Załącznik nr 2

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakup urządzeń podziału obciążenia ruchu wraz ze wsparciem dla systemu Load Balancer na okres 36 miesięcy. Urządzania 4 szt.

Przedmiotem zakupu jest dostarczenie urządzeń podziału obciążenia ruchu – Load Balancer - pozwalających na zbudowanie dwóch klastrów niezawodnościowych wraz z niezbędnym do tego wyposażeniem i licencjami. Zamawiający wymaga, aby każdy z klastrów składał się z dwóch identycznych urządzeń z których każde spełni poniższe wymagania:

Wymagania Ogólne:

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2023 r. poz. 1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. System podziału obciążenia dla ruchu przychodzącego i wychodzącego pracujący w warstwach 2,4,7. Musi zostać dostarczony w postaci komercyjnej platformy sprzętowej lub programowej. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
4. Wykonawca zobowiązany jest przeprowadzić montaż, uruchomienie i wstępną konfigurację klastrów urządzeń w dwóch lokalizacjach Zamawiającego w sposób umożliwiający przełączenie serwerów MS Exchange na dostarczone rozwiązanie.
5. Wykonawca zobowiązany jest do dostarczenia 5 Voucherów ważnych przez minimum rok od daty ich odebrania, potwierdzonej podpisaniem bez zastrzeżeń protokołu odbioru, na autoryzowane szkolenie producenta dostarczonego rozwiązania – obejmujące między innymi podstawy konfiguracji i zarządzania.
6. Wykonawca zobowiązany jest wycenić dodatkowo 180 h wsparcia na dodatkowe zmiany konfiguracyjne i rozwiązywanie problemów z dostarczonym rozwiązaniem – wsparcie może odbywać się w sposób zdalny.
7. W ramach dostawy, Wykonawca zobowiązuje się dostarczyć urządzenia w pełni wyposażone we wkładki SFP we wszystkich dostępnych portach. Wkładki SFP muszą być całkowicie

kompatybilne z dostarczanymi urządzeniami i zapewniać obsługę maksymalnej prędkości transmisji danych, jaką oferowane urządzenia są w stanie obsłużyć. Dodatkowo, Wykonawca zobowiązany jest do dostarczenia dokumentacji technicznej, potwierdzającej kompatybilność wkładek z urządzeniami. Wymagane jest aby dokumentacja techniczna wraz z wkładkami SFP były dostarczone równocześnie z load balancerami.

Wymagania Techniczne:

Architektura systemu

1. Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest, aby system pracował w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta. Nie dopuszcza się, aby elementy funkcji podstawowych zastosowane w systemie były opracowane przez firmy trzecie.
3. Powinna istnieć możliwość implementacji systemu w trybach: one-arm, reverse proxy, transparent proxy.
4. W zakresie sieciowym wymagana jest obsługa IEEE 802.3ad link aggregation.
5. Produkt nie powinien posiadać ograniczeń co do ilości obsługiwanych serwerów.
6. Powinna istnieć możliwość zdefiniowania co najmniej 10 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu.

Wymagane mechanizmy High Availability

1. System musi mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive oraz Active-Active.
2. Elementy systemu realizujące funkcje podstawowe muszą zostać dostarczone w postaci klastra.
3. Klastrowanie N+1 bazujące na Stateful session failover zarówno w trybie Active-Passive jak i Active-Active.
4. Synchronizacja konfiguracji pomiędzy elementami klastra w czasie rzeczywistym.
5. Pływające adresy IP oraz grupy dla Stateful failover. Failover jest anonsowany dla sąsiednich urządzeń sieciowych używając Gratuitous ARP.
6. Wbudowane mechanizmy decyzji o failover w oparciu o: reboot systemu, niedostępność interfejsów, brak komunikacji Heartbeat, brak dostępności adresu IP.
7. Synchronizacja konfiguracji po przeładowaniu urządzenia jak i w czasie pracy.

Parametry fizyczne systemu

1. System realizujący funkcje podstawowe musi dysponować minimum:
   - 4 portami Gigabit Ethernet RJ-45.
   - 4 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. Wbudowany port konsoli szeregowej.
3. Powierzchnia dyskowa typu SSD - minimum 120 GB.
4. Redundantne zasilanie typu hot-swap.

5. Obudowa urządzenia o wysokości do 1U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.

Parametry wydajnościowe

1. Przepływność: nie mniej niż 15 Gbps w warstwie 4 i nie mniej niż 12 Gbps w warstwie 7.
2. Ilość nowych połaczeń na sekundę w warstwie 4 – nie mniej niż 400 tysięcy.
3. Ilość transakcji HTTP na sekundę przy balansowaniu w warstwie 4 – nie mniej niż 1.5 miliona.
4. Ilość równoczesnych połączeń w warstwie 4 – nie mniej niż 12 milionów.
5. Ilość nowych połączeń na sekundę w warstwie 7 (1 połączenie obsługuje jedno żądanie http) – nie mniej niż 120 000.
6. Ilość nowych połączeń SSL (długość klucza 2048) na sekundę w warstwie 7 (1 połączenie obsługuje jedno żądanie http) – nie mniej niż 14 000.
7. Przepływność ruchu szyfrowanego SSL – nie mniej niż 6 Gbps.
8. Przepływność ruchu poddanego kompresji – nie mniej niż 10 Gbps.

Podstawowe funkcje systemu

System musi realizować co najmniej poniższe funkcje:

1. Podział obciążenia (loadbalancing) dla protokołów:
   - dns
   - ftp
   - http
   - https
   - ip
   - mysql
   - DIAMETER
   - radius
   - rdp
   - rtmp
   - rtsp
   - sip
   - smtp
   - tcp
   - udp
   - mssql – pozwala przekazywać połączenia read do wielu serwerów z puli jednocześnie przesyłając polecenie write tylko do jednego z nich
2. Mechanizmamy podziału obciążenia:
   - Round Robin
   - Weighted Round Robin
   - Least Connection
   - Fastest Response
   - Dynami Load
3. Wsparcie dla mechanizmów server persistence:
   - Source-IP
   - Source-IP Hash
   - Source-IP/Port Hash

- Hash Header
- Hash Request
- Persistent Cookie
- Rewrite Cookie
- Insert Cookie
- Hash Cookie
- Embedded Cookie
- RADIUS Attribute
- SSL Session ID
- RDP Cookie
- SIP Call ID

4. Weryfikacja stanu pracy serwerów, co najmniej w oparciu o protokoły:
   - dns
   - ftp
   - http
   - https
   - icmp
   - imap4
   - l2-detection
   - mysql
   - DIAMETER
   - pop3
   - radius accounting
   - radius
   - rtsp
   - sip
   - sip-tcp
   - smtp
   - snmp
   - snmp-custom
   - ssh
   - tcp
   - tcp-echo
   - tcphalf
   - tcpssl
   - udp
   - LDAP
   - Oracle
5. Możliwość kontroli produkcyjnej przy uruchamianiu serwerów (warm up rate limiting) oraz przy ich konserwacji (session ramp down)
6. Content routing.
7. Funkcja podmiany zawartości - content rewriting.
8. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”.
9. Obsługa języków skryptowych, umożliwiających manipulowanie żądaniami i odpowiedziami w transakcjach, z funkcją debugowania działania skryptów.

10. Podział obciążenia pomiędzy kilka łączy z funkcjami: health check oraz persistence, przy zastosowaniu metod rozkładania ruchu
11. Wyjściowy multi-homing Link Load Balancing używając funkcji virtual tunnel (enkapsulacja GRE) przy wielu łączach wychodzących przy zastosowaniu metod rozkładania ruchu
12. Load balancing serwerów pomiędzy różnymi data center.
13. Global Load ballancing w oparciu o protokół DNS.
14. Obsługa DNSSEC z możliwością definiowania list kontroli dostępu.
15. Możliwość zdefiniowania co najmniej 512 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
16. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
    - Protokołów dynamicznego routingu w oparciu o protokoły: OSPF oraz BGP
17. System musi wspierać IPv4 oraz IPv6
18. System musi posiadać wbudowaną integrację dla aplikacji opartych o microserwisy

Wymagane funkcje w zakresie SSL-offload:

1. Obsługa SSL Forward Proxy.
2. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3.
3. Bezpieczne dostarczanie aplikacji przy programowym wsparciu szyfrowania SSL.
4. Wparcie formatów certyfikatów: .cer, .pem, and .pfx (PKCS12).
5. Backup i odtwarzanie certyfikatów oraz kluczy prywatnych na dysk lokalny za pośrednictwem interfejsu GUI.
6. Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
7. Możliwość generowania CSR (Certificate Signing Request), self-signed Certificate oraz klucza prywatnego dla określonego hosta.
8. Możliwość dostosowania komunikatów błędów dla zdarzeń SSL.
9. Przepisywanie nagłówka HTTP do HTTPS Host, Request URL, Referer oraz jego manipulację za pomocą skryptów.
10. Wsparcie SSL end-to-end, jako SSL Server i/lub jako SSL Client.
11. Weryfikacja certyfikatu klienta, CRL (HTTP, FTP, LDAP) przez http, SCEP oraz OSCP.
12. Wspierane algorytmy, co najmniej: Elliptic Curve Diffie-Helman, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-SHA, ECDHE-RSA-RC4-SHA, ECDHE-RSA-DES-CBC3-SHA.
13. Wsparcie rozszerzeń TLS SNI w połączeniach: client <-> ADC oraz ADC <-> server.
14. Wspiercie wersji SSL/TLS dla serwerów wirtualnych oraz rzeczywistych: SSL, TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3.

Wymagane funkcje w zakresie akceleracji aplikacji:

1. Optymalizacja wydajności przy użyciu TCP connection multiplexing oraz TCP buffering.
2. Obsługa w czasie rzeczywistym tzw. Dynamic Web Content Compression w celu redukcji obciążenia serwerów z opcją wyboru typu kontentu oraz URI.
3. Selektywna kompresja dla typów MIME, co najmniej: Text, HTML, XML, Java Scripts, CSS, Custom (images).
4. Zaawansowany i wydajny Web cache bazujący na pamięci RAM.
5. W zakresie HTTP cache'owanie obiektów statycznych oraz dynamicznych.

6. Konfiguracja reguł w oparciu, o które działa cache. Powinny one uwzględniać co najmniej: max object size, TTL objects, refresh time interval.
7. Statystyki dostępu do cache bazujące na IP lub http hosts.
8. Obsługa Rate shaping oraz QoS dla: źródła, przeznaczenia i usług.

Wymagane funkcje w zakresie bezpieczeństwa aplikacji:

1. Ochrona przed atakami SYN flood oraz SYN Cookie.
2. Stateful firewall dla IPv4 oraz IPv6.
3. Funkcje Web Application Firewall z analizą w oparciu o sygnatury ochrony aplikacji web dostarczane przez producenta rozwiązania i aktualizowane zgodnie z harmonogramem.
4. Mechanizmy analizy i ochrony dla: XSS/SQL injection, HTTP protocol constraints, URL protection, wykrywanie botów, ochrona przed atakami typu Brute force.
5. HTTP authentication.
6. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
7. Wsparcie Geo-IP dla ochrony przed DDoS.
8. Limitowanie połączeń w oparciu o polityki.
9. Pełna obsługa OWASP top 10
10. Kreator pomagający w budowaniu polityki w warstwie 7
11. Wbudowany mechanizm CAPTCHA
12. Mechanizm API security Gateway pozwalający filtrować zapytania API pod kątem wyjątków bezpieczeństwa
13. Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall'u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcjonalności.
14. Skaner aplikacji WWW realizowany bezpośrednio na load balancerze lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcjonalności.
15. Wsparcie dla walidacji OpenAPI, JSON i XML.

Wymagane funkcje dodatkowe

1. Kontrola antywirusowa realizowana na systemie podziału obciążenia lub zewnętrznym systemie w oparciu o protokół icap. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
2. W ramach postępowania wymaganym jest dostarczenie licencji upoważniającej do współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
3. Analiza komunikacji HTTP w oparciu o bazy URL, dostarczane przez producenta rozwiązania.
4. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
5. Uwierzytelnianie użytkowników w oparciu o: lokalną bazę, LDAP, NTLM, RADIUS, Kerberos, SAML 2.0.

6. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
7. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
8. Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day.
9. Specjalny connector dla rozwiązania Kubernetes powalający synchronizować obiekty (service, nod, pod) i aktualizować je automatycznie.
10. Możliwość wykorzystania tokenów do zapewnienia bezpiecznego logowania do systemu.
11. Możliwość przełączenia systemu w tryb inspekcji SSL, z możliwością uruchomienia kategoryzacji filtrowanych stron internetowych.

Zarządzanie

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, SNMP v1, v2c, v3.
2. Musi dostarczać w GUI informacji o zalogowanych administratorach.
3. Możliwość aktualizacji oprogramowania, backupu i odtwarzania konfiguracji z poziomu GUI.
4. Wsparcie dla REST API do integracji z innymi produktami.
5. Wbudowane narzędzie pozwalające na podgląd komunikacji sieciowej, np. Packet Capture.
6. System musi posiadać co najmniej dwie partycje, na których przechowywane jest oprogramowania i konfiguracja.

Logowanie i Raportowanie

1. System musi zapewniać lokalne logowanie oraz raportowanie.
2. Możliwość logowania do wielu zewnętrznych serwerów syslog z możliwością określenia facility.
3. Obsługa powiadomień o zdarzeniach systemowych mailem.
4. Powiadomienia o zdarzeniach systemowych za pośrednictwem trapów SNMP, w tym co najmniej zużycie: CPU, RAM, Dysku.
5. Integracja ze Splunk

Sygnatury, subskrypcje

1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
   - Sygnatury ochrony dla aplikacji www na okres 36 miesięcy.
   - Sygnatury IPS na okres 36 miesięcy.
   - Sygnatury antywirusowe na okres 36 miesięcy.
   - Bazy reputacyjne adresów IP na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy od dnia zawarcia umowy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Zgłoszenia serwisowe będą

przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. W tym celu Wykonawca winien przedłożyć dokumenty:

- Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

2. Wykonawca będzie świadczył usługi wsparcia na dodatkowe zmiany konfiguracyjne i rozwiązywanie problemów z dostarczonym rozwiązaniem w liczbie 180 godzin przez okres 36 miesięcy od dnia zawarcia umowy lub do momentu wyczerpania środków.