

Załącznik nr 1 do SWZ – SOPZ
SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa urządzeń Application Delivery Controller (ADC) z wbudowaną obsługą funkcji Web Application Firewall (WAF) oraz Global Server Load Balancing (GSLB) w ramach projektu CCN”

1. Przedmiot zamówienia

Lp.	Przedmiot dostawy	Liczba sztuk dostarczanego Sprzętu	Termin dostawy
1.	Urządzenie Application Delivery Controller (ADC) z wbudowaną obsługą funkcji Web Application Firewall (WAF).	4 szt. (2 klastry HA)	do 4 tygodni od dnia zawarcia Umowy
2.	Urządzenie Global Server Load Balancing (GSLB).	4 szt. (2 klastry HA)	do 4 tygodni od dnia zawarcia Umowy
3.	System lub systemy centralnego zarządzania dla wszystkich funkcjonalności oferowanego rozwiązania (ADC, WAF oraz GSLB).	1 kpl.	do 4 tygodni od dnia zawarcia Umowy
4.	Wkładka światłowodowa QSFP+ 40Gb wariant LR, jednomodowa, LC, zgodna z oferowanym Application Delivery Controller.	8 szt.	do 4 tygodni od dnia zawarcia Umowy
5.	Wkładka światłowodowa SFP+ 10Gb wariant LR, jednomodowa, LC, zgodna z oferowanym Application Delivery Controller.	8 szt.	do 4 tygodni od dnia zawarcia Umowy
6.	Wkładka światłowodowa SFP+ 10Gb wariant LR, jednomodowa, LC, zgodna z oferowanym Global Server Load Balancing.	8 szt.	do 4 tygodni od dnia zawarcia Umowy
7.	Wkładka światłowodowa QSFP+ 40Gb wariant LR, jednomodowa, LC, zgodna z Juniper.	8 szt.	do 4 tygodni od dnia zawarcia Umowy
8.	Wkładka światłowodowa SFP+ 10Gb wariant LR, jednomodowa, LC, zgodna z Juniper.	24 szt.	do 4 tygodni od dnia zawarcia Umowy
9.	Wkładka światłowodowa SFP28 25Gb wariant LR, jednomodowa, LC, zgodna z Juniper.	8 szt.	do 4 tygodni od dnia zawarcia Umowy
10.	Patchcord światłowodowy, jednomodowy (duplex), Uniboot LC/PC - Uniboot LC/APC - 3m lub dłuższy (zgodny z wymaganiami)	28 szt.	do 4 tygodni od dnia zawarcia Umowy
11.	Wsparcie online inżyniera Wykonawcy – godziny do dowolnego wykorzystania w ciągu trwania wsparcia (rozliczenie godzinowe), jedna godzina to 60 minut	120 godz.	na żądanie w okresie obowiązywania wsparcia, tj. w okresie jednego roku od dnia podpisania protokołu odbioru rozwiązania, o którym mowa w pkt 1-10 powyżej

12.	Szkolenie (poziom podstawowy) autoryzowane przez producenta urzędów, stacjonarne lub zdalne z zakresu oferowanego rozwiązania dla 8 osób (zgodnie ze wskazaniem Zamawiającego). Szkolenie zakończone wydaniem certyfikatu uczestnictwa wraz z dostarczeniem materiałów szkoleniowych.	1 szt.	do 12 tygodni od dnia zawarcia Umowy
13.	Szkolenie (poziom zaawansowany) autoryzowane przez producenta urzędów, stacjonarne lub zdalne z zakresu oferowanego rozwiązania dla 8 osób (zgodnie ze wskazaniem Zamawiającego). Szkolenie zakończone wydaniem certyfikatu uczestnictwa wraz z dostarczeniem materiałów szkoleniowych.	1 szt.	do 12 tygodni od dnia zawarcia Umowy

2. Wymagania ogólne

Numer wymagania	Opis wymagania
1	O ile inaczej nie zaznaczono, wszelkie zapisy zawierające parametry techniczne należy odczytywać jako parametry minimalne.
2	Dostarczany Sprzęt musi być fabrycznie nowy, nieużywany, nieregenerowany, kompletny, wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego. Przez stwierdzenie "fabrycznie nowy" należy rozumieć sprzęt opakowany oryginalnie (opakowanie musi być nienaruszone i posiadać zabezpieczenie zastosowane przez producenta). Przez "wadę fizyczną" należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia.
3	Sprzęt musi zawierać wszystkie niezbędne oprogramowanie zapewniające jego pełną funkcjonalność, wraz z bezterminowym prawem do jego użytkowania przez Zamawiającego.
4	Sprzęt musi pochodzić z autoryzowanego kanału dystrybucji producenta i być objęty serwisem producenta, a wsparcie techniczne producenta będzie obsługiwane w języku polskim lub angielskim.
5	Oferent powinien dysponować autoryzacją producenta lub autoryzowanego partnera/dystrybutora producenta w zakresie sprzedaży oferowanych rozwiązań. Autoryzacja musi jednoznacznie potwierdzać, że Oferent jest uprawniony do dystrybucji, sprzedaży oraz świadczenia wsparcia dla oferowanego rozwiązania, przy czym autoryzacja musi obejmować możliwość realizacji tych działań na terytorium Rzeczypospolitej Polskiej.

3. Kryteria równoważności

Numer wymagania	Opis wymagania
1	W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne”.
2	W sytuacjach, kiedy Zamawiający opisuje szczegółowy przedmiot zamówienia poprzez odniesienie się do norm europejskich, ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy PZP, Zamawiający dopuszcza rozwiązania równoważne, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne”.
3	Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki Sprzęt, który posiada parametry techniczne i/lub funkcjonalne co najmniej równe do określonych w SOPZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy lub usługi spełniają wymagania określone przez Zamawiającego.

4. Wymagania szczegółowe

Poniższe wymagania dla urządzeń ADC z wbudowaną obsługą funkcji WAF oraz GSLB muszą być spełnione przez każde z urządzeń wchodzących w skład klastra wysokiej dostępności (HA) danego rozwiązania. Wszystkie urządzenia w danym rozwiązaniu muszą indywidualnie spełniać wymagania zawarte w SOPZ. W ramach klastra należy dostarczyć urządzenia o identycznych modelach, wydajności oraz funkcjonalnościach, wyposażone w taki sam zestaw licencji. Wszystkie opisane funkcjonalności muszą zostać dostarczone wraz z odpowiednim licencjonowaniem, jeżeli jest ono wymagane. Urządzenia muszą być gotowe do pracy w momencie odbioru.

Przedmiotem zamówienia jest dostawa do Zamawiającego fabrycznie nowego sprzętu, udzielenie przez Wykonawcę gwarancji na Sprzęt i Oprogramowanie oraz zapewnienie na oferowany Sprzęt i Oprogramowanie serwisu gwarancyjnego i wsparcia technicznego.

Application Delivery Controller z wbudowaną obsługą Web Application Firewall
Minimalne wartości wymagane przez Zamawiającego
<p>Specyfikacja urządzenia:</p> <p>I. Wymagania ogólne</p> <p>1. W ramach rozwiązania należy zaoferować łącznie 4 urządzenia o identycznych parametrach określonych w niniejszej specyfikacji. Urządzenia muszą być specjalizowanymi urządzeniami sieciowymi (tzw. appliance) mogącymi pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby i Active/Active.</p>

Application Delivery Controller z wbudowaną obsługą Web Application Firewall	
Minimalne wartości wymagane przez Zamawiającego	
2.	Oferowane rozwiązanie musi obsługiwać równoważenie obciążenia na poziomach Layer-3, Layer-4 i Layer-7. Równoważenie obciążenia na poziomie Layer-7 musi być realizowane na podstawie informacji o ruchu w warstwie aplikacji oraz operacji wykonywanych na poziomie aplikacji.
3.	Oferowane rozwiązanie musi jednocześnie obsługiwać funkcjonalność WAF (Web Application Firewall).
4.	Zamawiane urządzenia muszą być dostarczone wraz z platformą centralnego zarządzania w postaci maszyny wirtualnej lub rozwiązania appliance. Zamawiający dopuszcza aby urządzenia ADC i GSLB były obsługiwane przez ten sam system centralnego zarządzania.
5.	Urządzenia muszą być przystosowane do montażu w szafie rack 19 cali.
6.	Urządzenie musi być wyposażone w redundantne zasilacze dostosowane do napięcia zmiennego 220-230V. Wymagana jest redundancja w modelu 1:1, tzn. awaria pojedynczego zasilacza lub jednego z dwóch obwodów zasilających nie skutkuje degradacją funkcjonalną urządzenia.
7.	Urządzeniu musi umożliwiać wymianę uszkodzonego zasilacza w trakcie pracy urządzenia.
8.	Urządzenie musi być chłodzone przepływem powietrza w schemacie od przodu do tyłu. Za przód urządzenia przyjmuje się stronę z interfejsami ruchu produkcyjnego.
9.	Urządzenia muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane).
II. Interfejsy urządzenia	
1.	Urządzenia muszą być wyposażone co najmniej w następujące interfejsy, zgodne z odpowiednimi standardami IEEE 802.3: <ul style="list-style-type: none"> a) 4 porty 10GbE. Typ złącza interfejsu musi być określany przez wymienny moduł SFP+. b) 4 porty 40GbE. Typ złącza interfejsu musi być określany przez wymienny moduł QSFP+.
2.	Urządzenia muszą zapewniać pełną współpracę z modułami optycznymi pochodzącymi od producentów trzecich (Third-Party) i zgodnymi ze standardem MSA (Multi-Source Agreement). Zamawiający wymaga, aby urządzenia nie posiadały blokad programowych, które uniemożliwiałyby uruchomienie łącza lub ograniczały parametry transmisji po zastosowaniu modułu innego niż producenta urządzenia. Zastosowanie modułów optycznych producentów trzecich nie może stanowić podstawy do unieważnienia gwarancji na całe urządzenie ani do odmowy świadczenia wsparcia technicznego przez dostawcę lub producenta dostarczanego rozwiązania. Zamawiający nie wymaga, aby producent urządzenia świadczył wsparcie techniczne dla wszystkich modułów optycznych dostępnych na rynku ani aby moduły producentów trzecich były certyfikowane przez producenta urządzenia.

Application Delivery Controller z wbudowaną obsługą Web Application Firewall	
Minimalne wartości wymagane przez Zamawiającego	
<p>Wymaganiem Zamawiającego jest natomiast, aby zastosowanie modułów zgodnych ze standardem MSA:</p> <ul style="list-style-type: none"> a) nie powodowało blokady programowej interfejsu, b) nie ograniczało parametrów transmisyjnych portu, c) nie skutkowało unieważnieniem gwarancji na całe urządzenie ani odmową świadczenia wsparcia technicznego w zakresie niezwiązanym bezpośrednio z zastosowanym modułem. <p>3. Wszystkie interfejsy urządzenia objęte powyższą specyfikacją muszą znajdować się po tej samej jego stronie zwanej dalej stroną przednią. Zastrzeżenie to nie obejmuje interfejsów dedykowanych do zarządzania urządzeniem.</p> <p>4. Urządzenie musi posiadać porty do konfiguracji wysokiej dostępności (HA) o przepustowości nie mniejszej niż 1GE. Porty te nie wliczają się do liczby wymaganych interfejsów podanych w punkcie 1.</p> <p>5. Urządzenie musi być wyposażone w co najmniej jeden port szeregowy konsoli zarządzania oraz jeden port OOB management 1GbE RJ-45.</p> <p>6. System musi być wyposażony w lokalną, przestrzeń dyskową do składowania lokalnie logów oraz przechowywania konfiguracji.</p>	
III. Wymagania funkcjonalne Application Delivery Controller	
<p>1. Urządzenie muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q i obsługiwać minimum 4000 znaczników VLAN.</p> <p>2. Urządzenia muszą zapewniać agregację portów oraz wspierać protokół LACP.</p> <p>3. Urządzenia muszą wspierać Jumbo Frames.</p> <p>4. Urządzenia muszą obsługiwać sprzętowo routing IPv4 oraz IPv6, pakiety muszą być przetaczane bez udziału procesora zarządzającego urządzeniem.</p> <p>5. Urządzenia muszą obsługiwać routing statyczny oraz co najmniej następujące protokoły routingu dynamicznego: IS-IS, OSPF oraz BGPv4.</p> <p>6. Urządzenia muszą obsługiwać translację adresów NAT.</p> <p>7. Funkcje równoważenia obciążenia muszą obsługiwać zarówno protokół IPv4 jak i IPv6.</p> <p>8. Urządzenia oferowane w ramach rozwiązania muszą wspierać tworzenie wirtualnych podsystemów, które muszą działać w izolacji na poziomie aplikacji (izolacja tylko na poziomie routingu nie będzie wystarczająca). Jeśli wymagane są dodatkowe licencje, muszą one być uwzględnione w ofercie.</p> <p>9. Urządzenia muszą umożliwiać pracę w trybach: transparentnym oraz reverse proxy.</p> <p>10. Urządzenia muszą posiadać następujące funkcje:</p> <ul style="list-style-type: none"> a) równoważenie obciążenia serwerów i aplikacji, b) równoważenie obciążenia łączy wychodzących (outbound link load balancing). 	

Application Delivery Controller z wbudowaną obsługą Web Application Firewall	
Minimalne wartości wymagane przez Zamawiającego	
11. System musi obsługiwać co najmniej następujące algorytmy równoważenia obciążenia:	<ul style="list-style-type: none"> a) Round Robin, b) Weighted Round Robin, c) Least Connections, d) Weighted Least Connections, e) Fastest Response, f) Service Least Connection, g) Link Cost Load Balance, h) Source IP Hash, i) Least Request.
12. Urządzenia muszą obsługiwać równoważenie obciążenia dla szerokiego zakresu protokołów aplikacyjnych i transportowych, obejmujących co najmniej:	<ul style="list-style-type: none"> a) ICMP, b) TCP, c) UDP, d) HTTP, e) HTTPS, f) FTP, g) RTSP, h) SMTP, i) POP3, j) SNMP, k) DNS, l) RADIUS, m) LDAP.
13. Urządzenia muszą obsługiwać funkcje buforowania treści HTTP (HTTP caching) oraz kompresji HTTP (HTTP compression) w celu optymalizacji wydajności aplikacji.	
14. Rozwiązanie musi zapewniać obsługę Application Level Gateway (ALG).	
15. Urządzenia muszą wspierać mechanizmy skryptowania lub programowalne reguły logiczne umożliwiające zaawansowane sterowanie, kierowanie oraz modyfikację ruchu aplikacyjnego, w tym podejmowanie decyzji na podstawie parametrów sesji, nagłówków protokołów oraz stanu aplikacji.	
16. Urządzenia muszą zapewniać mechanizmy kontroli stanu pracy serwerów i usług (health check), umożliwiające monitorowanie zarówno dostępności serwera, jak i poprawności działania aplikacji. Obsługiwane metody muszą obejmować co najmniej:	<ul style="list-style-type: none"> a) ICMP, b) TCP, c) UDP, d) HTTP, e) HTTPS, f) FTP,

Application Delivery Controller z wbudowaną obsługą Web Application Firewall	
Minimalne wartości wymagane przez Zamawiającego	
<ul style="list-style-type: none"> g) RTSP, h) SMTP, i) POP3, j) SNMP, k) DNS, l) RADIUS, m) LDAP. 	<p>17. Urządzenia muszą zapewniać zaawansowaną obsługę kontroli stanu serwerów z wykorzystaniem zewnętrznych skryptów, w tym co najmniej w językach:</p> <ul style="list-style-type: none"> a) Python, b) TCL, c) Shell, d) Perl. <p>18. Operacje kryptograficzne SSL/TLS, w tym w szczególności SSL Offload, muszą być realizowane z wykorzystaniem dedykowanych zasobów sprzętowych (procesorów kryptograficznych lub kart akceleryjnych). Wszelkie wymagane komponenty sprzętowe oraz licencje muszą być uwzględnione w ofercie.</p> <p>19. Urządzenia muszą obsługiwać mechanizmy przywiązania sesji (Session Persistence) co najmniej w oparciu o następujące atrybuty:</p> <ul style="list-style-type: none"> a) cookie (hash, rewrite, custom, insert, passive), w tym możliwość bazowania na cookie aplikacyjnym lub jego części, b) szyfrowanie cookie generowanych przez system w celu utrzymania przywiązania sesji, c) adres źródłowy klienta, d) identyfikator sesji SSL, e) adres docelowy. <p>20. Rozwiązanie musi zapewniać funkcję SSL Offload, umożliwiającą odciążenie aplikacji i serwerów od operacji kryptograficznych, co najmniej dla protokołów HTTPS oraz SMTPS.</p> <p>21. Urządzenia muszą obsługiwać certyfikaty cyfrowe z kluczami typu ECDSA oparte na kryptografii krzywych eliptycznych (ECC), zarówno po stronie klienta, jak i po stronie puli serwerów.</p> <p>22. Wymagane jest sprzętowe wsparcie dla algorytmów kryptograficznych, w tym co najmniej: AES, AES-GCM, RSA, DSA, DH, ECDSA, ECDH oraz SHA-2, wraz z obsługą mechanizmu Perfect Forward Secrecy (PFS).</p> <p>23. Dla protokołu TLS 1.2 wymagana jest obsługa algorytmu AES-GCM zarówno po stronie klienta, jak i po stronie puli serwerów.</p> <p>24. Urządzenia muszą zapewniać pełne wsparcie dla protokołu TLS w wersji 1.3.</p> <p>25. Urządzenia muszą obsługiwać certyfikaty podpisane algorytmami opartymi o funkcję skrótu SHA-2, zarówno po stronie klienta, jak i po stronie puli serwerów.</p>

Application Delivery Controller z wbudowaną obsługą Web Application Firewall

Minimalne wartości wymagane przez Zamawiającego

26. Urządzenie musi umożliwiać przypisywanie wielu różnych certyfikatów TLS/SSL do jednego adresu IP, w zależności od nazwy domenowej aplikacji, z wykorzystaniem mechanizmu Server Name Indication (SNI). Funkcjonalność ta musi umożliwiać jednoczesną ochronę oraz obsługę wielu aplikacji lub serwisów webowych działających pod różnymi nazwami domenowymi na wspólnym adresie IP.
27. Funkcjonalność ta musi umożliwiać jednoczesną ochronę oraz obsługę wielu aplikacji lub serwisów webowych działających pod różnymi nazwami domenowymi na wspólnym adresie IP.
28. Urządzenia muszą zapewniać ochronę przed atakami DDoS.
29. Urządzenia muszą obsługiwać konta użytkowników z różnymi poziomami uprawnień administracyjnych, umożliwiając kontrolę dostępu do konfiguracji, monitoringu i zarządzania systemem.

IV. Parametry wydajnościowe

1. Urządzenie musi mieć minimalną przepustowość Layer-7 wynoszącą 40 Gbps. Przepustowość Layer-4 nie może być mniejsza niż ta wartość.
2. Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:
 - a) 500 k nowych połączeń Layer-7 na sekundę (CPS),
 - b) 1 M nowych połączeń Layer-4 na sekundę (CPS),
 - c) 90 M równoczesnych połączeń Layer-4,
 - d) 25 k połączeń SSL na sekundę (CPS) dla kluczy RSA 2048-bitowych,
 - e) 15 k połączeń SSL CPS dla ruchu SSL opartego na ECDHE,
 - f) przepustowość SSL na poziomie co najmniej 8 Gbps dla ruchu szyfrowanego.
3. Urządzenia muszą być wyposażony w dyski SSD.
4. Wszystkie funkcje i parametry wydajnościowe systemu muszą być weryfikowalne na oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub protokoły testów wykonane przez producenta.

V. Wymagania funkcjonalne Web Application Firewall

1. Rozwiązanie musi zawierać funkcje Web Application Firewall (WAF) do wykrywania i blokowania ataków na aplikacje web.
2. WAF musi obsługiwać następujące tryby pracy:
 - a) tryb blokowania (wykrywanie, logowanie, blokowanie)
 - b) tryb monitorowania (wykrywanie, logowanie).
3. WAF musi obsługiwać zarówno IPv4, jak i IPv6.
4. Do raportowania/analiz wysyłanych do zarządzania w chmurze mogą być używane wyłącznie metadane (bez faktycznego ruchu klienta).
5. Logowanie podejrzanych zdarzeń musi zawierać co najmniej:
 - a) podjęte działanie (blokuj/zezwalaj)
 - b) adres IP strony inicjującej połączenie wraz z informacją o kraju

Application Delivery Controller z wbudowaną obsługą Web Application Firewall	
Minimalne wartości wymagane przez Zamawiającego	
	<ul style="list-style-type: none"> c) adres URL wybranego zasobu d) typ ataku e) znacznik czasu f) kod CVE (jeśli dotyczy danego zdarzenia)
6.	<p>WAF musi zapewniać ochronę przed atakami z listy OWASP Top 10, a w szczególności:</p> <ul style="list-style-type: none"> a) SQL Injection, b) Cross-Site Scripting, c) Command Injection, d) Path Traversal, e) Backdoors, f) Brute Force, g) Cookie Poisoning, h) Server-Side Request Forgery, i) Log4J
7.	Ochrona musi obejmować ataki na strony logowania i rejestracji użytkowników.
8.	WAF musi zapewniać ochronę API dla REST, SOAP, JSON, XML i GraphQL.
9.	<p>Ochrona musi umożliwiać definiowanie progów szybkości (rate-limit) dla wykrywania ataków. W przypadku przekroczenia zdefiniowanego progu przez źródło ruchu, jego adres IP musi zostać automatycznie oznaczony jako złośliwy, z możliwością:</p> <ul style="list-style-type: none"> a) tymczasowej lub trwałej blokady ruch z danego adresu IP, b) rejestracji zdarzenia w systemie logowania i raportowania
10.	<p>WAF musi wykrywać anomalie w żądaniach/odpowiedziach HTTP, takie jak:</p> <ul style="list-style-type: none"> a) Nieprawidłowe lub nietypowe ścieżki URI, b) Występowanie znaków zerowych (null bytes), c) skompresowane treści żądań typu POST (np. np. gzip, deflate), d) podwójne lub nieprawidłowe kodowanie danych (w tym URL encoding i Unicode), e) nietypowe lub nieoczekiwane kody odpowiedzi HTTP, f) brakujące lub nietypowe nagłówki HTTP, w szczególności User-Agent, g) żądana generowanych przez narzędzia do skanowania i testów bezpieczeństwa, h) próby rozdzielania odpowiedzi HTTP (HTTP Response Splitting / CRLF Injection).
11.	WAF musi mieć możliwość automatycznego pobierania i aktualizacji list reputacyjnych (threat intelligence),
12.	WAF musi zapewniać selektywne blokowanie wyłącznie żądań jednoznacznie zidentyfikowanych jako ataki. Prawidłowy (czysty) ruch aplikacyjny musi być przekazywany do aplikacji, nawet jeśli pochodzi adresu IP o niskiej reputacji.
13.	Urządzenie musi umożliwiać identyfikację oraz obsługę ruchu na podstawie rzeczywistego adresu IP klienta, w tym adresu przekazywanego w nagłówkach HTTP (np. X-Forwarded-For lub równoważnych).
14.	WAF musi umożliwiać tworzenie reguł bezpieczeństwa opartych na wielu warunkach logicznych. Reguły muszą obsługiwać operatory logiczne AND oraz OR oraz umożliwiać filtrowanie i korelację na podstawie co najmniej następujących parametrów:

Application Delivery Controller z wbudowaną obsługą Web Application Firewall	
Minimalne wartości wymagane przez Zamawiającego	
a)	kraj pochodzenia ruchu (geolokalizacja),
	domena (Host / SNI),
c)	źródłowy adres IP,
	metoda HTTP (GET, POST, PUT, DELETE itp.),
e)	ścieżka URI,
	parametr żądania POST,
g)	parametr zapytania (query parameter),
	cookie żądania,
i)	nagłówek żądania HTTP,
	kod odpowiedzi HTTP,
k)	nagłówek odpowiedzi HTTP,
15.	WAF musi umożliwiać tworzenie i zarządzanie oddzielnymi zestawami reguł bezpieczeństwa dla poszczególnych chronionych adresów, aplikacji lub usług, z jednoczesną możliwością definiowania i stosowania globalnego zestawu reguł wspólnego dla wszystkich chronionych zasobów.
16.	WAF musi obsługiwać blokowanie ruchu oparte na geolokalizacji kraju pochodzenia adresu IP (country-based blocking), z możliwością definiowania wyjątków.
17.	Ochrona przed nowo odkrytymi podatnościami (CVE) oraz atakami typu zero-day musi być zapewniana poprzez automatyczne, regularne aktualizacje mechanizmów detekcji, sygnatur i/lub modeli behawioralnych, bez konieczności ręcznej ingerencji administratora.
18.	WAF musi zapewniać rozbudowany interfejs monitorowania w czasie rzeczywistym (real-time monitoring) dla chronionych aplikacji, obejmujący co najmniej:
a)	ruch aplikacyjny w czasie rzeczywistym,
b)	liczbę klientów uzyskujących dostęp do aplikacji,
c)	liczbę obsługiwanych żądań,
d)	alerty bezpieczeństwa zgodne z OWASP Top 10,
e)	alerty dotyczące stanu systemu oraz wykrywanych ataków,
f)	audyt i historię zmian konfiguracji,
g)	widok incydentów bezpieczeństwa z podziałem na aplikacje,
h)	widok incydentów bezpieczeństwa z podziałem na kraje,
i)	klasyfikację i typy ataków,
j)	czas trwania wykrytych ataków,
k)	adresy URL oraz katalogi objęte atakiem,
l)	szczegóły żądań i odpowiedzi, w tym nagłówki, treść oraz atrybuty,
m)	identyfikatory CVE powiązane z atakiem, o ile mają zastosowanie.
19.	WAF musi wspierać analizę zdarzeń bezpieczeństwa w czasie rzeczywistym (real-time security event forensics), umożliwiając wyszukiwanie, filtrowanie i korelację zdarzeń według kryteriów takich jak:
a)	zablokowane lub dozwolone żądania (URI/URL),
b)	dane wiadomości (nagłówki HTTP, treść żądania/odpowiedzi),
c)	adresy IP źródłowe wraz z informacją o geolokalizacji,

Application Delivery Controller z wbudowaną obsługą Web Application Firewall	
Minimalne wartości wymagane przez Zamawiającego	
<p>d) wykryte anomalie oraz klasyfikacje zdarzeń WAF.</p> <p>20. WAF musi umożliwiać tworzenie i personalizację pulpitów nawigacyjnych (custom dashboards), w tym możliwość wyświetlania lub ukrywania określonych statystyk, metryk i informacji o atakach.</p> <p>21. WAF musi zapewniać kontrolę dostępu opartą na rolach (Role-Based Access Control – RBAC), umożliwiając definiowanie różnych poziomów uprawnień administracyjnych oraz dostępu do konfiguracji, monitoringu i raportów.</p> <p>22. Wszystkie funkcje WAF wymagające dodatkowych licencji, subskrypcji lub modułów sprzętowych bądź programowych muszą być jednoznacznie wskazane i wliczone w oferowaną cenę, bez konieczności dokupowania dodatkowych licencji w okresie obowiązywania umowy.</p>	
VI. Zarządzanie urządzeniem	
<p>1. Urządzenia muszą mieć możliwość zarządzania lokalnego z linii poleceń (CLI) oraz graficznej konsoli Web GUI z wykorzystaniem protokołów: HTTPS oraz SSH, oraz współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>2. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.</p> <p>3. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>4. Urządzenie wspiera uwierzytelnienie dostępu administracyjnego w zewnętrznej bazie użytkowników z wykorzystaniem protokołów RADIUS i/lub TACACS+.</p> <p>5. Urządzenia muszą współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach v2c i v3.</p> <p>6. Urządzenia muszą mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>7. Urządzenia posiadają wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji.</p> <p>8. Urządzenia muszą umożliwiać cofanie zmian konfiguracyjnych do poprzednich wybranych wersji.</p> <p>9. Urządzenia muszą umożliwiać zarządzania systemem tylko z określonych adresów źródłowych IP.</p> <p>10. Urządzenia muszą umożliwiać przypisywania administratorom praw dostępu do określonych części systemu. System musi pozwalać na zdefiniowanie wielu administratorów o różnym poziomie uprawnień.</p>	

Application Delivery Controller z wbudowaną obsługą Web Application Firewall

Minimalne wartości wymagane przez Zamawiającego

VII. Logowanie

1. W ramach logowania urządzenia zapewniają przekazywanie danych o: zaakceptowanym ruchu, blokowaniem ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewniają możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
2. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
3. Wykonywanie operacji deszyfrowania ruchu musi być odnotowywane w logach urządzeń w dedykowanej do tego celu sekcji.
4. Urządzenia muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą protokołu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD.
5. Urządzenia muszą mieć możliwość integracji z rozwiązaniami typu SIEM na poziomie minimum przesyłaniu logów za pomocą protokołu Syslog.
6. Urządzenia musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 100 GB na potrzeby systemu operacyjnego i logów.
7. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasób dyskowy został wymontowany z urządzenia i pozostał w jego siedzibie.

VIII. System centralnego zarządzania

Wszystkie funkcje centralnego zarządzania muszą być objęte ofertą, bez konieczności zakupu dodatkowych licencji, modułów lub subskrypcji nieuwzględnionych w ofercie. Zamawiający dopuszcza aby urządzenia ADC i GSLB były obsługiwane przez ten sam system centralnego zarządzania.

1. Rozwiązanie musi być dostarczone w postaci komercyjnej, kompletnej platformy wirtualnej (virtual appliance działającego w środowisku minimum KVM oraz VMware) lub sprzętowej (appliance), na którą składać się będą 2 urządzenia pracujące w klastrze wysokiej dostępności. W danym centrum przetwarzania będzie znajdować się jedno urządzenie.
2. System musi zapewniać centralne zarządzanie wszystkimi dostarczonymi urządzeniami i instancjami Application Delivery Controller, niezależnie od formy wdrożenia.
3. Centralny system zarządzania musi umożliwiać co najmniej:
 - a) centralną konfigurację i dystrybucję polityk ADC i WAF,
 - b) centralne zarządzanie certyfikatami SSL/TLS (import, dystrybucja, odnowienie),
 - c) centralne zarządzanie regułami bezpieczeństwa i skryptami (np. TCL lub równoważnymi),
 - d) centralne aktualizacje sygnatur bezpieczeństwa oraz mechanizmów ochrony.

Application Delivery Controller z wbudowaną obsługą Web Application Firewall	
Minimalne wartości wymagane przez Zamawiającego	
4.	System centralnego zarządzania musi zapewniać monitoring w czasie rzeczywistym, obejmujący co najmniej: <ul style="list-style-type: none">a) status i dostępność urządzeń oraz usług,b) ruch aplikacyjny i statystyki wydajnościowe,c) zdarzenia i alerty bezpieczeństwa,d) wykorzystanie zasobów systemowych.
5.	System musi umożliwiać audyt zmian konfiguracji, w tym: <ul style="list-style-type: none">a) rejestrację kto, kiedy i jakiej zmiany dokonał,b) możliwość przeglądu historii zmian,c) możliwość cofnięcia (rollback) zmian konfiguracji.
6.	System musi obsługiwać kontrolę dostępu opartą na rolach (RBAC), umożliwiając: <ul style="list-style-type: none">d) definiowanie ról użytkowników,e) przypisywanie uprawnień administracyjnych i operacyjnych,f) ograniczenie dostępu do wybranych obiektów, aplikacji lub funkcji.
7.	System centralnego zarządzania musi udostępniać interfejs programistyczny (API) umożliwiający integrację z zewnętrznymi systemami automatyzacji, orkiestracji i monitoringu.
8.	System musi pozwalać na łatwą zamianę zarządzanego urządzenia, które uległo awarii, na nowe urządzenie tego samego modelu bez konieczności ponownego wykonywania jego pełnej konfiguracji czy ręcznego przenoszenia konfiguracji.

Global Server Load Balancing**Minimalne wartości wymagane przez Zamawiającego**

Specyfikacja urządzenia:

I. Wymagania ogólne

1. W ramach rozwiązania należy zaoferować łącznie 4 urządzenia o identycznych parametrach określonych w niniejszej specyfikacji. Urządzenia muszą być specjalizowanymi urządzeniami sieciowymi (tzw. appliance) mogącymi pracować jako pojedyncze urządzenie oraz jako para wysokiej dostępności (HA) w trybach Active/Standby i Active/Active.
2. Oferowane rozwiązanie musi obsługiwać globalne równoważenia obciążenia serwerów oparte na protokole DNS.
3. Zamawiane urządzenia muszą być dostarczone wraz z platformą centralnego zarządzania w postaci maszyny wirtualnej lub rozwiązania appliance. Zamawiający dopuszcza aby urządzenia ADC i GSLB były obsługiwane przez ten sam system centralnego zarządzania.
4. Urządzenia muszą być przystosowane do montażu w szafie rack 19 cali.
5. Urządzenie musi być wyposażone w redundantne zasilacze dostosowane do napięcia zmiennego 220-230V. Wymagana jest redundancja w modelu 1:1, tzn. awaria pojedynczego zasilacza lub jednego z dwóch obwodów zasilających nie skutkuje degradacją funkcjonalną urządzenia.
6. Urządzeniu musi umożliwiać wymianę uszkodzonego zasilacza w trakcie pracy urządzenia.
7. Urządzenie musi być chłodzone przepływem powietrza w schemacie od przodu do tyłu. Za przód urządzenia przyjmuje się stronę z interfejsami ruchu produkcyjnego.
8. Urządzenia muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu (tzw. data plane) od zasobów służących do zarządzania urządzeniem (tzw. management plane).

II. Interfejsy urządzenia

1. Urządzenia muszą być wyposażone co najmniej w następujące interfejsy, zgodne z odpowiednimi standardami IEEE 802.3:
 - a) 4 porty 1/10GbE SFP/SFP+. Typ złącza interfejsu musi być określany przez wymienny moduł SFP/SFP+.Urządzenia muszą zapewniać pełną współpracę z modułami optycznymi pochodzącymi od dowolnego producenta, zgodnymi ze standardem MSA (Multi-Source Agreement). Zamawiający wymaga, aby urządzenie nie posiadało blokad programowych, które uniemożliwiałyby uruchomienie łącza lub ograniczały parametry transmisji po zastosowaniu modułu innego niż producenta urządzenia. Zastosowanie modułów optycznych producentów trzecich nie może stanowić podstawy do unieważnienia gwarancji na całe urządzenie ani do odmowy świadczenia wsparcia technicznego przez dostawcę lub producenta dostarczanego rozwiązania.

Global Server Load Balancing	
Minimalne wartości wymagane przez Zamawiającego	
<ol style="list-style-type: none"> 2. Wszystkie interfejsy urządzenia objęte powyższą specyfikacją muszą znajdować się po tej samej jego stronie zwanej dalej stroną przednią. Zastrzeżenie to nie obejmuje interfejsów dedykowanych do zarządzania urządzeniem. 3. Urządzenie musi posiadać porty do konfiguracji wysokiej dostępności (HA) o przepustowości nie mniejszej niż 1GE. Porty te nie wliczają się do liczby wymaganych interfejsów podanych w punkcie 1. 4. Urządzenie musi być wyposażone w co najmniej jeden port szeregowy konsoli zarządzania oraz jeden port OOB management GbE RJ-45. 5. System musi być wyposażony w lokalną, przestrzeń dyskową do składowania lokalnie logów oraz przechowywania konfiguracji. 	
III. Wymagania funkcjonalne Global Server Load Balancing.	
<ol style="list-style-type: none"> 1. Urządzenie muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q i obsługiwać minimum 4000 znaczników VLAN. 2. Urządzenia muszą zapewniać agregację portów oraz wspierać protokół LACP. 3. Urządzenia muszą wspierać Jumbo Frames. 4. Urządzenia muszą obsługiwać sprzętowo routing IPv4 oraz IPv6, pakiety muszą być przetaczane bez udziału procesora zarządzającego urządzeniem. 5. Urządzenia muszą zapewniać wsparcie dla protokołu IPv6, w tym obsługiwać rekordy DNS typu A (IPv4) oraz AAAA (IPv6). 6. Urządzenia muszą obsługiwać globalne równoważenia obciążenia (GSLB) oparte na protokole DNS, z możliwością pracy w trybie serwera (Authoritative DNS) oraz proxy. 7. Funkcje GSLB muszą umożliwiać stosowanie konfigurowalnych mechanizmów sprawdzania stanu zasobów (health check). 8. Mechanizmy health check muszą umożliwiać integrację z algorytmami globalnego równoważenia obciążenia. 9. W przypadku niedostępności wszystkich zasobów (członków grupy), system GSLB musi umożliwiać generowanie odpowiedzi DNS typu: <ol style="list-style-type: none"> a) NOERROR, b) NODATA. 10. Funkcje GSLB muszą umożliwiać kierowanie ruchu na podstawie geolokalizacji klienta. 11. Funkcje GSLB muszą umożliwiać stosowanie wag w politykach globalnego równoważenia obciążenia. 12. Urządzenia muszą wspierać wykorzystanie następujących metryk w politykach GSLB: <ol style="list-style-type: none"> a) Round Trip Delay Time (RTT / aRDT – active Round Trip Time) - pomiar czasu opóźnienia w obie strony, b) Connection Load - obciążenie wynikające z liczby i/lub stanu połączeń, c) Active Connections / Connection Count - liczba aktywnych połączeń, 	

Global Server Load Balancing	
Minimalne wartości wymagane przez Zamawiającego	
<p>d) Session Capacity - dostępna pojemność sesji,</p> <p>e) Number of Sessions (Num-Session) - całkowita liczba sesji,</p> <p>f) Connection Count by Site - liczba połączeń w danej lokalizacji / centrum danych.</p> <p>13. Funkcje GSLB muszą umożliwiać pomiar czasu opóźnienia w obie strony (round trip delay time).</p> <p>14. Funkcje GSLB muszą wspierać pomiar liczby aktywnych połączeń.</p>	
IV. Parametry wydajnościowe	
<p>1. Urządzenia muszą być wyposażony w dyski SSD.</p> <p>2. Wszystkie funkcje i parametry wydajnościowe systemu muszą być weryfikowalne w oparciu o oficjalną (publicznie dostępną) dokumentację producenta lub protokoły testów wykonane przez producenta.</p>	
VI. Zarządzanie urządzeniem	
<p>1. Urządzenia muszą mieć możliwość zarządzania lokalnego z linii poleceń (CLI) oraz graficznej konsoli Web GUI z wykorzystaniem protokołów: HTTPS oraz SSH, oraz współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>2. Nie jest dopuszczalne, aby istniała konieczność instalacji lub pobierania dedykowanego oprogramowania/klienta na stacji administratorów w celu zarządzania systemem.</p> <p>3. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>4. Urządzenie wspiera uwierzytelnienie dostępu administracyjnego w zewnętrznej bazie użytkowników z wykorzystaniem protokołów RADIUS i/lub TACACS+.</p> <p>5. Urządzenia muszą współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach v2c i v3.</p> <p>6. Urządzenia muszą mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>7. Urządzenia posiadają wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podgląd pakietów, monitorowanie procesowania sesji.</p> <p>8. Urządzenia muszą umożliwiać cofanie zmian konfiguracyjnych do poprzednich wybranych wersji.</p> <p>9. Urządzenia muszą umożliwiać zarządzania systemem tylko z określonych adresów źródłowych IP.</p> <p>10. Urządzenia muszą umożliwiać przypisywania administratorom praw dostępu do określonych części systemu. System musi pozwalać na zdefiniowanie wielu administratorów o różnym poziomie uprawnień.</p>	
VII. Logowanie	

Global Server Load Balancing	
Minimalne wartości wymagane przez Zamawiającego	
<ol style="list-style-type: none"> 1. W ramach logowania urządzenia zapewniają przekazywanie danych o: aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewniają możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 2. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i równoważenia ruchu. 3. Urządzenia muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą protokołu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD. 4. Urządzenia muszą się integrować z rozwiązaniami typu SIEM na poziomie minimum przesyłaniu logów za pomocą protokołu Syslog. 5. Urządzenia musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 100 GB na potrzeby systemu operacyjnego i logów. 6. W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasób dyskowy został wymontowany z urządzenia i pozostał w jego siedzibie. 	<p>VIII. System centralnego zarządzania i monitorowania</p> <p>Wszystkie funkcje centralnego zarządzania muszą być objęte ofertą, bez konieczności zakupu dodatkowych licencji, modułów lub subskrypcji nieuwzględnionych w ofercie. Zamawiający dopuszcza aby urządzenia ADC i GSLB były obsługiwane przez ten sam system centralnego zarządzania.</p> <ol style="list-style-type: none"> 1. Rozwiązanie musi być dostarczone w postaci komercyjnej, kompletnej platformy wirtualnej (virtual appliance działającego w środowisku minimum KVM oraz VMware) lub sprzętowej (appliance), na którą składać się będą 2 urządzenia pracujące w klastrze wysokiej dostępności. W danym centrum przetwarzania będzie znajdować się jedno urządzenie. 2. System musi zapewniać centralne zarządzanie wszystkimi dostarczonymi urządzeniami i instancjami Global Server Load Balancing, niezależnie od formy wdrożenia. 3. Centralny system zarządzania musi umożliwiać co najmniej: <ol style="list-style-type: none"> a) centralną konfigurację i dystrybucję konfiguracji GSLB, b) centralne zarządzanie skryptami (np. TCL lub równoważnymi). 4. System centralnego zarządzania musi zapewniać monitoring w czasie rzeczywistym, obejmujący co najmniej: <ol style="list-style-type: none"> a) status i dostępność urządzeń oraz usług, b) statystyki wydajnościowe, c) wykorzystanie zasobów systemowych. 5. System musi umożliwiać audyt zmian konfiguracji, w tym: <ol style="list-style-type: none"> a) rejestrację kto, kiedy i jakiej zmiany dokonał, b) możliwość przeglądu historii zmian, c) możliwość cofnięcia (rollback) zmian konfiguracji.

Global Server Load Balancing**Minimalne wartości wymagane przez Zamawiającego**

6. System musi obsługiwać kontrolę dostępu opartą na rolach (RBAC), umożliwiając:
 - a) definiowanie ról użytkowników,
 - b) przypisywanie uprawnień administracyjnych i operacyjnych,
 - c) ograniczenie dostępu do wybranych obiektów, aplikacji lub funkcji.
7. System centralnego zarządzania musi udostępniać interfejs programistyczny (API) umożliwiający integrację z zewnętrznymi systemami automatyzacji, orkiestracji i monitoringu.
8. System musi pozwalać na łatwą zmianę zarządzanego urządzenia, które uległo awarii, na nowe urządzenie tego samego modelu bez konieczności ponownego wykonywania jego pełnej konfiguracji czy ręcznego przenoszenia konfiguracji.

Wkładka światłowodowa SFP+ 10Gb (ADC)	
L.p.	Minimalne wartości wymagane przez Zamawiającego
1	Wkładka światłowodowa SFP+ 10Gbps wariant LR, jednomodowa, LC, zgodna z oferowanymi urządzeniami Application Delivery Controller.
2	Oferowany model musi być w pełni kompatybilny i certyfikowany przez producenta oferowanego urządzenia Application Delivery Controller (wymienione na oficjalnej liście wspieranego osprzętu producenta).
3	Zastosowanie dostarczonych wkładek nie może w żaden sposób ograniczać warunków gwarancji ani nie może wymagać ich wymiany na inny model podczas procesu diagnostycznego prowadzonego przez wsparcie techniczne producenta w przypadku zgłoszenia awarii urządzenia.

Wkładka światłowodowa QSFP+ 40Gb (ADC)	
L.p.	Minimalne wartości wymagane przez Zamawiającego
1	Wkładka światłowodowa QSFP+ 40Gbps wariant LR, jednomodowa, LC, zgodna z oferowanymi urządzeniami Application Delivery Controller.
2	Oferowany model musi być w pełni kompatybilny i certyfikowany przez producenta oferowanego urządzenia Application Delivery Controller (wymienione na oficjalnej liście wspieranego osprzętu producenta).
3	Zastosowanie dostarczonych wkładek nie może w żaden sposób ograniczać warunków gwarancji ani nie może wymagać ich wymiany na inny model podczas procesu diagnostycznego prowadzonego przez wsparcie techniczne producenta w przypadku zgłoszenia awarii urządzenia.

Wkładka światłowodowa SFP+ 10Gb (GSLB)	
L.p.	Minimalne wartości wymagane przez Zamawiającego
1	Wkładka światłowodowa SFP+ 10Gbps wariant LR, jednomodowa, LC, zgodna z oferowanymi urządzeniami Global Server Load Balancing.
2	Oferowany model musi być w pełni kompatybilny i certyfikowany przez producenta oferowanego urządzenia Global Server Load Balancing (wymienione na oficjalnej liście wspieranego osprzętu producenta).
3	Zastosowanie dostarczonych wkładek nie może w żaden sposób ograniczać warunków gwarancji ani nie może wymagać ich wymiany na inny model podczas procesu diagnostycznego prowadzonego przez wsparcie techniczne producenta w przypadku zgłoszenia awarii urządzenia.

Wkładka światłowodowa SFP+ 10Gb (Juniper)	
L.p.	Minimalne wartości wymagane przez Zamawiającego
1	Wkładka światłowodowa SFP+ 10Gbps wariant LR, jednomodowa, LC, zgodna z Juniper.
2	Oferowany model musi być w pełni kompatybilny i certyfikowany przez Juniper (wymienione na oficjalnej liście wspieranego osprzętu producenta).
3	Zastosowanie dostarczonych wkładek nie może w żaden sposób ograniczać warunków gwarancji ani nie może wymagać ich wymiany na inny model podczas procesu diagnostycznego prowadzonego przez wsparcie techniczne producenta w przypadku zgłoszenia awarii urządzenia.

Wkładka światłowodowa QSFP+ 40Gb (Juniper)	
L.p.	Minimalne wartości wymagane przez Zamawiającego
1	Wkładka światłowodowa QSFP+ 40Gbps wariant LR, jednomodowa, LC, zgodna z Juniper.
2	Oferowany model musi być w pełni kompatybilny i certyfikowany przez Juniper (wymienione na oficjalnej liście wspieranego osprzętu producenta).
3	Zastosowanie dostarczonych wkładek nie może w żaden sposób ograniczać warunków gwarancji ani nie może wymagać ich wymiany na inny model podczas procesu diagnostycznego prowadzonego przez wsparcie techniczne producenta w przypadku zgłoszenia awarii urządzenia.

Wkładka światłowodowa SFP28 25Gb (Juniper)	
L.p.	Minimalne wartości wymagane przez Zamawiającego
1	Wkładka światłowodowa SFP28 25Gbps wariant LR, jednomodowa, LC, zgodna z Juniper.
2	Oferowany model musi być w pełni kompatybilny i certyfikowany przez Juniper (wymienione na oficjalnej liście wspieranego osprzętu producenta).
3	Zastosowanie dostarczonych wkładek nie może w żaden sposób ograniczać warunków gwarancji ani nie może wymagać ich wymiany na inny model podczas procesu diagnostycznego prowadzonego przez wsparcie techniczne producenta w przypadku zgłoszenia awarii urządzenia.

Patchcordsy światłowodowe	
L.p.	Minimalne wartości wymagane przez Zamawiającego
1	Patchcordsy muszą być aktualnie produkowane i sprzedawane przez producenta patchcordów. Zamawiający nie dopuszcza patchcordów będących w opracowaniu lub będących prototypem u producenta patchcordów.
2	Patchcordsy muszą być zakończone z każdej strony pojedynczym duplexowym wtykiem typu LC Uniboot.
3	Wtyki typu LC Uniboot muszą posiadać uchwyt/mechanizm do równoczesnego odblokowania dźwigni zatrzasków dla włókien w obu złączach patchcordu światłowodowego. Uchwyt/mechanizm ten musi pozwalać na odłączenie wtyku typu LC Uniboot od złącza w panelu światłowodowym poprzez pociągnięcie osłonki wtyku typu LC Uniboot lub innego elementu będącego przedłużeniem standardowych dźwigni służących do odblokowania i odłączenia złączy światłowodowych. Nie dopuszcza się standardowych złączy światłowodowych, gdzie odłączenie złączy patchcordu od złącza w panelu światłowodowym odbywa się tylko poprzez naciśnięcie dźwigni złączy patchcordu. Nie dopuszcza się rozwiązań, gdzie pociągnięcie za patchcord światłowodowy spowoduje odłączenie złączy patchcordu od złącza w panelu światłowodowym.
4	Patchcordsy muszą posiadać dwa włókna światłowodowe jednomodowe (duplex) umieszczone w jednej wspólnej izolacji/powłoce patchcordu.
5	Odległość pomiędzy włóknami światłowodowymi we wtyku typu LC Uniboot: 6,25mm.
6	Łączna długość wtyku typu LC Uniboot wraz osłoną/tubą/odgiętką znajdującą się bezpośrednio za wtykiem typu LC Uniboot nie może przekroczyć 75 mm liczonych od czoła złącza światłowodowego do końca osłony/tuby/odgiętki.
7	Osłona/tuba/odgiętka znajdującą się bezpośrednio za wtykiem typu LC Uniboot musi być elastyczna i musi umożliwiać zgięcie patchcordu oraz musi być połączona z

Patchcordsy światłowodowe	
L.p.	Minimalne wartości wymagane przez Zamawiającego
	wtykiem typu LC Uniboot. Średnica końca osłony/tuby/odgiętki nie może być większa niż 4,5 mm.
8	Jeśli uchwyt dla równoczesnego odblokowania dźwigni zatrasków dla włókien w obu złączach patchcordu światłowodowego (będący przedłużeniem standardowych dźwigni służących do odblokowania i odłączenia złączy światłowodowych) jest elementem mocowanym do wtyku typu LC Uniboot to jego długość nie może przekroczyć 76 mm liczonych od czoła złącza światłowodowego do końca uchwytu.
9	Powłoka patchcordu światłowodowego jednomodowego SM pomiędzy wtykami typu LC Uniboot wraz z osłonami/tubami/odgiętkami musi mieć na całej swojej długości jednakową średnicę.
10	Fabryczna polaryzacja włókien światłowodowych prosta: A-A, B-B (polaryzacja prosta).
11	Wtyki typu LC Uniboot muszą umożliwiać wielokrotną zmianę polaryzacji włókien światłowodowych we wtykach typu LC Uniboot.
12	Powłoka patchcordu musi być wykonana z materiału typu LSZH (z ang. Low Smoke Zero Halogen).
13	Straty wtrąceniowe dla pojedynczego włókna światłowodowego wraz z dwoma złączami: $\leq 0,30\text{dB}$.
14	Włókna światłowodowe jednomodowe SM muszą być wykonane w standardzie G.657.A2 (OS2) (SM 9/125 μm)
15	Patchcordsy światłowodowe jednomodowe SM Uniboot muszą posiadać metrykę zawierającą co najmniej następujące informacje: a) numer/nazwę produktu, b) datę produkcji, c) typ włókna światłowodowego, d) typ złączy światłowodowych, e) długość patchcordu światłowodowego, f) średnicę patchcordu światłowodowego, g) wynik pomiaru strat wtrąceniowych dla całego patchcordu (dla każdego pojedynczego włókna światłowodowego wraz z dwoma złączami) wyrażony w decybelach lub wynik pomiaru strat wtrąceniowych dla każdego złącza wyrażony w decybelach, h) wynik pomiaru strat odbiciowych dla całego patchcordu (dla każdego pojedynczego włókna światłowodowego wraz z dwoma złączami) wyrażony w decybelach lub wynik pomiaru strat odbiciowych dla każdego złącza wyrażony w decybelach.

5. Gwarancja i wsparcie techniczne dla urządzeń

- Zamawiający wymaga, aby Wykonawca przedstawił wycenę dostawy oferowanego sprzętu wraz z gwarancją niezawodności działania Urządzeń oraz wsparciem technicznym na okres 3 lat.

Okres trwania powyższego terminu zaczyna biec od daty podpisania protokołu odbioru Przedmiotu Umowy. Ponadto wykonawca zobowiązany jest do dostarczenia kart gwarancyjnych.

Przedstawiona wycena musi obejmować:

- koszt dostawy sprzętu,

- b. koszt gwarancji producenta lub autoryzowanego partnera producenta,
- c. koszt wsparcia technicznego obejmującego co najmniej dostęp do aktualizacji oprogramowania, baz sygnatur, mechanizmu kategoryzacji stron www, poprawek bezpieczeństwa oraz możliwość zgłaszania awarii i usterek.

Wykonawca zobowiązuje się na czas trwania gwarancji zapewnić wsparcie techniczne Urządzeń obejmujące minimum:

- 1) prace serwisanta aż do rozwiązania problemu;
 - 2) zdalną pomoc techniczną w zakresie oprogramowania;
 - 3) bezpłatne uaktualnienia oprogramowania, firmware i dokumentacji;
 - 4) licencje na używanie i kopiowanie uaktualnień oprogramowania, dostęp do baz danych i inne potrzebne do prawidłowego działania Urządzeń;
 - 5) zdalną diagnostykę i pomoc techniczną;
 - 6) dostęp do serwisu elektronicznego obejmującego bazę wiedzy zawierającą wykaz znanych symptomów nieprawidłowego działania oprogramowania oraz sposobów naprawy, jak również, opisy i specyfikacje produktów oraz dokumentację techniczną,
 - 7) dostawę materiałów i części niezbędnych do usunięcia usterki/awarii Urządzeń.
2. Wykonawca zobowiązuje się na czas trwania gwarancji do nieodpłatnego usuwania zgłaszanych przez Zamawiającego usterek i awarii Urządzeń uniemożliwiających lub utrudniających jego pełną eksploatację. Naprawy gwarancyjne dokonywane będą w miejscu siedziby Zamawiającego, a w przypadku wystąpienia konieczności naprawy przedmiotu umowy poza siedzibą Zamawiającego, Wykonawca zapewni:
- a) serwis gwarancyjny świadczony w trybie 24x7,
 - b) wymianę sprzętu lub bezpłatne dostarczenie i uruchomienie nowego urządzenia zastępczego o parametrach równoważnych z oferowanymi w trybie NBD (Next Business Day),
 - c) odbiór na własny koszt wadliwego Urządzenia w terminie nie przekraczającym 1 dnia roboczego,
 - d) dostawę naprawionego Urządzenia na własny koszt.
3. Wykonawca zobowiązuje się do podjęcia czynności serwisowych w czasie nie przekraczającym jednego dnia roboczego od momentu zgłoszenia.
4. Wykonawca zapewni dostęp do pomocy technicznej, umożliwiając zgłaszanie wad lub usterek za pomocą Internetu lub telefonicznie.
5. Gwarancja udzielona zostaje bez ograniczeń terytorialnych, tj. obejmuje terytorium Rzeczypospolitej Polskiej i całego świata. Dla uniknięcia wątpliwości przyjmuje się, że Wykonawca usunie wszystkie zgłoszone Awarie, Wady lub inne zgłoszone wady nawet pomimo zakończenia okresu gwarancyjnego, o ile zostały one zgłoszone przed zakończeniem terminu obowiązywania gwarancji.
6. W celu przystąpienia do naprawy osoba upoważniona przez Wykonawcę zgłosi się do miejsca używania Urządzeń w Siedzibie Zamawiającego lub w innym miejscu wskazanym przez Zamawiającego na terenie Warszawy. Jeśli w ocenie Wykonawcy naprawa w lokalizacji wskazanej w zgłoszeniu Awarii/Wady przez Zamawiającego nie jest możliwa, Wykonawca odbierze Urządzenia i dostarczy po naprawie na własny koszt i na własną odpowiedzialność.

7. Na czas naprawy poza lokalizacją wskazaną w zgłoszeniu Awarii/Wady przez Zamawiającego, Urządzenia będą zabierane bez dysków twardych (nośniki pamięci), które zostaną wymontowane przez przedstawiciela Wykonawcy pod nadzorem Zamawiającego. Nośniki pamięci zostaną ponownie zamontowane przez przedstawiciela Wykonawcy pod nadzorem Zamawiającego, po czym nastąpi sprawdzenie poprawności funkcjonowania naprawionych Urządzeń.
8. Czas skutecznej naprawy Urządzeń musi nastąpić w terminie do 30 Dni roboczych, licząc od momentu zgłoszenia Awarii/Wady. W ramach rozszerzonego wsparcia technicznego Wykonawca dostarczy Urządzenie zastępcze na czas naprawy. Dostarczenie Urządzenia zastępczego nastąpi w trybie Następny Dzień Roboczy (NBD) od momentu potwierdzenia zasadności zgłoszenia.

6. Szkolenia i transfer wiedzy

Zamawiający wymaga aby wraz z dostawą urządzeń przeprowadzone były szkolenia dla 8 osób. Wykonawca zapewnia lokalizację i zasoby do przeprowadzenia szkoleń w minimum 2 turach.

Wymagania ogólne dla szkoleń:

- 1) Szkolenia muszą pochodzić od producenta dostarczanej technologii.
- 2) Szkolenia swoim zakresem muszą odpowiadać dostarczonemu modelowi produktów.
- 3) Łączna ilość dni szkoleniowych dla jednego inżyniera nie może być mniejsza niż 10 dni szkoleniowych zawierających teorię i praktykę.
- 4) W ramach szkolenia dostarczana będzie dokumentacja w języku angielskim lub polskim w formie papierowej lub elektronicznej (na adres e-mail wskazany w umowie).
- 5) Wszelkie wymagane ćwiczenia praktyczne muszą być zrealizowane na dostępnym środowisku testowym w ramach szkolenia.

Minimalny zakres szkoleń:

- 1) Początkowa konfiguracja systemów w zakresie interfejsów, zarządzania, uprawnień, itp
- 2) Omówienie i konfiguracja kont administracyjnych lokalnych jak i centralnego uwierzytelnienia. Przydzielanie uprawnień.
- 3) Obsługa interfejsów graficznych (GUI) jak i linii poleceń (CLI)
- 4) Omówienie i konfiguracja routingu w zakresie statycznych jak i dynamicznych protokołów.
- 5) Omówienie konfiguracji Load balancingu (ADC)
- 6) Omówienie i konfiguracja metod utrzymania sesji
- 7) Polityki i access listy – omówienie i konfiguracja
- 8) Budowa bezpiecznych reguł firewall włączając w to wszystkie dostępne funkcje dostarczonych urządzeń.
- 9) Szyfrowanie i inspekcja SSL/TLS. Zarządzanie certyfikatami.
- 10) Omówienie i konfiguracja Web Application Firewall
- 11) Omówienie i konfiguracja Limitowania połączeń i ochrony DoS
- 12) Omówienie szyfrowania, API i zaawansowanej logiki ruchu
- 13) Zagadnienia związane z konfiguracją i działaniem klastrów wysokiej dostępności. Podstawowe praktyki jak i konfiguracje zaawansowane.

- 14) Diagnostyka i rozwiązywanie problemów.
- 15) Tworzenie kopii zapasowych
- 16) Optymalizacja działania, sposoby monitorowania.
- 17) Najlepsze praktyki konfiguracji urządzeń
- 18) Najlepsze praktyki utrzymania urządzeń
- 19) Wykonywanie aktualizacji oprogramowania
- 20) Centralne zarządzanie:
 - a. Architektura i konfiguracja
 - b. Zabezpieczenie komunikacji z zarządzanymi urządzeniami
 - c. Konfiguracja kont i uprawnień
 - d. Centralna rejestracja i zarządzanie urządzeniami
 - e. Teoretyczne i praktyczne aspekty zarządzania konfiguracjami urządzeń
 - f. Audytowanie wykonanych działań przez administratora
 - g. Monitorowanie systemu centralnego zarządzania
 - h. Diagnostyka systemu centralnego zarządzania
 - i. Najlepsze praktyki pracy z systemem centralnego zarządzania

Asysta przy wdrożeniu i wsparcie techniczne

W pierwszym roku wsparcia, licząc od daty odbioru sprzętu, dostawca zobowiązany jest do świadczenia usług asysty we wdrożeniu i wsparcia w utrzymaniu zainstalowanego systemu w infrastrukturze Zamawiającego w zakresie przedstawionym poniżej. Oczekiwana minimalna ilość dni roboczych inżyniera przeznaczonych na usługi to 24 MD nie mniej niż 1 MD kwartalnie w okresie trwania umowy.

Wykonawca będzie świadczył Asystę Techniczną w zakresie obsługi zgłoszeń i zapotrzebowania wsparcia Zamawiającego, przez oddelegowanych do wykonania prac certyfikowanych inżynierów, fizycznej obecności, elektronicznej i telefonicznej komunikacji w Dni Robocze, w języku polskim.

Asysta Techniczna Wykonywana będzie w siedzibie Zamawiającego w Warszawie przy ul. Kolska 12 i będzie realizowana na sprzęcie udostępnionym przez Zamawiającego lub w bezpieczny sposób zdalny uzgodniony z Zamawiającym.

Wykonawca do realizacji usługi Asysty w utrzymaniu i wsparcia technicznego musi dysponować co najmniej dwiema osobami (inżynierami) posiadającymi umiejętności w zakresie rozwiązywania problemów związanych z bieżącym administrowaniem, konfiguracją i utrzymaniem oferowanego rozwiązania (z czego muszą oni posiadać potwierdzenie kompetencji aktualnym certyfikatem producenta na poziomie N lub N-1 gdzie N oznacza najwyższy z możliwych certyfikatów producenta w dziedzinie oferowanego rozwiązania).

Oczekiwany minimalny zakres udzielenia asysty w utrzymaniu i wsparciu technicznym Zamawiającego:

- asysta podczas wdrażania infrastruktury,
- pośredniczenie w rozwiązywaniu problemów technicznych zgłoszonych do producenta,
- wsparcie techniczne w zakresie działania systemu, wprowadzanych zmian konfiguracyjnych,
- diagnostyka systemu w wypadku nieprawidłowego działania lub wątpliwości administratorów Zamawiającego,
- rekomendacja dla aktualizacji oprogramowania,

- asysta podczas aktualizacji oprogramowania.

Każdorazowa aktualizacja oprogramowania obejmować musi następujące elementy:

- weryfikacja stabilności nowego oprogramowania
- sprawdzenie znanych błędów nowej wersji i ocena ryzyka w środowisku Zamawiającego,
- wykonanie kopii zapasowej konfiguracji i danych,
- przeprowadzenie aktualizacji,
- wykonanie testów poprawnego działania systemu,
- poprawa dokumentacji,
- weryfikacja zaleceń producenta w tym reakcji na znalezione problemy, poprawki podatności,
- analiza poprawności działania wdrożonego systemu i jego komponentów,
- dostrojenie/rekonfiguracja systemu (zmiana parametrów/ustawień),
- analiza i rekomendowanie możliwości optymalizacji,
- możliwości integracji z innymi systemami Zamawiającego,
- asysta podczas testów odtworzeniowych
- utwardzenie konfiguracji zgodnie z dobrymi praktykami po zakończonym wdrożeniu

Czas Reakcji Wykonawcy na otrzymane Zgłoszenie wynosi 1 Dzień Roboczy. W przypadku Zgłoszenia otrzymanego po godzinie 16.00, Czas Reakcji liczy się od godziny 8.00 następnego Dnia Roboczego. Zgłoszenie uważa się za otwarte po przestaniu go przez Zamawiającego do Wykonawcy mailem na ustalony z Wykonawcą adres.

Czas wizyty przeznaczony na wykonanie Asysty Technicznej Wykonawcy liczony jest od chwili przystąpienia do pracy certyfikowanego inżyniera w obszarze danego rozwiązania w siedzibie Zamawiającego. Usługi asysty w utrzymaniu i wsparciu technicznym rozliczane będą w kwantach nie mniejszych niż 0,5 dnia roboczego (MD) – tj. 4 godziny robocze.

Potwierdzeniem wykonania zleconych prac i wykorzystanego czasu w danym okresie rozliczeniowym będzie protokół odbioru prac wykonanych na rzecz Zamawiającego w ramach Asysty Technicznej podpisany na koniec każdego trzymiesięcznego okresu rozliczeniowego przez obie strony. Wykonawca musi dostarczyć kwartalnie raport z wykorzystanych i pozostałych dni roboczych w ramach usług Asysty i Wsparcia Technicznego. Rozbudowa Systemu o nowe moduły, karty i licencje nie powoduje zmiany zakresu Asysty i Wsparcia Technicznego.