Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest: dostawa rozwiązania do ochrony webaplikacji klasy Web Application Firewall (WAF), składającego się z urządzeń, oprogramowania, wraz z licencjami i wparciem technicznym, instalacją, konfiguracją i uruchomieniem.

Celem uruchomionego rozwiązania jest ochrona aplikacji i usług, które są wystawiane do Internetu przez Sieć Badawczą Łukasiewicza przed atakami z Internetu.

Rozwiązanie będzie wykorzystywane w ramach całej Sieci Badawczej Łukasiewicz, tj. w Centrum Łukasiewicz oraz w Instytutach wchodzących w skład Sieci Badawczej Łukasiewicz, zwanej dalej SBŁ. Sieć Badawcza Łukasiewicz została stworzona i działa w oparciu o ustawę SBŁ. Sieć Badawczą Łukasiewicz tworzą Centrum Łukasiewicz i Instytuty działające w ramach Sieci, które są odrębnymi od siebie państwowymi osobami prawnymi. Aktualna lista Instytutów wchodzących w skład Sieci Badawczej Łukasiewicz znajduje się na stronie internetowej https://lukasiewicz.gov.pl/instytuty-lista/, przy czym lista ta może w czasie trwania Umowy ulec zmianie. Użytkownikami rozwiązania mogą być zarówno pracownicy Centrum Łukasiewicz, jak i Instytutów Sieci Badawczej Łukasiewicz.

Słownik:

1. „System" – oprogramowanie wraz z licencjami, w tym współpracujące ze sobą moduły: Moduł LB oraz Moduł WAF; Moduł WAF oraz Moduł LB Systemu mogą być zlokalizowane obydwa na jednym urządzeniu lub na dwóch urządzeniach, każdy z modułów na osobnym urządzeniu, w lokalizacjach wskazanych przez Zamawiającego. System musi realizować wszystkie wymagania określone dla Modułu LB oraz Modułu WAF, a także inne wymagania przypisane do Systemu.
2. „Moduł LB" – oznacza funkcjonalność Systemu dotyczącą rozkładu ruchu pomiędzy serwerami webaplikacji oraz inne funkcjonalności optymalizujące kierowanie ruchu.
3. „Moduł WAF" – oznacza funkcjonalność ochrony webaplikacji w ramach Systemu oraz inne funkcjonalności optymalizujące działanie webaplikacji.
4. „Rozwiązanie" – oznacza wszystkie urządzenia, oprogramowanie i licencje spełniające wymagania Zamawiającego, w szczególności klaster wysokiej dostępności, składający się z dwóch Systemów. Rozwiązanie musi realizować wszystkie funkcje, które realizuje System, jednocześnie realizując funkcje wysokiej dostępności.

Wymagania:

1. System musi realizować co najmniej następujące funkcje:
   a) rozkład ruchu pomiędzy serwerami aplikacji Web,
   b) selektywny http caching,
   c) selektywna kompresja danych,
   d) terminowanie sesji SSL,
   e) filtrowanie pakietów,
   f) optymalizacja i akceleracja aplikacji,
   g) ochrona przed atakami na aplikacje internetowe i serwery WWW (Web Application Firewall).
2. Zamawiający nie dopuszcza Rozwiązania realizowanego w postaci maszyny (maszyn) wirtualnej w środowisku serwerowym (VMware, Hyper-V, vCloud, KVM, Oracle VM, VirtualBox itp.) Zastrzeżenie to nie dotyczy licencji laboratoryjnych.
3. Moduł LB musi umożliwiać realizację rozdziału ruchu w oparciu o informację z warstw 4-7 modelu ISO/OSI.

4. Moduł LB musi realizować obsługę inteligentnego równoważenia ruchu dla farm serwerów przy wsparciu dla protokołów:
   a) TCP,
   b) UDP,
   c) FTP,
   d) SFTP,
   e) SMTP,
   f) HTTP,
   g) HTTPS.
5. Moduł LB musi mieć możliwość inteligentnego równoważenia ruchu w oparciu o algorytmy:
   a) round-robin,
   b) cykliczny,
   c) ważony,
   d) obciążenia serwerów,
   e) ilości połączeń,
   f) czasu odpowiedzi,
   g) hashingu (URL, Domain, source IP, Destination IP).
6. Moduł LB musi umożliwiać mechanizm dowiązania sesji (session persistant) w oparciu o:
   a) cookie,
   b) adres źródłowy,
   c) adres docelowy,
   d) identyfikator sesji SSL,
   e) identyfikator SESSIONID.
7. Moduł LB ma umożliwiać monitorowanie stanów serwerów i na tej podstawie dokonywania decyzji o przełączaniu w oparciu o:
   a) ping,
   b) TCP,
   c) URL,
   d) skrypty.
8. Moduł LB ma wspierać content switching w oparciu o następujące polityki:
   - URL,
   - URL query,
   - URL wildcard Domain,
   - source IP,
   - destination IP,
   - nagłówek http,
   - dane HTTP i TCP.
9. Moduł LB ma zapewniać mechanizmy ograniczenia ruchu dla poszczególnych serwerów w oparciu o:
   a) użycie pasma,
   b) source IP,
   c) destination IP.
10. Moduł LB ma zapewnić kontrolę:
    a) nad ilością połączeń TCP i zapytań HTTP
    b) nad priorytetyzacją ruchu dla krytycznych aplikacji.
11. System musi umożliwiać:

a) obsługę list kontroli dostępu dla 3 i 4 warstwy ISO/OSI,
b) zabezpieczenie przed atakami http DOS, przynajmniej Slow Read, Slow HTTP POST (RUDY), Slow HTTP Headers (slowloris), HTTP Flood,
c) kontrolę nad ICMP i UDP.

12. Moduł LB musi umożliwiać obsługę sieci co najmniej w zakresie:
    a) routingu statycznego,
    b) link Aggregation 802.3ad,
    c) VLAN 802.1q.
13. Rozwiązanie musi wspierać wysoką dostępność w trybie:
    a) active/passive,
    b) active/active.
14. Moduł 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 Moduł WAF profilu aplikacji Web. Pozytywny model bezpieczeństwa musi kontrolować co najmniej:
    a) wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URL-a,
    b) typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT),
    c) dopuszczalne metody http,
    d) dopuszczalne cookie,
    e) dopuszczalne parametry w polityce,
    f) parametry dynamiczne,
    g) typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany),
    h) oraz dopuszczalne parametry w danym servlecie,
    i) długość zapytań,
    j) nazwy hosta,
    k) wystąpienia i długości parametrów (per każdy parametr),
    l) wystąpienia i długości nagłówków,
    m) wystąpienia i długości cookies,
    n) oczekiwanych typów znaków per każdy parametr,
    o) typowy rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku,
    p) URL-i podatnych na CSRF.
15. Budowany przez Moduł WAF profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego.
16. Oprócz pozytywnego modelu zabezpieczeń Moduł WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń). Sygnatury będą automatycznie aktualizowane. Jeżeli aktualizacja sygnatur wymaga dostarczenia subskrypcji lub licencji, to będą one dostarczone wraz z Rozwiązaniem.
17. Tworzenie przez Moduł WAF profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się przy zachowaniu następujących wymagań:
    a) musi być realizowane na podstawie analizy ruchu sieciowego, w szczególności na podstawie publicznego ruchu produkcyjnego,
    b) algorytmy tworzenia profilu bezpieczeństwa Modułu WAF powinny odrzucać nadużycia w procesie nauki,
    c) musi być rozszerzane na podstawie raportu z analizy skanera podatności webaplikacji.
18. Musi istnieć możliwość definicji zaufanych adresów źródłowych, z których algorytm tworzenia profilu bezpieczeństwa Modułu WAF będzie akceptować wszystkie zachowania jako

prawidłowe, tak aby administrator mógł przyspieszyć proces tworzenia profilu bezpieczeństwa.

19. Moduł WAF musi mieć możliwość selektywnego włączania/wyłączania sygnatur per parametr.
20. Moduł WAF musi mieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa.
21. Moduł WAF musi mieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http.
22. Moduł WAF musi automatycznie wykrywać błędne wyniki dodatnie (false positive) i wyłączać odpowiadające nim sygnatury dla danego parametru.
23. Moduł WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force.
24. Moduł 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.
25. Moduł WAF musi posiadać mechanizm zabezpieczenia przed manipulacją cookie serwera aplikacyjnego, który powinien być oparty o wstrzykiwanie cookie z podpisem oryginalnego cookie aplikacji.
26. Moduł WAF musi chronić przed kradzieżą sesji poprzez porównywanie „odcisku palca" (fingerprint) przeglądarki z sesją użytkownika.
27. Moduł WAF musi posiadać mechanizm zabezpieczenia przed Cross-Site Request Forgery, który powinien dodawać losowy token do odpowiedzi http zawierających odwołania do chronionego zasobu (servleta).
28. Wstrzykiwanie przez Moduł WAF dodatkowych informacji (cookie, tokeny, JavaScript), nie może powodować degradacji wydajności oferowanego urządzenia.
29. Moduł WAF musi zapewniać możliwość wyboru polityki bezpieczeństwa na podstawie:
    a) host,
    b) URI,
    c) nagłówków,
    d) cookie.
30. Dla każdej chronionej aplikacji internetowej System powinien wykorzystywać sygnatury zapewniające ochronę co najmniej następujących technologii i systemów:

a) bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, Sybase, IBM DB2, CouchDB, Elasticsearch, MongoDB, SQLite, Sybase/ASE,

b) systemu operacyjnego: Windows, Linux, UNIX,

c) języka aplikacji, frameworku, biblioteki: ASP, ASP.NET, PHP, Java Servlets, JavaScript, AngularJS, Backbone.js, CodeIgniter, Django, Java Server Faces, BEA WebLogic, CGI, Elasticsearch, Front Page Server Extension, Lotus Domino, Macromedia ColdFusion, Outlook Web Access, SSI, WebDAV, jQuery, SSI, Apache Struts, ef.js, Ember.js, Express.js, GraphQL, Handlebars, JavaServer Faces, Laravel, MooTools, Moustache, Python, React, RequireJS, Ruby, Spring Boot, UIKit, Underscore.js, Vue.js, WebDAV, Zend, ZURB Fundation,

d) serwera WWW, silników: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy, Jenkins, Jetty, Joomla, Macromedia JRun, Nginx, Node.js, Oracle Application Server, Oracle Identity Manager, Redis, Typo3 CMS.

31. Moduł WAF musi posiadać mechanizmy ochrony przed atakami DoS oraz DDoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http).
32. Moduł WAF musi wykrywać oraz blokować ataki typu Slowloris.
33. Moduł WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez:
    a) wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania,
    b) mechanizmy 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).
34. Moduł WAF powinien umożliwiać proaktywne wykrywanie i blokowanie botów (jw.), zanim wywołają atak DDoS, web scraping lub brute force.
35. Moduł WAF musi zawierać moduł Sztucznej Inteligencji, który na bieżąco obserwuje ruch od użytkowników końcowych, celem budowy i utrzymania modelu prawidłowego ruchu do aplikacji. Moduł WAF na podstawie behawioralnej analizy ruchu bieżącego i zbudowanego modelu, powinien wykrywać i chronić aplikację przed atakiem DDoS w warstwie 7. W systemie nie może być żadnego licencyjnego limitu dla tej funkcji.
36. Moduł WAF powinien kategoryzować boty i umożliwiać przepuszczanie ruchu od pożytecznych botów (np. search enginy), blokując ruch od szkodliwych botów.
37. Moduł WAF w zakresie ochrony przed DDoS powinien wykrywać ataki per:
    a) source IP,
    b) URL,
    c) globalnie – website.
38. Moduł WAF musi umożliwiać dobór odpowiedzi w zależności do rodzaju naruszenia.
39. Moduł WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania określonej liczby incydentów wykonywanych w zdefiniowanym czasie przez tego użytkownika.
40. Moduł WAF powinien umożliwiać usuwanie nagłówków serwera aplikacyjnego zdradzających technologię oraz wersję oprogramowania; bez uszczerbku na wydajności Modułu WAF.
41. Moduł WAF powinien umożliwiać wstrzykiwanie nagłówków np. w celu ochrony przed clickjackingiem.
42. Moduł WAF powinien umożliwiać podmianę kodów statusów zwracanych przez serwer aplikacyjny; bez uszczerbku na wydajności Modułu WAF.
43. W obrębie licencji Modułu WAF dostarczony musi być moduł ochrony protokołu HTTP, HTTPS, oraz FTP, SFTP, API.
44. Moduł WAF musi posiadać wsparcie dla aplikacji AJAX oraz JSON.
45. Moduł WAF powinien wyświetlać strony blokowania (błędu) w technologiach AJAX i JSON.

46. Moduł WAF musi posiadać wsparcie dla Google Web Toolkit.
47. Moduł WAF musi posiadać możliwość ochrony komunikacji XML poprzez:
    a) wybór dozwolonych metod SOAP,
    b) szyfrację /deszyfrację fragmentów wiadomości SOAP,
    c) wsparcie dla WS-Security (szyfracja, deszyfracja, weryfikacja i podpisywanie),
    d) definiowanie możliwości użycia załączników wiadomości SOAP,
    e) włączanie/wyłączanie podążania za odnośnikami do schematów SOAP,
    f) walidację SOAPAction Header,
    g) włączanie/wyłączanie możliwości użycia DTD,
    h) włączanie/wyłączanie możliwości użycia zewnętrznych referencji,
    i) włączanie/wyłączanie możliwości użycia początkowych białych znaków,
    j) włączanie/wyłączanie możliwości użycia numerycznych nazw,
    k) włączanie/wyłączanie możliwości użycia Processing Instructions,
    l) włączanie/wyłączanie możliwości użycia CDATA,
    m) ograniczenie długości: dokumentu, elementu, nazwy, wartości atrybutu, Namespace,
    n) ograniczenia ilości: zagnieżdżeń w dokumencie, dzieci per element, atrybutów per element, deklaracji NameSpace-ów,
    o) definicję dopuszczalnych znaków,
    p) definicję sygnatur.
48. Moduł WAF musi posiadać funkcję sprawdzania reputacji adresów IP dostających się do chronionych aplikacji zwaną dalej serwisem reputacyjnym.
49. Serwis reputacyjny powinien być dostępny jako rozszerzenie systemu, bez konieczności wprowadzania zmian w architekturze sprzętowej oraz programowej proponowanego rozwiązania.
50. Serwis reputacyjny musi realizować co najmniej następujące funkcje:
    a) automatyczną aktualizację informacji o zagrożeniach,
    b) rozpoznawanie i blokowanie komunikacji dla co najmniej poniższych:
        i. anonimowych proxy,
        ii. sieci Botnet,
        iii. aktywnych źródeł usług oferujących lub dystrybuujących malware, rootkity, robaki oraz wirusy,
        iv. źródeł ataków DDoS/DoS,
        v. źródeł Exit Node sieci Tor,
        vi. adresów IP zainfekowanych przez malware,
        vii. adresów IP świadczących usługi hostingowe dla phishingu lub fraudów,
        viii. źródeł ataków cross-site scripting, iFrame injection, SQL injection, cross domain injection czy domain password brute force,
        ix. źródłowych adresów IP skanerów służących do rekonesansu poprzez skanowanie hostów oraz domen,
    c) weryfikowanie adresu źródłowego na podstawie X-Forwarded-For (XFF).
51. Wraz z Rozwiązaniem należy dostarczyć subskrypcję dla serwisu reputacyjnego.
52. Moduł WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach podstawowych opłat wsparcia.
53. Moduł WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. Mechanizmy normalizacji muszą wspierać/wykrywać:
    a) directory traversal,

b) kodowanie typu „%u”,
c) kodowanie typu IIS backslash,
d) IIS Unicode codepoints,
e) Bare byte decoding,
f) Apache whitespace,
g) bad unescape,
h) wstrzykiwanie komentarzy (np. <!-- -->).

54. Mechanizm normalizacji Modułu WAF powinien umożliwiać definiowanie maksymalnego zagnieżdżonego kodowania.
55. System musi wspierać następujące tryby pracy:
    a) tryb wykrywania, logowania i blokowania ataków,
    b) tryb wykrywania i logowania ataków bez blokowania,
    c) tryb uczenia się bez blokowania,
    d) tryb uczenia się z blokowaniem i logowaniem.
56. Moduł WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji; oraz dowolnie inny ciąg znaków zdefiniowany poprzez PCRE regular expression.
57. Moduł WAF musi chronić ruch przesyłany po IPv6 bez degradacji wydajności wynikającej z innych czynników niż różnice protokołów IPv4 i IPv6.
58. System musi umożliwiać weryfikację działającego na urządzeniu firmware, czy nie uległ on modyfikacji (TPM Chain of Custody).
59. System musi posiadać następujące funkcje zarządzania siecią:
    a) obsługa protokołu SNMP v1/v2c/v3,
    b) możliwość budowania własnych zdarzeń SNMP z własnymi numerami OID,
    c) zewnętrzny syslog,
    d) zbieranie danych i ich wyświetlanie,
    e) zbieranie danych zgodnie z ustawieniami administratora,
    f) osobna brama domyślna dla interfejsu zarządzającego,
    g) zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy),
    h) dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.
60. System musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.
61. System musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki:
    a) czas odpowiedzi per serwer,
    b) czas odpowiedzi per URI,
    c) ilość sesji użytkownika,
    d) przepustowość,
    e) adres źródła,
    f) kraj,
    g) User Agent (wykorzystywana przez klienta aplikacja),
    h) metoda dostępu.
62. System musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji.
63. System 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.

64. System musi oferować stworzenie minimum 10 partycji administracyjnych oraz 10 jednoczesnych domen routingu. Partycje administracyjne i domeny routingu muszą być dostępne również, jeżeli urządzenie pracuje w formie klastra.
65. System musi umożliwiać zarządzanie za pomocą interfejsu graficznego przez przeglądarkę internetową, w tym co najmniej przy pomocy Google Chrome, Microsoft IE, Mozilla Firefox, przy wykorzystaniu protokołu https.
66. System musi umożliwiać zarządzanie przez:
    a) CLI, SSH,
    b) REST API.
67. System musi umożliwiać uwierzytelnienie do interfejsu administracyjnego w oparciu o:
    a) LDAP,
    b) RADIUS,
    c) certyfikaty.
68. Autoryzacja administratorów Systemu musi bazować na rolach użytkowników.
69. Moduł uwierzytelnienia i autoryzacji Systemu musi posiadać co najmniej następujące funkcje:
    a) obsługa IPv6,
    b) definiowanie polityki dostępu poprzez graficzny edytor. W graficznym edytorze można wybierać konkretne obiekty konfiguracyjne (elementy uwierzytelnienia, konfiguracji dostępu, dostępnych zasobów, itp.) oraz najczęstsze powtarzające się konfiguracje kopiować do makr,
    c) obsługa szyfrowania danych przy użyciu protokołu DTLS,
    d) wsparcie dla SSO poprzez SAML 2.0 w trybie IdP (Identity Provider) jak i SP (Service Provider), wsparcie dla profilu SAML ECP,
    e) wsparcie dla OAuth 2.0 w trybie: klient, serwer zasobów (resource server) oraz serwer autoryzacji (authorization server),
    f) obsługa nie mniej niż 5 tysięcy jednocześnie uwierzytelnionych sesji z wykorzystaniem SAML lub OAuth 2.0,
    g) uwierzytelnienie użytkowników przy wykorzystaniu: formularzy, certyfikatów cyfrowych, SecurID, Kerberos SSO, tokenów RSA, Radius, LDAP/LDAPS, Oracle Access Manager, kart smart cards, uwierzytelnienia wieloskładnikowego,
    h) wsparcie dla platform klientów VPN: Windows, Mac, Linux, Android, iPad, iPhone oraz przeglądarek: IE, Firefox, Chrome,
    i) inspekcja stacji klienta sprawdzająca poprawność pracy aplikacji (antywirus, firewall, dostępność plików, rejestrów (Windows), procesów, CPU ID (Windows), HDD ID (Windows) dla systemów Windows, Linux, Mac,
    j) możliwość utworzenia bezpiecznego wirtualnego pulpitu na czas trwania sesji użytkownika,
    k) wsparcie dla CAPTCHA,
    l) wsparcie dla tzw. "step-up authentication",
    m) wsparcie dla Microsoft ActiveSync oraz Outlook Anywhere z wykorzystaniem NTLM,
    n) możliwość generacji jednorazowych tokenów (OTP) i wysyłanie ich mailem lub integrując się z zewnętrzną bramką poprzez SMS,
    o) możliwość definiowania per grupa użytkowników (np. Active Directory)/lub per użytkownik limitu pasma przydzielonego dla użytkownika do ściągania informacji,
    p) możliwość wykorzystania wirtualnej klawiatury do procesu logowania użytkownika,
    q) definiowanie reguł dostępu użytkownika bazując na listach uwzględniających parametry warstwy 4 oraz 7 modelu ISO OSI,

r) funkcja SSO (gromadzenia parametrów uwierzytelnienia użytkownika - credential caching),

s) możliwość budowania dynamicznej strony www, w zależności od użytkownika, jego przynależności do danej grupy, zawierającej udostępnione aplikacje,

t) wsparcie dla VMWare View oraz Citrix XenApp/XenDesktop,

u) wsparcie dla proxy PCoIP, Blast oraz Blast Extreme dla rozwiązania VMware Horizon,

v) wsparcie dla przekierowania USB dla VMware Horizon,

w) dopuszcza się, że część z powyższych wymagań dotyczących uwierzytelniania i autoryzacji będzie realizowana przy użyciu aplikacji agenta dla systemu Windows, musi istnieć możliwość automatycznego aktualizowania wersji aplikacji agenta, nie może być ograniczenia liczby aplikacji agentów instalowanych w środowisku Zamawiającego.

70. Rozwiązanie musi być dostarczone w formie klastra wysokiej dostępności (HA) złożonego z dwóch Systemów tego samego typu pracujących w trybie active – passive z opcją realizacji trybu active-active.
71. Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy Systemami, aby uniknąć ponownej negocjacji po przełączeniu ruchu.
72. Klaster wysokiej dostępności musi zapewniać synchronizację:
    a) konfiguracji,
    b) stanu połączeń,
    c) przywiązywania sesji (*Session persistence*).
73. Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu weryfikacji stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover).
74. System musi spełniać wymogi z tabeli 1.

Tabela 1. Wymagania dla każdego urządzenia systemu

Lp.	Parametr	Wymagania
1.	Pamięć	Nie mniej niż 32GB
2.	Dysk twardy	Jeden dysk SSD o pojemności nie mniejszej niż 480 GB
3.	Przepływność dla warstwy 4	Nie mniej niż 17 Gbps
4.	Przepływność dla warstwy 7	Nie mniej niż 9 Gbps
5.	Ilość jednocześnie obsługiwanych połączeń	Nie mniej niż 17 milionów
6.	Ilość transakcji SSL na sekundę dla klucza o długości 2048	Nie mniej niż 4,5 tysiąca
7.	Ilość transakcji SSL na sekundę dla szyfru ECDSA P-256	Nie mniej niż 4,5 tysiąca
8.	Przepływność ruchu szyfrowanego	Nie mniej niż 7 Gbps
9.	Ilość połączeń na sekundę w warstwie 4	Nie mniej niż 140 tysięcy
10.	Kompresja	Nie mniej niż 7 Gbps

11.	Gęstość interfejsów	Nie mniej niż 4 interfejsy z możliwością obsadzenia wkładkami SFP+ 10G (SR lub LR), nie mniej niż cztery interfejsy miedziane 1 Gb / 10 Gb, oddzielny interfejs zarządzania, port konsolowy, interfejs szeregowy failover, port USB Dopuszcza się tylko moduły w pełni wspierane przez producenta tego urządzenia.
12.	Obudowa	Przeznaczona do montażu w szafie rack 19”, wysokość nie większa niż 1 U
13.	Zasilanie	Nie mniej niż dwa redundantne zasilacze - prąd zmienny 230V AC
14.	MTBF platformy	Nie mniej niż 180 tysięcy godzin

75. Zakres usługi wdrożeniowej:
    a) wykonanie projektu technicznego i uzgodnienie go z Zamawiającym,
    b) instalacja sprzętu w lokalizacjach wskazanych przez Zamawiającego znajdujących się na terenie Aglomeracji Warszawskiej i Aglomeracji Poznańskiej,
    c) konfiguracja i uruchomienie Rozwiązania w trybie wysokiej dostępności,
    d) skonfigurowanie ochrony/mitygacji ataków dla wskazanej przez Zamawiającego adresacji/listy usług, składających się z minimum 3 usług/aplikacji,
    e) wymagane konfiguracje ochrony/mitygacji:
        i. ochrona anty-DdoS,
        ii. Bot Protection,
        iii. negatywny i pozytywny model bezpieczeństwa dla usług/aplikacji,
    f) wykonanie testów akceptacyjnych potwierdzających prawidłowość działania rozwiązania,
    g) sporządzenie dokumentacji powykonawczej.

76. Przeprowadzenie warsztatów dla Zamawiającego:
    a) warsztaty zostaną przeprowadzone w terminie do 2 tygodni od zakończenia wdrożenia,
    b) w warsztatach może uczestniczyć min. 15 wskazanych przez Zamawiającego osób, będącymi pracownikami z jednostek SBŁ,
    c) warsztaty odbędą się w formule online,
    d) warsztaty zostaną nagrane w postaci materiału wideo do późniejszego odtworzenia przez Zamawiającego i tylko na użytek wewnętrzny,
    e) warsztaty będą trwać min. 5 godzin zegarowych,
    f) warsztaty odbędą się między godzinami 9:00 a 16:00, w dni robocze,
    g) warsztaty odbędą się na środowisku będącym odzwierciedleniem środowiska SBŁ, na zbliżonej konfiguracji, przy czym dopuszcza się przeprowadzenie warsztatów na środowisku produkcyjnym,
    h) w ramach warsztatów zostanie przedstawiona funkcjonalność Rozwiązania,
    i) warsztaty zostaną przeprowadzone przez trenera Wykonawcy, posiadającego doświadczenie w zakresie prowadzenia warsztatów z zakresu rozwiązań do ochrony webaplikacji klasy Web Application Firewall.

77. Wymagana jest roczna gwarancja producenta i roczne wsparcie Wykonawcy dla dostarczonego Rozwiązania.
78. W zakresie gwarancji producenta Wykonawca zapewni:

a) dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta,

b) sposób obsługi zgłoszeń gwarancyjnych w trybie 10x5,

c) wymiana sprzętu następnego dnia roboczego po identyfikacji usterki,

d) w przypadku awarii urządzenia i konieczności wysłania go na wymianę lub serwis, dyski z dotychczasowych urządzeń muszą pozostać u Zamawiającego.

79. Wymagania dotyczące wsparcia Wykonawcy:

a) wsparcie będzie realizowane co najmniej w dni robocze w godzinach 8:00-16:00, w języku polskim. Wsparcie będzie standardowo świadczone zdalnie, natomiast w przypadku braku możliwości rozwiązania problemu zgłoszenia zdalnie, będzie realizowane poprzez świadczenie jej na miejscu, w zlokalizowanych na terenie Polski jednostkach SBŁ, których zgłoszenie dotyczy, lub w których istnieje możliwość jego rozwiązania. Jednostki SBŁ zlokalizowane są na terenie Aglomeracji Łódzkiej, Aglomeracji Górnośląskiej, Aglomeracji Warszawskiej, Aglomeracji Krakowskiej, Aglomeracji Trójmiejskiej, Aglomeracji Wrocławskiej, Aglomeracji Poznańskiej oraz w Opolu, Kędzierzynie-Koźlu, Legnicy, Toruniu, Puławach i Radomiu. Ze względu na rozwój Sieci Łukasiewicz lista lokalizacji może ulec zmianie,

b) wsparcie obejmuje obsługę zgłoszeń następujących kategorii:
   - błędów i usterek,
   - weryfikacji poprawności działania Rozwiązania na zgłoszenie Zamawiającego,
   - potrzeby konsultacji i wsparcie w zakresie analizy zdarzeń bezpieczeństwa,
   - potrzeby konsultacji i wsparcie w realizacji zmian w konfiguracji w zakresie uzgodniony z administratorami SBŁ wskazanymi przez Zamawiającego,

c) Wykonawca zapewni poziom wsparcia w zakresie obsługi zgłoszeń zgodnie z tabelą i opisem poniżej:

Kategoria zgłoszenia	**Maksymalny czas reakcji**	**Maksymalny czas naprawy lub uruchomienia Obejścia**	**Maksymalny czas realizacji zgłoszenia**
Błąd krytyczny	do 8 godzin roboczych	do 16 godzin roboczych	nie dotyczy
Błąd poważny	do 8 godzin roboczych	do 32 godzin roboczych	nie dotyczy
Usterka	do 8 godzin roboczych	do 48 godzin roboczych	nie dotyczy
Weryfikacja poprawności działania Rozwiązania	do 8 godzin roboczych	nie dotyczy	do 32 godzin roboczych
Konsultacje i wsparcie w zakresie analizy zdarzeń bezpieczeństwa	do 8 godzin roboczych	nie dotyczy	do 40 godzin roboczych
Konsultacje i wsparcie w realizacji zmian w konfiguracji	do 8 godzin roboczych	nie dotyczy	Do 48 godzin roboczych

Godziny robocze – godziny między 8:00 a 16:00 w dniach roboczych.

Błąd krytyczny - błąd po stronie Rozwiązania lub inna nieprawidłowość Rozwiązania lub jego konfiguracji uniemożliwiająca korzystanie z usług Rozwiązania, w szczególności:

- uniemożliwiająca ochronę webaplikacji (niepoprawna praca funkcji WAF)
- uniemożliwiająca równoważenie obciążenia serwerów (niepoprawna praca funkcji LB)
- naruszająca bezpieczeństwo Rozwiązania (dostęp do danych lub funkcji usługi z pominięciem mechanizmów zabezpieczeń);

Błąd poważny - nieprawidłowość działania Rozwiązania, która wpływa w istotny sposób na wyniki pracy, ogranicza funkcjonalność usług, w wyniku czego praca jest utrudniona, ale możliwa;

Usterka – drobna uciążliwość, która nie wpływa w sposób istotny na działanie Rozwiązania i nie utrudnia pracy;

Obejście – rozwiązanie błędu lub usterki, które pozwala użytkownikom, pomimo istnienia nieprawidłowości, na korzystanie z Rozwiązania w inny niż opisany w dokumentacji sposób, przy czym jeżeli sposób ten wnosi drobną uciążliwość, która nie wpływa w sposób istotny na działanie Rozwiązania i nie utrudnia pracy, to rozwiązanie docelowe powinno być dostarczone w czasie 48 godzin roboczych, przy czym czas ten będzie wydłużony o czas potrzebny na rozwiązanie przyczyn zewnętrznych, takich jak: naprawa środowiska sprzętowo-systemowego, łącza internetowego, naprawa błędu przez producenta Rozwiązania, oczekiwanie na okno serwisowe umożliwiające wykonanie prac,

UWAGA: od czasu naprawy będzie odliczany czas potrzebny na usunięcie zaistniałych przeszkód, a nieleżących po stronie Wykonawcy, w szczególności:

- czas naprawy przeszkód występujących w środowisku informatycznym Zamawiającego;
- czas oczekiwania na okno serwisowe wyznaczane przez Zamawiającego,
- czas naprawy błędu w oprogramowaniu po stronie producenta oprogramowania liczony od momentu zgłoszenia dokonanego przez Wykonawcę u producenta.

Wykonawca zobowiązany jest do dochowania należytej staranności mającej na celu niezwłoczne powiadomienie o takiej wadzie producenta oprogramowania oraz do współpracy z producentem oprogramowania w zakresie jej usunięcia,

d) Wykonawca zobowiązany jest podjąć niezwłocznie po przyjęciu zgłoszenia czynności zmierzające do jego zdiagnozowania oraz podjęcia naprawy, jednak nie później niż w terminach wskazanych powyżej. O rozpoczęciu diagnozy, wyniku diagnozy oraz podjęciu czynności zmierzających do naprawy błędu lub usterki Wykonawca niezwłocznie powiadomi Zamawiającego drogą elektroniczną,

e) w ramach wsparcia, Wykonawca zobowiązany jest zapewnić Zamawiającemu dostęp do dedykowanego przedstawiciela Wykonawcy pełniącego funkcję opiekuna technicznego klienta (z ang. technical account manager / customer success specialist),

f) Zamawiający ma mieć możliwość przesyłania zgłoszeń co najmniej na adres mailowy opiekuna technicznego klienta ze strony Wykonawcy. Wykonawca ma przedstawić raporty z obsługi tych zgłoszeń, w szczególności SLA, na żądanie Zamawiającego,

g) Wykonawca nie ponosi odpowiedzialności za Błędy lub Usterki Systemu w przypadku, gdy Błędy lub Usterki Systemu są spowodowane brakiem implementacji nowej wersji Systemu, pomimo że wymagał jej producent a Wykonawca informował o takiej konieczności,

h) Wykonawca nie ponosi odpowiedzialności za oprogramowanie podmiotów trzecich stanowiące części składowe środowiska informatycznego Zamawiającego, które w połączeniu z Systemem może powodować problemy w środowisku informatycznym Zamawiającego. Nie zwalnia to Wykonawcy z identyfikacji źródła problemu, udziału w pracach diagnostycznych i dążenia do rozwiązania problemów występujących na poziomie integracji oprogramowania podmiotów trzecich i producenta WAF,

i) Wykonawca nie ponosi odpowiedzialności za szkody powstałe w organizacji Zamawiającego w przypadku:

1) użytkowania Systemu niezgodnie z przeznaczeniem opisanym w dokumentacji dostarczonej wraz z Systemem, nieprzestrzegania instrukcji użytkowania przez Zamawiającego, jego pracowników, inne osoby przez niego upoważnione, pod warunkiem, że instrukcja ta stanowi załącznik dostarczony wraz z Systemem lub,

2) w sytuacji ingerencji w System przez osoby nieuprawnione powodujące wady lub błędy Oprogramowania, lub

3) modyfikacji Systemu wprowadzonych bez autoryzacji Wykonawcy lub producenta bądź dokonywaniem napraw Systemu przez osoby nieuprawnione.

Terminy realizacji:

1. Dostawa w terminie do 8 tygodni od dnia zawarcia umowy.
2. Wdrożenie (instalacja, konfiguracja, uruchomienie) w terminie 14 tygodni od dnia zawarcia umowy.
3. Przeprowadzenie warsztatów w terminie 4 tygodni od zakończenia wdrożenia.
4. Roczna gwarancja producenta i roczne wsparcie Wykonawcy dla dostarczonego Rozwiązania.