Załącznik nr1 do zapytania ofertowego Sława, 25-03-2022r.

BI.271.1.2022

OPIS PRZEDMIOTU ZAMÓWIENIA

Nazwa zamówienia

Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz usługami wsparcia technicznego i gwarancji.

Kody CPV

32420000-3 Urządzenia sieciowe.

35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.

Przedmiot zamówienia

(1) Przedmiotem zamówienia jest dostawa urządzeń klasy NGFW (ang. Next Generation Firewall) w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU - projekt „Cyfrowa Gmina

(2) Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Dzień Roboczy - oznacza dzień od poniedziałku do piątku nie będący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.

Godziny ekspercie - usługi konsultacji (tzw. ang. Professional Services), których przedmiotem będą miedzy innymi zagadnienia wskazane w OPZ, dotyczące obsługi, konfiguracji I eksploatacji Urządzeń, bieżących problemów dotyczących funkcjonowania Urządzeń, ich konfiguracji, wyjaśniania wątpliwości lub rozwiązania zagadnień z tego zakresu przedstawianych przez Zamawiającego, związanych z obsługą Urządzeń, świadczone w miejscu zainstalowania Urządzeń lub zdalnie, na warunkach wskazanych w OPZ, w terminach uzgodnionych zgodnie z postanowieniami Umowy również poza Dniami Roboczymi oraz poza Godzinami Roboczymi.

Hardware Appliance - ang. Hardware Appliance oznacza urządzenie fizyczne wraz z oprogramowaniem do którego Producent dostarcza wsparcie techniczne.

SSL/TLS - ang. Secure Socket Layer / Transport Layer Security oznacza protokół szyfrowania komunikacji sieciowej. (ze wsparciem co najmniej w wersji TLS 1.2 lub TLS 1.3).

Urządzenia - oznacza przedmiot zamówienia opisany w pkt. III.1 niniejszego dokumentu.

Szkolenie certyfikowane – oferowane przez producenta sprzętu szkolenie z zakresu konfiguracji i administrowania dostarczonego rozwiązania zakończone uzyskaniem certyfikatu.

Wsparcie producenta - oznacza oferowane przez producenta Urządzeń aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla poszczególnych urządzeń przez zdefiniowany okres czasu.

(3) Przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, a Zamawiający dopuszcza rozwiązania równoważne opisywanym i takim odniesieniom towarzyszą wyrazy "lub równoważne".

(4) W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp., Zamawiający nie odrzuci oferty tylko dlatego, że oferowane dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp., że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

(5) W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp., zamawiający nie odrzuci oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107, że dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.

(6) W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.

(7) Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.

III. Specyfikacja wymagań

Przedmiotem zamówienie jest dostawa urządzeń klasy NGFW, opisanych w pkt. III.1

III.1 Dostawa urządzeń

Przedmiotem zamówienia jest dostawa:

(a) dwóch urządzeń klasy NGFW (ang. Next Generation Firewall), zwanych dalej „NGFW”, w tym:

(i) jednego NGFW typu 1,

(ii) jednego NGFW typu 2

zwanych łącznie „Urządzeniami”, w terminie 8 tygodni od dnia podpisania umowy.

III.1.1 Wymagania ogólne dla Urządzeń:

Lp.	Opis wymagania	Parametry minimalne
1.	Parametry montażowe	Urządzenia fizyczne z przedmiotu zamówienia muszą być a) NGFW Typ 1 -przystosowane do montażu w szafach RACK 19" i być dostarczone z odpowiednimi elementami montażowymi. b) NGFW Typ 2 – obudowa typu Desktop
2.	Zasilacze	Urządzenia wchodzące w skład niniejszego przedmiotu zamówienia muszą być wyposażone w zasilacze 230V Dla NGFW Typ 1 – wymagana dwa zasilacze zapewniające redundancję (pracę w pełni wyposażonego urządzenia podczas awarii jednego z nich) Dla NGFW Typ 2 – wymagany zasilacz pojedynczy.
3.	Jednorodność, szyfrowanie i dodatkowe kryteria bezpieczeństwa	1. Dostarczone Urządzenia muszą pochodzić od tego samego producenta oraz nie mogą znajdować się na liście (typu „end-of-life" oraz „end-ofsupport"), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025. 2. NGFW powinno posiadać zgodność z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3" lub wyższym lub równoważnym* ; 3. NGFW powinno posiadać zgodność z profilem zabezpieczeń Common Criteria – „PP-Module for Virtual Private Network (VPN) Gateways" w wersji 1.0 lub wyższym lub równoważnym* .
4.	Wydajność	Dla NGFW – typ 1: NGFW musi mieć wydajność przetwarzania ruchu sieciowego w trybie ochrony FW (ang. FireWall) – min 30 Gbps, IPS (ang. Intrusion prevention systems) – min 5,5Gbps i pełnej ochrony przed zagrożeniami (threat protection) – min. 1,2 Gbps. Dla NGFW – typ 2: NGFW musi mieć wydajność przetwarzania ruchu sieciowego w trybie ochrony FW (ang. FireWall) – min 7 Gbps, IPS (ang. Intrusion prevention systems) – min 1,2Gbps i pełnej ochrony przed zagrożeniami (threat protection) – min. 300Mbps.
5.	Interfejsy fizyczne	Dla NGFW – typ 1: Min. 8 interfejsów GigabitEthernet, Min. 2 interfejsy 1 SFP oraz jeden port rozszerzeń. Dla NGFW – typ 2: Min. 8 interfejsów GigabitEthernet, Min. 1 interfejs 1 SFP oraz jeden port rozszerzeń.
6.	Pamięć wewnętrzna na system operacyjny	NGFW typ 1 musi być wyposażone co najmniej w jeden dysk SSD o pojemności minimum 100Gb NGFW typ 2 musi być wyposażone co najmniej w jeden dysk SSD o pojemności 60Gb
7.	Routing i protokół IP	1 Musi umożliwić obsługę protokołów routingu m.in.: OSPF, RIP/RIPv2 oraz routing statyczny.

		2 Musi zapewnić ochronę ruchu sieciowego opartego o protokół IP: IPv4 oraz IPv6. 3 Musi umożliwić wykonywanie translacji adresów IP (statycznej i dynamicznej). 4 NGFW musi obsługiwać protokół Ethernet wraz z obsługą sieci VLAN.
8.	Wymagane modele wdrożeń NGFW	NGFW musi umożliwić ochronę ruchu sieciowego w: 1 Drugiej warstwie modelu OSI – L2. 2 Trzeciej warstwie modelu OSI – L3. 3 Trybie transparentnym (urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych, przez które przechodzi ruch sieciowy).
9.	Tryby pracy IPS w NGFW	1. Aktywny (IPS). 2. Pasywny (IDS).
10.	Kontrola aplikacji	1. Musi wykrywać aplikacje w ruchu sieciowym, m.in. P2P (np. torrent), web drive (np. google drive), web mail (np. gmail). 2. System musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania.
11.	Filtrowanie ruchu sieciowego	1. Musi zapewniać filtrowanie w oparciu o kategorie (co najmniej): Adult, Gambling, Social Networking, video stream oraz w oparciu o kategorie lub aktualizowaną bazę adresów IP (lub URL) związanych z Malware, Phishing, C&C, TOR (lub TOR Exit Node lub TOR Relay Node), Proxy anonimizujące, przy czym producent dostarcza predefiniowany zestaw kategorii i przypisaną do nich bazę adresów IP lub URL. Baza adresów i kategorii musi być cyklicznie aktualizowania przez Producenta (przez okres wsparcia technicznego). 2. Musi zapewnić możliwość ręcznego definiowania dodatkowych kategorii bez użycia zewnętrznych narzędzi oraz możliwość przypisywanie do nich adresów URL i domen.
12.	Funkcjonalność aktualizacji i ochrony NGFW	1. NGFW musi posiadać moduł wykrywania i blokowania ataków oparty o sygnatury. 2. Baza sygnatur moduły inspekcji IPS (ang. Intrusion Prevention System) musi być pobierana (ręcznie i automatycznie) z serwerów producenta na Konsolę. 3. Możliwość blokowania ruchu sieciowego na podstawie: • adresów IP • reputacji (IP, domen lub URL) • sygnatur IPS • domen • URL • geolokalizacji (np. adresy IP pochodzących z konkretnych państw). 4. Rozpoznawanie i blokowanie niedozwolonych aplikacji i protokołów sieciowych.

		5. Musi umożliwiać automatyczne dodawanie z zewnętrznych serwerów listy (tzw. Feed) zawierających złośliwe adresy IP, domeny lub URL. 6. Musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 7. Ochrona przed atakami typu flood. 8. Możliwość ochrony przed exploitami i blokowanie ruchu sieciowego z nim związanego w celu ochrony podatnych aplikacji lub usług. 9. Musi posiadać sygnatury wykrywające i blokujące zapytania DNS i ruch sieciowy do domen uznanych za złośliwe. 10. Musi posiadać funkcję wykrywania aktywności sieci typu Botnet. 11. Wykrywanie zagrożeń tj. ataki na podatne aplikacje i infrastrukturę. 12. Musi odczytywać oryginalne adresy IP z pola „X-Forwarded-For” w nagłówku http. 13. Musi umożliwiać tworzenie polityk bezpieczeństwa w oparciu o mechanizmy geolokalizacji. Baza geolokalizacji musi być aktualizowana w sposób automatyczny (przez producenta NGFW). 14. Musi posiadać rozwiązanie klasy Sanbox do ochrony przez zadrożeniami typu Zero-Day. 15. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll., dokumentów w tym .doc, .docx, .docm, .rtf, plików .pdf, archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. 16. System zapewniający analizę strukury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego.
13.	Ochrona IPS - możliwe reakcje na wykryte zdarzenia bezpieczeństwa w przetwarzanym ruchu sieciowym	1. Monitoring z alertowaniem. 2. Blokowanie. 3. Bez inspekcji (aby wybrany na podstawie IP ruch nie był przesyłany do silnika inspekcji IPS).
14.	VPN	1. System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2. 2. System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). 3. System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. 4. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.

		5. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. 6. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. 7. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. 8. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN. 9. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. 10. Urządzenie musi obsługiwać połączenia L2TP over IPsec. 11. Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej.
15.	Zarządzanie pasmem (QoS)	1. NGFW musi zapewniać zarządzanie pasmem (QoS) sieci. 2. Musi zapewnić limitowanie ruchu sieciowego w oparciu o co najmniej następujące parametry: rozpoznany ruch sieciowy aplikacji oraz adresy IP (źródłowy i docelowy).
16.	Kontrola ruchu szyfrowanego	1. Musi mieć możliwość przesyłania ruchu zaszyfrowanego (co najmniej TLS/SSL) do zewn. deszyfratora. 2. Musi mieć możliwość definiowania polityk bezpieczeństwa w kontekście ruchu szyfrowanego. 3. Musi posiadać możliwość deszyfracji ruchu (co najmniej TLS/SSL w oparciu o zaimportowanie klucza prywatnego) w celu jego analizy oraz szyfrowania ruchu z powrotem
17.	Zarządzanie	1. NGFW powinien być zarządzany przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). 2. Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administraotra, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów. 3. Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administraotra, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów. 4. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.

		5. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. 6. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 7. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. 8. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). 9. System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. 10. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). 11. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). 12. Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. 13. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji . 14. Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.
18.	Uwierzytelnianie i obsługa użytkowników	1. Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. 2. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. 3. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+. 4. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.

		5. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). 6. Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. 7. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. 8. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. 9. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. 10. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. 11. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.
19.	Logowanie i raportowanie	12. System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. 13. System powinien umożliwiać składowanie oraz archiwizację logów. 14. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 15. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. 16. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa 17. System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. 18. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. 19. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. 20. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. 21. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do serwera syslog. 22. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym,

		miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. 23. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. 24. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. 25. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
20	Wsparcie producenta	Minimum do 30 września 2023
21	Gwarancja na sprzęt	36 miesięcy

*Wymaganie nie jest obligatoryjne i stanowi kryterium oceny ofert, opisane w Rozdziale I SWZ

Kryteria oceny oferty

1. Przy wyborze oferty Zamawiający będzie się kierował następującym kryteriami:

Kryteria oceny oferty

Cena: znaczenie 80 pkt

Godziny eksperckie

(1) -brak godzin – 0pkt.

(2)5 godzin – 5pkt.

(3) 10 godzin – 10pkt.

Voucher na certyfikowane szkolenie

(1) – brak vouchera – 0 pkt.
(2) – voucher – 10 pkt.

Ocena ofert będzie przeprowadzona według poniższego wzoru:

K=[(Cmin/Cof x60pkt+ H x 10pkt + V x 10 pkt]

K	współczynnik oceny oferty (liczony z dokładnością do czterech miejsc po przecinku),
Cmin	najniższa cena spośród wszystkich ocenianych ofert (łącznie z podatkiem VAT w PLN),
Cof	cena ocenianej oferty (łącznie z podatkiem VAT w PLN),
H	Ilość punktów za oferowane godziny eksperckie
V	Ilość punktów za oferowany voucher.
P	ilość punktów zdobytych za podwyższone parametry względem wymagań minimalnych

2. Oferta, która uzyska największą wartość współczynnika K, liczonego według powyższego wzoru, zostanie uznana przez Zamawiającego za ofertę najkorzystniejszą.

3. Ocenie w kryterium „cena” zostanie poddana jednostkowa cena brutto podana w Formularzu Oferty.

4. Maksymalna możliwa współczynnik oceny oferty wynosi 100pkt.

5. Oferta Wykonawcy, która uzyska łącznie najwyższy współczynnik oceny oferty uznana zostanie za najkorzystniejszą.

6. Jeżeli Zamawiający nie będzie mógł wybrać oferty najkorzystniejszej z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z najniższą ceną.

7. Ocenie będą podlegać wyłącznie oferty nie podlegające odrzuceniu.