PROJEKT – OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia

Rozbudowa systemu loadbalancer wraz z usługami gwarancji i wsparcia technicznego na okres 36 miesięcy.

II. Kody CPV

32420000-3 Urządzenia sieciowe
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa
72611000-6 Usługi w zakresie wsparcia technicznego

III. Przedmiot zamówienia

Przedmiot zamówienia obejmuje:

rozbudowę posiadanego przez Zamawiającego systemu loadbalancer poprzez dostawę, montaż i uruchomienie urządzeń wraz z oprogramowaniem oraz świadczenie usług gwarancji i wsparcia technicznego dla dostarczonych urządzeń, zgodnie z opisem wskazanym w pkt VI OPZ albo równoważnych, zgodnie z opisem równoważności określonym w pkt VII, VIII i IX OPZ, wraz z przekazaniem dokumentacji.

IV. Termin realizacji

(1) Przedmiot zamówienia polegający na dostawie, montażu i uruchomieniu urządzeń wraz z oprogramowaniem zgodnie z opisem wskazanym w pkt VI OPZ albo równoważnych, zgodnie z opisem równoważności określonym w pkt VII i VIII OPZ;

(2) Gwarancja i wsparcie techniczne dla dostarczonych urządzeń, zgodnie z opisem wskazanym w pkt VI OPZ albo równoważnych, zgodnie z opisem równoważności określonym w pkt VII i IX OPZ, będą świadczone przez okres 36 miesięcy od dnia odbioru wskazanego w protokole odbioru końcowego.

V. Wymagania ogólne

(1) Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży na rzecz Skarbu Państwa – Ministra Cyfryzacji. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego użytkownika i licencjobiorcę Urządzeń i Oprogramowania jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji, z adresem korespondencyjnym przy ul. Królewskiej 27, 00-060 Warszawa, NIP

525-295-50-37, REGON 525189465. Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z przedmiotu zamówienia, w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją systemów na rzecz Ministra Cyfryzacji.

(2) Urządzenia muszą być fabrycznie nowe, nieużywane wcześniej, objęte gwarancją i wsparciem technicznym, zgodnie z opisem wskazanym w pkt VI OPZ oraz zasadami wskazanymi w pkt IX OPZ oraz posiadać najnowszą dostępną stabilną wersję oprogramowania.

(3) Wszelkie opakowania, wypełniacze oraz inne odpady wniesione w ramach dostawy urządzeń zostaną zutylizowane przez Wykonawcę, chyba że Zamawiający zadecyduje inaczej.

(4) Urządzenia muszą być kompletne, tj.: mieć wszystkie komponenty zapewniające właściwą instalację i użytkowanie.

(5) Przedmiot zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 z późn. zm.), dalej: „Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, Urządzenia i Oprogramowanie muszą być zgodne z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.

(6) Wykonawca oświadcza, że jest świadomy, iż z uwagi na wymogi bezpieczeństwa obowiązujące w Lokalizacji, osoby wyznaczone przez Wykonawcę do realizacji Umowy mogą być zobowiązane do okazania służbom ochrony obiektów, przed rozpoczęciem realizacji przedmiotu Umowy w danej Lokalizacji, poświadczenia bezpieczeństwa dostępu do informacji niejawnych na poziomie min. „POUFNE” oraz posiadać obywatelstwo polskie.

VI. Szczegółowy opis przedmiotu zamówienia

Zamawiający wymaga dostarczenia, montażu i uruchomienia urządzeń wraz z oprogramowaniem do rozbudowy posiadanego przez Zamawiającego systemu loadbalancer F5 VELOS CX410 wraz z gwarancją i wsparciem technicznym, zgodnych z poniższym opisem:

#	Numer SKU	Ilość	Opis produktu
1	F5-VEL-BTA-BX110	4	VELOS BX110 Blade for CX410 Best Bundle Chassis
2	F5-SVC-VEL-PRE-L1-3	12	Level 1-3 Premium Service for VELOS (24x7)
3	F5-SVC-VEL-RMA-2	12	Next-Business-Day Hardware Replacement Service (RMA) for VELOS
4	F5-SVC-RMA-OPT	12	RMA Removable Hard Drive and Compact Flash Card Fee (per unit)
5	F5-UPG-VEL-QSFP+SR4	8	VELOS QSFP+ 40GBASE-SR4 Transceiver (100 m, Field Upgrade)

albo równoważnych, zgodnie z opisem równoważności określonym w pkt VII, VIII i IX OPZ, wraz z przekazaniem dokumentacji.

VII. Kryteria stosowane w celu oceny równoważności

(1) Zamawiający przez „rozwiązanie równoważne" rozumie urządzenia wraz z oprogramowaniem zapewniające, bez dodatkowych nakładów finansowych po stronie Zamawiającego, minimalne funkcjonalności wskazane w pkt VIII OPZ poniżej.

(2) Zamawiający w zakresie każdego elementu przedmiotu zamówienia wymienionego w pkt VI powyżej, wskazał poniżej kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania rozwiązania równoważnego, na Wykonawcy spoczywa obowiązek wykazania jego równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne wszystkich kryteriów równoważności.

(3) W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych przypadkach) nie będzie poprawnie współpracować z posiadanym przez Zamawiającego systemem loadbalancer lub spowoduje zakłócenia w funkcjonowaniu tego systemu, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania posiadanego przez Zamawiającego systemu loadbalancer, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.

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

(5) Wszelkie niezbędne prace adaptacyjne (jeśli wystąpi potrzeba ich wykonania), zostaną zrealizowane przez Wykonawcę na jego koszt. Wykonawca dostarczy dokumentację przeprowadzonych prac adaptacyjnych.

(6) Wykonawca zapewni Zamawiającemu odpowiednie szkolenia z zakresu obsługi rozwiązania równoważnego w zakresie nie mniejszym niż 24 godziny robocze dla minimum 4 użytkowników rozwiązania równoważnego.

VIII. Wymagania funkcjonalne dla przedmiotu zamówienia

Lp.	Opis wymagania	Parametry minimalne
1.	Wymagania podstawowe	Zastosowane rozwiązanie sprzętowe i software'owe musi gwarantować poprawne wykonywanie zaimplementowanych na obecnie pracującym systemie loadbalancer (przed rozbudową) reguł i polityk. Ich ewentualna konwersja/przeniesienie nie może skutkować ich błędnym wykonaniem, koniecznością tworzenia nowych lub indywidualnego przepisywania poszczególnych na nowy system.

Lp.	Opis wymagania	Parametry minimalne
2.	Ogólne	1. Urządzenie musi obsługiwać co najmniej następujące funkcjonalności: a. zaawansowany system klasy load balancer, b. terminacja SSL, c. obsługa DNS, d. wbudowany, zaawansowany system klasy WAF. 2. Urządzenie musi zapewniać obsługę IPv4 oraz IPv6. 3. Urządzenie musi posiadać co najmniej dwa interfejsy QSFP28 40/100Gbps z możliwością breakoutu na 4x10Gbps lub 4x25Gbps. 4. Urządzenie 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 2027. 5. Klucze prywatne zapisane na dysku muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.
3.	Przepustowość	1. Minimum 10 Gbps z możliwością zwiększenia poprzez rozbudowę klastra. 2. Przepustowość z włączonym modułem WAF i inspekcjonującymi ruch politykami WAF oraz terminacją SSL/TLS musi być nie niższa niż 5 Gbps. Musi istnieć możliwość jej zwielokrotnienia do 40Gbps poprzez dodanie modułów rozszerzających, bez konieczności wymiany całego urządzenia. Nieakceptowalne jest również rozbudowywanie urządzenia (w celu zwiększenia przepustowości) o kolejne urządzenia/rozwiązania wymagające dodatkowego miejsca w szafie rack oraz zasilania. Parametry powinny być spełnione przy min. charakterystyce ruchu: dla ruchu TLS – AES128-SHA, z kluczem min. 2048b, dla ruchu L7 – min. 50 żądań L7 na jedno połączenie TCP z odpowiedzią min. 5kB (wszystkie warunki muszą być spełnione równocześnie).
4.	Tryb proxy	1. Urządzenie LB musi umożliwić pracę w trybie forward proxy. 2. Urządzenie LB musi umożliwiać pracę w trybie reverse proxy. 3. Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.
5.	Funkcje load balancera	1. Urządzenie LB musi świadczyć, co najmniej następujące usługi w warstwach 4-7: a. SSL Offload

Lp.	Opis wymagania	Parametry minimalne
		b. Inspekcja warstwy aplikacji, w tym inspekcja nagłówka HTTP; c. Modyfikacja, usuwanie, dodawanie elementów nagłówka HTTP; d. Ukrywanie zasobów; e. Zmiana odpowiedzi serwera; f. Przepisywanie odpowiedzi (response rewriting); g. Multipleksowanie połączeń HTTP. 2. Urządzenie LB musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. 3. Urządzenie musi zapewniać selektywny HTTP caching. 4. Urządzenie musi zapewniać selektywną kompresja danych. 5. Urządzenie LB musi zapewniać funkcjonalność stanowej zapory sieciowej umożliwiającej kontrolę ruchu sieciowego w warstwie 3 i 4 ISO/OSI, przy spełnieniu następujących wymagań: a. Zarządzanie regułami bezpieczeństwa musi być realizowane za pomocą wbudowanego w Urządzenie LB interfejsu graficznego; b. Reguły definiujące ruch muszą zawierać oprócz adresu, adresów IP również możliwość wskazanie lokalizacji (w ruchu źródłowym oraz ruchu docelowym) tzw. Geolokalizacja; c. Urządzenie LB musi chronić przed atakami typu flood, sweep, teardrop oraz smurf; d. Urządzenie LB powinno umożliwiać uruchomienie proxy SSH, które umożliwia np. blokowanie ściągania lub wgrywania plików po SCP lub SFTP, ustawienie czy użytkownik ma dostęp do shella; e. Urządzenie LB musi wykrywać nieprawidłowe protokoły przechodzące przez otwarte porty (np. otwarty port 80 dla ruchu http, gdy na tym porcie odbywa się ruch ssh); f. Urządzenie LB musi posiadać wsparcie obsługi protokołów routingu statycznych i dynamicznych: BGP/BGP-4, OSPF, RIP/RIPv2. 6. Urządzenie musi wspierać mechanizm pojedynczego logowania SSO (ang. Single Sign-On) oraz mieć możliwość uruchomienie usługi dostawcy tożsamości (Identity Provider).

Lp.	Opis wymagania	Parametry minimalne
6.	Metody równoważenia obciążenia	1. Urządzenie musi zapewnić rozkład ruchu pomiędzy serwerami aplikacji Web. 2. Urządzenie musi zapewniać metody równoważenia obciążenia: a. Cykliczna; b. Ważona; c. Najmniejsza liczba połączeń; d. Najszybsza odpowiedź serwera e. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera; f. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie; g. Dynamicznie ważona oparta na SNMP/WMI; h. Definiowana na podstawie grupy priorytetów dla serwerów. 3. Urządzenie zapewnia buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera. 4. Obsługiwane są mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP halfopen, 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. 5. Obsługiwane są mechanizmy przywiązywania sesji: cookie, adres źródłowy, adres docelowy, SSL/TLS ID, RDP login name, JSESSIONID, SIP call ID. 6. Mechanizmy wsparcia przywiązania sesji muszą zawierać możliwość ukrycia typu urządzenia oraz topologii wewnętrznej. 7. 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. Urządzenie 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.
7.	Optymalizacja i akceleracja aplikacji	1. Urządzenie LB musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci: a. LAN;

Lp.	Opis wymagania	Parametry minimalne
		b. WAN; c. Urządzenia mobilne; d. Urządzenie LB powinno mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control); e. Urządzenie LB musi wspierać multipleksacje wielu zapytań HTTP w tej samej sesji TCP; f. Urządzenie LB powinno umożliwiać kompresję zwracanej zawartości HTTP; g. Użycie kompresji zwracanej zawartości HTTP w Urządzeniu LB powinno być zależne od: i. Listy dozwolonych URI; ii. Listy wykluczonych URI; iii. Listy kompresowalnych Content-Type; iv. Listy wykluczonych Content-Type. 2. Urządzenie LB musi posiadać funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu co najmniej następujących atrybutów: a. Cookie; b. Adres źródła; c. SIP call ID; d. Identyfikator sesji SSL/TLS; e. Microsoft Terminal Services (RDP) – nazwa użytkownika; f. Adres docelowy; g. Tworzone przez administratora Urządzenia LB przy wykorzystaniu języka skryptowego z punktu 9.
8.	Obsługa DNS	1. Urządzenie musi zapewniać globalne, inteligentne sterowanie ruchem wykorzystując usługę DNS jako mechanizm rozdziału ruchu (Global Solution Load Balancing), w ramach którego zapewni: a. Monitorowanie stanu pracy usług korzystając z monitorów działających w warstwie sieci, transportowej oraz aplikacji modelu ISO/OSI; b. Rozdzielanie ruchu korzystając co najmniej z metod: i. Cykliczna; ii. Ważona; iii. Na podstawie adresów IP klienta usługi (topologii); iv. Obciążenia serwera; v. Najmniejszej liczby połączeń; c. Mechanizmy utrzymywania sesji polegające na kierowaniu zapytań z lokalnego serwera DNS

Lp.	Opis wymagania	Parametry minimalne
		klienta aplikacji zawsze do tego samego centrum danych i serwera aplikacji; d. Wbudowany w system operacyjny język skryptowy, umożliwiający analizę i zmianę parametrów w protokole DNS; e. Ochronę serwerów DNS z wykorzystanie DNSSEC, a także na zastosowanie list kontroli dostępu umożliwiających filtrowanie ruchu DNS bazując na typie rekordu; f. 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; g. Konwersja rekordów między IPv4 i IPv6; h. Wsparcie dla usług geolokacji, możliwość przekierowania ruchu do najbliższej geograficznie lokalizacji; i. Wybór lokalizacji na podstawie ilości urządzeń pośredniczących oraz ilości przetwarzanych danych; j. Możliwość wysyłania zapytań dotyczących obciążenia do urządzeń firm trzecich. 2. Możliwość bezpośredniego odpytywania serwerów o obciążenie. 3. Możliwość przekierowania ruchu do innej lokalizacji po przekroczeniu zdefiniowanego progu ilości sesji.
9.	Możliwości programowania LB	Urządzenie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy: • Analiza, zmiana oraz zastępowanie parametrów w nagłówku HTTP oraz w zawartości pakietów. • Obsługa protokołów: HTTP, TCP, XML, RSTP, SIP. • Musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS. • Język skryptowy musi bazować na języku programowania TCL (ang. Tool Command Language). • Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego. • Urządzenie LB musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji. • Urządzenie posiada możliwość delegowania złożonych zadań do silnika NodeJS i użycia bibliotek “społecznościowych” (np. celem parsowania

Lp.	Opis wymagania	Parametry minimalne
		protokołów, które jeszcze nie zostały zaimplementowane w urządzeniu)
10.	Tryb pracy WAF	Urządzenie LB musi wspierać następujące tryby pracy: • Tryb wykrywania, logowania i blokowania ataków; • Tryb wykrywania i logowania ataków bez blokowania; • Tryb uczenia się bez blokowania; • Tryb uczenia się z blokowaniem i logowaniem.
11.	Funkcje WAF	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. 2. Pozytywny model bezpieczeństwa musi kontrolować co najmniej: a. wystąpienie URL, długość URL, zabezpieczenie przed tzw. clickjackiem dla danego URL; b. typ serwletu występujący pod danym URL-em – format komunikacji (http form, JSON, XML); c. dopuszczalne metody HTTP; d. dopuszczalne cookie; e. dopuszczalne parametry w polityce; f. parametry dynamiczne; g. typ/format parametrów (np. alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML); h. dopuszczalne parametry w danym serwlet i. długość zapytań; j. wystąpień i długość parametrów (per każdy parametr); k. wystąpień i długości nagłówków; l. wystąpień i długości cookies; m. oczekiwanych typów znaków per każdy parametr; n. typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku; o. URL podatnych na CSRF. 3. Profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego. 4. Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń). 5. Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na

Lp.	Opis wymagania	Parametry minimalne
		podstawie analizy ruchu sieciowego (w szczególności na podstawie publicznego ruchu produkcyjnego). 6. 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. 7. Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr. 8. Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa. 9. Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http. 10. WAF musi posiadać mechanizmy ochrony przed atakami: a. SQL Injection; b. Cross-Site Scripting; c. Cross-Site Request Forgery; d. Session hijacking; e. Command Injection; f. Cookie/Session Poisoning; g. Parameter/Form Tampering; h. Forceful Browsing; i. Brute Force Login; j. Web Scraping; k. Cookie manipulation/poisoning; l. Dynamic Parameter tampering; m. Buffer Overflow; n. Stealth Commanding; o. Unused HTTP Methods; p. Malicious File Uploads; q. Hidden Field Manipulation. 11. Mechanizm zabezpieczenia przed Cross-Site Request Forgery powinien dodawać losowy token do odpowiedzi http zawierających odwołania do chronionego zasobu (servleta). 12. WAF musi posiadać mechanizmy ochrony przed atakami DDoS lub DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http). 13. Rozwiązanie nie posiada żadnego limitu licencyjnego dla funkcji podanej w punkcie 11.12. 14. WAF musi blokować ataki typu Slow Loris. 15. WAF powinien rozróżniać rzeczywistych użytkowników od automatów podczas ataku DDoS lub DoS poprzez: a. Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania;

Lp.	Opis wymagania	Parametry minimalne
		b. Mechanizmu browser fingerprinting, w celu wykrycia tzw. headless browser; c. Sygnatury botów; d. Wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik); e. 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. 16. WAF powinien: a. umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania. b. umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack'iem. 17. WAF powinien umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności WAF. 18. W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP. 19. WAF musi posiadać wsparcie dla aplikacji działających w technologiach AJAX oraz JSON. 20. WAF powinien wyświetlać strony blokowania (błędu) w technologiach AJAX i JSON. 21. WAF musi posiadać wsparcie dla Google Web Toolkit. 22. WAF musi posiadać możliwość ochrony komunikacji XML poprzez: a. walidację Schema/WSDL; b. wybór dozwolonych metod SOAP; c. Definiowanie możliwości użycia załączników wiadomości SOAP; d. Walidację SOAPAction Header; e. Włączanie/wyłączanie możliwości użycia DTD; f. Włączanie/wyłączanie możliwości użycia zewnętrznych referencji; g. Włączanie/wyłączanie możliwości użycia CDATA; h. Ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace; i. Definicję dopuszczalnych znaków; j. Definicję sygnatur. 23. WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego.

Lp.	Opis wymagania	Parametry minimalne
		24. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach wsparcia, zapewnionego razem z Systemem LB. 25. WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać, co najmniej: a. Directory traversal; b. Kodowanie typu %; c. Kodowanie typu IIS backslash; d. IIS Unicode codepoints; e. Bare byte decoding; f. Apache whitespace; g. Bad unescape; h. Wstrzykiwanie komentarzy (np. <!-- -->). 26. WAF musi umożliwiać integracje z systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach. 27. WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolne inne ciągi znaków zdefiniowane poprzez PCRE wyrażenia regularne. 28. Urządzenie LB powinno umożliwiać proaktywne wykrywanie i blokowanie botów (j.w.), zanim wywołają atak DDoS lub DOS, web scraping lub brute force. 29. Urządzenie 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 regułę, która zablokuje atak oraz atakujące adresy IP. Funkcja ta musi działać przynajmniej dla dwóch skonfigurowanych aplikacji. 30. Urządzenie LB powinno kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów. 31. Moduł ochrony przed DDoS lub DoS L7 powinien wykrywać ataki per: a. Source IP; b. Obszar geolokacyjny; c. URL; d. Globalnie – website. 32. 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/.

Lp.	Opis wymagania	Parametry minimalne
		33. Urządzenie LB powinno umożliwiać automatyczny zapis przykładowego ruchu do plików zgodnych z formatem tcpdump, w momencie wykrycia ataku DDoS lub DoS: a. Urządzenie LB powinno umożliwiać definicję maksymalnego czasu próbki ruchu; b. Maksymalnej pojemności próbki ruchu; c. Interwału czasowego pomiędzy pobieraniem próbki ruchu. 34. Urządzenie LB musi zapewniać możliwość wyboru polityki bezpieczeństwa na podstawie: a. Host; b. URN; c. Nagłówków; d. Cookie. 35. Dla każdej chronionej aplikacji internetowej Urządzenie LB powinno umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do: a. Bazy danych: Oracle, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2; b. System Operacyjny: Windows, Linux, UNIX; c. 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.
12.	Terminacja SSL/TLS	1. Urządzenie LB musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów. 2. Wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2. Wsparcie dla Perfect Forward Secrecy. 3. Dla protokołu TLS 1.2 wymagana jest obsługa AESGCM zarówno od strony klienta, jak i od strony puli serwerów. 4. Wsparcie dla protokołu TLS 1.3. 5. Urządzenie LB musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów. 6. Urządzenie LB musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL/TLS.

Lp.	Opis wymagania	Parametry minimalne
13.	Zarządzanie ruchem szyfrowanym SSL/TLS	1. Przedmiot zamówienia musi mieć możliwość zarządzania przepływem szyfrowanego ruchu w całym łańcuchu zabezpieczeń. 2. Przedmiot zamówienia musi mieć możliwość uruchomienia podglądu ruchu zaszyfrowanego SSL/TLS z uwzględnieniem poniższych wymagań: a. Optymalizacij ruchu szyfrowanego poprzez wydajne przetwarzanie i dekodowanie ruchu SSL/TLS – z wykorzystaniem różnych parametrów szyfrowania; b. Kontroli ruchu przychodzącego i wychodzącego SSL w celu identyfikacji potencjalnych zagrożeń oraz wykrywanie anomalii w sieci; c. Rozdzielenia ruchu SSL na różne ścieżki, co pozwoli na dedykowane przetwarzanie ruchu dla różnych aplikacji lub usług.
14.	Klastrowanie i wysoka dostępność	1. Przedmiot zamówienia musi obejmować możliwość budowy klastra równoważącego ruch (AA) złożonego z n+1 tego samego typu pracujących w trybie active-standby z możliwością realizacji trybu active-active. 2. Klaster wysokiej dostępności powinien zapewniać synchronizację: a. Stanu połączeń; b. Przywiązywania sesji (Session persistence). 3. Wykrycie awarii Urządzenia LB (pracujących pracującego w klastrze) odbywać się musi przy użyciu, weryfikacji stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover).
15.	Integracja z systemami zewnętrznymi	1. Urządzenie LB musi zapewniać możliwość klonowania puli serwerów umożliwiającą wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS. 2. Musi umożliwić wysyłanie informacji dotyczącej Przepływów (ang. Flow - np. Netflow) do zewnętrznych systemów zajmujących się analizą przepływów (ang. Flow). 3. Musi umożliwić dodawanie w nagłówku HTTP informacji dot. XFF (X-Forwarded-For). 4. Musi umożliwić wysyłanie logów do systemu klasy SIEM (zarejestrowanych zdarzeń bezpieczeństwa w module WAF oraz systemowych i audytowych z Urządzenia LB). 5. Urządzenie LB musi umożliwić dodawanie informacji dot. źródłowych adresów IP pochodzacych z XFF w nagłówku HTTP do logów wysyłanych do SIEM.

Lp.	Opis wymagania	Parametry minimalne
16.	Zarządzanie	1. Urządzenie LB musi posiadać co najmniej następujące interfejsy administracyjne: a. GUI przy wykorzystaniu protokołu HTTPS; b. Zarządzanie poprzez SSH; c. Zarządzanie poprzez REST API. 2. Autoryzacja administratorów Urządzenia LB musi bazować na rolach użytkowników. 3. Musi umożliwić (równolegle) pracę min. 10 użytkownikom administracyjnym Systemu LB. 4. Urządzenie LB musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS. 5. Urządzenie LB musi posiadać następujące funkcje zarządzania siecią: a. Obsługa protokołu SNMP v1/v2c/v3; b. Zewnętrzny syslog; c. Zbieranie danych i ich wyświetlanie; d. Zbieranie danych zgodnie z ustawieniami administratora; e. Osobna brama domyślna dla interfejsu zarządzającego; f. Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy). 6. Urządzenie LB musi posiadać moduł analizy ruchu HTTP. 7. Moduł analizy ruchu HTTP powinien zbierać następujące metryki: a. Czas odpowiedzi per serwer; b. Czas odpowiedzi per URI; c. Ilość sesji użytkownika; d. Przepustowość; e. Adres źródła; f. User Agent (wykorzystywana przez klienta aplikacja); g. Metoda dostępu.

IX. Zasady świadczenia usług gwarancji i wsparcia technicznego

(1) Wykonawca zobowiązany jest zapewnić wsparcie techniczne i gwarancję producenta urządzeń lub autoryzowanego partnera serwisowego współpracującego z producentem na 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 urządzeń, przez okres 36 miesięcy, od dnia odbioru wskazanego w protokole odbioru końcowego.

(2) Do obowiązków Wykonawcy należy usuwanie awarii najpóźniej do końca następnego dnia roboczego, następującego po dniu, w którym została zgłoszona awaria.

(3) Za chwilę zgłoszenia awarii Strony uznają chwilę przesłania zgłoszenia do Wykonawcy.

(4) W razie nieusunięcia awarii urządzenia w terminie wskazanym w pkt 2 powyżej, Wykonawca dostarczy na czas naprawy urządzenie zastępcze o parametrach technicznych nie gorszych od parametrów technicznych urządzenia naprawianego oraz zapewniających nie gorszy poziom bezpieczeństwa do lokalizacji, w której znajduje się urządzenie. W takim przypadku czas usunięcia awarii to 15 dni roboczych od dokonania zgłoszenia awarii przez Zamawiającego;

(5) W ramach gwarancji Zamawiającemu przysługuje m.in. uprawnienie do naprawy lub wymiany uszkodzonego urządzenia z zastrzeżeniem, że uszkodzone nośniki danych stanowią własność Zamawiającego i nie podlegają zwrotowi Wykonawcy w ramach wymiany, natomiast pozostałe uszkodzone elementy Wykonawca zobowiązany jest odebrać na swój koszt.

(6) W ramach wsparcia technicznego Zamawiający ma prawo w szczególności do:

(a) dostępu do nowych wersji fabrycznie zainstalowanego oprogramowania, sterowników i firmware'u w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z tego oprogramowania;

(b) wsparcia technicznego realizowanego w miejscu instalacji urządzeń;

(c) obsługi świadczonej w języku polskim;

(d) dokonywania zgłoszeń awarii: 24 godziny na dobę, 7 dni w tygodniu;

(e) dostępności inżyniera serwisu w szczególności na wypadek zaistnienia konieczności konsultacji, rozwiania wątpliwości lub rozwiązania bieżących problemów Zamawiającego z obsługą systemu loadbalancer: w dni robocze, w godzinach 8:00 – 16:00.