Sygn. akt: KIO 917/22

WYROK

z dnia 26 kwietnia 2022 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Anna Wojciechowska

Protokolant: Adam Skowroński

po rozpoznaniu na rozprawie w Warszawie w dniu 21 kwietnia 2022 r. odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 1 kwietnia 2022 r. przez **wykonawcę Comp S.A. z siedzibą w Warszawie** w postępowaniu prowadzonym przez **zamawiającego Centralny Ośrodek Informatyki z siedzibą w Warszawie**

przy udziale **wykonawcy IT Solution Factor sp. z o.o. z siedzibą w Warszawie** zgłaszającego przystąpienie do postępowania odwoławczego po stronie zamawiającego

orzeka:

1. **Umarza postępowanie odwoławcze w zakresie zarzutów z lit. a, b oraz e odwołania, wycofanych przez odwołującego.**
2. **Oddala odwołanie.**
3. **Kosztami postępowania obciąża wykonawcę Comp S.A. z siedzibą w Warszawie** i zalicza w poczet kosztów postępowania odwoławczego kwotę 15 000 zł 00 gr (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez wykonawcę Comp S.A. z siedzibą w Warszawie tytułem wpisu od odwołania.

Stosownie do art. 579 ust. 1 i 580 ust. 1 i 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t. j. Dz. U. z 2021 r., poz. 1129 z późn. zm.) na niniejszy wyrok – w terminie 14 dni od dnia jego doręczenia - przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w **Warszawie.**

Przewodniczący: ……..

Sygn. akt KIO 917/22

Uzasadnienie

Zamawiający – Centralny Ośrodek Informatyki z siedzibą w Warszawie - prowadzi postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (tekst jednolity Dz. U. 2021 r., poz. 1129 z późn. zm. – dalej „ustawa pzp"), pn. *„dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją", nr postępowania: COI-ZAK.262.46.2021.* Ogłoszenie o zamówieniu opublikowane zostało w Dzienniku Urzędowym Unii Europejskiej w dniu 22 listopada 2022 r., za numerem 2021/S 226-594351.

W dniu 1 kwietnia 2022 r. odwołanie wniósł wykonawca Comp S.A. z siedzibą w Warszawie – dalej Odwołujący. Odwołujący wniósł odwołanie wobec wyboru najkorzystniejszej oferty wykonawcy IT Solution Factor sp. z o.o. z siedzibą w Warszawie – dalej Przystępujący lub „ITSF", oraz zaniechania odrzucenia oferty tego Wykonawcy.

Odwołujący zarzucił Zamawiającemu naruszenie art. 226 ust. 1 pkt 5 ustawy pzp w zw. z art. 16 pkt 1 - 3 ustawy pzp poprzez zaniechanie odrzucenia oferty złożonej ITSF pomimo iż jest ona niezgodna z warunkami zamówienia, gdyż: a. oferowane FG-401F nie spełnia wymagania posiadania dwóch dysków, b. brak jest wsparcia producenta dla urządzeń z oferowaną wersją oprogramowania, c. brak jest wsparcia producenta dla funkcjonalności VPN, d. brak jest certyfikacji FIPS, e. brak jest spełnienia CommonCriteria.

Odwołujący w oparciu o wyżej wskazane zarzuty wniósł o uwzględnienie odwołania, jak również nakazanie Zamawiającemu:

1) unieważnienia czynności polegającej na wyborze oferty Przystępującego jako najkorzystniejszej w postępowaniu,

2) powtórzenia czynności badania i oceny ofert z uwzględnieniem zarzutów postawionych w odwołaniu, i w konsekwencji odrzucenie oferty złożonej przez ITFS,

3) ponowienia czynności wyboru oferty najkorzystniejszej w postępowaniu.

Uzasadniając zarzuty podlegające rozpoznaniu:

Odnośnie braku wsparcia producenta dla funkcjonalności VPN Odwołujący wskazał, że zgodnie z Rozdziałem II - OPZ Specyfikacja wymagań - Pkt III.4 Zasady świadczenia usług Wsparcia Producenta, Zamawiający wymagał: „(1) Wykonawca zobowiązany jest

zapewnić wsparcie producenta tych urządzeń (dalej określanego jako „Producent”) lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta dla dostarczonych subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pkt II powyżej. (2) Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów. (3) Dostęp do uaktualnień sygnatur/ reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez producenta wraz z niezbędnymi danymi logowania, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych”. Wymaganie powyższe, jest niespełnione dla funkcjonalności wymaganej w pkt III. 1.2 pkt 17 w tabeli - Wymagania Zasady świadczenia usług Wsparcia Producenta VPN opisanej w pkt 17.1 i 17.2, w zakresie wymagania min. 100 tuneli VPN SSL:

	VPN	17.1 NGFW typ 2 i 3 muszą posiadać funkcjonalność VPN: 17.1.1 SSL VPN: w sumie (typ 2 i 3) min. 100 równoległych tuneli oraz 17.1.2 min. 100 tuneli IPSEC per Typ 2 i 3 (w sumie min. 200). 17.2 NGFW typ 1 musi posiadać funkcjonalność zestawiania min. 100 tuneli IPSEC.

Z wykazu zaoferowanych licencji załączonych w ofercie ITFS wynika, że w ramach spełnienia powyższego wymagania w zakresie zapewnienia 100 tuneli VPN został zaoferowany darmowy klient VPN (brak w wykazie licencji w ofercie ITFS licencji VPN i EMS).

Dowód:
https://docs.fortinet.com/document/forticlient/7.0.3/administrationguide/269675/feature-comparison-of-forticlient-standalone-and-licensedversions

Oznacza to, że zaoferowane rozwiązanie w zakresie funkcjonalności VPN nie spełnia wymagania dotyczącego konieczności zapewnienia wsparcia technicznego zgodnie wymaganiem Zamawiającego.

Dowód:

https://docs.fortinet.com/document/forticlient/7.0.3/administrationguide/269779/standalone-vpn-client

lub opis dla starszej wersji:

https://docs.fortinet.com/document/forticlient/6.2.0/newfeatures/673187/free-vpn-client

Zgodnie z informacją zawartą w przywołanym linku: „This version does not include central management, technical support, or some advanced features.” (tłumaczenie: „Ta wersja nie zawiera centralnego zarządzania, wsparcia technicznego oraz niektórych zaawansowanych funkcjonalności”). Biorąc pod uwagę powyższe wymagania SWZ (wymaganie ma charakter obligatoryjny) Odwołujący stwierdził, że rozwiązanie zaoferowane przez ITFS nie spełnia wymagania i oferta powinna zostać odrzucona jako niezgodna z warunkami zamówienia.

Odnośnie braku certyfikacji FIPS Odwołujący wskazał, że zgodnie z Rozdziałem II - OPZ Specyfikacja wymagań - pkt III.1.1 . Wymagania ogólne dla Urządzeń, pkt 3 w tabeli, ppkt 3.5 Zamawiający wymagał: „NGFW i Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny*.”

W swojej ofercie ITFS wskazuje, że spełnia wymaganie dla NGFW i Konsolę Zarządzającą. Dodatkowo w Odpowiedziach technicznych, strona 30-31 ITFS wyjaśnia oraz uzupełnia dokument, jednakże wyjaśnienie to nie potwierdza spełnienia Wymagania. Na cytowanej stronie jest informacja o urządzeniu FG-2500E i systemie operacyjnym FortiOS 6.0 i 6.2, ale brak na liście urządzeń certyfikowanych, urządzeń zaoferowanych przez firmę ITFS, tj. modeli: FG1801 F oraz Konsoli Zarządzającej.

https://csrc.nist.gov/proiects/cryptographic-module-validationprogram/certificate/3814

Dowód:

Sprawdzając na oficjalnej stronie NIST w advanced search:

https://csrc.nist.gov/proiects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Advanced.Vendor=fortinet.Standard=140-2CertificateStatus=Active.ValidationYear=0

pobieramy opis „Security Policy”:

httes://csrc.nist.gov/CSRC/media/proiects/crvptoeraehic-module-validation-program/documents/security-policies/140sp3814.pdf

a w nim na stronie 8 mamy „FIPS-compliant appliances", gdzie znajduje się oferowane urządzenie: FG-3301 E, natomiast brak jest na tej liście zaoferowanych urządzeń FG-1801F oraz brak Konsoli Zarządzania (FAZ1 OOF oraz FMG-400G).

Ponadto, dla Konsoli Zarządzania, w skład której wchodzą FortiAnalyzer FAZ100F oraz FortiManager FMG-400G informacje znajdujące się na stronie producenta wykazują certyfikację FIPS dla wersji 5.2, a nie w wersji 6.2, na którą powołuje się ITFS:

https://www.fortinet.com/corDorate/about-us/product-certifications/fips

Certyfikat dla Fortianalyzer i FortiManager w wersji 5.2, do których można znaleźć odnośniki w powyższym linku, obejmuje wersję testowaną 5.2.4 oraz urządzenia FortiAnalyzer-200D a także FortiManager-4000D. Dodatkowo oferowane urządzenia wchodzące w skład Konsoli Zarządzającej (FAZ-IOOF oraz FMG-400G) nie są na liście wspieranych urządzeń w Release Notes certyfikowanej wersji 5.2.4, a w przypadku FMG-400G nawet nie występuje na liście wspieranych urządzeń w Release Notes wersji 6.2.7, na którą powołuje się ITSF.

Dowód: potwierdzenie:

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/1b0404a4-ff37-11e8-8524-f8bc1258b856/fortianaLyzer-v5.2.4release-notes.pdf

https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/d36e3071-031d-11e9-b86b-00505692583a/fortimanager-5.2.4-release-notes.pdf

https://docs.fortinet.com/document/fortimanager/6.2.7/releasenotes/676521/supported-models

Odwołujący stwierdził, że żaden z przytoczonych dokumentów i linków do wskazanych stron nie potwierdzają spełnienia wymagania dla urządzeń FG1801F oraz dla Konsoli Zarządzania (FAZ-IOOF oraz FMG-400G). Powyższe oznacza, iż treść oferty nie odpowiada SWZ i oferta podlega odrzuceniu jako niezgodna z warunkami zamówienia.

Niespełnianie przez oferowane urządzenia wymagań wyspecyfikowanych w OPZ należy traktować jako niezgodność z warunkami zamówienia, a zatem oferta ITFS powinna zostać odrzucona na podstawie art. 226 ust. 1 pkt 5 ustawy pzp.

W dniu 20 kwietnia 2022 r. Zamawiający złożył odpowiedź na odwołanie, w której wniósł o oddalenie odwołania w części, w zakresie zarzutów 1-3, ze względu na brak

naruszenia wskazanych w odwołaniu przepisów oraz odrzucenie odwołania w zakresie zarzutu 5 ze względu na brak interesu prawnego Odwołującego we wniesieniu odwołania w zakresie tego zarzutu. Ponadto Zamawiający oświadczył, że na podstawie art. 522 ust. 4 ustawy pzp, uwzględnia odwołanie w części, objętej zarzutem 4.W złożonej odpowiedzi oraz na rozprawie przedstawił uzasadnienie faktyczne i prawne swojego stanowiska.

W dniu 20 kwietnia 2022 r. Przystępujący złożył pismo procesowe, w którym wniósł o oddalenie odwołania w całości. W złożonym piśmie oraz na rozprawie przedstawił uzasadnienie faktyczne i prawne swojego stanowiska.

Izba ustaliła, co następuje:

Izba ustaliła, że odwołanie czyni zadość wymogom proceduralnym zdefiniowanym w Dziale IX ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych, tj. odwołanie nie zawiera braków formalnych oraz został uiszczony od niego wpis. Izba ustaliła, że nie zaistniały przesłanki określone w art. 528 ustawy pzp, które skutkowałyby odrzuceniem odwołania.

Izba stwierdziła, że Odwołujący wykazał przesłanki dla wniesienia odwołania określone w art. 505 ust. 1 i 2 ustawy pzp, tj. posiadanie interesu w uzyskaniu danego zamówienia oraz możliwości poniesienia szkody w wyniku naruszenia przez Zamawiającego przepisów ustawy pzp.

Do postępowania odwoławczego po stronie Zamawiającego, zachowując termin ustawowy oraz wskazując interes w uzyskaniu rozstrzygnięcia na korzyść Zamawiającego zgłosił skuteczne przystąpienie wykonawca IT Solution Factor sp. z o.o. z siedzibą w Warszawie.

Izba postanowiła dopuścić dowody z dokumentacji przedmiotowego postępowania, odwołanie wraz z załącznikami, odpowiedź na odwołanie wraz z załącznikami, zgłoszenie przystąpienia wraz z załącznikami, pismo procesowe Przystępującego oraz

- dowody złożone przez Odwołującego: (dowody wraz z tłumaczeniem na język polski: dowód nr IX.5 – informacje ze strony producenta Fortinet odnośnie czterech wersji oprogramowania VPN FortiClient i braku wsparcia producenta oraz zrzut ze strony producenta odnośnie braku wsparcia dla funkcjonalności VPN przez FortiClient wersja 6.2.X, 6.4.X oraz 7.0.X, dowód nr IX.3 – zrzut ze strony producenta odnośnie oprogramowania FortiClient 6.2.7. i braku wsparcia dla „24x7”, IX.4 (1) – zrzut ze strony producenta odnośnie „Standalone VPN client”, iż należy potwierdzić świadomość, że to darmowe oprogramowanie

nie ma wsparcia producenta, IX.4 (2) – zrzut ze strony producenta odnośnie „Free VPN client”, iż należy potwierdzić świadomość, że to darmowe oprogramowanie nie ma wsparcia producenta, wyciąg z Wikipedii odnośnie FIPS 140-2, dowód nr X.3.1. – tożsamy z linkiem z oferty Przystępującego – odnośnie certyfikacji FIPS, certyfikat #3184, program weryfikacji modułów kryptograficznych, moduł: FortiOS 6.0. i 6.2., X.3.2. – zrzut ze strony NIST odnośnie certyfikowanych modułów, X.3.3. – polityka bezpieczeństwa FIPS Tabela 2 urządzenia zgodne z FIPS potwierdzone przez dostawcę, X.6.1. - FortiAnalyzer wspierane modele ze strony producenta Fortinet, X.6.2. - FortiManager wspierane modele ze strony producenta Fortinet, X.6.3. - zrzut ze strony FortiManager 6.2.7. brak wspieranego modelu FMG440G, X.0 – dokument ze strony producenta odnośnie FortiOS 6.2. oraz FortiGate NFGW, FIPS 140-2, certyfikacje uwagi techniczne, certyfikowane modele, X.0.1. – tożsamy z linkiem Przystępującego w formularzu ofertowym, przepisy rządowe FIPS, widok przez FortiOS 6.2. poziom 2, X.0.2. – definicja standardu FIPS, modułu krytograficznego, X.0.3. - Dokumentacja FortiManager 6.2.7, gdzie urządzenie model FMG-400G nie jest na liście wspieranych urządzeń dla oprogramowania w wersji 6.2.7),

- dowody złożone przez Przystępującego (w części wskazanej przez Przystępującego w piśmie procesowym, dotyczącej zarzutów podlegających rozpoznaniu: dowód nr 11-16- specyfikacje techniczne urządzeń Fortinet wraz z tłumaczeniem na język polski, do których linki zostały podane również w formularzu ofertowym Wykonawcy, dowód nr 16a oraz 16b1 i 16b2 – opis usługi FortiCare wraz z tłumaczeniem na język polski, dowód nr 17 oraz 18 - zrzut z ekranu z portalu support.fortinet.com wraz z tłumaczeniem na język polski, dowód nr 40a – oświadczenie producenta co do wsparcia producenta funkcjonalności VPN oraz certyfikacji FIPS 140-2 urządzenia GR 1801F, dowód nr 19 i 20 – certyfikat tożsamy z linkiem w ofercie wraz z tłumaczeniem, dowód nr 21 oraz 22 - przepisy rządowe FIPS, dowód nr 23 oraz 24 – certyfikat wraz z tłumaczeniem ze strony NIST, dowód nr 25 oraz 26 – zrzut ze strony Program Walidacji Algorytmów Kryptograficznych dla procesora CP9 wraz z tłumaczeniem na język polski, dowód nr 27 i 28 – zrzut ze strony Fortinet odnośnie możliwości CP9 FortiOS 6.2.7. wraz z tłumaczeniem, dowód nr 29, 30, 31, 32 – zrzuty ze strony Fortinet na potwierdzenie, że w urządzeniu FG 1801F jest procesor CP9 wraz z tłumaczeniem na język polski, dowód nr 33 i 34 - FIPS 140-2 Niezastrzeżona polityka bezpieczeństwa FortiOS 6.0 i 6.2. wraz z tłumaczeniem, dowód nr 35 i 36 – wydruk ze strony Fortinet odnośnie konsoli FortiManager wraz z tłumaczeniem, dowód nr 36a (47) - zrzut z wiersza poleceń systemu FortiManager FMG-400G oraz zrzut ekranu z uruchamiającego się przykładowego urządzenia FortiAnalyzer FAZ-1000F, dowód nr 37 i 38 – wydruk ze strony

Fortinet odnośnie FortiAnalyzer wraz z tłumaczeniem, dowód nr 39 i 40 – certyfikat 3884 dotyczący oferty Odwołującego wraz z tłumaczeniem oraz dowód nr 6 i 7 – dokument wraz z tłumaczeniem: FortiOS - Informacje o wydaniu Wersja 6.2.7.)

Na podstawie tych dokumentów, jak również biorąc pod uwagę oświadczenia, stanowiska i dowody złożone przez strony i uczestnika postępowania w trakcie posiedzenia i rozprawy, Krajowa Izba Odwoławcza ustaliła i zważyła:

Odwołanie podlegało oddaleniu.

W zakresie podniesionych zarzutów Izba ustaliła następujący stan faktyczny:

Zgodnie z pkt 4 Rozdziału I: SWZ: *„4. Opis przedmiotu zamówienia oraz zamówienia częściowe. 4.1. Przedmiotem zamówienia jest dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją. Przedmiot zamówienia został szczegółowo opisany w rozdziale II SWZ – Opis przedmiotu zamówienia. 4.2. Wszystkie wymagania określone w rozdziale II SWZ – Opis przedmiotu zamówienia stanowią wymagania minimalne, a ich spełnienie jest obligatoryjne – z wyjątkiem wymagań wyraźnie oznaczonych jako przedmiot kryterium oceny ofert. Niespełnienie ww. wymagań minimalnych będzie skutkować odrzuceniem oferty na podstawie art. 226 ust. 1 pkt 5 ustawy Pzp, jako niezgodnej z warunkami zamówienia."*

W myśl pkt 6 Rozdziału I: SWZ: *„6. Informacja o przedmiotowych środkach dowodowych 6.1. Zamawiający żąda złożenia wraz z ofertą przedmiotowych środków dowodowych – na potwierdzenie zgodności oferowanych dostaw z wymaganiami określonymi w rozdziale II SWZ – Opis przedmiotu zamówienia oraz kryteriami oceny ofert określonymi w opisie kryteriów oceny ofert w pkt. 19 niniejszego Rozdziału I SWZ tj.: 6.1.1. Wykaz parametrów oferowanych lub opis sposobu spełniania wymagań zawartych w OPZ – składany wraz z ofertą w celu potwierdzenia parametrów wymaganych w OPZ – stanowiący załącznik nr 6 do Formularza oferty; 6.1.2. Wykaz parametrów oferowanych lub opis sposobu spełniania wymagań zawartych w OPZ – składany wraz z ofertą w celu potwierdzenia zgodności z kryteriami określonymi w opisie kryteriów oceny ofert – stanowiący załącznik nr 7 do Formularza oferty; 6.1.3. Wskazanie – odpowiednio w załączniku 6 lub 7 do Formularza oferty – miejsca w dokumentacji urządzenia/oprogramowania, w którym znajduje się potwierdzenie spełnienie danego wymagania (nazwa dokumentu, numer strony dokumentu, pkt, etc. oraz adres strony WWW pod którym dokument jest opublikowany, a także publicznie i powszechnie dostępny bez konieczności logowania). W przypadku jeśli wskazanie opisanego wyżej miejsca nie jest możliwe lub nie jest wystarczające, wykonawca powinien*

opisać sposób spełnienia danego wymagania dołączając inne przedmiotowe środki dowodowe na potwierdzenie spełnienia danego wymagania (np. zrzut konfiguracji, karta katalogowa, specyfikacja techniczna, dokumentacja licencyjna, dokumentacja oprogramowania) lub przedstawić oświadczenie producenta urządzenia/oprogramowania, z którego wynika sposób spełnienia danego wymagania. 6.2. Zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane dostawy/usługi spełniają określone przez Zamawiającego wymagania, cechy lub kryteria. 6.3. Jeżeli wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie. 6.4. Postanowienia pkt 6.3 powyżej nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzeniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub gdy pomimo złożenia przedmiotowego środka dowodowego oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania. 6.5. Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści przedmiotowych środków dowodowych."

Zgodnie z pkt 13.2.9. SWZ: *„13.2.9. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski. Zamawiający dopuszcza możliwość składania przedmiotowych środków dowodowych, wskazanych w pkt [6] w języku angielskim – również poprzez wskazanie dokumentów i publikacji producentów zredagowanych w języku angielskim lub ich części lub fragmentów – w Wykazie parametrów oferowanych lub opis sposobu spełniania wymagań zawartych w OPZ stanowiącym załącznik nr 5 do Formularza oferty oraz w Wykazie parametrów oferowanych lub opis sposobu spełniania wymagań zawartych w OPZ stanowiącym załącznik nr 6 do Formularza oferty."*

Zgodnie z pkt II OPZ: Przedmiot zamówienia: *„(1) Przedmiotem zamówienia jest dostawa urządzeń systemu klasy NGFW (ang. Next Generation Firewall) wraz z usługami wsparcia oraz gwarancją producenta i świadczeniem w ramach prawa opcji godzin eksperckich na rzecz Zamawiającego. (2) Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji: (…) Urządzenia: oznacza przedmiot zamówienia opisany w pkt. III.1 niniejszego dokumentu. (…) Wsparcie producenta: oznacza oferowane przez producenta Urządzeń aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane dla poszczególnych urządzeń przez zdefiniowany okres czasu."*

W myśl pkt III OPZ: Specyfikacja wymagań: *„Przedmiotem zamówienie jest dostawa urządzeń klasy NGFW, opisanych w pkt. III.1 oraz przeprowadzenie ich pierwszej instalacji i uruchomienia, w ramach usług opisanych w pkt. III.2. a następnie świadczenie usług opisanych w pkt. III.2 – III.4. III.1. Dostawa Urządzeń. Przedmiotem zamówienia jest dostawa:*

(a) sześciu urządzeń klasy NGFW (ang. Next Generation Firewall), zwanych dalej „NGFW", w tym: (i) dwóch NGFW typu 1, (ii) dwóch NGFW typu 2 (iii) dwóch NGFW typu 3, (b) dwóch konsol zarządzających w/w NGFW, zwanych dalej „Konsolami Zarządzającymi". zwanych łącznie „Urządzeniami", w terminie czterech tygodni od dnia podpisania umowy. III.1.1. Wymagania ogólne dla Urządzeń: (…) 3. Jednorodność, szyfrowanie i dodatkowe kryteria bezpieczeństwa 3.1 Urządzenia wchodzące w skład Systemu NGFW muszą pochodzić od tego samego producenta oraz nie mogą znajdować się na liście (typu „end-of-life" oraz „end-of-support"), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025. (…) 3.5 NGFW i Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny *Zamawiający wskazuje następujące warunki równoważności dla normy FIPS 140-2 lub 140-3 i uzna za normę równoważną opisywanej, normę która: 1. Definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące, 2. Została wydane przez NIST (ang. National Institute of Standards and Technology) lub została wydana przez podmiot prawa publicznego, powołany przez co najmniej jedno z Państw Członkowskich Unii Europejskiej lub NATO, do definiowania standardów bezpieczeństwa przetwarzania informacji, 3. Opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji, 4. Została wskazana w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa III.1.2. Wymagania dla urządzeń NGFW (…) 17. VPN 17.1 NGFW typ 2 i 3 muszą posiadać funkcjonalność VPN: 17.1.1 SSL VPN: w sumie (typ 2 i 3) min. 100 równoległych tuneli oraz 17.1.2 min. 100 tuneli IPSEC per Typ 2 i 3 (w sumie min. 200). 17.2 NGFW typ 1 musi posiadać funkcjonalność zestawiania min. 100 tuneli IPSEC. 17.3 NGFW typ 2 i 3 muszą posiadać funkcjonalność VPN typu clientless (Ilość wspieranych równoległych tuneli VPN typu clientless w sumie min. 100) albo należy dostarczyć dedykowane dwa urządzenia umożliwiające: 17.3.1 konfigurację HA (ang. High availability) w trybie active/active. 17.3.2 zestawienie w sumie min. 100 tuneli vpn typu clientless 17.3.3 wraz z systemem musi być*

dostarczona możliwość zarządzania (on-prem). 17.3.4 każde z tych urządzeń będą posiadały min. 2 porty SFP, 2 porty SFP+ i port w celu zdalnego zarządzania. 17.3.5 każde z tych urządzeń będzie posiadało dwa zasilacze typu hot-plug. 17.4 NGFW musi posiadać mechanizm terminowania w/w (wszystkich) typów VPN ze wsparciem IPv6 i IPv4. 17.5 VPN w NGFW musi wspierać mechanizm pojedynczego logowania SSO (ang. Single Sign-On). 17.6 Autoryzacja kont vpn musi być możliwa z wykorzystaniem co najmniej usługi katalogowej (AD i LDAP). (…) III.4.Zasady świadczenia usług Wsparcia Producenta. (1) Wykonawca zobowiązany jest zapewnić wsparcie producenta tych urządzeń (dalej określanego jako „Producent") lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta dla dostarczonych subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pkt II powyżej. (2) Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów. (3) Dostęp do uaktualnień sygnatur/reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez producenta wraz z niezbędnymi danymi logowania, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych."

Zgodnie z załącznikiem nr 5 do Formularza oferty: COI-ZAK.262.46.2021 – wzór wykazu parametrów oferowanych lub opis sposobu spełniania wymagań zawartych w OPZ – składany wraz z ofertą w celu potwierdzenia parametrów wymaganych w OPZ Wykonawcy byli zobowiązani oświadczyć o spełnieniu bądź nie danego wymagania OPZ, przedstawić opis oferowanych parametrów lub sposobu spełnienia wymagania oraz *„Wskazanie miejsca w dokumentacji [publicznie i powszechnie dostępnej na stronach WWW producenta.] urządzenia/oprogramowania, w którym znajduje się potwierdzenie spełnienie danego wymagania (nazwa dokumentu, numer strony dokumentu, pkt, etc. oraz adres strony WWW pod którym dokument jest opublikowany, a także publicznie i powszechnie dostępny bez konieczności logowania). W przypadku jeśli wskazanie opisanego wyżej miejsca nie jest możliwe lub nie jest wystarczające, wykonawca powinien opisać sposób spełnienia danego wymagania dołączając inne przedmiotowe środki dowodowe na potwierdzenie spełnienia danego wymagania (np. zrzut konfiguracji, karta katalogowa, specyfikacja techniczna,*

dokumentacja licencyjna, dokumentacja oprogramowania) lub przedstawić oświadczenie producenta urządzenia/oprogramowania, z którego wynika sposób spełnienia danego wymagania."

W załączniku nr 5 Zamawiający wskazał m.in.:

- III.1.1 Lp. 3: *„3.2 NGFW lub Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny."*

- III.1.2 Lp. 17 *„17.1 NGFW typ 2 i 3 muszą posiadać funkcjonalność VPN: 17.1.1 SSL VPN: w sumie (typ 2 i 3) min. 100 równoległych tuneli oraz 17.1.2 min. 100 tuneli IPSEC per Typ 2 i 3 (w sumie min. 200). 17.2 NGFW typ 1 musi posiadać funkcjonalność zestawiania min. 100 tuneli IPSEC. 17.3 NGFW typ 2 i 3 muszą posiadać funkcjonalność VPN typu clientless (Ilość wspieranych równoległych tuneli VPN typu clientless w sumie min. 100) albo należy dostarczyć dedykowane dwa urządzenia umożliwiające: 17.3.1 konfigurację HA (ang. High availability) w trybie active/active. 17.3.2 zestawienie w sumie min. 100 tuneli vpn typu clientless 17.3.3 wraz z systemem musi być dostarczona możliwość zarządzania (on-prem). 17.3.4 każde z tych urządzeń będą posiadały min. 2 porty SFP, 2 porty SFP+ i port w celu zdalnego zarządzania. 17.3.5 każde z tych urządzeń będzie posiadało dwa zasilacze typu hot-plug.; Dodatkowo, należy wskazać Urządzenia (zawarte w tabeli pkt 7 Formularza Oferty), które będą realizować wymaganie pkt 17.3 – 17.3.5 OPZ)."*

Przystępujący w złożonym Formularzu oferty w pkt 4 oświadczył: *„4.2. w przypadku wyboru mojej oferty zobowiązuję się do zrealizowania przedmiotu zamówienia, zgodnie z warunkami zapisanymi w SWZ."*

W Tabeli cenowej nr 1 [sprzęt NGFW spełniający parametry opisane w pkt III 1.1 i III.1.2 III.1.3.Opisu przedmiotu zamówienia] Przystępujący wskazał: poz. 1: *„Dostawa sprzętu NGFW wraz z Gwarancją i wsparciem technicznym przez 36 miesięcy Typ 1 Producent Fortinet Model FG-3301E"*, poz. 2: *„Dostawa sprzętu NGFW wraz z Gwarancją i wsparciem technicznym przez 36 miesięcy Typ 2 Producent Fortinet Model FG-1801F. 13"*, poz. 3: *„Dostawa sprzętu NGFW wraz z Gwarancją i wsparciem technicznym przez 36 miesięcy Typ 3 Producent Fortinet Model FG-401E"*, poz. 4: *„Dostawa Konsol Zarządzających NGFW wraz z Gwarancją i wsparciem technicznym przez 36 miesięcy Producent Fortinet Model FMG-400G + FAZ-1000F."*

W pkt 6. Wykaz zaoferowanych licencji/subskrypcji Przystępujący wskazał m.in.:

„1. FG-3301E Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

2. FG-3301E Secure RMA Service

3. FG-1801F Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

4. FG-1801F Secure RMA Service

5. FG-401F Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

6. FG-401F Secure RMA Service

7. FMG-400G 24x7 FortiCare Contract

8. FMG-400G Secure RMA Service

9. FAZ-1000F 24x7 FortiCare Contract

10. FAZ-1000F Secure RMA Service"

W pkt III.1.1 Lp. 3: 3.2 NGFW lub Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny załącznika nr 5 do Formularza oferty Przystępujący oświadczył, że spełnia, podał: *„NGFW z zainstalowanym systemem operacyjnym FortiOS dostarcza mechanizm szyfrowania danych, który posiadała certyfikacje FIPS 140-2"* i wskazał linki: https://www.fortinet.com/corporate/about-us/product-certifications/fips

https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3814

W pkt III.1.2 Lp. 17 załącznika nr 5 do Formularza ofertowego:

Pkt 17.1. i 17.2. Przystępujący oświadczył, że spełnia i wskazał: *„NGFW typ 2 i 3 posiadają funkcjonalność VPN: - SSL VPN: w sumie (typ 2 i 3) min. 5000 równoległych tuneli oraz - min. 2000 tuneli IPSEC per Typ 2 i 3 NGFW typ 1 posiada funkcjonalność zestawiania min. 40000 tuneli IPSEC."* oraz podał linki:

„Firewall typ 2. Opis VPN strona 5. Concurrent SSL-VPN Users, Gateway-to-Gateway IPsec VPN Tunnels

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1800f-series.pdf

Firewall typ 3. Opis VPN strona 5. Concurrent SSL-VPN Users, Gateway-to-Gateway IPsec VPN Tunnels

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_400E.pdf

Firewall typ 1. Opis VPN strona 5. Gateway-to-Gateway IPsec VPN Tunnels

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-3300e-series.pdf"

Pkt 17.3. Przystępujący oświadczył, że spełnia i wskazał: *„NGFW typ 2 i 3 posiadają funkcjonalność VPN: - SSL VPN: w sumie (typ 2 i 3) min. 5000 równoległych tuneli oraz - min. 2000 tuneli IPSEC per Typ 2 i 3"* oraz podał linki:

„https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-1800f-series.pdf

Firewall typ 3. Opis VPN strona 5. Concurrent SSL-VPN Users, Gateway-to-Gateway IPsec VPN Tunnels

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_400E.pdf

Opis funkcjonalności SSL VPN Web Model

https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/579694/ssl-vpn-web-mode-for-remote-user"

Pismem z dnia 31 stycznia 2022 r. Zamawiający zwrócił się do Wykonawcy z wezwaniem do wyjaśnienia/uzupełnienia przedmiotowych środków dowodowych oraz wyjaśnienia treści oferty w pkt 6 wskazując: *„6) Zamawiający, w postanowieniu pkt III.1.1. ppkt 3.4 Opisu przedmiotu zamówienia postawił następujące wymaganie „3.5 NGFW i Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny." Wykonawca, na potwierdzenie że oferowane rozwiązanie spełnia ten wymóg przedstawił dokument dotyczący „FortiOS 6.0 and 6.2" w którym nie są wymienione żadne z Urządzeń wskazanych w ofercie Wykonawcy. Zamawiający powziął zatem wątpliwość, czy zarówno NGFW jak i Konsola Zarządzająca dostarczają mechanizm szyfrowanie danych, zgodny z ppkt 3.4 przy jednoczesnym spełnieniu pozostałych wymogów OPZ. Zamawiający wzywa zatem Wykonawcę do wyjaśnienia z czego ma wynikać fakt, że wskazane w ofercie Urządzenia: NGFW tj. FG-1801F, FG-401E, FG-3301E lub Konsola Zarządzająca tj. FMG-400G, FAZ-1000F, dostarczają mechanizm szyfrowania danych, który posiadający certyfikacje FIPS 140-2 lub 140-3 lub równoważny albo do przedłożenia przedmiotowych środków dowodowych potwierdzających takie oświadczenie Wykonawcy. Dodatkowo Zamawiający*

wzywa Wykonawcę do wskazania, która wersja „FortiOS" zapewni takie funkcjonowanie Urządzeń, które będzie zgodne z FIPS 140-2 (lub 140-3) i jednocześnie będzie spełniać pozostałe wymagania OPZ."

Pismem z dnia 7 lutego 2022 r. Przystępujący wyjaśnił i uzupełnił: *„Wyjaśnienie, uzupełnienie dokumentu. Potwierdzenie spełnienia certyfikacji szyfrowania ruchu dla oferowanego urządzenia można znaleźć pod następującym linkiem:*

https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3814

W wyżej wymienionym dokumencie jest potwierdzenie spełnienia certyfikacji FIPS 140-2 dla oferowanego urządzenia z systemem operacyjnym FortiOS 6.2 w tym oferowanej wersji FortiOS 6.2.7

Dodatkowa informacja na stronie producenta:

https://www.fortinet.com/corporate/about-us/product-certifications/fips

Dodatkowo informujemy, że pozostałe funkcjonalności wymagane w OPZ są spełnione w oferowanej wersji oprogramowania NGFW FortiOS 6.2.7."

W pierwszej kolejności wskazania wymaga, że Izba umorzyła postępowanie odwoławcze co do zarzutów z lit. a, b oraz e odwołania, wycofanych przez odwołującego.

W zakresie zarzutów wycofanych Izba umorzyła postępowanie odwoławcze na podstawie art. 568 pkt 2 ustawy pzp, ponieważ oświadczenie o cofnięciu części zarzutów odwołania uznać należy za oświadczenie najdalej idące złożone przez Stronę, która zainicjowała postępowanie odwoławcze. Złożenie takiego oświadczenia warunkuje zakończenie postępowania odwoławczego co do zarzutów wycofanych bez ich merytorycznego rozpoznania. Odwołujący podejmuje bowiem decyzję o ostatecznym zaniechaniu kontynuowania sporu przed Izbą w tym zakresie.

Przechodząc do zarzutów podlegających rozpoznaniu Izba uznała, że oferta Przystępującego nie wykazuje niezgodności z warunkami zamówienia podnoszonych przez Odwołującego.

Na wstępnie podnieść należy, że zgodnie z art. 226 ust. 1 pkt 5 ustawy pzp: *„1. Zamawiający odrzuca ofertę, jeżeli: (…) 5) jej treść jest niezgodna z warunkami zamówienia."* Natomiast w myśl art. 7 pkt 29 ustawy pzp: *„Ilekroć w niniejszej ustawie jest mowa o: 29) warunkach zamówienia – należy przez to rozumieć warunki, które dotyczą zamówienia lub*

postępowania o udzielenie zamówienia, wynikające w szczególności z opisu przedmiotu zamówienia, wymagań związanych z realizacją zamówienia, kryteriów oceny ofert, wymagań proceduralnych lub projektowanych postanowień umowy w sprawie zamówienia publicznego."

Podkreślić należy, że na gruncie nowej ustawy pzp i wykładni art. 226 ust. 1 pkt 5 ustawy pzp, aktualne pozostają tezy orzecznictwa i stanowisko doktryny dotyczące art. 89 ust. 1 pkt 2 poprzedniej ustawy pzp. Aby zamawiający był uprawniony odrzucić ofertę na podstawie przywołanego przepisu jest zobowiązany przeprowadzić analizę porównawczą treści oferty oraz warunków zamówienia (w szczególności, co do zakresu, ilości, jakości, warunków realizacji i innych elementów istotnych dla wykonania zamówienia), które stanowią merytoryczne postanowienia oświadczeń woli odpowiednio: zamawiającego, który w szczególności przez opis przedmiotu zamówienia precyzuje i uszczegóławia, jakiego świadczenia oczekuje po zawarciu umowy w sprawie zamówienia publicznego, oraz wykonawcy, który zobowiązuje się do wykonania tego świadczenia w razie wyboru złożonej przez niego oferty (zdefiniowanej w art. 66 kodeksu cywilnego) jako najkorzystniejszej. Dokonanie takiego porównania przesądza o tym, czy treść złożonej w postępowaniu oferty odpowiada warunkom zamówienia. Niezgodność treści oferty z warunkami zamówienia zachodzi więc, gdy zawartość merytoryczna złożonej w danym postępowaniu oferty nie odpowiada ukształtowanym przez zamawiającego i zawartym w SWZ wymaganiom. Istotnym jest, że niezgodność oferty z warunkami zamówienia musi po pierwsze być oczywista i niewątpliwa, czyli zamawiający musi mieć pewność co do niezgodności oferty z jego oczekiwaniami, przy czym postanowienia SWZ powinny być jasne i klarowne (tak też: wyrok z dnia 22 września 2020 roku, sygn. akt: KIO 1864/20; wyrok z dnia 20 stycznia 2020 roku, sygn. akt: KIO 69/20). Po drugie, odrzucenie oferty nie może nastąpić z błahych, czysto formalnych powodów nie wpływających na treść złożonej oferty, jak również gdy zamawiający ma możliwość poprawienia błędów jakie zawiera oferta.

Odnosząc się do zarzutu dotyczącego braku wsparcia producenta dla funkcjonalności VPN Izba stwierdziła, że Zamawiający prawidłowo ocenił, iż oferta Przystępującego nie wykazuje takiej niezgodności z warunkami zamówienia.

Podkreślenia wymaga, że ocena Izby czynności Zamawiającego wobec zarzutu zaniechania odrzucenia oferty Przystępującego opierała się przede wszystkim na dokumentacji przedmiotowego postępowania i wymagań wobec zamówienia w niej sprecyzowanych oraz

treści oferty Przystępującego, gdyż to na tym materiale bazował również Zamawiający dokonując czynności w postępowaniu.

Zauważyć zatem należy, że w zakresie usługi wsparcia producenta Zamawiający, jak wynika z poczynionych ustaleń faktycznych, sprecyzował swoje wymagania w pkt III.4 SWZ odnosząc się zbiorczo do wsparcia producenta urządzeń. Niewątpliwie pkt III.4 precyzuje, iż urządzenia muszą posiadać opisane przez Zamawiającego wsparcie, przez co Zamawiający rozumie: oprogramowanie – licencje. Z dokumentacji nie wynika, aby Zamawiający co do spełnienia postawionych wymagań w zakresie wsparcia producenta wymagał od wykonawców potwierdzenia w postaci przedmiotowych środków dowodowych – brak takiej pozycji w załączniku nr 5 do Formularza ofertowego. W pkt 6 Formularza oferty Zamawiający wymagał natomiast wskazania zaoferowanych licencji/subskrypcji. W tym zakresie Przystępujący wskazał m.in. na oprogramowanie „24x7 FortiCare". Co do braku wsparcia producenta funkcjonalności VPN Odwołujący odwołał się do pkt III 1.2. L.p. 17 Tabeli, w tym pkt 17.1. i 17.2. załącznika nr 5 do Formularza ofertowego wskazując, że z uwagi na brak w wykazie licencji Przystępującego dodatkowej licencji dotyczącej wsparcia funkcjonalności VPN to uznać należy, że został zaoferowany darmowy klient VPN, który takiego wsparcia nie zapewnia. Izba zwraca uwagę, że sama konstrukcja zarzutu wskazuje, że twierdzenia Odwołującego są nietrafione. Uzasadnienie zarzutu w ogóle nie referuje do treści oferty złożonej przez Przystępującego, a opiera się na założeniach własnych Odwołującego, co powoduje że już z tych względów zarzut należało uznać za niezasadny. Dalej podnieść należy, że w pkt III. 1.2. L.p. 17 pkt 17.1. i 17.2 Tabeli załącznika nr 5 do Formularza ofertowego, Przystępujący wskazał po pierwsze, iż funkcjonalność VPN jest zapewniona co do wszystkich trzech typów oferowanych urządzeń NGFW, a ponadto odesłał Zamawiającego we wskazanych linkach do specyfikacji technicznej oferowanych urządzeń w wersji angielskiej (dopuszczonej przez Zamawiającego). Izba korzystając z dowodu nr 12, 14 i 16 Przystępującego zawierających tłumaczenie na język polski specyfikacji technicznych urządzeń ustaliła, że wynika z nich po pierwsze zaoferowanie funkcjonalności VPN (czego Odwołujący nie kwestionował), po drugie wynika, że zaoferowane urządzenia posiadają system operacyjny FortiOS, w ramach którego działa usługa FortiCare jako wsparcie producenta urządzeń. Postanowienia w tym zakresie są podobne dla specyfikacji technicznych każdego z urządzeń oferowanych przez Przystępującego, przykładowo dla FG-1801F: *„Procesor sieciowy. Nowy, przełomowy procesor sieciowy SPU NP7 firmy Fortinet jest zintegrowany z funkcjami systemu FortiOS i zapewnia: ▪ Najwyższą wydajność zapory firewall dla IPv4/IPv6, SCTP i ruchu multicast z bardzo małymi opóźnieniami ▪ akcelerację*

sieci VPN, CAPWAP i tuneli IP ▪ Zapobieganie włamaniom na podstawie anomalii, odciążanie sum kontrolnych i defragmentacja pakietów ▪ Kształtowanie ruchu i szeregowanie priorytetów." I dalej: *„Usługi FortCare. Firma Fortinet pragnie pomóc swoim klientom w osiągnięciu sukcesu. Każdego roku usługi FortiCare pomagają tysiącom organizacji w pełni wykorzystać możliwości rozwiązania Fortinet Security Fabric. Zatrudniamy ponad 1000 ekspertów, którzy pomagają przyspieszyć wdrożenie technologii, zapewniają niezawodną pomoc w ramach zaawansowanego wsparcia oraz oferują proaktywną opiekę w celu maksymalizacji bezpieczeństwa i wydajności wdrożeń Fortinet."* Nie ulega wątpliwości, że skoro usługa wsparcia FortiCare obejmuje całe urządzenie to również zapewnione jest wsparcie co do objętej specyfikacją techniczną urządzenia funkcjonalności VPN. Dowód nr 16a wraz z tłumaczeniem na język polski – dowód nr 16b1 oraz nr 16b2 Przystępującego: specyfikacja usługi Fortinet – FortiCare potwierdza wsparcie techniczne producenta. Dowód nr 17 wraz z tłumaczeniem, czyli dowodem nr 18 Przystępującego - zrzut z ekranu z portalu support.fortinet.com, dodatkowo potwierdza możliwość zgłoszenia do producenta problemów technicznych dla urządzenia 1800F z wykupioną usługą 24x7 FortiCare także w zakresie funkcjonalności VPN. Z dowodu nr 40a Przystępującego wynika oświadczenie producenta Fortinet potwierdzające zapewnienie przez producenta wsparcia dla wszystkich funkcjonalności urządzenia w tym również funkcjonalności SSL VPN oraz IPSec VPN. Wyżej wskazane dowody mają jednak wyłącznie charakter wzmacniający wynikający z samej oferty Przystępującego wniosek, iż wsparcie techniczne funkcjonalności VPN zostało zaoferowane. Izba uznała dowody przedłożone przez Odwołującego (dowód dodatkowy złożony poza skoroszytem nr IX.5, dowód nr IX.3, IX.4 (1), IX.4 (2) jako nieprzydatne dla rozstrzygnięcia, gdyż odnoszą się one do oprogramowania VPN FortiClient, które nie zostało zaoferowane przez Przystępującego i mogły jedynie dowodzić prawdziwości założeń własnych Odwołującego, iż konieczne było zaoferowanie dodatkowych licencji oprogramowania VPN i wsparcia, nie mających oparcia w treści złożonej przez Przystępującego oferty oraz w wymaganiach SWZ.

Przechodząc do zarzutu dotyczącego braku certyfikacji FIPS Izba stwierdziła, że oferta Przystępującego nie wykazuje niezgodności z warunkami zamówienia co do tego wymagania. Uzasadnienie zarzutów Odwołującego opierało się na trzech twierdzeniach. Pierwsze zakładało, iż Zamawiający wymagał, aby zarówno urządzenia NGFW jak i kontrola zarządzająca dostarczały mechanizm szyfrowania danych, który będzie posiadał certyfikacje FIPS 140-2 lub 140-3 lub równoważny. Drugie opierało się na takiej wykładni postanowień SWZ, zgodnie z którą wykonawcy byli zobowiązani przedstawić przedmiotowe środki

dowodowe potwierdzające posiadanie certyfikacji FIPS 140-2 lub 140-3 lub równoważne dla sprzętu: urządzenia i kontroli zarządzającej. Natomiast trzecie wskazywało, że Przystępujący oświadczył w załączniku nr 5 Formularza ofertowego, iż spełnia wymaganie co do certyfikacji FIPS zarówno poprzez oferowane urządzenia jak i kontrolę zarządzającą. W ocenie Izby, w świetle dokumentacji postępowania, jak i treści oferty Przystępującego wszystkie te twierdzenia są chybione.

W pierwszej kolejności Izba zwraca uwagę na postanowienia dokumentacji postępowania. Jak wynika z ustaleń faktycznych Zamawiający w OPZ w pkt III.1.1. określił: *„3.5 NGFW i Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny*",* natomiast w załączniku nr 5 do Formularza ofertowego, wymagał: *„3.2 NGFW lub Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny."* Nie ulega wątpliwości, że postanowienia dokumentacji pozostają wobec siebie w sprzeczności co do wymagania certyfikacji FIPS. W pierwszym postanowieniu koniunkcja „i" wskazuje, iż wymaganiem objęte zostały zarówno urządzenia jak i konsola zarządzająca. Drugie natomiast – „lub" wskazuje, że wystarczające dla spełnienia wymagania będzie jeśli wyłącznie urządzenia lub wyłącznie konsola lub urządzenia i konsola „*będą dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny".* W sytuacji stwierdzonej rozbieżności dokumentacji postępowania należy dokonać korzystnej dla Wykonawcy wykładni jej treści. Zgodnie z ugruntowanym orzecznictwem Izby wykonawca nie może ponosić negatywnych konsekwencji niejednoznaczności i niejasności postanowień SWZ. Jak już zostało podniesione odrzucenie oferty na podstawie art. 226 ust. 1 pkt 5 ustawy pzp może nastąpić wyłącznie w sytuacji, gdy niezgodność z warunkami zamówienia jest oczywista w świetle spójnych wymagań określonych w dokumentacji postępowania, co w niniejszej sprawie nie ma miejsca. Podkreślić należy, że wykładnia niejednoznacznych postanowień powinna prowadzić do zaakceptowania przez Zamawiającego zarówno zaoferowania przez wykonawcę wyłącznie urządzeń, które „*będą dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny",* jak i wyłącznie konsoli, która będzie *„dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny",* a także urządzeń i konsoli, które „*będą dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny".* Zauważyć należy, że Zamawiający uwzględnił w tej części odwołanie

wskazując, iż oczekiwał aby zarówno urządzenia jak i konsola dostarczały ww. mechanizmy, a w jego ocenie konsole oferowane przez Przystępującego nie spełniają tego wymagania. Zdaniem Izby, oczekiwania Zamawiającego nie zostały jednoznacznie wyrażone w treści dokumentacji postępowania. Niezasadna okazała się również argumentacja, że wezwanie Zamawiającego z dnia 31 stycznia 2022 r. wskazywało, że i urządzenia i konsola miały dostarczać ww. mechanizmy szyfrowania. Z wezwania Zamawiającego, podobnie jak z treści SWZ wynika rozbieżność co do wymagań Zamawiającego. Z jednej strony Zamawiający wskazuje, że *„powziął zatem wątpliwość, czy zarówno NGFW jak i Konsola Zarządzająca dostarczają mechanizm szyfrowanie danych, zgodny z ppkt 3.4 przy jednoczesnym spełnieniu pozostałych wymogów OPZ.”,* a z drugiej *„Zamawiający wzywa zatem Wykonawcę do wyjaśnienia z czego ma wynikać fakt, że wskazane w ofercie Urządzenia: NGFW tj. FG-1801F, FG-401E, FG-3301E lub Konsola Zarządzająca tj. FMG-400G, FAZ-1000F, dostarczają mechanizm szyfrowania danych, który posiadający certyfikacje FIPS 140-2 lub 140-3 lub równoważny albo do przedłożenia przedmiotowych środków dowodowych potwierdzających takie oświadczenie Wykonawcy.”,* a więc o wykazanie wymagania co do urządzeń lub konsoli. Z treści wezwania wynikają zatem podobne niejednoznaczności jak z treści dokumentacji postępowania. Podkreślenia również wymaga, że niezasadne są twierdzenia Zamawiającego o nadrzędności postanowień OPZ. Izba zwraca uwagę, że w załączniku nr 5 Formularza ofertowego wykonawcy wykazywali spełnienie wymagań Zamawiającego. Skoro w treści samego Formularza Zamawiający dopuszcza urządzenia lub konsole to zastosowanie się do tych postanowień nie może rodzić po stronie Wykonawcy negatywnych konsekwencji. Podobnie zresztą jak zastosowanie się do treści wezwania, które również taką alternatywę określało. Zauważyć należy, że Przystępujący wskazał w Formularzu, iż oferuje: *„NGFW z zainstalowanym systemem operacyjnym FortiOS dostarcza mechanizm szyfrowania danych, który posiadała certyfikacje FIPS 140-2.”* W tym miejscu zaznaczenia wymaga, że chybione są twierdzenia Odwołującego, iż Przystępujący oświadczył, że oferuje zarówno urządzenia jak i konsolę, które dostarczając ww. mechanizmy. Wykonawca złożył oświadczenie wyłącznie, że urządzenia NGFW dostarczają ww. mechanizmy posiadające certyfikację FIPS.

Odnosząc się dalej do argumentacji Odwołującego, że nawet wszystkie urządzenia NGFW, a konkretnie urządzenie FG-1801F nie spełnia wymagania, gdyż nie posiada certyfikacji FIPS 140-2 podkreślić należy, że Izba w całości podziela stanowisko Przystępującego co do wykładni oczekiwań Zamawiającego. W ocenie Izby z postanowienia *„NGFW lub Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał*

odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny." wynika jednoznacznie, że Zamawiający nie określił w jaki sposób, na jakim poziomie urządzenie ma dostarczać mechanizm szyfrowania danych posiadający certyfikację. Urządzenia mają jedynie dostarczać takie mechanizmy, które posiadają certyfikację FIPS, co nie oznacza że to urządzenia muszą taką certyfikację posiadać. Interpretacja taka jest zgodna zresztą z oczekiwaniami Zamawiającego. Wynika to m.in. z treści wezwania Przystępującego do wyjaśnienia z dnia 31 stycznia 2022 r., w którym Zamawiający stwierdza: „*Dodatkowo Zamawiający wzywa Wykonawcę do wskazania, która wersja „FortiOS" zapewni takie funkcjonowanie Urządzeń, które będzie zgodne z FIPS 140-2 (lub 140-3) i jednocześnie będzie spełniać pozostałe wymagania OPZ."* Zamawiający dopuszczał bowiem rozwiązanie, iż dostarczenie mechanizmów szyfrowania posiadających certyfikację może odbywać się na poziomie systemu operacyjnego urządzenia, czyli urządzenie będzie dostarczało mechanizmy szyfrowania danych posiadające certyfikację FIPS 140-2. Izba zauważa, że Zamawiający uwzględniając ten zarzut odwołania podniósł, że w jego ocenie konsola zarządzająca nie dostarcza mechanizmów szyfrujących posiadających certyfikację FIPS 140-2. Zamawiający nie miał zatem wątpliwości odnośnie spełnienia wymagania co do urządzeń oferowanych przez Przystępującego, a jedynie wskazywał, że oczekiwał jego wykazania również względem konsoli, która to interpretacja niejasnych postanowień SWZ, jak już zostało podniesione, nie mogła prowadzić do odrzucenia oferty Przystępującego.

Izba zwraca uwagę, że Przystępujący na potwierdzenie powyższego wymagania załączył link do certyfikatu, z którego wynika, iż system FortiOS 6.0 i 6.2 posiada certyfikację FIPS 140-2 poziom 1. Jak już zostało wskazane, do oferty załączył również specyfikacje techniczne urządzeń, z których wynika że posiadają system operacyjny FortOS. Ponadto, w odpowiedzi na wezwanie Zamawiającego z 31 stycznia 2022 r. wskazał natomiast, że jest to system FortiOS 6.2.7., podał link do certyfikatu na stronie NIST oraz dodatkowej informacji o certyfikacji na stronie Fortinet – przepisy rządowe, gdzie wskazano, że *„FIPS 140-2 Poziom 1 dotyczy firmware'u lub oprogramowania (np. FortiOS. Certyfikat Poziomu 1 dotyczy efektywnie wszystkich modeli obsługiwanych przez certyfikowaną(e) wersję(y)."* (wynika z dowodu nr 21 wraz z tłumaczeniem). Certyfikacja FIPS 140-2 jest zatem na poziomie 1 czyli oprogramowania, co w świetle postanowień SWZ należało uznać za dopuszczalne.

W konsekwencji uznać należało na podstawie złożonej oferty oraz wyjaśnień, że Przystępujący spełnił wymagania Zamawiającego, gdyż zaoferował mechanizmy szyfrowania danych posiadające certyfikację FIPS 140-2 dostarczane razem z urządzeniem na poziomie systemu operacyjnego.

Założenia Odwołującego, iż Wykonawca powinien wykazać, że certyfikacja jest na poziomie urządzenia były w ocenie Izby błędne. W konsekwencji złożone przez Odwołującego dowody na potwierdzenie powyższego założenia (X.3.2.-X.3.3., X.6.1.-X.6.3. oraz X.0.3.) Izba uznała za nieprzydatne dla rozstrzygnięcia. Zgodnie z definicją FIPS w Wikipedii (dowód Odwołujący): jest to rządowy standard bezpieczeństwa komputerowego używany do zatwierdzania modułów kryptograficznych. Ponadto, jak wskazuje dowód nr X.0.2 złożony przez Odwołującego: definicja standardu FIPS 140-2 - to wymogi bezpieczeństwa dla modułów kryptograficznych. Zgodnie z przywołaną przez Odwołującego definicją moduł kryptograficzny to: *„zestaw sprzętu, oprogramowania i/lub oprogramowania układowego, który implementuje zatwierdzone funkcje bezpieczeństwa (w tym algorytmy kartograficzne i generowanie kluczy) i jest zawarty w granicach kryptograficznych."* Z definicji tej wynika, że także oprogramowanie układowe może być modułem dostarczającym mechanizmy szyfrowania posiadające certyfikację, co potwierdza, że Przystępujący spełnił wymóg, iż urządzenia (z systemem operacyjnym FortOS) dostarczają mechanizmy szyfrowania posiadające certyfikację FIPS 140-2. W ocenie Izby dowód nr X.0. Odwołującego wskazuje jedynie, że producent przeprowadza także certyfikację FIPS 140-2 na oprogramowanie i urządzenia, co oznaczałoby że byłby to poziom 2 (dowód nr 21 Przystępującego: przepisy rządowe: Federalny Standard Przetwarzania Informacji (FIPS 140-2 i 140-3): *„FIPS 140-2 Poziom 2 obejmuje sprzęt (np. urządzenie FortiGate, układy scalone FortiASIC) - certyfikat Poziomu 2 dotyczy dokładnej kombinacji certyfikowanych układów i modelu sprzętu."* W dokumencie tym wymieniono modele certyfikowane, a więc urządzenia. Natomiast certyfikat #3184 w modułach nie określa modeli urządzeń, a wyłącznie oprogramowanie FortiOS 6.0. i 6.2, poziom 1. Certyfikat do polityki bezpieczeństwa odnosi się natomiast wyłącznie w zakresie sekcji „Działanie zgodne ze standardem FIPS 140-2." Ponadto, jak wynika z dowodu nr 33 wraz z tłumaczeniem, złożonego przez Przystępującego z „FIPS 140-2 Niezastrzeżona polityka bezpieczeństwa FortiOS 6.0 i 6.2." przed Tabelą 2, na którą powoływał się Odwołujący wskazano na różne rozwiązania: *„Zakres fizycznej granicy kryptograficznej to FortiGate-2500E, natomiast walidowane moduły to moduły firmware FortiOS 6.0 i 6.2. (…) Każde załadowane oprogramowanie firmware, które nie jest wymienione na certyfikacie modułu, nie wchodzi w zakres tej walidacji i wymaga oddzielnej walidacji FIPS 140-2. Moduł może być również wykonany na dowolnym z poniższych urządzeń FortiGate/FortiWiFi/FortiGateRugged i pozostaje zgodny z FIPS-compliance potwierdzonym przez producenta."* Co więcej, jak już wskazano z dowodu nr 21 wraz z tłumaczeniem złożonego przez Przystępującego wynika, że *„FIPS 140-2 Poziom 1 dotyczy*

firmware'u lub oprogramowania (np. FortiOS. Certyfikat Poziomu 1 dotyczy efektywnie wszystkich modeli obsługiwanych przez certyfikowaną(e) wersję(y).”, a więc wszystkie urządzenia z tym oprogramowaniem będą dostarczały mechanizmy szyfrujące dane posiadające certyfikację. Jak już podniesiono, Zamawiający nie wymagał certyfikacji na poziomie sprzętu. Dowód nr 39 i 40 Przystępującego wraz z tłumaczeniem przedstawia certyfikat z oferty Odwołującego, który jako moduły certyfikowane podaje oprogramowanie i urządzenia, a także poziom certyfikacji 2. Dowód ten potwierdza, że certyfikaty odnoszą się do różnych poziomów, które jednak nie zostały określone przez Zamawiającego w wymaganiach i za dopuszczalny należało uznać poziom 1 – certyfikację oprogramowania.

Oznacza to, że wszystkie urządzenia NGFW zaoferowane przez Przystępującego, jako obsługiwane przez oprogramowanie FortiOS 6.2.7. dostarczają mechanizmy szyfrowania danych posiadające certyfikację (oprogramowanie FortOS 6.0. i 6.2. posiada certyfikat FIPS 140-2 poziom 1). Dodatkowo tylko wskazania wymaga, że dowód nr 6 i 7 – dokument wraz z tłumaczeniem: FortiOS - Informacje o wydaniu Wersja 6.2.7. potwierdza, że wszystkie oferowane przez Przystępującego urządzenia posiadają oprogramowanie systemowe FortiOS wersja 6.2.7. W konsekwencji w ocenie Izby zaoferowanie urządzeń z oprogramowaniem systemowym, posiadającym certyfikację FIPS spełnia wymóg aby urządzenia dostarczały mechanizmy szyfrowania danych posiadające certyfikację FIPS 140-2.

Wobec powyższego uznać należało, że Przystępujący zaoferował urządzenia spełniające wymaganie Zamawiającego co do certyfikacji FIPS i przedstawił na potwierdzenie przedmiotowe środki dowodowe. Zaznaczenia przy tym wymaga, że dodatkowe dowody Przystępującego dotyczące ewentualnego posiadania certyfikacji FIPS na poziomie urządzeń czy konsoli Izba uznała za nieprzydatne dla rozstrzygnięcia, ponieważ ocena czynności Zamawiającego w postępowaniu bazuje na materiale dowodowym, którym dysponował Zamawiający na etapie badania i oceny oferty, a który wykazywał spełnienie przez Przystępującego wymagań co do ww. certyfikacji nie potwierdzając przesłanki odrzucenia oferty na podstawie art. 226 ust. 1 pkt 5 ustawy pzp.

Mając na względzie powyższe orzeczono jak w sentencji.

O kosztach postępowania odwoławczego orzeczono stosownie do jego wyniku na podstawie art. 575 oraz art. 574 ustawy pzp, a także w oparciu o przepisy § 5 pkt 1 oraz § 8 ust. 2 zdanie 1 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz. U. z 2020 r., poz. 2437 ze zm.) zaliczając na poczet niniejszego postępowania odwoławczego koszt wpisu od odwołania uiszczony przez Odwołującego.

Przewodniczący: ……