2025-172441

Załącznik nr 1 do Zapytania

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest **rozbudowa aktualnie wykorzystywanych loadbalancerów F5 oraz zakup nowych.**

I. **Termin realizacji zamówienia:** do 60 dni kalendarzowych.

II. **Zamówienie obejmuje:**

1. Rozbudowę posiadanego systemu równoważenia obciążenia poprzez dostawę oraz instalację i wdrożenie urządzeń wraz z gwarancją oraz oprogramowaniem zarządzającym.
2. W ramach zamówienia podstawowego należy rozbudować środowisko o urządzenia spełniające wymagania opisane w pkt. IV i V oraz dostawę oprogramowania zarządzającego opisanego w pkt. VII.
3. W ramach zamówienia opcjonalnego należy rozbudować środowisko o licencje opisane w pkt. VI.
4. Musi istnieć możliwość zestawienia klastra wysokiej dostępności (HA) pomiędzy urządzeniami posiadanymi przez Zamawiającego oraz oferowanymi urządzeniami.
5. Dostawca zobowiązany jest do wdrożenia dostarczonych urządzeń. Sposób i zakres wdrożenia został szczegółowo opisany w pkt. VIII.
6. Świadczenie gwarancji na system równoważników obciążeń opisanej w pkt. IX.

III. **Opis systemu:**

Zamawiający posiada system równoważenia obciążenia składający się z 8 urządzeń typu F5 VELOS CX410. Każde urządzenie wyposażone jest w dwa moduły blade BX110 oraz licencje ASM, LTM. Zamawiający posiada oprogramowanie do zarządzania F5 BIG-IQ.

IV. **Urządzenia typu LoadBalancer (6 sztuk):**

L.p.	Cecha	Wymagania minimalne i jakościowe
1.	Funkcje	System musi spełniać co najmniej następujące funkcje: • Rozkład ruchu pomiędzy serwerami aplikacji Web • Selektywny http caching • Selektywna kompresja danych • Terminowanie sesji SSL • Filtrowanie pakietów • Optymalizacja i akceleracja aplikacji • Ochrona przed atakami na aplikacje internetowe i serwery WWW (Web Application Firewall) Wszystkie funkcje wymienione w specyfikacji muszą być dostępne w obrębie jednego urządzenia.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
2.	Klucze prywatne	Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.
3.	Metody równoważenia obciążenia	System musi posiadać co najmniej następujące metody równoważenia obciążenia: • Cykliczna • Ważona • Najmniejsza liczba połączeń • Najszybsza odpowiedź serwera • Najmniejsza liczba połączeń i najszybsza odpowiedź serwera • Najmniejsza liczba połączeń I najszybsza odpowiedź serwera w zdefiniowanym czasie • Dynamicznie ważona oparta na SNMP/WMI • Definiowana na podstawie grupy priorytetów dla serwerów System musi mieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego
4.	Język skryptowy	Rozwiązanie 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, sip, • Musi posiadać funkcję inspekcji protokołu LDAP oraz RADIUS Język skryptowy musi być kompatybilny z językiem programowania obecnie wykorzystywanym Tool Command Language z własnymi komendami. System musi posiadać możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego.
5.	Tryb pracy	Rozwiązanie musi pracować w trybie pełnego proxy. Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.
6.	Dodatkowe mechanizmy	• Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, echo (port 7/TCP), TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, RADIUS, POP3, IMAP, SMTP, SNMP, SOAP, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne. • System musi mieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług.
7.	Optymalizacja i akceleracja aplikacji	Urządzenie musi: • optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci: LAN, WAN, CELL (komórkowy) • mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control)

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
		• wspierać multipleksacje wielu zapytań http w tej samej sesji TCP • umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od: Listy dozwolonych URI, Listy wykluczonych URI, Listy kompresowalnych Content-Type, Listy wykluczonych Content-Type
8.	WAF – model bezpieczeństwa	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. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej: • wystąpienie URL-i długość URL-i, • typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT) • przejścia pomiędzy URL-ami (servletami) • dopuszczalne metody http, • dopuszczalne cookie, • dopuszczalne parametry w polityce, • parametry dynamiczne, • typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany) • oraz dopuszczalne parametry w danym serwlecie • długość zapytań • nazwy hosta • wystąpień i długość parametrów (per każdy parametr) • wystąpień i długości nagłówków • wystąpień i długości cookies • oczekiwanych typów znaków per każdy parametr • typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku • URL-i podatnych na CSRF
9.	WAF - profil aplikacji web	Profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego
10.	WAF - sygnatury	System musi posiadać: • pozytywny model zabezpieczeń WAF • funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń) • możliwość selektywnego włączania/wyłączania ochrony sygnaturowej per chroniona aplikacja. System musi mieć gwarancję dostępności do aktualizacji paczek sygnatur przez cały okres gwarancji.
11.	WAF – profil bezpieczeństwa	Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego. • W szczególności na podstawie publicznego ruchu produkcyjnego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
		• Algorytmu tworzenia profilu bezpieczeństwa WAF powinny odrzucać nadużycia w procesie nauki.
12.	WAF – adresy zaufane	Musi istnieć 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.
13.	WAF – sygnatury	Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr. Dla każdej chronionej aplikacji internetowej urządzenie powinno umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do: • Bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2 • System Operacyjny: Windows, Linux, UNIX • Język aplikacji, frameworki: ASP, ASP .NET, PHP, Java, BEA WebLogic, CGI, Elasticsearch, Front Page Server Extension, Java Servlets/JSP, Lotus Domino, Macromedia ColdFusion, JRun, Outlook Web Access, SSI, WebDAV, JQuery, SSI, WebDAV, jQuery • Serwer WWW: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy.
14.	WAF – parametry HTTP	Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań HTTP.
15.	WAF - Polityki bezpieczeństwa	Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa. System musi zapewniać możliwość wyboru polityki bezpieczeństwa na podstawie: • Host • URL • Nagłówków • Cookie
16.	WAF – brute force	WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force.
17.	WAF – ochrona przed atakami	WAF musi posiadać mechanizmy ochrony przed atakami: • SQL Injection, • Cross-Site Scripting, • Cross-Site Request Forgery, • Session hijacking, • Command Injection, • Cookie/Session Poisoning, • Parameter/Form Tampering,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
		• Forceful Browsing, • Bot Protection • Brute Force Login, • Web Scraping • Cookie manipulation/poisoning • Dynamic Parameter tampering • Buffer Overflow • Stealth Commanding • Unused HTTP Methods • Malicious File Uploads • Hidden Field Manipulation • Slow Loris
18.	WAF - Cookie	Mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego powinien być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji.
19.	WAF - Cross-Site Request Forgery	Mechanizm zabezpieczania musi mieć możliwość wyboru dla jakich metod ma zostać włączona ochrona, przy czym musi co najmniej dla POST, GET i HEAD.
20.	WAF – wydajność	Wstrzykiwanie przez WAF dodatkowych informacji (cookie, tokeny, JavaScript), nie powinno powodować degradacji wydajności oferowanego urządzenia.
21.	WAF - DoS	WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą liczbą zapytań http) WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez: • Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania • Mechanizm browser fingerprinting, w celu wykrycia tzw. headless browser • Sygnatur botów • Wykorzystanie CAPTCHA (tylko w przypadku, gdy powyższe mechanizmy nie rozstrzygają czy podłączony jest rzeczywisty użytkownik). System powinien umożliwiać proaktywne wykrywanie i blokowanie botów (j.w.), zanim wywołają atak DDoS, web scraping lub brute force. System powinien kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów. Moduł ochrony przed DDoS powinien wykrywać ataki per: • Source IP, • Obszar geolokacyjny, • URL,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
		• Globalnie – website Powinna istnieć możliwość przypisania różnych poziomów detekcji ataków (D)DoS dla danych URL-i portalu lub aplikacji. Np. /infoportal/* powinien posiadać luźniejszą politykę detekcji i zapobiegania ataków DDoS niż /sklep/*. System powinien wykrywać i chronić przed atakami DDoS na tzw. ciężkie serwlety, czyli serwlety wywołujące złożone operacje obliczeniowe np. skomplikowane zapytania do baz danych. Wykrycie ataku na ciężkie serwlety powinno opierać się przynajmniej o liczbę zapytań (TPS) oraz czas odpowiedzi. System powinien umożliwiać zapis przykładowego ruchu do plików zgodnych z formatem TCP dump, w momencie wykrycia ataku (D)DoS. • System powinien umożliwiać definicję maksymalnego czasu próbki ruchu, • Maksymalnej pojemności próbki ruchu, • Interwału czasowego pomiędzy pobieraniem próbki ruchu. System musi mieć możliwość nauczenia się prawidłowego ruchu do aplikacji i na podstawie behawioralnej heurystyki chronić aplikację przed atakiem DDoS w warstwie 7, automatycznie budując regułę, która zablokuje atak oraz atakujące adresy IP. W systemie nie może być żadnego licencyjnego limitu dla tej funkcji.
22.	WAF - logi	WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o aktywności pochodzącej z numeru IP lub z danego komputera.
23.	WAF - nagłówki	WAF powinien umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności WAF-a. WAF powinien umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed Clickjack-iem.
24.	WAF – kod statusu	WAF powinien umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności WAF-a
25.	WAF – AJAX i JSON	WAF musi posiadać wsparcie dla aplikacji AJAX oraz JSON. WAF powinien wyświetlać stron blokowania (błędu) w technologiach AJAX i JSON. Dopuszcza się możliwość prezentacji strony blokowania zaimportowanej z zewnętrznego źródła.
26.	WAF – Google Web Toolkit	WAF musi posiadać wsparcie dla Google Web Toolkit.
27.	WAF – XML	WAF musi posiadać możliwość ochrony komunikacji XML poprzez: • walidację Schema/WSDL, • wybór dozwolonych metod SOAP, • szyfrację /deszyfrację fragmentów wiadomości SOAP, • Wsparcie dla WS-Security (szyfracja, deszyfracja, weryfikacja i podpisywanie),

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
		• Definiowanie możliwości użycia załączników wiadomości SOAP, • Włączanie/wyłączanie podążania za odnośnikami do schematów SOAP, • Walidację SOAPAction Header, • Włączanie/wyłączanie możliwości użycia DTD • Włączanie/wyłączanie możliwości użycia zewnętrznych referencji • Włączanie/wyłączanie możliwości użycia początkowych białych znaków • Włączanie/wyłączanie możliwości użycia numerycznych nazw • Włączanie/wyłączanie możliwości użycia Processing Instructions • Włączanie/wyłączanie możliwości użycia CDATA • Ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace • Ograniczenia liczby: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów • Definicję dopuszczalnych znaków • Definicję sygnatur.
28.	WAF – reputacja IP	Funkcja sprawdzania reputacji adresów IP dostających się do chronionych aplikacji. Serwis reputacyjny powinien być dostępny jako rozszerzenie systemu w przyszłości (Zamawiający nie wymaga dostarczenie licencji w niniejszym postępowaniu), bez konieczności wprowadzania zmian w architekturze sprzętowej oraz programowej proponowanego rozwiązania.
29.	WAF – blokowanie zapytań	WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach podstawowych opłat gwarancji.
30.	WAF - normalizacja	WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać: • Directory traversal • Kodowanie typu %u • Kodowanie typu IIS backslash • IIS Unicode codepoints • Bare byte decoding • Apache whitespace • Bad unescape • Wstrzykiwanie komentarzy (np. <! -- -->) Mechanizm normalizacji powinien umożliwiać definiowanie maksymalnego zagnieżdżonego kodowania.
31.	WAF - tryby pracy	Urządzenie 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

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
32.	WAF - antywirus	WAF musi umożliwiać integracje z systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach.
33.	WAF – DLP	WAF musi wykrywać i maskować numery kart kredytowych, numery PESEL, numery Dowodu Osobistego, wyciekających z chronionej aplikacji; oraz dowolnie inny ciąg znaków zdefiniowany poprzez PCRE regular expression. Włączenie funkcji maskowania numerów kart kredytowych, Pesel, Dowodu Osobistego nie może powodować degradacji wydajności oferowanego urządzenia.
34.	WAF – IPv6	WAF musi chronić ruch przesyłany po IPv6 bez degradacji wydajności wynikającej z innych czynników niż różnice protokołów IPv4 i IPv6.
35.	Szyfrowanie i maskowanie pól	System musi umożliwiać szyfrowanie oraz maskowanie wskazanych pól (np. pole do wprowadzania danych typu hasło) w czasie rzeczywistym, wprowadzanym w przeglądarce internetowej.
36.	Interfejsy administracyjne	System musi posiadać co najmniej następujące interfejsy administracyjne: • GUI przy wykorzystaniu protokołu https (TLS 1.2 i nowsze) • Zarządzanie poprzez SSH • Zarządzanie poprzez API REST
37.	Autoryzacja	Autoryzacja administratorów systemu musi bazować na rolach użytkowników
38.	Podtrzymywanie sesji	System musi posiadać funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu co najmniej następujących atrybutów: Cookie (hash, rewrite, custom, insert, passive) • Adres źródła • SIP call ID • Identyfikator sesji SSL • Adres docelowy Tworzone przez administratora systemu przy wykorzystaniu języka skryptowego z punktu 5
39.	Połączenia	System musi posiadać funkcję definiowania maksymalnej liczby obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.
40.	Kopia ruchu	System musi zapewniać możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS.
41.	Certyfikaty i protokoły	System musi zapewniać: • obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów, • Dla protokołu TLS 1.2 obsługę AES-GCM zarówno od strony klienta, jak i od strony puli serwerów, • obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
		• sprzętowe wsparcie dla algorytmów AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH, SHA2, • wsparcie dla Perfect Forward Secrecy.
42.	TLS 1.3	Urządzenie musi wspierać protokół TLS 1.3. Dla protokołu TLS 1.3 wymagana jest obsługa CHACHA20-POLY1305 zarówno od strony klienta, jak i od strony puli serwerów.
43.	VLAN	System musi obsługiwać sieci VLAN w standardzie 802.1q
44.	LACP	System musi obsługiwać agregację linków w standardzie 802.3ad (LACP)
45.	Jumbo Frames	System musi obsługiwać Jumbo Frames
46.	VXLAN	System musi posiadać funkcjonalność bramy VXLAN
47.	Usługi warstw 4-7	System musi świadczyć, co najmniej następujące usługi w warstwach 4-7: • Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http • Ukrywanie zasobów • Zmiana odpowiedzi serwera • Przepisywanie odpowiedzi (response rewriting) • Ochrona przed atakami typu DoS/DDoS • Ochrona przed atakami typu SYN Flood • Multipleksowanie połączeń http • Kompresja I cache'owanie http
48.	Wsparcie HTTP/2	Wsparcie dla HTTP/2, w tym wsparcie dla kompresji nagłówków
49.	Konfiguracja połączeń przez serwer	System musi posiadać funkcję definiowania maksymalnej liczby obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.
50.	Zarządzanie	System musi posiadać następujące funkcje zarządzania: • Obsługa protokołu SNMP v1/v2c/v3 • Zewnętrzny syslog • Zbieranie danych i ich wyświetlanie • Zbieranie danych zgodnie z ustawieniami administratora • Osobna brama domyślna dla interfejsu zarządzającego • Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot) • Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy) • Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu system Każde urządzenie modularne musi być wyposażone w minimum dwa redundantne moduły zarządzające. Urządzenie musi być zarządzane za pomocą posiadanego przez Zamawiającego systemu F5 BIQ-IQ.
51.	Szablony konfiguracji	System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
		klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.
52.	Moduł analizy	System musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki: • Czas odpowiedzi per serwer • Czas odpowiedzi per URI • Liczba sesji użytkownika • Przepustowość • Adres źródła • Kraj • User Agent (wykorzystywana przez klienta aplikacja) • Metoda dostępu w
53.	Walidacja certyfikatów	System musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL.
54.	Domeny routingu	Rozwiązanie musi oferować wsparcie dla tzw. domen routingu (Virtual Routing and Forwarding). Rozwiązanie takie oferuje separację ruchu sieciowego do różnych aplikacji. Musi umożliwiać poprawnie działanie rozwiązania, kiedy podłączone VLANy do urządzenia mają takie same podsieci i adresy IP.
55.	Obudowa	Obudowa modularna zawierająca co najmniej 8 slotów na moduły typu blade. Musi zapewniać możliwość zwiększenia wydajności poprzez dołożenie kolejnych modułów blade bez potrzeby dodatkowej rekonfiguracji całości systemu. Przeznaczona do montażu w szafie rack 19”, wysokość nie większa niż 4U.
56.	Rozbudowa	Każde urządzenie modularne musi mieć możliwość obsadzenia co najmniej ośmioma (8) urządzeniami typu blade.
57.	Wirtualizacja	Urządzenie musi umożliwiać podział urządzenia na wirtualne części, przy czym każda taka część musi pracować logicznie jako niezależne urządzenie z niezależnym oprogramowaniem (każda cześć może posiadać inną wersję oprogramowania). Urządzenie musi umożliwić podział na minimum 20 wirtualnych instancji per jeden moduł blade.
58.	Klaster	Możliwość tworzenia klastrów wysokiej dostępności (HA) złożonych z minimum dwóch urządzeń modularnych tego samego typu. Klaster musi mieć możliwość pracy w trybie active – standby, active-active oraz klastra N+1.
59.	Klaster - synchronizacja	Klaster wysokiej dostępności musi zapewniać synchronizację: • Konfiguracji • Stanu połączeń • Przywiązywania sesji (Session persistence)
60.	Klaster - Wykrycie awarii	Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu weryfikacji stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover). Wyzwalaczami przełączenia się klastra wysokiej dostępności musi być minimum: awaria interfejsu i brak dostępności bramy domyślnej.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
61.	Klaster – kopiowanie sesji	Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu.
62.	Licencje	Licencje na system muszą być przypisane do urządzenia modularnego, nie do poszczególnych urządzeń typu blade – umożliwiając w ten sposób łatwą rozbudowę i wymianę urządzeń. Jeśli do obsługi wymienionych w niniejszym dokumencie funkcjonalności potrzebne są licencje, należy je dostarczyć. Urządzenie musi mieć możliwość pełnienia funkcji autorytatywnego DNS oraz balansowania ruchu w oparciu o DNS (Global Server Load Balancing): a. Rozwiązanie powinno wspierać rozrzucanie ruchu DNS do serwerów DNS firm trzecich na podstawie następujących algorytmów: • cykliczna • ważona • najmniejsza liczba połączeń • najszybsza odpowiedź serwera • najmniejsza liczba połączeń i najszybsza odpowiedź serwera • najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie • dynamicznie ważona oparta na SNMP/WMI • definiowana na podstawie grupy priorytetów dla serwerów b. Powinna istnieć możliwość definiowania nazw dla których jest implementowany mechanizm GSLB (Global Server Load Balancing). c. Mechanizm GSLB powinien obsługiwać następujące typy rekordów: • A • AAAA • CNAME • MX • NAPTR • SRV d. Serwery autorytatywne z funkcją GSLB powinny pracować w klastrze N+M, tak, że kompletne odcięcie jednego centrum przetwarzania danych nie spowoduje utraty synchronizowanych informacji pomiędzy pozostałymi. e. W przypadku gdy nie jest możliwe asynchroniczne otrzymanie informacji o stanie zasobów / serwerów wirtualnych, powinna istnieć możliwość zdefiniowania i użycia monitora stanu aplikacji / serwera wirtualnego. f. Rozwiązanie GSLB powinno wspierać co najmniej następujące metody monitorowania: • http, https • IMAP • LDAP • MSSQL, MySQL, PostgresSQL • NNTP • POP3

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

L.p.	Cecha	Wymagania minimalne i jakościowe
		• RADIUS i RADIUS Accounting • SIP • SNMP • SMTP • SOAP • TCP • UDP

V. <u>Urządzenia typu blade: 30 sztuk.</u>

Lp.	Cecha	Wymagania minimalne
1.	Pamięć	Nie mniej niż 128GB per moduł blade
2.	Dysk twardy	Dysk SSD o pojemności nie mniejszej niż 960GB
3.	Przepływność dla warstwy 4	Nie mniej niż 95 Gbps
4.	Przepływność dla warstwy 7	Nie mniej niż 95 Gbps
5.	Liczba transakcji SSL na sekundę dla klucza o długości 2048	Nie mniej niż 100 tysięcy
6.	Liczba transakcji SSL na sekundę dla szyfru ECDSA P-256	Nie mniej niż 70 tysięcy
7.	Przepływność ruchu szyfrowanego	Nie mniej niż 50 Gbps
8.	Liczba zapytań na sekundę w warstwie 7	Nie mniej niż 3 000 000
9.	Liczba połączeń na sekundę w warstwie 4	Nie mniej niż 1 200 000
10.	Kompresja sprzętowa	Nie mniej niż 65 Gbps
11.	Gęstość interfejsów per moduł blade	Minimum 2 porty, które mogą być obsadzone wkładkami 40 Gigabit Ethernet na QSFP+ z możliwością pracy w trybie 4x10GbE lub wkładkami 100GbE QSFP28 z możliwością pracy w trybie 4x25GbE, port USB. Należy zapewnić 2 wkładki 40 Gigabit Ethernet QSFP+ SR4 oraz 2 kable QSFP+ na 4 duplex LC o długości 3 metrów. Dopuszcza się tylko moduły w pełni wspierane przez producenta tego urządzenia.
12.	Interfejsy per urządzenie modułowe	Dedykowany interfejs zarządzania, port konsolowy, port USB.
13.	Zasilanie	Redundantne 230V AC
14.	Wymagana certyfikacja	IEC 62368-1:2014 EN 62368-1:2014+A11:2017 ETSI EN 300 386 V1.6.1 (2012) Class A EN 55032:2012/AC:2013 Class A EN 55024:2010 Class A IEC 63000:2018
15.	Dodatkowe wymagania	Możliwość instalacji w posiadanych przez Zamawiającego urządzeniach F5 VELOS CX410. Możliwość instalacji w urządzeniach typu load balancer dostarczonych w ramach postepowania.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

VI. Zamówienie – licencje DNS

Dostawa licencji dla 4 urządzeń Zamawiającego VELOS CX410 umożliwiających pełnienie funkcji autorytatywnego DNS oraz balansowania ruchu w oparciu o DNS (Global Server Load Balancing):

a. Rozwiązanie powinno wspierać rozrzucanie ruchu DNS do serwerów DNS firm trzecich na podstawie następujących algorytmów:
   - cykliczna
   - ważona
   - najmniejsza liczba połączeń
   - najszybsza odpowiedź serwera
   - najmniejsza liczba połączeń i najszybsza odpowiedź serwera
   - najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie
   - dynamicznie ważona oparta na SNMP/WMI
   - definiowana na podstawie grupy priorytetów dla serwerów

c. Powinna istnieć możliwość definiowania nazw dla których jest implementowany mechanizm GSLB (Global Server Load Balancing).

d. Mechanizm GSLB powinien obsługiwać następujące typy rekordów:
   - A
   - AAAA
   - CNAME
   - MX
   - NAPTR
   - SRV

e. Serwery autorytatywne z funkcją GSLB powinny pracować w klastrze N+M, tak, że kompletne odcięcie jednego centrum przetwarzania danych nie spowoduje utraty synchronizowanych informacji pomiędzy pozostałymi.

f. W przypadku gdy nie jest możliwe asynchroniczne otrzymanie informacji o stanie zasobów / serwerów wirtualnych, powinna istnieć możliwość zdefiniowania i użycia monitora stanu aplikacji / serwera wirtualnego.

g. Rozwiązanie GSLB powinno wspierać co najmniej następujące metody monitorowania:
   - http, https
   - IMAP
   - LDAP
   - MSSQL, MySQL, PostgresSQL
   - NNTP
   - POP3
   - RADIUS i RADIUS Accounting
   - SIP
   - SNMP
   - SMTP
   - SOAP
   - TCP
   - UDP

VII. Wymagania – oprogramowanie zarządzające

Lp.	Cecha	Wymagania minimalne

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

1.	Architektura	System zarządzający musi być dostarczony w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń wirtualnych pracujących w trybie active – standby. System musi być dostarczony w postaci tzw. software appliance przynajmniej umożliwiając uruchomienie go w środowisku VMWare, Microsoft Hyper-V.
2.	Funkcjonalności	System musi zapewniać co najmniej: • zarządzanie licencjami na urządzeniach • przechowywanie archiwalnych konfiguracji • możliwość porównania konfiguracji między sobą (np. właśnie zmienioną a tą, która jest na urządzeniu) • umożliwiać przeprowadzenie zdalnie aktualizacji zarządzanych systemów • zbierać zdarzenia i tworzyć polityki dla systemu Web Application Firewall • zarządzać certyfikatami • wizualizować obecne oraz historyczne obciążenie platformy
3.	Skalowalność	Dedykowany system zarzadzania musi umożliwiać zarządzanie minimum 10 instancjami oprogramowania z możliwością rozbudowy w przyszłości o kolejne instancje.
4.	Raportowanie	Moduł raportowania musi umożliwiać zbudowanie klastra urządzeń odpowiedzialnych za przechowywanie i udostępnianie logów na urządzeniach wirtualnych. Klaster przechowywania logów musi być kompatybilny z technologią Elasticsearch.

VIII. Wdrożenie:

W ramach wdrożenia Wykonawca zobowiązany jest do:

1. instalacji fizycznej urządzeń,
2. podłączenia kabli,
3. konfiguracji urządzeń niezbędnej do uruchomienia (adresacja interfejsów, konfiguracja uwierzytelniania, konfiguracja usług NTP, DNS, SNMP, Syslog),
4. instalacji i konfiguracji systemu do zarządzania urządzeniami,
5. konfiguracja odpowiednich systemów wirtualnych,
6. konfiguracji klastrów HA,
7. przeprowadzenia testów,
8. opracowania projektu wdrożeniowy oraz dokumentację powykonawczą dla oferowanego systemu i rozbudowy urządzeń zawierające co najmniej:
   a. dla projektu wdrożeniowego:
      - harmonogram wdrożenia,
      - diagramy połączeniowe dla wszystkich komponentów sieci zamawiającego powiązanych z dostarczonymi urządzeniami,
      - konfigurację przewidzianą dla wszystkich urządzeń oraz propozycje zmian dla istniejących urządzeń połączonych z przedmiotem zamówienia,
      - koncepcję testów,
      - plan awaryjny „backout” dla każdego kroku wdrożenia,
      - koncepcję testów redundancji wykonywanych po zakończeniu wdrożenia.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem

b. dla dokumentacji powykonawczej:
   - diagramy połączeń,
   - opis wszystkich funkcjonalności wdrożonych podczas uruchamiania systemu,
   - pełne konfiguracje urządzeń,
   - wyniki testów redundancji.

IX. Gwarancja

Lp.	Cecha	Wymagania minimalne
1.	Gwarancja	Wymagane jest 3 letnie świadczenie usług gwarancyjnych na dostarczone urządzenia i oprogramowanie. Świadczenie usług gwarancyjnych powinno zawierać: • dostęp do portalu producenta systemu, • dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta, • sposób obsługi zgłoszeń gwarancyjnych w trybie 7x24, • w 4 godziny przyjęcie zgłoszenia wady, • naprawa urządzenia: 24 godziny od zgłoszenia wady, • w przypadku braku możliwości naprawy wady wymiana sprzętu: 2 dnia roboczego od zgłoszenia. Nośniki danych zostają u Zamawiającego.

Nazwy własne oraz sformułowania określone przez Zamawiającego zostały użyte ze względu na posiadane przez niego rozwiązania technologiczne.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

20 LAT POLSKI W UE
Dobrze, że jesteśmy razem