Opis funkcjonalności i wdrożenia Load Balancer'ów

Wymagania

ID	WYMAGANIE	WYMAGANIE SZCZEGÓŁOWE
WNFLB1-001	System – funkcje	System musi realizować 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 - Moduł SSL VPN (bez licencji) - Globalnego równoważenia obciążenia za pomocą protokołu DNS - Ochrona przed atakami na aplikacje internetowe i serwery WWW (Web Application Firewall) Wszystkie wymienione w niniejszym dokumencie funkcje muszą być dostępne w obrębie jednego urządzenia.
WNFLB1-002	System – klucze prywatne	Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej
WNFLB1-003	System – metody równoważenia obciążenia	System musi posiadać co najmniej następujące metody równoważenia obciążenia: 1) Cykliczna 2) Ważona 3) Najmniejsza liczba połączeń 4) Najszybsza odpowiedź serwera 5) Najmniejsza liczba połączeń i najszybsza odpowiedź serwera 6) Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie 7) Dynamicznie ważona oparta na SNMP/WMI 8) Definiowana na podstawie grupy priorytetów dla serwerów
WNFLB1-004	System – język skryptowy	Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy: 1) Analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakie-

		tów 2) Obsługa protokołów: http, tcp, xml, rtsp, sip 3) Musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS 4) Język skryptowy musi bazować na języku programowania Tool Command Language lub równoważnym, z własnymi komendami. 5) Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego 6) Producent systemu musi dostarczyć darmową, specjalizowaną aplikację do analizy poprawności składni skryptów pisanych przy wykorzystaniu języka skryptowego wyżej opisanego. 7) Aplikacja musi posiadać wbudowane szablony skryptów oraz funkcję automatycznego uzupełniania wpisywanych komend.
WNFLB1-005	System – proxy	Rozwiązanie musi pracować w trybie pełnego proxy. Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.
WNFLB1-006	System – integracja	Rozwiązanie musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji
WNFLB1-007	System – mechanizmy równoważenia obciążenia	Rozwiązanie musi wspierać następujące mechanizmy równoważenia obciążenia: round robin, ważona, dynamicznie ważona (na podstawie SNMP/WMI), najmniejsza liczba połączeń, najszybsza odpowiedź, observer, predictive, grupy priorytetów, możliwość modyfikacji za pomocą języka skryptowego
WNFLB1-008	System – buforowanie połączeń	Wymagane jest buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera
WNFLB1-009	**S**ystem – monitorowanie stanu serwerów	Rozwiązanie musi obsługiwać następujące 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, 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.
WNFLB1-010	System – przywiązywanie sesji	System musi posiadać funkcje przywiązywania sesji przy wykorzystaniu co najmniej

		następujących atrybutów: 1) Cookie (hash, rewrite, custom, insert, passive) 2) Adres źródłowy 3) Adres docelowy 4) SSL ID 5) RDP login name 6) JSESSIONID 7) SIP call ID
WNFLB1-011	System – usługi w warstwach 4-7	System musi świadczyć co najmniej następujące usługi w warstwach 4-7: 1) Inspekcja warstwy 7 2) Wstrzykiwanie nagłówków http 3) Ukrywanie zasobów 4) Zmiana odpowiedzi serwera 5) Przepisywanie odpowiedzi 6) Zaszyfrowane cookies 7) Ochrona przed atakami typu DoS/DDoS 8) Ochrona przed atakami typu SYN Flood 9) Multipleksacja zapytań http 10) Kompresja i cache'owanie HTTP
WNFLB1-012	System – optymalizacja i akceleracja aplikacji	System musi posiadać funkcje optymalizacji i akceleracji aplikacji: 1) Urządzenie musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci: a) LAN b) WAN c) CELL (komórkowy) 1) Urządzenie powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta. 2) Urządzenie musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control) 3) Urządzenie musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP 4) Urządzenie musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od: a) Listy dozwolonych URI b) Listy wykluczonych URI c) Listy kompresowalnych Content-Type d) iv. Listy wykluczonych Content-Type
WNFLB1-013	System – moduł SSL VPN Wymienione w tej sekcji	Moduł SSL VPN musi posiadać co najmniej następujące funkcje:

	funkcjonalności będą dostępne po wykupieniu odrębnej licencji. Przedmiot zamówienia nie obejmuje dostarczenia takiej licencji	1) Obsługa trybów portal access, application tunnel, network access 2) - Obsługa IPv6 3) - Definiowanie polityki dostępu poprzez graficzny edytor 4) Obsługa szyfrowania danych przy użyciu protokołu DTLS 5) Wsparcie dla SSO poprzez SAML 2.0 w trybie IdP (Identity Provider) jak i SP (Service Provider) 6) Wsparcie dla OAuth 2.0 w trybie: klient, serwer zasobów (resource server) oraz serwer autoryzacji (authorization server) 7) Uwierzytelnienie użytkowników przy wykorzystaniu: formularzy, certyfikatów cyfrowych, SecurID, Kerberos SSO, tokenów RSA, Radius, LDAP, Oracle Access Manager, kart smart cards, uwierzytelnienia wieloskładnikowego 8) Wsparcie dla platform klientów VPN: Windows, Mac, Linux, Android, iPad, iPhone oraz przeglądarek: IE, Firefox, Chrome 9) Inspekcja stacji klienta sprawdzająca poprawność pracy aplikacji (antywirus, firewall, dostępność plików, rejestrów, procesów, CPU ID, HDD ID) dla systemów Windows, Linux, Mac 10) Możliwość utworzenia bezpiecznego wirtualnego pulpitu na czas trwania sesji użytkownika 11) Wsparcie dla CAPTCHA 12) Możliwość wykorzystania wirtualnej klawiatury do procesu logowania użytkownika 13) Definiowanie reguł dostępu użytkownika bazując na listach uwzględniających parametry warstwy 4 oraz 7 modelu ISO OSI. 14) Funkcja SSO (gromadzenia parametrów uwierzytelnienia użytkownika - credential caching) 15) Wsparcie dla VMWare View oraz Citrix XenApp/XenDesktop 16) Funkcja raportowania, uwzględniająca błędne uwierzytelnienie, nazwę użytkownika, przydzielone zasoby, lokalizację geograficzną. 17) Obsługa funkcji szyfrowania site-to-site IPSec VPN 18) Moduł SSL VPN musi posiadać mechanizm raportowy, uwzględniający nie mniej niż: a) Błędne próby uwierzytelnienia b) Informacje o użytkownikach c) Zasoby, do których odwołują się użytkownicy d) Lokalizacja (Geolocation) 19) Obsługa nie mniej niż 500 jednocześnie

		pracujących użytkowników z możliwością licencyjnej rozbudowy do 10 tysięcy licencji.
WNFLB1-014	System – sterowanie ruchem	Rozwiązanie musi zapewniać globalne, inteligentne sterowanie ruchem wykorzystując usługę DNS jako mechanizm rozdziału ruchu (Global Solution Load Balancing), w ramach którego zapewni: 1) Monitorowanie stanu pracy usług korzystając z monitorów działających w warstwie sieci, transportowej oraz aplikacji modelu ISO/OSI 2) Rozdzielanie ruchu korzystając co najmniej z metod: a) Cykliczna b) Ważona c) Na podstawie adresów IP klienta usługi (topologii) d) Obciążenia serwera e) Najmniejszej liczby połączeń 1) Mechanizmy utrzymywania sesji polegające na kierowaniu zapytań z lokalnego serwera dns klienta aplikacji zawsze do tego samego centrum danych i serwera aplikacji 2) Wbudowany w system operacyjny język skryptowy, umożliwiający analizę i zmianę parametrów w protokole DNS 3) Ochronę serwerów DNS z wykorzystanie DNSSEC a także na zastosowaniu list kontroli dostępu umożliwiających filtrowanie ruchu DNS bazując na typie rekordu 4) Możliwość pracy, jako serwer DNS obsługujący następujące rekordy: A, NS, CNAME, SOA, PTR, HINFO, MX, TXT, AFSDB, SIG, KEY, AAAA, LOC, SRV, NAPTR, KX, CERT, DNAME, OPT, DS, SSHFP, IPSECKEY, RRSIG, NSEC, DNSKEY, DHCID, NSEC3, NSEC3PARAM, HIP, TKEY, TSIG, IXFR, AXFR, ANY, ZXFR, DLV 5) Konwersja rekordów między IPv4 i IPv6 6) Wsparcie dla usług geolokacji, możliwość przekierowania ruchu do najbliższej geograficznie lokalizacji 7) Wybór lokalizacji na podstawie ilości urządzeń pośredniczących oraz ilości przetwarzanych danych 8) Możliwość wysyłania zapytań dotyczących obciążenia do urządzeń firm trzecich 9) Możliwość bezpośredniego odpytywania serwerów o obciążenie 10) Możliwość przekierowania ruchu do innej lokalizacji po przekroczeniu zdefiniowanego progu ilości sesji

WNFLB1-015	System – firewall aplikacyjny pozytywny model bezpieczeństwa	WAF (ang. WAF - Web Application Firewall) 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: 1) wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URL-a. 2) - typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT) 3) przejścia pomiędzy URL-ami (servletami) 4) dopuszczalne metody http, 5) dopuszczalne cookie, 6) dopuszczalne parametry w polityce, 7) parametry dynamiczne, 8) typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany) oraz dopuszczalne parametry w danym serwlecie 9) długość zapytań 10) nazwy hosta 11) wystąpień i długość parametrów (per każdy parametr) 12) wystąpień i długości nagłówków 13) wystąpień i długości cookies 14) oczekiwanych typów znaków per każdy parametr 15) typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku 16) URL-i podatnych na CSRF
WNFLB1-016	System – firewall aplikacyjny - funkcje	Profil aplikacji web musi być tworzony na podstawie analizy ruchu sieciowego. WAF musi umożliwiać definiowania dopuszczalnego przepływu sekwencji zapytań w obrębie aplikacji z uwzględnieniem jej logiki biznesowej. WAF musi posiadać funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń). Tworzenie profilu bezpieczeństwa Web Application Firewall dla danej aplikacji musi odbywać się na podstawie analizy ruchu sieciowego: 1) W szczególności na podstawie publicznego ruchu produkcyjnego. 2) Algorytmy tworzenia profilu bezpieczeństwa WAF powinny odrzucać nadużycia w procesie nauki. 3) 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. 4) Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr 5) Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki bezpieczeństwa 6) Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów zapytań http 7) WAF musi posiadać funkcjonalność automatycznego wykrywania stron logowania użytkowników oraz automatycznie włączać dla tych stron ochronę przed atakami brute force. 8) W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP, SMTP oraz FTP.
WNFLB1-017	System – firewall aplikacyjny – ochrona przed atakami	WAF musi posiadać mechanizmy ochrony przed atakami: 1) SQL Injection, 2) Cross-Site Scripting, 3) Cross-Site Request Forgery, 4) Session hijacking, 5) Command Injection, 6) Cookie/Session Poisoning, 7) Parameter/Form Tampering, 8) Forceful Browsing, 9) Brute Force Login, 10) Web Scraping 11) Cookie manipulation/poisoning 12) Dynamic Parameter tampering 13) Buffer Overflow 14) Stealth Commanding 15) Unused HTTP Methods 16) Malicious File Uploads 17) - Hidden Field Manipulation WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http). WAF musi blokować ataki typu Slow Loris. WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez: 1) Wstrzykiwanie skryptu JavaScript i weryfikacji rezultatów jego wykonania 2) Mechanizmu browser fingerprinting, w celu wykrycia tzw. headless broser 3) Sygnatur botów 4) 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. WAF musi umożliwiać blokowanie zapytań z danego obszaru geograficznego. Aktualizacje bazy geolokacyjnej powinny być dostępne w ramach podstawowych opłat wsparcia. WAF musi umożliwiać automatyczne budowanie polityk w oparciu o skanowanie przez zewnętrznych dostawców. WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku. WAF musi umożliwiać integracje systemami antywirusowymi po protokole ICAP w celu wykrywania wirusów w przesyłanych plikach. WAF musi wykrywać i maskować numery kart kredytowych, wyciekających z chronionej aplikacji.
WNFIB1-018	System – serwis reputacyjny	Serwis reputacyjny powinien być dostępny jako rozszerzenie systemu, bez konieczności wprowadzania zmian w architekturze sprzętowej oraz programowej proponowanego rozwiązania. Wraz z rozwiązaniem należy dostarczyć 5 letnią subskrypcję dla serwisu reputacyjnego. Serwis reputacyjny musi realizować co najmniej następujące funkcje: 1) Automatyczna aktualizacja informacji o zagrożeniach nie rzadziej niż co 5 minut 2) Rozpoznawać i blokować komunikację dla minimum poniższych: a) Anonimowych proxy b) Sieci Botnet c) Aktywnych źródeł usług oferujących lub dystrybuujących malware, rootkity, robaki oraz wirusy d) Źródeł ataków DDoS/DoS e) Adresów IP zainfekowanych przez malware f) Adresów IP świadczących usługi hostingowe dla phishingu lub fraudów. g) Źródeł ataków cross-site scripting, iFrame injection, SQL injection, cross domain injection czy domain password brute force h) Źródłowych adresów IP skanerów służących do rekonesansu poprzez skanowanie hostów oraz domen 1) Weryfikacja adresu źródłowego na podstawie X-Forwarded-For (XFF)
WNFLB1-019	System – funkcjonalność zapory	Rozwiązanie musi zapewniać funkcjonalność stanowej zapory sieciowej umożliwiającej kontrolę ruchu sieciowego oraz ochronę przed atakami

		typu DoS w warstwie 3 i 4 ISO/OSI 1) Rozwiązanie musi zapewniać funkcjonalność NAT/PAT/Dynamiczny PAT 2) System musi zapewniać ochronę DoS/DDoS przynajmniej dla protokołów HTTP/HTTPS, SIP, DNS 3) Rozwiązanie musi posiadać możliwość automatycznego dostosowania progów DDoS. 4) Zarządzanie regułami bezpieczeństwa musi być realizowane za pomocą wbudowanego w system interfejsu graficznego. 5) Rozwiązanie musi chronić przed atakami typu flood, sweep, teardrop oraz smurf. 6) Wykrywanie anomalii w protokołach i pakietach SYN/ICMP/ACK/UDP/TCP/IP4/IP6/ DNS/ARP. 7) Rozwiązanie musi wspierać Remote Triggered Black Hole. 8) Rozwiązanie musi umożliwiać uruchomienie proxy SSH, które umożliwia np. blokowanie ściąganie lub wgrywanie plików po SCP lub SFTP, ustawienie czy użytkownik ma dostęp do shella czy nie. 9) Rozwiązanie musi wykrywać nieprawidłowe protokoły przechodzące przez otwarte porty (np. otwarty port 80 dla ruchu http, gdy na tym porcie odbywa się ruch ssh). 10) Zarządzanie regułami bezpieczeństwa musi być realizowane za pomocą wbudowanego w system interfejsu graficznego. 11) Rozwiązanie musi chronić przed atakami typu flood, sweep, teardrop oraz smurf 12) Rozwiązanie musi obsłużyć mitygację minimum 100 wektorów ataków DDoS. 13) Rozwiązanie musi posiadać wsparcie obsługi protokołów routingowych BGP, OSPF, RIP, ISIS, BFD.
WNFLB1-020	System – tryby pracy	Urządzenie musi wspierać następujące tryby pracy: 1) Tryb wykrywania, logowania i blokowania ataków 2) Tryb wykrywania i logowania ataków bez blokowania 3) Tryb uczenia się bez blokowania 4) Tryb uczenia się z blokowaniem i logowaniem
WNFLB1-021	System – połączenia	System 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.

WNFLB1-022	System – VLAN	System musi obsługiwać sieci VLAN w standardzie 802.1q
WNFLB1-023	System – agregacja linków	System musi obsługiwać agregację linków w standardzie 802.3ad (LACP)
WNFLB1-024	System – interfejsy administracyjne	System musi posiadać co najmniej następujące interfejsy administracyjne: 1) GUI przy wykorzystaniu protokołu HTTPS 2) Zarządzanie poprzez SSH 3) Zarządzanie poprzez SOAP-SSL 4) Zarządzanie poprzez API REST
WNFLB1-025	System – autoryzacja	Autoryzacja administratorów systemu musi bazować na rolach użytkowników
WNFLB1-026	System – uwierzytelnienie użytkowników	System musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.
WNFLB1-027	System – zarządzanie siecią	System musi posiadać następujące funkcje zarządzania siecią: 1) Obsługa protokołu SNMP v1/v2c/v3 2) Zewnętrzny syslog 3) Zbieranie danych i ich wyświetlanie 4) Zbieranie danych zgodnie z ustawieniami administratora 5) Osobna brama domyślna dla interfejsu zarządzającego 6) Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot) 7) Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy) Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.
WNFLB1-028	System – szablony konfiguracji aplikacji	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 Zamawiającego. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.
WNFLB1-029	System – moduł analizy ruchu	System powinien posiadać moduł analizy ruchu

	http	http. Moduł powinien zbierać następujące metryki: 1) Czas odpowiedzi per serwer 2) Czas odpowiedzi per URI 3) Ilość sesji użytkownika 4) Przepustowość 5) Adres źródła 6) Kraj 7) User Agent (wykorzystywana przez klienta aplikacja) 8) Metoda dostępu
WNFLB1-030	System - partycje	Rozwiązanie musi oferować podział na tzw. partycje administracyjne. Zdefiniowany użytkownik może zarządzać konfiguracją tylko i wyłącznie wewnątrz swojej partycji. 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. Rozwiązanie musi oferować stworzenie minimum 1000 partycji administracyjnych oraz 1000 jednoczesnych domen routingu. Partycje administracyjne i domeny routingu muszą być dostępne również, jeżeli urządzenie pracuje w formie klastra.
WNFLB1-031	Urządzenia - klaster	System musi być dostarczony w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1. W ramach klastra musi istnieć możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu Klaster wysokiej dostępności musi zapewniać synchronizację: 1) Konfiguracji 2) Stanu połączeń 3) Przywiązywania sesji (Session persistence)
WNFLB1-032	Urządzenia – wykrywanie awarii	Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu, co najmniej następujących metod: 1) Weryfikacja stanu pracy urządzenia poprzez

		analizę aktywności w sieci (network failover) 2) Weryfikacji stanu pracy urządzenia poprzez interfejs szeregowy (serial failover)
WNFLB1-033	Urządzenia – pamięć	Nie mniej niż 32GB w każdym z urządzeniu
WNFLB1-034	Urządzenia – dysk twardy	Jeden dysk o pojemności nie mniejszej niż 500GB w każdym z urządzeniu
WNFLB1-035	Urządzenia – przepływność dla warstwy 4	Nie mniej niż 20 Gbps dla każdego z urządzeń
WNFLB1-036	Urządzenia – przepływność dla warstwy 7	Nie mniej niż 20 Gbps dla każdego z urządzeń
WNFLB1-037	Urządzenia – przepustowość wewnętrznej magistrali	Nie mniej niż 168 Gbps dla każdego z urządzeń
WNFLB1-038	Urządzenia – ilość jednocześnie obsługiwanych połączeń	Nie mniej niż 28 milionów dla każdego z urządzeń
WNFLB1-039	Urządzenia – ilość transakcji SSL	Ilość transakcji SSL na sekundę dla klucza o długości 2048 nie mniej niż 10000 dla każdego z urządzeń
WNFLB1-040	Urządzenia – ilość transakcji SSL	Ilość transakcji SSL na sekundę dla szyfru ECDSA P-256 nie mniej niż 6500 dla każdego z urządzeń
WNFLB1-041	Urządzenia – przepływność ruchu szyfrowanego	Nie mniej niż 10 Gbps dla każdego z urządzeń
WNFLB1-042	Urządzenia – ilość połączeń na sekundę w warstwie 4	Nie mniej niż 250 tysięcy dla każdego z urządzeń
WNFLB1-043	Urządzenia – kompresja software	Nie mniej niż 6 Gbps dla każdego z urządzeń
WNFLB1-044	Urządzenia – gęstość interfejsów	Dla każdego z urządzeń: Nie mniej niż osiem interfejsów z możliwością obsadzenia wkładkami SFP (T, SX lub LX), nie mniej niż cztery interfejsy z możliwością obsadzenia wkładkami SFP+ 10G (SR lub LR), oddzielny interfejs zarządzania, port konsolowy, interfejs szeregowy failover, port USB Należy zapewnić 2 wkładki 10 Gigabit Ethernet SFP+ SR oraz 2 wkładki 1 Gigabit Ethernet SFP SX.
WNFLB1-045	Urządzenia – zarządzanie	Dla każdego z urządzeń panel i wyświetlacz LCD z funkcjami: 1) ustawienia adresu IP na potrzeby zarządzania, ustawienia parametrów portu szeregowego, wyświetlania podstawowych alarmów, 2) możliwości restartu urządzenia,

		3) wyświetlania informacji o systemie 4) funkcjonalność „Always On Management”
WNFLB1-046	Urządzenia – obudowa	Przeznaczona do montażu w szafie rack 19”, wysokość nie większa niż 5 U dla każdego z urządzeń
WNFLB1-047	Urządzenia - zasilanie	Nie mniej niż dwa redundantne zasilacze - prąd zmienny 230V AC dla każdego z urządzeń
WNFLB1-048	Gwarancja	Wymagana jest 5 letnia gwarancja producenta. W obrębie gwarancji zawarte musi być: 1) Dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta 2) Sposób obsługi zgłoszeń gwarancyjnych w trybie 5x8 3) Wymiana sprzętu następnego dnia roboczego po identyfikacji usterki

Wymagania dotyczące wdrożenia Load Balancer’ów:

1. Wdrożenie Load Balancer’ów obejmuje:
   1) dostawę i sprawdzenie kompletności urządzeń,
   2) przygotowanie docelowej konfiguracji urządzeń zgodnie z wytycznymi Zamawiającego,
   3) weryfikację poprawnego działania urządzeń,
   4) montaż fizyczny urządzeń,
   5) podłączenie urządzeń do infrastruktury Zamawiającego.
2. Zamawiający wymaga przeprowadzenia testów bezpieczeństwa aplikacji internetowych polegających na przeprowadzeniu testów penetracyjnych obejmujących skanowanie portów, badanie podatności aplikacji internetowych na znane luki w bezpieczeństwie, weryfikację poprawności działania firewalla, ocenę poprawności reakcji systemu zabezpieczeń na wykonywane ataki DDOS, w tym co najmniej:
   1) flooding,
   2) smurfing,
   3) IP fragmentation,
   4) syn flood,
   5) nuking.

Testy muszą zakończyć się pełnym raportem z przeprowadzonych czynności.

3. Testy akceptacyjne, obciążeniowe i bezpieczeństwa aplikacji zostaną uzgodnione z Zamawiającym na etapie projektowym.