość nauczenia się prawidłowego ruchu do aplikacji i na podstawie behawioralnej heurystyki chronić aplikację przed atakiem DDoS lub DoS w warstwie 7, automatycznie budując regułą, która zablokuje atak oraz atakujące adresy IP. Funkcja ta musi działać przynajmniej dla dwóch skonfigurowanych aplikacji. 12.29. System LB powinien kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów.[14] 12.30. Moduł ochrony przed DDoS lub DoS L7 powinien wykrywać ataki per: 12.30.1. Source IP 12.30.2. Obszar geolokacyjny 12.30.3. URL 12.30.4. Globalnie - website 12.31. Powinna istnieć możliwość przypisania różnych poziomów detekcji ataków DDoS lub DoS dla danych URL-i portalu np. /infoportal/ powinien posiadać luźniejszą politykę detekcji i zapobiegania ataków DDoS lub DoS niż /portal/.[15] 12.32. System LB powinien umożliwiać automatyczny zapis przykładowego ruchu do plików zgodnych z formatem tcpdump, w momencie wykrycia ataku DDoS lub DoS:

[13] Stanowi kryterium oceny ofert.
[14] Stanowi kryterium oceny ofert.
[15] Stanowi kryterium oceny ofert.

		12.32.1. System LB powinien umożliwiać definicję maksymalnego czasu próbki ruchu, 12.32.2. Maksymalnej pojemności próbki ruchu, 12.32.3. Interwału czasowego pomiędzy pobieraniem próbki ruchu.[16] 12.33. System LB musi zapewniać możliwość wyboru polityki bezpieczeństwa na podstawie: 12.33.1. Host 12.33.2. URN 12.33.3. Nagłówków 12.33.4. Cookie 12.34. Dla każdej chronionej aplikacji internetowej System LB powinien umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do: 12.34.1. Bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2 12.34.2. System Operacyjny: Windows, Linux, UNIX 12.34.3. Język aplikacji, frameworki: ASP, ASP .NET, PHP, Java, BEA WebLogic, CGI, Elasticsearch, Front Page Server Extension, Java Servlets/JSP, Outlook Web Access, WebDAV, JQuery, WebDAV. Serwer WWW: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy.[17]
13.	Terminacja SSL/TLS	13.1. System LB musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów. 13.2. Wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy. 13.3. Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów. 13.4. Wsparcie dla protokołu TLS 1.3. 13.5. System LB musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów.

[16] Stanowi kryterium oceny ofert.
[17] Stanowi kryterium oceny ofert.

		13.6. System LB musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL/TLS.
14.	Zarządzanie	14.1. System LB musi posiadać co najmniej następujące interfejsy administracyjne: 14.1.1. GUI przy wykorzystaniu protokołu https 14.1.2. Zarządzanie poprzez SSH 14.1.3. Zarządzanie poprzez API REST 14.2. Autoryzacja administratorów Systemu LB musi bazować na rolach użytkowników. 14.3. Musi umożliwić (równolegle) pracę min. 10 użytkownikom administracyjnym Systemu LB. 14.4. System LB musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS. 14.5. System LB musi posiadać następujące funkcje zarządzania siecią: 14.5.1. Obsługa protokołu SNMP v1/v2c/v3 14.5.2. Zewnętrzny syslog 14.5.3. Zbieranie danych i ich wyświetlanie 14.5.4. Zbieranie danych zgodnie z ustawieniami administratora 14.5.5. Osobna brama domyślna dla interfejsu zarządzającego 14.5.6. Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy) 14.6. System LB musi posiadać moduł analizy ruchu http. 14.7. Moduł analizy ruchu http powinien zbierać następujące metryki: 14.7.1. Czas odpowiedzi per serwer 14.7.2. Czas odpowiedzi per URI 14.7.3. Ilość sesji użytkownika 14.7.4. Przepustowość 14.7.5. Adres źródła 14.7.6. User Agent (wykorzystywana przez klienta aplikacja) 14.7.7. Metoda dostępu[18]
15.	Integracja z zewnętrznymi systemami	15.1. System LB musi zapewniać możliwość klonowania puli serwerów umożliwiającą wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS.

[18] Stanowi kryterium oceny ofert.

		15.2. Musi umożliwić wysyłanie inf. dot. Przepływów (ang. Flow - np. Netflow) do zewnętrznych systemów zajmujących się analizą przepływów (ang. Flow). 15.3. Musi umożliwić dodawanie w nagłówku HTTP informacji dot. XFF (X-Forwarded-For). 15.4. Musi umożliwić wysyłanie logów do systemu klasy SIEM (zarejestrowanych zdarzeń bezpieczeństwa w module WAF oraz systemowych I audytowych z Systemu LB). 15.5. System LB musi umożliwić dodawanie informacji dot. źródłowych adresów IP pochodzacych z XFF w nagłówku HTTP do logów wysyłanych do SIEM.
16.	Klastering i wysoka dostępność	16.1. Licencje na System LB muszą obejmować możliwość budowy klastra wysokiej dostępności (HA) złożonego z dwóch Wirtualnych Appliance tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1. 16.2. Klaster wysokiej dostępności powinien zapewniać synchronizację: 16.2.1. Stanu połączeń 16.2.2. Przywiązywania sesji (Session persistence).[19] 16.3. Wykrycie awarii Systemu LB (pracujących w klastrze) odbywać się musi przy użyciu, weryfikacji stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover).

[19] Stanowi kryterium oceny ofert.

III.2 Zasady realizowania Godzin eksperckich w ramach prawa opcji

(1) Zamawiający wymaga zapewnienia przez Wykonawcę Godzin eksperckich świadczonych przez autoryzowany podmiot współpracujący z producentem przedmiotu zamówienia opisanego w pkt III.1 powyżej (dalej określanego jako „**Producent**"), w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta w wymiarze łącznie 480 godzin, przez okres od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt III.1powyżej do końca grudnia 2022r.

(2) Osoba/y realizująca Godziny eksperckie musi być ekspertem w obszarze związanym z technologią dot. **Systemu LB** oraz legitymować się ważnym i aktualnym certyfikatem Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta.

(3) W ramach Godzin eksperckich będzie m.in. na żądanie Zamawiającego:

(a) opracowanie i dostarczenie projektu wdrożenia Systemu LB oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Godzin eksperckich,

(b) opracowanie i dostarczenie procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,

(c) wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt III.1powyżej,

(d) konsultacje dot. utrzymania, eksploatowania oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez urządzenia stanowiące przedmiot zamówienia, o którym mowa w pkt III.1powyżej,

(4) Zamawiający wymaga zapewnienia realizacji Godzin eksperckich, na podstawie zleceń przekazywanych przez personel Zamawiającego, wskazany w zawartej wykonawca Umowie, wskazujących przedmiot zamawianych usług, a Wykonawca będzie zobowiązany zapewnić rozpoczęcie świadczenia takich usług nie później niż w terminie 3 dni roboczych od dnia przekazania Wykonawcy zlecenia.

III.3 Zasady świadczenia usług wsparcia technicznego

(1) Wykonawca zobowiązany jest zapewnić wsparcie Producenta Systemu LB (dalej określanego jako „**Producent**”) lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta, dla dostarczonych subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pktIII.1.

(2) Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów.

(3) Dostęp do uaktualnień sygnatur/reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez producenta wraz z niezbędnymi danymi logowania, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych w trybie 24/7/365.

(4) Zgłoszone serwisowe będą usuwane w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.