Załącznik nr 1.2 do SWZ

**Opis przedmiotu zamówienia – specyfikacja techniczna oferowanego sprzętu**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Nazwa oferowanego urządzenia:** | |  |
|  | **Producent:** | |  |
|  | **Typ/model/kod producenta:** | |  |
|  | **Zadanie nr 1: Firewall typ 1 – 1 szt.** | | |
|  | **parametr** | **Minimalne wymagania** | |
|  | **Wymóg podstawowy** | **Zamawiający zamierza wykorzystywać urządzenie w trybie zapory sieciowej i kontrolera do posiadanych urządzeń Access Point. Wymagana jest pełna zgodność z posiadanymi urządzeniami FortiAPs.** | |
|  | Wymagania Ogólne | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:   * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. | |
|  | Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwiający agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto dający możliwość tworzenia interfejsów redundantnych. | |
|  | Interfejsy, Dysk, Zasilanie: | 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:  * 5 portami Gigabit Ethernet RJ-45. * 5 portów anteny WWAN * 2 porty obsługujące karty SIM (nano) z obsługą technologii 5G  1. System Firewall pozwalający skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q. 2. System Firewall posiadający wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB. 3. System jest wyposażony w zasilanie AC. | |
|  | Parametry wydajnościowe: | 1. W zakresie Firewall’a obsługujący nie mniej niż 720000 tys. jednoczesnych połączeń oraz 85 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.8 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 4.5 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.25 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1,1 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. | |
|  | Funkcje Systemu Bezpieczeństwa: | W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 12. Rozwiązanie posiadające wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). | |
|  | Polityki, Firewall | 1. Polityka Firewall uwzględniająca: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizujący translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 2. Umożliwiający wykorzystanie w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 3. Polityka firewall umożliwiająca filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 4. Umożliwiający ustawienie przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. | |
|  | Połączenia VPN | 1. System umożliwiający konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewniający:  * Wsparcie dla IKE v1 oraz v2. * Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19, 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Umożliwiający wybor tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. * Umożliwiający ustawienie maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. * Umożliwiający monitorowanie wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. * Obsługujący mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.   Producent rozwiązania posiadający w ofercie oprogramowanie klienckie VPN, umożliwiające realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn powinno być dostępne jako opcja i nie wymagane w implementacji. | |
|  | Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewniające obsługę:   1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Umożliwiający filtrowanie tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitorujący dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. | |
|  | Funkcje SD-WAN | 1. System umożliwiający wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspierający zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). | |
|  | Zarządzanie pasmem | 1. System Firewall umożliwiający zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System dający możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwalający zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewniający możliwość zarządzania pasmem dla wybranych kategorii URL. | |
|  | Ochrona przed malware | 1. Silnik antywirusowy umożliwiający skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System umożliwiający skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System dysponujący sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System współpracujący z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.   Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. | |
|  | Ochrona przed atakami | 1. Ochrona IPS opierająca się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System chroniący przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu powinien mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System zapewniający wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. System dysponujący sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA. 7. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). 8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.   Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. | |
|  | Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwiająca kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawierająca minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawierająca kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu powinien mieć możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).   System dający możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). | |
|  | Kontrola WWW | 1. Moduł kontroli WWW korzystający z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW dostarczający kategorie stron zabronionych prawem np.: Hazard. 4. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwiający statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwalający definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW dający możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator powinien mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.   System pozwalający określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. | |
|  | Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwiający weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. System dający możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego. 2. System umożliwiający budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.   Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. | |
|  | Zarządzanie | 1. Elementy systemu bezpieczeństwa powinny posiadać możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3. Umożliwiający włączenie mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System współpracujący z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiający przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5. System dający możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję Firewall umożliwiający wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8. Umożliwiający przypisywanie administratorom praw do zarządzania określonymi częściami systemu (RBM).   Umożliwiający zarządzanie systemem tylko z określonych adresów źródłowych IP. | |
|  | Logowanie | 1. Elementy systemu bezpieczeństwa realizujący logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. Elementy systemu bezpieczeństwa realizujący logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze lub musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej 3. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewniający możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 4. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 5. Umożliwiający włączenie logowania per reguła w polityce firewall. 6. System zapewnia możliwość logowania do serwera SYSLOG.   Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. | |
|  | Testy wydajnościowe oraz funkcjonalne | Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy. | |
|  | Serwisy i licencje | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres udzielonej gwarancji ze wsparciem serwisowym. | |
|  | Gwarancje i wsparcie | System jest objęty serwisem gwarancyjnym producenta przez okres min 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | |

**\*Uwaga, wymagane jest uzupełnienie tabeli**

**Wykonawca zobowiązany jest do podania nazwy oferowanego urządzenia, producenta, typu/modelu /kodu producenta. Podane dane oraz uzupełniona kolumna pn: Parametry oferowane muszą pozwolić Zamawiającemu na jednoznaczną identyfikację oferowanego produktu.**

**Każdorazowo gdy Zamawiający używa nazwy własnej, certyfikatu, standardu lub normy należy przez to rozumieć treść danego parametru łącznie ze sformułowaniem 'lub równoważny".**

**DOKUMENT NALEŻY PODPISAĆ KWALIFIKOWANYM PODPISEM ELEKTRONICZNYM.**

Rozwiązania równoważne – odpowiednio dla każdego z zadań:

1. W przypadku użycia w SWZ lub załącznikach odniesień 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, Zamawiający dopuszcza rozwiązania równoważne opisywanym. Wykonawca analizując opis przedmiot zamówienia powinien założyć, że każdemu odniesieniu o którym mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy użytemu w opisie przedmiotu zamówienia dla każdego z zadań towarzyszy wyraz „lub równoważne”.
2. W przypadkach użycia w SWZ lub załącznikach nazw własnych, dopuszcza się złożenie oferty z asortymentem równoważnym do wskazanego przedmiotu zamówienia. Zamawiający określił referencyjnego producenta/dostawcę, w celu dokładnego sprecyzowania wymagań, jaki musi spełniać oferowany przez Wykonawców asortyment. Wykonawca analizując opis przedmiot zamówienia powinien założyć, że każdemu odniesieniu o którym mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy użytemu w opisie przedmiotu zamówienia dla każdego z zadań towarzyszy wyraz „lub równoważne”. Zamawiający dopuszcza zaoferowanie asortymentu i rozwiązań, równoważnych jakościowo, eksploatacyjnie i technicznie do materiałów wskazanych przez Zamawiającego z określeniem referencyjnego producenta/dostawcy. Wykonawca składający ofertę z asortymentem równoważnym, musi spełnić warunki określone w niniejszym SWZ pod rygorem odrzucenia oferty jako niezgodnej z treścią SWZ.
3. W przypadku, gdy w SWZ lub załącznikach zostały użyte znaki towarowe, oznacza to, że są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Wykonawca może zastosować asortyment równoważny, lecz o parametrach technicznych i jakościowych podobnych lub lepszych, których zastosowanie w żaden sposób nie wpłynie negatywnie na prawidłowe funkcjonowanie rozwiązań przyjętych w opisie przedmiotu zamówienia dla każdego z zadań. Wykonawca, który zastosuje standardy równoważne będzie obowiązany wykazać w trakcie realizacji zamówienia, że zastosowane przez niego rozwiązania spełniają wymagania określone przez Zamawiającego. Użycie w SWZ lub załącznikach oznakowania oznacza, że Zamawiający akceptuje także wszystkie inne oznakowania potwierdzające, że dane dostawy spełniają równoważne wymagania. W przypadku, gdy Wykonawca z przyczyn od niego niezależnych nie może uzyskać określonego przez Zamawiającego oznakowania lub oznakowania potwierdzającego, że dane dostawy spełniają równoważne wymagania, Zamawiający w terminie przez siebie wyznaczonym akceptuje inne odpowiednie środki dowodowe, w szczególności dokumentację producenta, o ile dany Wykonawca udowodni, że dostawy, które mają zostać przez niego wykonane, spełniają wymagania określonego oznakowania lub określone wymagania wskazane przez Zamawiającego.

Wykonawca, który powołuje się na produkty równoważne wyszczególnione w formularzu Opis przedmiotu zamówienia – specyfikacja techniczna oferowanego sprzętu odpowiednio dla każdego z zadań zobowiązany jest:

 - W przypadku oferowania rozwiązania równoważnego, Wykonawca jest zobowiązany wykazać, że oferowane przez niego rozwiązanie równoważne spełnia wymagania określone przez Zamawiającego, poprzez załączenie do oferty dowodów potwierdzających, że rozwiązanie równoważne spełnia wszystkie parametry równoważności. Dowody te powinny zawierać informacje umożliwiające Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne poszczególnych parametrów równoważności,

- Zamawiający wymaga, aby zaoferowane przez Wykonawcę rozwiązania równoważne nie wiązały się z koniecznością wykonania dodatkowych prac testowych, migracyjnych czy integracyjnych po stronie Zamawiającego, tym samym poniesienia niezaplanowanych, dodatkowych kosztów