

Sygn. akt: KIO 1549/21

WYROK
z dnia 12 lipca 2021 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Andrzej Niwicki
Członkowie: Izabela Niedziałek-Bujak
Aneta Młacka
Protokolant: Konrad Wyrzykowski

po rozpatrzeniu na rozprawie dnia 9 lipca 2021 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 24 maja 2021 r. przez wykonawcę **Netsecure Sp. z o.o., ul. Świętokrzyska 30/63, 00-116 Warszawa** w postępowaniu prowadzonym przez **Transportowy Dozór Techniczny, ul. Puławska 125, 02-707 Warszawa**

orzeka:

1.A. Umarza postępowanie w zakresie zarzutu opisanego w punkcie I.4 oraz II.4 odwołania;

B. Uwzględni pozostałe zarzuty odwołania i nakazuje zamawiającemu:

- zmianę w pkt III.1.2 opisu przedmiotu zamówienia przez nakazanie określenia znacznika czasu na poziomie co najmniej 4 lat;

- zmianę treści opisu przedmiotu zamówienia przez dopuszczenie zastosowania ofert równoważnych rozwiązaniu Palo Alto wraz z określeniem kryteriów oceny równoważności.

2. kosztami postępowania obciąża **Transportowy Dozór Techniczny, ul. Puławska 125, 02-707 Warszawa** i zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy), uiszczoną przez **Netsecure Sp. z o.o. siedzibą w Warszawie** tytułem wpisu od odwołania.

2.1. Zasądza od zamawiającego **Transportowy Dozór Techniczny, ul. Puławska 125, 02-707 Warszawa** na rzecz wykonawcy **Netsecure Sp. z o.o., ul. Świętokrzyska 30/63, 00-116 Warszawa** kwotę **18 600 zł 00 gr** (słownie osiemnaście tysięcy sześćset złotych zero groszy) tytułem zwrotu kosztów postępowania odwoławczego, w tym 15 000 zł z tytułu zwrotu wpisu od odwołania oraz 3 600 zł z tytułu wynagrodzenia pełnomocnika strony.

Stosownie do art. 579 ust. 1 oraz 580 ust. 1 i 2 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129) 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 1549/21

Uzasadnienie

Zamawiający: Transportowy Dozór Techniczny z siedzibą w Warszawie prowadzi postępowanie, którego przedmiotem jest dostawa sprzętu sieciowego, nr referencyjny postępowania: ZP 7/2021. Ogłoszono w Dz.UUE 12 maja 2021 r. nr 2021/S 092-237667, SWZ zamieszczono na stronie www Zamawiającego 12 maja 2021 r.

Netsecure sp. z o.o. z siedzibą w Warszawie wniósł odwołanie od niezgodnej z przepisami ustawy - Prawo zamówień publicznych (PZP) czynności Zamawiającego, polegającej na sformułowaniu treści Specyfikacji Warunków Zamówienia (SWZ), w tym Opisu Przedmiotu Zamówienia stanowiącego zał. do SWZ (OPZ) w sposób sprzeczny z przepisami prawa, w szczególności w zakresie:

1. określenia w pkt III.1.2 OPZ, iż „Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat”,

2. określenia w punktach:

a.III.1.4 OPZ - w zakresie wymagania wyposażenia urządzenia w co najmniej jeden port konsoli USB Micro-B,

b.III.1.5 OPZ - w zakresie wymagania, „Urządzenia firewall muszą posiadać budowę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (Data Plane).”

c.III.1.6 OPZ - w zakresie wymagania: „Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.”

d.III.1.7 OPZ – wymagania: „Urządzenie musi obsługiwać 4000 znaczników VLAN ”

e.III.1.22 OPZ - wymagania: „Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu”

f.III.1.27 OPZ -wymagania: „Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa”

g.III.2.3 OPZ - w zakresie wymagania: „Dysk musi mieć możliwość wymiany bez potrzeb rozkręcania urządzenia” takich cech dostaw, że wprawdzie każda z nich z osobna cechuje również niektóre produkty konkurencyjne, ale ich zestawienie wskazuje na konkretny produkt w postaci PA220, PA820, PA3220 oraz system zarządzania Panorama PAN25 niezasadnie uprzywilejowując producenta - Palo Alto,

3.opisania przedmiotu zamówienia w ten sposób, że wskazuje w sposób pośredni na konkretnego producenta, bez zastosowania wyrazów „lub równoważny” oraz bez określenia kryteriów stosowanych w celu oceny równoważności;

4.zawarcia w SWZ, w rozdziale 7, pkt 1, ppkt 2 b wymogu: „wykaże, iż będzie dysponował przez cały okres realizacji zamówienia zespołem co najmniej trzech osób umożliwiającym realizację zamówienia na odpowiednim poziomie technicznym i wdrożeniowym tj. [...] osobą pełniącą funkcję konsultanta posiadająca certyfikat CIHE”.

Powyższym czynnościom zarzuca naruszenie następujących przepisów:

1. Ad. 1 - art. 99 ust. 2 oraz 4, art. 16 pkt 1 i 3 PZP przez sformułowanie wymagania w ten sposób, że nie jest w żaden sposób powiązane z oferowanym produktem (nie stanowi „cechy dostaw”), a jest powiązane jedynie z ogólnym ratingiem producenta, utrudnia konkurencję, wymóg w sposób faktyczny dyskwalifikuje producentów, którzy znajdują się w raportach Gartner przez okres krótszy powodując iż jedynym producentem spełniającym wymóg OPZ jest Palo Alto, a wyeliminowany jest Fortinet, obecny w raporcie od 4 lat.,

2.Ad. 2 - art. 99 ust. 2 oraz 4, art. 16 pkt 1 PZP przez zawarcie w OPZ takich cech dostaw, wymienionych w pkt 1.2 odwołania, że wprawdzie każda z nich z osobna cechuje niektóre produkty konkurencyjne, ale ich zestawienie wskazuje na konkretny produkt w postaci PA220, PA820, PA3220 oraz system zarządzania Panorama PAN25, niezasadnie uprzywilejowując producenta - Palo Alto i eliminując producenta Fortinet,

3.Ad. 3 - art. 99 ust. 5 i 6 PZP przez zaniechanie opisania przedmiotu zamówienia z zastosowaniem wyrazów „lub równoważny” oraz zaniechanie określenia kryteriów stosowanych w celu oceny równoważności, pomimo iż OPZ wskazuje pośrednio na konkretnego producenta: Palo Alto,

4.Ad. 4 - art. 16 pkt 1 i 3, art. 112 ust. 1 oraz ust. 2 pkt 4 PZP, art. 116 ust. 1 PZP, art. 124 pkt 2 PZP przez sformułowanie warunku udziału w postępowaniu w sposób nieproporcjonalny, niezapewniający równego traktowania wykonawców, niezapewniający zachowania uczciwej konkurencji, całkowicie oderwany od przedmiotu zamówienia, ponieważ przedmiot zamówienia nie wymaga wykonywania przez Wykonawcę czynności, które certyfikat CIHE potwierdza.

III.W związku z powyższym, wnosi o uwzględnienie odwołania i nakazanie Zamawiającemu modyfikacji SWZ przez:

1.usunięcie z pkt III.1.2 OPZ wymogu, aby „producent oferowanego rozwiązania był obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise NetWork Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat”, względnie - o usunięcie znacznika czasu lub nakazanie określenia go na poziomie 4 lat;

2.usunięcie z treści OPZ postanowień wskazanych w punkcie 1.2 niniejszego odwołania, względnie nakazanie dopuszczenia zastosowania ofert równoważnych rozwiązaniu Palo Alto wraz z określeniem kryteriów oceny równoważności;

3.dopuszczenie zastosowania ofert równoważnych rozwiązaniu Palo Alto wraz z określeniem kryteriów oceny równoważności;

4.usunięcie z treści SWZ wymagania posiadania przez konsultanta certyfikatu CIHE.

I. Działanie Zamawiającego forsuje rozwiązanie konkurencyjne - Palo Alto, naruszając przepisy PZP oraz przepisy regulujące dyscyplinę finansów publicznych.

1. Zamawiający zastrzegł w pkt III.1.2 OPZ, iż „Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat”. Jedynym producentem spełniającym wymóg jest Palo Alto, a wyeliminowany jest producent Fortinet, obecny w raporcie od 4 lat.

Zamawiający uznał, że obecność w raporcie Gartner przekłada się na jakość produktu.

Sposób ujęcia wymagania eliminuje z wyścigu o zamówienie większość lub całość konkurencji Palo Alto.

2. art. 99 ust. 2 oraz 4 PZP, art. 16 pkt 1 PZP przez zawarcie w OPZ takich cech dostaw, wymienionych w pkt 1.2 odwołania, że wprawdzie każda z nich z osobna cechuje również niektóre produkty konkurencyjne, ale ich zestawienie wskazuje na konkretny produkt w postaci PA220, PA820, PA3220 oraz system zarządzania Panorama PAN25., niezasadnie uprzywilejowując producenta - Palo Alto i eliminując producenta Fortinet.

Zamawiający przewidział następujące cechy dostaw (opisano je w tabeli wraz z innymi twierdzeniami właściwymi dla poszczególnych parametrów, z odniesieniem do orzecznictwa):

Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia może blokować funkcjonowanie części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.

III.1.6 OPZ Tak Nie posiada architektury tożsamej/identycznej z Palo Alto, wybór rozwiązań odbywać się powinien na podstawie rzeczywistego ruchu w sieci Klienta, który ma być chroniony Zapis faworyzujący producenta o konkretnej architekturze (PaloAltoNetworks) bez uzasadnienia merytorycznego - w konkurencyjnych do PaloAlto firewallach nadmierne obciążenie data plane jest niwelowane przez zastosowanie odpowiednio wydajnego urządzenia tak jak ma to miejsce przy każdym innym elemencie infrastruktury sieciowej czy bezpieczeństwa. Z reguły oddzielny Data Plane od ControlPlane jest stosowany przy wielogigowych przepływnościach - pozostawienie tego zapisu naraża Zamawiającego na wydatkowanie nieracjonalnych środków na zakup przewymiarowanych urządzeń. W szczególności dotyczy to jednostek terenowych Zamawiającego (inspektoratów) gdzie pracuje maksymalnie do 20-30 osób, które wykonując pracę biurową nie są w stanie wygenerować ruchu który może jakkolwiek zagrozić wydajnościom

nawet małych firewalli gdzie szczególnie konkurencyjną do PaloAlto Networks ofertę posiada właśnie dyskryminowany Fortinet.

Urządzenie musi obsługiwać 4000 znaczników VLAN III.1.7 OPZ tak. W adekwatnym wydajnościowo rozwiązaniu nie. Jak wynika z analiz wcześniejszych OPZ na zakup systemu antywirusowego Zamawiający posiada obecnie ok. 350 użytkowników. Gdyby założyć rozłożenie 350 pracowników na oddziały Zamawiającego to średnio w lokalizacji pracuje poniżej 20 osób. Najlepsze praktyki związane z segmentacją sieci mówią o kilku do kilkunastu VLAN w lokalizacji. Wymóg Zamawiającego jest zatem przewymiarowany. Wymóg posiadania 4 tys VLAN (sieci wirtualnych) dla urządzeń firewalla przy zatrudnieniu do 20 osób per jednostka terenowa sprawia, że wymóg byłby adekwatny gdyby Zamawiający około 20 -krotnie zwiększył zatrudnienie i jednocześnie chciał dla każdego użytkownika wydzielić odrębny segment wirtualny (VLAN) aby budować oddzielne polityki bezpieczeństwa między segmentami co w perspektywie cyklu życia produktu jest nieprawdopodobne i nieracjonalne.

Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Skoro Zamawiający oczekuje centralnego systemu zarządzania i raportowania dla wszystkich NGFW to raportowanie nie powinno odbywać się bezpośrednio z poziomu pojedynczych urządzeń firewall tylko właśnie z tego systemu. Właśnie system centralnego zarządzania jest miejscem dedykowanym do przechowywania logów oraz generowania raportów dla całego środowiska.

Wynik raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu.

Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa III.1.27 OPZ

Tak. W kształcie opisanym przez Zamawiającego - nie (ponieważ dotyczy to faktycznie wyglądu interfejsu) Każdy wiodący producent firewalli umożliwi konfigurację reguł NAT jak i polityk bezpieczeństwa gdyż jest to podstawowa funkcjonalność tych urządzeń.

Dysk musi mieć możliwość wymiany bez potrzeb rozkręcania urządzenia III.2.3 OPZ. Procedura wymiany dysków w praktyce nie występuje podczas eksploatacji systemu, w sytuacji awarii firewalla wymianie podlega całe urządzenie. Zapis ogranicza konkurencję i nie znajduje uzasadnienia. Czy istnieje inne rozwiązanie niż Palo Alto, które spełnia wszystkie w/w cechy?

NIE. Zamawiający dokonał doboru technologii (np. III.1.5 OPZ, III.1.6 OPZ, III.1.27 OPZ) i przesadzonych parametrów minimalnych (np. 4000 znaczników VLAN - III.1.7 OPZ) w taki sposób, aby faworyzować rozwiązanie Palo Alto. Opis przedmiotu zamówienia powinien być zatem skorelowany z rzeczywistymi, faktycznymi potrzebami zamawiającego. Przepisy nie definiują wprawdzie pojęcia „uzasadnionych potrzeb zamawiającego”, jednak ukształtowane ono zostało w orzecznictwie KIO, która jako zobiektywizowane potrzeby traktuje rzeczywiste, faktyczne potrzeby zamawiającego, zarówno co do oczekiwanych funkcjonalności, jak i wyspecyfikowanych parametrów oraz jakości, oparte na faktycznych i zobiektywizowanych okolicznościach.

3.naruszenie art. 99 ust. 5 i 6 PZP przez zaniechanie opisu przedmiotu zamówienia z zastosowaniem wyrazów „lub równoważny” oraz zaniechanie określenia kryteriów stosowanych w celu oceny równoważności, pomimo iż OPZ wskazuje pośrednio na konkretnego producenta: Palo Alto.

4.naruszenie art. 16 pkt 1 i 3, art. 112 ust. 1 oraz ust. 2 pkt 4, art. 116 ust. 1, art. 124 pkt 2 PZP przez sformułowanie warunku udziału dot. certyfikatu CIHE potwierdza. (zarzut cofnięty)

III. Żądania

1.Odwołujący sformułował żądanie: nakazanie usunięcia z pkt III.1.2 OPZ wymogu, aby „producent oferowanego rozwiązania był obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat”, względnie - o usunięcie znacznika czasu lub nakazanie określenia go na poziomie 4 lat

Odwołujący mógłby sformułować tylko żądanie dalej idące, tj. nakazania całkowitego wykreślenia w/w postanowienia, które nie powinno mieć miejsca w zamówieniach publicznych. Odwołujący dla uproszczenia formułuje również wniosek ewentualny o usunięcie wymogu „przynajmniej od 5 lat”, bez zastępowania jej jakimkolwiek innym okresem lub przynajmniej zastąpienie wymogu okresem 4 lat, aby mógł wziąć udział w postępowaniu.

2.W związku z zarzutem naruszenia art. 99 ust. 2 oraz 4 PZP, art. 16 pkt 1 PZP przez zawarcie w OPZ takich cech dostaw, wymienionych w pkt 1.2 odwołania, że wprawdzie każda z nich z osobna cechuje również niektóre produkty konkurencyjne, ale ich zestawienie wskazuje na konkretny produkt w postaci PA220, PA820, PA3220 oraz system zarządzania Panorama PAN25, niezasadnie uprzywilejowując producenta - Palo Alto i eliminując producenta Fortinet, Odwołujący sformułował żądanie: nakazania usunięcia z treści OPZ postanowień wskazanych w punkcie 1.2 odwołania, względnie nakazanie dopuszczenia zastosowania ofert równoważnych rozwiązaniu Palo Alto wraz z określeniem kryteriów oceny równoważności.

Jako równoważne Odwołujący wskazuje przykładowo następujące rozwiązania:

a.W odniesieniu do III.1.4 OPZ - w zakresie wymagania wyposażenia urządzenia w co

najmniej jeden port konsoli USB Micro-B: każde inne rozwiązanie zapewniające podłączenie się do konsoli obsługujące powszechny standard RJ45 (zwykły kable sieciowy)

b.W odniesieniu do III.1.5 OPZ - w zakresie wymagania, „Urządzenia firewall muszą posiadać budowę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów i pamięci przetwarzających ruch sieciowy (tzw. Data Plane).” - Wykonawca wskazuje, że równoważnym rozwiązaniem jest np. odseparowanie zasobów na poziomie logicznym.

c.W odniesieniu do III.1.6 OPZ - w zakresie wymagania: „Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.” - Wykonawca wskazuje, że równoważnym rozwiązaniem jest np. odseparowanie zasobów na poziomie logicznym a przede wszystkim właściwy dobór (sizing) urządzeń.

d.III.1.7 OPZ - w zakresie wymagania: „Urządzenie musi obsługiwać 4000 znaczników VLAN.” - Wykonawca wskazuje że równoważnym rozwiązaniem jest np. ilość znaczników powiązana z ilością segmentów sieci, którą klient planuje uruchomić w okresie najbliższych 3-5 lat czyli okresie eksploatacji firewalli.

e.III.1.22 OPZ - w zakresie wymagania: „Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników w przestrzeni wskazanego okresu czasu” - Wykonawca wskazuje, że równoważnym rozwiązaniem jest np. tworzenie raportów w formatach umożliwiających ich edycję np. w środowisku Windows (gdyż na takim pracuje Zamawiający)

f.III.1.27 OPZ - w zakresie wymagania: „Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa” - Wykonawca wskazuje, że równoważnym rozwiązaniem jest np. firewall posiadający funkcjonalność tworzenia polityk bezpieczeństwa oraz reguły translacji adresów NAT.

g.III.2.3 OPZ - w zakresie wymagania: „Dysk musi mieć możliwość wymiany bez potrzeb rozkręcania urządzenia” - Wykonawca wskazuje, że równoważnym rozwiązaniem jest np. możliwość wymiany przez odkręcenie śrub zabezpieczających, stosowane powszechnie (co nie zmienia faktu, że w urządzeniach firewall dysków najzwyczajniej się nie wymienia).

W związku z zarzutem naruszenia art. 99 ust. 5 i 6 Ustawy PZP przez zaniechanie opisanie przedmiotu zamówienia z zastosowaniem wyrazów „lub równoważny” oraz zaniechanie określenia kryteriów stosowanych w celu oceny równoważności, pomimo iż OPZ wskazuje pośrednio na konkretnego producenta: Palo Alto, odwołujący sformułował żądanie nakazania modyfikacji SWZ poprzez dopuszczenie zastosowania ofert równoważnych rozwiązaniu Palo Alto wraz z określeniem kryteriów oceny równoważności.

4. zarzut i żądanie z niego wywodzone zostały cofnięte (dotyczy certyfikatu CIHE).

Zamawiający: Transportowy Dozór Techniczny w Warszawie w odpowiedzi na odwołanie wniósł o oddalenie odwołania w całości.

Uzasadniając stanowisko wskazał, co następuje.

I. W sprawie interesu we wniesieniu odwołania Zamawiający wskazuje, iż Odwołujący posiada w swojej ofercie handlowej sprzęt sieciowy w zakresie bezpieczeństwa sieci oparty na rozwiązaniach producenta Fortinet, jak również producenta Palo Alto, a także innych producentów i ma możliwość złożenia oferty. Odwołujący stara się przeforsować takie zmiany w SWZ, aby móc złożyć ofertę konkretnego producenta. Twierdzenie Odwołującego wskazuje na forsowanie konkretnego rozwiązania - Fortinet”.

Zamawiający nadmienia, że jest podmiotem powołanym w drodze ustawy jako specjalistyczna jednostka dozoru technicznego i wskazuje na zakres jego zadań i kompetencji stosownie do postanowień ustawy z 21 grudnia 2000 r. o dozorcze technicznym (Dz. U. z 2021, poz. 272 z późn. zm.) oraz innych aktów prawnych prawa krajowego i europejskiego oraz nowych działań.

Zamawiający opisał produkt, który chce nabyć, przez podanie cech, które zagwarantują najlepszą jakość. Wymóg żądania produktów jak najlepszej jakości jest uzasadniony charakterem zamówienia, który jest niezbędny do osiągnięcia opisanego celu w stopniu jak najwyższym. Zamawiający ma prawo opisać przedmiot zamówienia, uwzględniając swoje potrzeby, a przy tym zapewniając sobie uzyskanie oczekiwanego efektu, gwarantującego zaspokojenie określonych potrzeb, nawet jeżeli przez to nie zostaną dopuszczeni do postępowania wszyscy wykonawcy działający na danym rynku. Zamawiający podkreśla iż celem zamówienia jest osiągnięcie jak najwyższego poziomu bezpieczeństwa systemów informatycznych. W dobie coraz częstszych ataków hakerskich skierowanych na podmioty publiczne bezpieczeństwo informatyczne stanowi dla niego najwyższą wartość. Na Zamawiającym ciąży ustawowe zadania w zakresie bezpieczeństwa w sektorze transportu i zadania te są realizowane poprzez odpowiedni standard infrastruktury informatycznej.

II. Odnosząc się do podniesionych przez Odwołującego zarzutów:

Ad. 1 w zakresie określenia w pkt III.1.2 OPZ wymogu „stażu” w raportach Gartnera Zamawiający stwierdził, że - twierdzenie Odwołującego, że jedynym producentem spełniającym wymóg OPZ jest Palo Alto – jest nieprawdziwe. Na rynku jest co najmniej dwóch producentów którzy posiadają rozbudowany kanał sprzedaży w Polsce, co zapewnia konkurencyjne i rynkowe warunki do przeprowadzenia postępowania.

Obowiązkiem Zamawiającego jest wybór rozwiązania, które zapewni bezpieczeństwo przedsięwzięcia zarówno pod kątem wypełnienia wymagań technicznych, jak również stabilności producenta wybranego systemu, ze względu na fakt, że budowany system będzie użytkowany przez wiele lat i w tym czasie musi być dla niego zapewnione stabilne wsparcie techniczne, aktualizacje oprogramowania i reguł wykrywania ataków, które umożliwią utrzymanie wysokiego poziomu ochrony w zmieniającym się otoczeniu cyber-zagrożeń.

Zamawiający podkreśla iż celem zamówienia jest osiągnięcie jak najwyższego poziomu bezpieczeństwa systemów informatycznych. Odwołujący w treści odwołania forsuje urządzenie Fortinet, jednak to urządzenie nie spełnia standardów Zamawiającego w zakresie bezpieczeństwa. Zamawiający przyjął założenie, iż zakup rozwiązania spośród producentów, którzy zaliczają się w określonym czasie do liderów na rynku gwarantuje wypełnienie wyżej wymienionych celów. Zatem sformułowanie wymagania co do producenta lidera jest powiązane z oferowanym produktem. Jak wskazał sam Odwołujący na rynku istnieją dwa rozwiązania spełniające wymogi Zamawiającego. Sporny zapis nie utrudnia

konkurencji i nie dyskwalifikuje wykonawców, którzy oferują na rynku różne rozwiązania.

Ad 2 W zakresie zarzutu dotyczącego określenia wymagań określonych w Opisie Przedmiotu Zamówienia nieuzasadnionych obiektywną potrzebą Zamawiającego Odwołujący podnosi następujące argumenty: Ad.

a) III 1.4 OPZ

Odwołujący twierdzi, że „Wymaganie jest nieuzasadnione obiektywną potrzebą Zamawiającego ponieważ port konsoli USB MicroB jest dokładnie takim samym portem jak np. USB Typ-B. Tym samym nie ma podstaw do ograniczania portu konsolowego do konkretnego standardu./.../”

Zamawiający wskazuje, że wymaganie było podyktowane obiektywną potrzebą z uwagi na fakt, że Zamawiający posiada na wyposażeniu kable konsolowe USB- USB microB oraz przejściówki portów USB microB do USB typ C. Niezależnie od powyższego Zamawiający w dniu 01.06.2021 r. dokonał zmiany treści SWZ i pkt III 1.4 OPZ brzmi następująco:

„Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 lub w co najmniej jeden port konsoli w standardzie USB oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 BASE-T. Wymagane jest dostarczenie wraz z oferowanymi urządzeniami odpowiednich kabli konsolowych, które umożliwiają podłączenie ich do komputera przez port USB 2.0 lub 3.0.”

Ad. b) III 1.5 OPZ

Odwołujący twierdzi: „Wymaganie nieuzasadnione obiektywną potrzebą Zamawiającego ponieważ Wiele wiodących producentów urządzeń FW opiera separację na oddzielnych systemach wirtualnych a nie procesorach. Ten wymóg wyklucza wielu wiodących producentów firewalli. Z punktu widzenia wydajności rozwiązania i ochrony przed przeciążeniem zarówno technologia rozdziela Control Plane od Data Plane poprzez dedykowany procesor czy system wirtualny jest całkowicie równoważna. Producenci stosują wiele metod zapewniających wysoką wydajność swoich rozwiązań, a często jak np. Fortigate czy Checkpoint stosują różne architektury w zależności od modelu konkretnego firewalla./.../

Wobec powyższej argumentacji Zamawiający wskazuje:

Wymaganie jest uzasadnione obiektywną potrzebą. Wymagana funkcjonalność daje możliwość zarządzania tym urządzeniem w przypadku zablokowania części odpowiedzialnej za ruch sieciowy poprzez atak skierowany na urządzenie, który spowoduje przeciążenie procesora urządzenia. Wymóg oddzielnej separacji opartej na procesorach podyktowany jest faktem, że w przypadku zastosowania rozwiązania programowego istnieje możliwość zablokowania całego urządzenia poprzez wykorzystanie całej mocy procesora, która uniemożliwi w przypadku skutecznego ataku zarządzanie urządzeniem, zatem błędnym jest twierdzenie, iż nie ma to wpływu na funkcjonalność i wydajność urządzenia. Zamawiający jak i Odwołujący nie ma możliwości przewidzenia w jakim zakresie nastąpi atak typu DoS, DDoS i który może doprowadzić do zablokowania urządzenia co będzie miało przełożenie na zastosowanie odpowiednio wydajnego procesora.

Na rynku urządzeń typu firewall są dostępne rozwiązania z separacją ruchu Management Plane i Data Plane.

Odnosząc się do stwierdzenia Odwołującego, że „Obecnie żądane przez Zamawiającego minimalne wydajności odpowiadają dokładnie konkretnym modelom PaloAlto /.../” Zamawiający informuje, że przy specyfikowaniu wymagań opierał się na charakterystyce ruchu sieciowego i planowaniu wzrostu tego ruchu z uwagi na rozwój firmy, a proponowane parametry wydajnościowe urządzeń określił jako wymagania minimalne.

Na rynku urządzeń typu firewall są dostępne rozwiązania spełniające wymagania wydajności.

Ad.c) III 1.6 OPZ

Odwołujący twierdzi, że:

„Zapis faworyzuje producenta o konkretnej architekturze (PaloAltoNetworks) bez uzasadnienia merytorycznego - w konkurencyjnych do PaloAlto firewallach nadmierne obciążenie data plane jest niwelowane przez zastosowanie odpowiednio wydajnego urządzenia tak jak ma to miejsce przy każdym innym elemencie infrastruktury sieciowej czy bezpieczeństwa. Z reguły oddzielny Data Plane od ControlPlane jest stosowany przy wielogigowych przepływnościach - pozostawienie tego zapisu naraża Zamawiającego na wydatkowanie nieracjonalnych środków na zakup przewymiarowanych urządzeń. W szczególności dotyczy to jednostek terenowych Zamawiającego (inspektoratów) gdzie pracuje maksymalnie do 20-30 osób, które wykonując pracę biurową nie są w stanie wygenerować ruchu który może jakkolwiek zagrozić wydajnościom nawet małych firewalli gdzie szczególnie konkurencyjną do PaloAlto Networks ofertę posiada właśnie dyskryminowany przez klienta Fortinet.”

Wobec powyższej argumentacji Zamawiający wskazuje:

Zapis nie faworyzuje żadnego producenta. Wymaganie może mieć odniesienie do większości urządzeń sieciowych czy to z separacją sprzętową czy też z separacją programową (wirtualną), także w przypadku znacznego obciążenia ruchem części odpowiedzialnej za obsługę ruchu sieciowego nie powinno to wpływać na część urządzenia odpowiedzialną za zarządzanie i monitorowanie urządzenia czy to przez zastosowanie separacji sprzętowej czy też zastosowanie wydajnego urządzenia. Sam Odwołujący w odwołaniu w tabeli w pkt. 2 wskazuje, iż istnieją na rynku takie rozwiązania przynajmniej, że mogą być one wydajniejsze.

Zapis jest podyktowany potrzebami ponieważ zarządzanie urządzeniami IT w jednostkach terenowych odbywa się w sposób zdalny. Struktura organizacyjna Zamawiającego składa się z Wydziałów, Oddziałów terenowych oraz zespołów rozproszonych w różnych lokalizacjach na terenie całego kraju. Ponadto Inspektorzy TDT pracują w terenie w lokalizacji użytkowników danych urządzeń technicznych, które znajdują się pod dozorem TDT.

Dowód: Zał 13 - Zarządzenie nr 17 Ministra Infrastruktury nadanie statutu Transportowemu Dozorowi Technicznemu (Dz. Urz. Mł z 2019 r. poz. 35 z późn. zm.).

Konieczność zdalnego zarządzania urządzeniami, stabilna praca urządzenia jak i możliwość jego zarządzania w

przypadku dużego obciążenia jest dla Zamawiającego najważniejsza. Wymagana funkcjonalność wpływa na komfort użytkownika a co najmniej administrowania urządzeniem sieciowym w przypadku nadmiernego obciążenia urządzenia. Ponadto opis tej funkcji nie dotyczy wyłącznie architektury i rozwiązań stosowanych przez różnych producentów a dotyczy wyłącznie tego, iż moduł zarządzania ruchem nie może być podatny na obciążenie ze strony modułu odpowiedzialnego za obsługę tego ruchu.

Argumenty Odwołującego dotyczące nieracjonalnych zakupów są nietrafione ponieważ:

-Zamawiający posiada infrastrukturę wielogigowych przepływów,

-Zamawiający zakłada wzrost obciążenia w dalszej perspektywie czasowej z uwagi na plany w zakresie rozbudowy własnego potencjału jako wyspecjalizowanej jednostki dozoru technicznego. Wynikać to będzie z przepisów, które będą obowiązywały od 4 września 2021 r. w zw. z przepisami ustawy z 14 sierpnia 2020 r. o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw (Dz. U z 2020 r., poz. 1517). Zgodnie z art. 73d ust. 2 i art. 73d ust. 4 ww. ustawy który nakłada na TDT obowiązek wymiany danych z ok. 370 starostwami na terenie całego w zakresie wymagań homologacyjnych oraz planowanych zmian w zakresie nadzoru nad stacjami kontroli pojazdów i przeniesienie nadzoru ze starostw do TDT, jak również przepisów rozp. PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/1020 z czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011, które określa TDT jako jednostkę nadzoru rynku w zakresie urządzeń technicznych określonych w tym rozporządzeniu.

- Zamawiający musi uwzględnić zwiększony ruch (większa liczba stacji, więcej wideokonferencji, segmentacji pasm to powoduje, że wymaganie jest w pełni uzasadnione).

Odwołujący nie może czynić zarzutów na podstawie własnych subiektywnych założeń ani dokonywać własnych wyliczeń obciążenia urządzenia zwłaszcza, że Odwołujący nie skierował żadnych pytań do Zamawiającego w tym zakresie. Odwołujący nie zna specyfiki i planów rozbudowy Zamawiającego. Jak sam Odwołujący wskazuje: „w konkurencyjnych do PaloAlto firewallach nadmierne obciążenie data plane jest niwelowane przez zastosowanie odpowiednio wydajnego urządzenia tak jak ma to miejsce przy każdym innym elemencie infrastruktury sieciowej czy bezpieczeństwa” zatem zarzut ograniczenia konkurencji jest niezasadny ponieważ Zamawiający w tym wymaganiu nie odnosił się wyłącznie do urządzeń producenta Palo Alto, ale do wielu innych rozwiązań. Żądanie Odwołującego nie może się opierać na zamiarze zaferowania urządzeń, które są tańsze, a nie spełniają wymagań Zamawiającego.

Ad.

d) III 1.7 OPZ

Odwołujący twierdzi: „Wymaganie nieuzasadnione obiektywną potrzebą Zamawiającego ponieważ - Jak wynika z analiz wcześniejszych OPZ na zakup systemu antywirusowego Zamawiający posiada obecnie ok 350 użytkowników komputerów. Gdyby założyć proporcjonalne rozłożenie 350 pracowników na oddziały Zamawiającego to oznacza, że średnio w lokalizacji Zamawiającego pracuje poniżej 20 osób. Najlepsze praktyki związane z segmentacją sieci mówią o kilku do kilkunastu VLAN w lokalizacji. Wymóg Zamawiającego jest zatem istotnie przewymiarowany. Wymóg posiadania 4 tys VLAN (sieci wirtualnych) dla urządzeń firewalla przy zatrudnieniu jak wykazano wyżej do 20 osób per jednostka terenowa sprawia, że wymóg byłby adekwatny gdyby Zamawiający około 20 -krotnie zwiększył zatrudnienie i jednocześnie chciał dla każdego użytkownika wydzielić odrębny segment wirtualny (VLAN) aby budować oddzielne polityki bezpieczeństwa pomiędzy tymi segmentami co w perspektywie cyklu życia produktu jest nieprawdopodobne a w praktyce nieracjonalne.”

Zamawiający wskazuje, że wymaganie jest w pełni uzasadnione obiektywną potrzebą Zamawiającego. Wynikać to będzie z przepisów ustawy – Prawo o ruchu drogowym i obowiązkiem wymiany danych z starostwami na terenie całego kraju w zakresie wymagań homologacyjnych oraz planowanych zmian w zakresie nadzoru nad stacjami kontroli pojazdów i przeniesienie nadzoru ze starostw do TDT, jak również przepisów UE jw.

Zastosowana u Zamawiającego polityka „zero-trust” wymaga podziału na wiele segmentów sieci a urządzenie nie może stanowić ograniczenia w tym zakresie, ponadto „zero-trust” [pol. Zero zaufania] oparte jest na przekonaniu, że każdy użytkownik, urządzenie oraz adres IP uzyskujący dostęp do zasobu stanowi zagrożenie. Dopóki nie udowodni, że jest inaczej. Dlatego nawiązując do tej koncepcji, nigdy nie powinniśmy ufać, a zawsze weryfikować. Tylko w ten sposób, jesteśmy w stanie zapewnić najwyższy poziom bezpieczeństwa.

Zamawiający wskazuje, że twierdzenie Odwołującego o wymaganiach konfiguracji na urządzeniach 4000 interfejsów VLAN oparte jest na błędnym zinterpretowaniu tego zapisu, który mówi wyłącznie możliwości wprowadzenia w urządzeniu 4000 identyfikatorów/ znaczników, a nie mówi o konieczności tworzenia 4000 subinterfejsów L3 lub 4000 vlanów.

Treść OPZ wskazuje jednoznacznie, że Urządzenie musi obsługiwać 4000 znaczników VLAN a nie 4000 VLAN. Co najmniej kilku producentów Firewall oferuje rozwiązania spełniające wymaganie obsługi co najmniej 4000 znaczników VLAN.

FortiGate, który nie ma włączonych VDOM, może mieć maksymalnie 255 interfejsów w transparentnym trybie pracy. Dotyczy to każdego pojedynczego VDOM. W trybie NAT liczba może wynosić od 255 do 8192 interfejsów na VDOM, w zależności od modelu FortiGate. Te liczby obejmują sieci VLAN, inne interfejsy wirtualne i interfejsy fizyczne. Aby mieć więcej niż 255 interfejsów skonfigurowanych w transparentnym trybie operacyjnym, należy skonfigurować wiele VDOM-ów, które umożliwią podzielenie łącznej liczby interfejsów na wszystkie VDOM-y.

Ad. e) III 1.22 OPZ

Odwołujący twierdzi: „Wymaganie nieuzasadnione obiektywną potrzebą Zamawiającego ponieważ Skoro Zamawiający oczekuje centralnego systemu zarządzania i raportowania dla wszystkich NGFW to raportowanie nie powinno odbywać się bezpośrednio z poziomu pojedynczych urządzeń firewall tylko właśnie z tego systemu. Właśnie system centralnego zarządzania jest miejscem dedykowanym do przechowywania logów oraz generowania raportów dla całego środowiska.”

Zamawiający wskazuje, że wymaganie jest uzasadnione. Celem jest zapewnienie możliwości nieprzerwanej kontroli poziomu bezpieczeństwa infrastruktury Zamawiającego i analizy incydentów bezpieczeństwa nawet w przypadku braku komunikacji między urządzeniem Firewall a centralnym systemem zarządzania. Infrastruktura Zamawiającego jest rozproszona przestrzennie, na terenie całego kraju, a jej poszczególne węzły łączą się z jej punktem centralnym poprzez sieć niezależnego dostawcy (dostawców). Konieczne jest ograniczenie ryzyka znacznej utraty funkcji bezpieczeństwa w czasie awarii po stronie dostawcy łączy. Rozwiązanie, w którym, pomimo braku połączenia do centralnego systemu zarządzania, administratorzy mają możliwość analizy logów i tworzenia raportów bezpośrednio na urządzeniach Firewall jest najbardziej optymalne i efektywne kosztowo. Strukturę organizacyjną opisano wyżej z powołaniem na statut. Ponadto, zgodnie z § 20 ust 1 rozp. Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Zamawiający musi przewidzieć awarie komunikacji z systemem centralnego zarządzania lub samą jego awarią i mieć możliwość utrzymywania systemów w odpowiednim standardzie wymaganym przepisami prawa.

Niezależnie od powyższego Zamawiający zmienił OPZ pkt III.1.22.: „Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF i CSV. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Sposób realizacji możliwy jest również jako rozwiązanie równoważne przez dostarczenie dodatkowego, lokalnego systemu logowania który powinien mieć takie same możliwości w każdej lokalizacji objętej postępowaniem. Po odzyskaniu połączenia z punktem centralnym musi być możliwe zsynchronizowanie lokalnych logów i raportów z lokalnych systemów z centralnym systemem zarządzania. W przypadku rozwiązania z dodatkowym lokalnym systemem logowania w każdej lokalizacji, musi zostać zapewniony poziom redundancji zasilania i dysków, który umożliwi kontynuację pracy nawet w wypadku awarii jednego z tych komponentów. Istnieją rozwiązania spełniające wymaganie.

Ad.

f. III 1.27 OPZ

Zamawiający wskazuje, że wymaganie jest uzasadnione, z doświadczenia translację adresów NAT ustawia się sporadycznie, zaś polityki bezpieczeństwa są modyfikowane często. Zatem takie zdefiniowanie interfejsu jest najbardziej korzystne z uwagi na rozdzielanie tych polityk, co znacznie wpływa na przejrzystość rozwiązania. W związku z tym interfejs użytkownika jest również funkcjonalnością urządzenia i niejednokrotnie umożliwia interakcję z urządzeniem.

Na rynku producentów urządzeń Firewall oferuje się rozwiązania spełniające wymaganie rozdzielania reguł NAT od polityk bezpieczeństwa.

Nowa generacja zapory sieciowej Palo Alto Networks obsługuje różne typy reguł, które współpracują ze sobą, aby bezpiecznie używać aplikacje w sieci.

Ad.

g. III 2.3 OPZ Zamawiający wskazuje, że wymaga wyposażenia urządzenia w wymiowane dyski systemowe z uwagi na uzasadnioną potrzebę podyktowaną jest względami praktycznymi z uwagi na umieszczanie urządzeń w szafach wraz z innymi urządzeniami serwerowymi czy też sieciowymi co wiąże się z demontażem urządzeń, okablowania sieciowego jak i zasilania a w przypadku awarii dysku nie jest wymagana wymiana całego urządzenia tylko wymiana dysku bez potrzeby wymiowania całego urządzenia.

Odwolujący błędnie założył, iż „Procedura wymiany dysków w praktyce nie występuje podczas eksploatacji systemu, a w sytuacji awarii firewalla wymianie podlega całe urządzenie” z uwagi na to iż dyski czy to talerzowe czy też dyski SSD są urządzeniami elektronicznymi i zawsze mogą ulec uszkodzeniom podczas normalnej eksploatacji. Zamawiający ma wiedzę, iż producenci stosują również rozwiązania zabezpieczające (np. stosowanie plomb gwarancyjnych) przed otwarciem urządzenia w celu samodzielnej wymiany dysku, a co mogło by spowodować utratę uprawnień gwarancyjnych na zakupione urządzenie ale nie takiego rozwiązania Zamawiający oczekuje.

Zamawiający w przypadku wymagań co do wielkości dysku, określił wymaganie minimalne z uwagi na konieczność przechowywania znacznej logów systemowych w długim okresie czasu z uwagi na przepisy rozp. RM z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, /.../ i zgodnie z § 20 ust 4 „Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata”.

Ponadto na rynku producentów urządzeń Firewall oferuje się rozwiązania spełniające wymagania, które umożliwiają wymianę dysków bez konieczności rozkręcania urządzenia.

Na rynku „NGFW” są co najmniej dwa rozwiązania spełniające wymagania opisane w OPZ.

Zamawiający w OPZ zawarł wymagania proporcjonalne do swoich potrzeb. Przedmiot zamówienia jest zgodny obiektywnymi i uzasadnionymi potrzebami. Odwołujący nie zna obiektywnych i uzasadnionych potrzeb Zamawiającego jedynie ze zakładu.

Odwolujący nie może kształtować potrzeb Zamawiającego i zakładać, że zabezpieczenia sieciowe mają dotyczyć aktualnego stanu Zamawiającego. Odwołujący oparł swoje założenia na informacjach, które sam zdobył, a nie zwrócił się z zapytaniem o stan użytkowników komputerów aktualny i planowany czy stan baz danych aktualnych i planowanych. Zamawiający w najbliższym czasie planuje wzrost ilości użytkowników komputerów i baz danych, ponieważ przygotowuje się do podjęcia nowych działań i celem, jaki musi osiągnąć jest zapewnienie możliwości nieprzerwanej kontroli poziomu bezpieczeństwa obecnej i planowanej infrastruktury Zamawiającego i analizy incydentów

bezpieczeństwa nawet w przypadku braku komunikacji między urządzeniem Firewall a centralnym systemem zarządzania. Jest to niezbędnie dla prawidłowego, nieprzerwanego funkcjonowania Zamawiającego jako jednostki, która prowadzi działalność zgodnie z ustawą z 21 grudnia 2000 r. o dozorcze technicznym. Zamawiający zakłada wzrost obciążenia w dalszej perspektywie czasowej z uwagi na plany w zakresie rozbudowy własnego potencjału jako wyspecjalizowanej jednostki dozoru technicznego zgodnie ze zmianą prawa o ruchu drogowym.

Zamawiającego obowiązuje art. 17 Pzp, zgodnie z którym udziela zamówienia w sposób zapewniający najlepszą jakość dostaw, uzasadnioną charakterem zamówienia, w ramach środków, które przeznaczyć na realizację i uzyskanie najlepszych efektów zamówienia, w tym efektów społecznych, środowiskowych oraz gospodarczych, o ile którykolwiek z tych efektów jest możliwy do uzyskania w danym zamówieniu, w stosunku do poniesionych nakładów”.

W związku z powyższym Zamawiający opisał produkt, który chce nabyć, przez podanie tych cech, które zagwarantują najlepszą jakość. Wymóg żądania produktów najlepszej jakości jest uzasadniony charakterem zamówienia i o osiągnięciem celu w stopniu jak najwyższym.

Zamawiający ma prawo opisać przedmiot zamówienia, uwzględniając potrzeby i zapewniając uzyskanie oczekiwanego efektu, gwarantującego zaspokojenie potrzeb, nawet jeżeli nie zostaną dopuszczeni wszyscy wykonawcy na rynku. Przywołał orzecznictwo KIO.

Ad.3 Zamawiający zauważa, że dokonał opisu przedmiotu zamówienia za pomocą określenia cech przedmiotu zamówienia oraz jego funkcjonalności. W treści OPZ brak wskazań na konkretny produkt, a tym bardziej na konkretnego wykonawcę. 01.06.2021 dokonano zmiany SWZ pkt III.1.22 opz: „Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF i CSV. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Sposób realizacji możliwy jest również jako rozwiązanie równoważne przez dostarczenie dodatkowego, lokalnego systemu logowania który powinien mieć takie same możliwości w każdej lokalizacji objętej postępowaniem. Po odzyskaniu połączenia z punktem centralnym musi być możliwe”

Uwzględniając dokumentację postępowania o udzielenie zamówienia publicznego, jak również biorąc pod uwagę stanowiska stron przedstawione w pismach procesowych, jak też podczas rozprawy, Izba stwierdziła, iż odwołanie w zakresie rozpoznawanych zarzutów zasługuje na uwzględnienie.

Uznaje się, że spełniona jest materialnoprawna przesłanka wniesienia odwołania uregulowana w art. 505 ustawy – Prawo zamówień publicznych wobec wykazania przez wykonawcę, że ma on interes w uzyskaniu zamówienia i może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy w szczególności przez treść opisu przedmiotu zamówienia mogącą niezasadnie ograniczyć krąg potencjalnych wykonawców w postępowaniu. Oceny tej nie zmienia wskazanie przez zamawiającego, że odwołujący będzie mógł złożyć ofertę w przedmiotowym postępowaniu z uwagi na fakt, że dysponuje on w swojej ofercie handlowej produktami Palo Alto, co do których niesporne jest, że spełniają wymogi przedmiotowe zamówienia. Można w tym miejscu zauważyć, że zamawiający taką oceną, co najmniej pośrednio, potwierdził postawione w odwołaniu zarzuty naruszenia art. 99 ustawy pzp przez opis przedmiotu zamówienia prowadzący do wskazania konkretnego produktu i rozwiązania, pomimo nie oznaczenia go wprost nazwą producenta i produktu.

W zakresie wymogu z pkt III.1.2 OPZ za niesporny uznano walor oceny firm przedstawiany przez Gartner Inc. w ćwiartkach kwadratu, tu w ćwiartce lidera. Zajmowanie miejsca w grupie liderów oznacza, że dany producent i jego produkty mają wysoki poziom i są gotowi do wykorzystania w praktyce. Nie wydaje się istotny tak długi staż zajmowania pozycji lidera, jak wymaga zamawiający tj. okres pięcioletni, który także w systemie zamówień publicznych w odniesieniu do dostaw i usług, byłby nadmiarowy. W ocenie Izby sama obecność w grupie liderów jest gwarancją, że zarówno producent, jak i produkt spełniają wysokie wymagania. Skoro zatem wobec przyjęcia znacząco długiego okresu, szereg produktów i firm ulega eliminacji, skład orzekający uznaje konieczność przywrócenia konkurencyjności w tym zakresie, na poziomie co najmniej żądanym przez odwołującego.

Skład orzekający uznaje za niezbywalne prawo zamawiającego opisanie przedmiotu zamówienia zgodnie z obiektywnymi jego potrzebami. Zamawiający może przy tym określić oczekiwane parametry produktu na wysokim poziomie, także, jeśli miałyby to nawet wiązać się z niemożnością zaoferowania przedmiotu zamówienia przez znaczną liczbę uczestników rynku właściwego. Dopuszczalne i uzasadnione może być także określanie potrzeb zamawiającego wynikających z przewidywanych do wykonywania przyszłych zadań, w tym wypadku wynikających z nowych przepisów ustawy – Prawo o ruchu drogowym, z których wynika konieczność bieżącej współpracy ze wszystkimi starostwami powiatowymi w Polsce i samorządami miast wykonującymi zadania powiatowe.

Natomiast Izba nie uznaje, że udowodniono zostało twierdzenie zamawiającego o dostępnych na rynku różnych produktach różnych producentów, które spełniają parametry opisane w Opisie Przedmiotu Zamówienia. O ile dla poszczególnych parametrów opisywanych i kwestionowanych w odwołaniu można było wiarygodnie wskazać więcej niż jeden produkt, to łącznie takiego twierdzenia nie sposób obronić w odniesieniu do całości przedmiotu zamówienia. Wiarygodna i nie zaprzeczona jest także teza odwołania, że zamawiający preferuje konkretne rozwiązanie konkretnego producenta jakkolwiek wprost nie wymienionego z nazwy w treści opisu przedmiotu zamówienia.

Zakładając, że taki opis jest optymalny z punktu widzenia uzasadnionych potrzeb zamawiającego należy potwierdzić, że w rozpatrywanych okolicznościach spełnione zostały przesłanki przewidziane w art. 99 ust. 5 ustawy pzp tj. dokonano opisu przedmiotu zamówienia przez wskazanie cech charakterystycznych konkretnego produktu pochodzącego od konkretnego producenta. Konsekwencją takiego opisu jest ustawowy obowiązek wskazania w opisie, iż dopuszcza się produkt równoważny ze wskazaniem stosownie do art. 99 ust. 6 ustawy pzp, w opisie przedmiotu zamówienia kryteriów stosowanych w celu oceny równoważności. Stąd rozstrzygnięcie zawarte w sentencji wyroku.

Wskazując na powyższe, orzeczono, jak w sentencji.

O kosztach postępowania orzeczono stosownie do wyniku sprawy na podstawie art. 575 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.) oraz § 7 ust. 1 pkt 1 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania

odwoławczego, ich rozliczenia oraz wysokości i sposobu pobierania wpisu wysokości wpisu od odwołania (Dz. U. poz. 2437).

Przewodniczący:

.....

.....