sygn. akt: **KIO 2582/23**

WYROK

z dnia 25 września 2023 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący:Emil Kuriata

Protokolant: Adam Skowroński

po rozpoznaniu na rozprawie w dniu 21 września 2023 r., w Warszawie, odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 1 września 2023 r. przez wykonawcę **Apex.IT sp. z o.o., ul. Marcina Flisa 6; 02-188 Warszawa,** w postępowaniu prowadzonym przez zamawiającego **Akademia Górniczo-Hutnicza w Krakowie, Akademickie Centrum Komputerowe CYFRONET AGH, ul. Nawojki 11; 30-950 Kraków**,

orzeka:

1. **Umarza postępowanie odwoławcze w zakresie w jakim zamawiający uwzględnił odwołanie oraz w zakresie w jakim odwołujący wycofał zarzuty, tj. art. 16 pkt 1 i 3 w zw. z art. 99 ust. 4 ustawy Pzp w zakresie żądań z pkt 1, 3, 5 i 6 odwołania.**
2. **W pozostałym zakresie oddala odwołanie**.
3. Kosztami postępowania obciąża **Apex.IT sp. z o.o., ul. Marcina Flisa 6; 02-188 Warszawa** i:
   3.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez wykonawcę **Apex.IT sp. z o.o., ul. Marcina Flisa 6; 02-188 Warszawa,** tytułem wpisu od odwołania,
   3.2. zasądza od **Apex.IT sp. z o.o., ul. Marcina Flisa 6; 02-188 Warszawa**na rzecz zamawiającego **Akademia Górniczo-Hutnicza w Krakowie, Akademickie Centrum Komputerowe CYFRONET AGH, ul. Nawojki 11; 30-950 Kraków** kwotę 4 597 zł 10 gr (słownie: cztery tysiące pięćset dziewięćdziesiąt siedem złotych, dziesięć groszy) stanowiącą koszty postępowania odwoławczego poniesione z tytułu dojazdu na posiedzenie i rozprawę oraz wynagrodzenia pełnomocnika.

Stosownie do art. 579 ust. 1 i art. 580 ust. 1 i 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2023 r. poz. 1605) 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 2582/23**

Uzasadnienie

Zamawiający – Akademia Górniczo-Hutnicza w Krakowie, Akademickie Centrum Komputerowe CYFRONET AGH prowadzi postępowanie o udzielenie zamówienia publicznego, którego przedmiotem jest *„Dostawa rozległego Systemu zabezpieczeń ruchu sieciowego w postaci rozwiązań klasy Next Generation Firewall (NGFW) wraz z komponentem o charakterze zarządczym dla wszystkich urządzeń (firewalli typu NGFW)”.*

Ogłoszenie o zamówieniu zostało opublikowane w Dz.U.U.E. z dnia 21 sierpnia 2023 r., pod nr 2022/S159 - 5049382023.

3 września 2023 roku, wykonawca Apex.IT sp. z o.o. z siedzibą w Warszawie (dalej „*Odwołujący*”) wniósł odwołanie do Prezesa Krajowej Izby Odwoławczej.

Odwołujący zarzucił zamawiającemu naruszenie art. 16 pkt 1 i 3 w związku z art. 99 ust.4 ustawy Pzp, poprzez sformułowanie wymagań przedmiotowych w opisie przedmiotu zamówienia („OPZ”) w sposób naruszający uczciwą konkurencję, poprzez ograniczenie kręgu wykonawców do podmiotów oferujących preferowane przez zamawiającego rozwiązania informatycznego producenta Palo Alto oraz naruszenie art. 99 ust.1 ustawy Pzp, poprzez opisanie przedmiotu zamówienia w sposób niejednoznaczny.

W związku z powyższym odwołujący wniósł o uwzględnienie odwołania oraz:

1) nakazanie zamawiającemu zmiany wymagania pkt 3 d) część Specyfikacja komponentu zabezpieczającego OPZ w sposób następujący:

„*Każde z urządzeń NGFW wchodzące w skład komponentu zabezpieczającego musi być wyposażone w:*

(…)

d) pamięć trwałą przeznaczoną na system operacyjny oraz dzienniki zdarzeń (logi) lub umożliwiać przekazywanie logów do centralnego systemu logowania i raportowania”,

2) nakazanie zamawiającemu zmiany wymagania pkt 29 e) część Specyfikacja komponentu zabezpieczającego OPZ w części dotyczącej interfejsów i wkładek w sposób następujący:

„*e) dla ewentualnych urządzeń w funkcji Inspekcji SSL/TLS, wymaganych jest co najmniej 4 interfejsów 10Gbps i wkładek o przepustowości 10 Gbps (transmisja na odległość min. 10 km) (Zamawiający nie dopuszcza zastosowania w tym celu żadnego z podstawowych interfejsów 10Gbps, tzn. w takim wypadku każdy komponent zabezpieczający musi być wyposażony w 4 dodatkowe, w stosunku do wymagań SWZ interfejsy)*",

względnie:

„e) dla ewentualnych urządzeń w funkcji Inspekcji SSL/TLS, wymaganych jest co najmniej 4 interfejsów 25Gbps i wkładek o przepustowości 25Gbps (transmisja na odległość min. 10 km)

(Zamawiający nie dopuszcza zastosowania w tym celu żadnego z podstawowych interfejsów 25Gbps, tzn. w takim wypadku każdy komponent zabezpieczający musi być wyposażony w 4 dodatkowe, w stosunku do wymagań SWZ interfejsy)",

3)nakazanie zamawiającemu zmiany ostatniego zdania w pkt 28 część Specyfikacja komponentu zabezpieczającego OPZ w sposób następujący:

„Bez względu na użyte rozwiązanie, wymaga się wydajności minimum 20 Gbps przepustowości dla inspekcji SSL/TLS (ang. SSL Inspection Throughput) oraz obsługę 75 wirtualnych instancji (analogicznie do NGFW), gdzie przypadku rozwiązania bazującego na NGFW komponentu zabezpieczającego wydajność 20 Gbps musi być osiągnięta przy jednoczesnym wykorzystaniu usług IPS/AV/Anty-Spyware i VPN)",

4)nakazanie zamawiającemu zmiany pkt 31 c) część Specyfikacja komponentu zabezpieczającego OPZ w sposób następujący:

„*Zestawianie tuneli SSL VPN z wykorzystaniem klienta VPN dostarczonego przez producenta urządzenia NGFW dla co najmniej 30000 użytkowników, w tym 5.000 użytkowników na pełnych uprawnieniach, a pozostali na uprawnieniach odpowiednich dla dostępu darmowego w zakresie przewidzianym przez producenta*",

5)nakazanie zamawiającemu zmiany wymagania pkt 20 część Specyfikacja komponentu zabezpieczającego OPZ w sposób następujący poprzez wprowadzenie definicji „VW Sandboxingu";

6)nakazanie zamawiającemu zmiany wymagania pkt 29 d) część Specyfikacja komponentu zabezpieczającego OPZ w sposób następujący:

„*element dodatkowy musi spełniać adekwatne wymagania zdefiniowane dla całego Systemu*",

7)obciążenie zamawiającego kosztami postępowania odwoławczego.

Odwołujący wskazał, że zamierza ubiegać się o udzielenie zamówienia będącego przedmiotem postępowania, które wchodzi w zakres ekonomicznego zainteresowania odwołującego. Wobec tego, z uwagi na zainteresowanie odwołującego niniejszym postępowaniem, opis przedmiotu zamówienia przekłada się na sytuację odwołującego w postępowaniu i możliwość złożenia konkurencyjnej oferty, a w konsekwencji na możliwość zawarcia umowy w sprawie zamówienia objętego postepowaniem oraz osiągnięcie zysku z jego realizacji. Zaskarżone przez odwołującego zapisy SWZ w praktyce silnie redukują szanse odwołującego o pozyskanie zamówienia, gdyż wywołują konieczność skalkulowania oferty z oparciu o dodatkowe elementy w stosunku do ofert składanych na preferowane przez zamawiającego rozwiązanie producenta Palo Alto. Taka praktyka zamawiającego w praktyce powoduje nieuzasadnione ograniczenie liczby wykonawców mogących złożyć w postępowaniu ofertę zgodną z SWZ. Zamawiający, dopuszczając się naruszenia podstawowych zasad i obowiązków wynikających z Ustawy, w sposób bezprawny i bezzasadny, uniemożliwia odwołującemu, zainteresowanemu udziałem w postępowaniu, przygotowanie realnie konkurencyjnej i rzetelnej oferty (zawierającej rozwiązania informatyczne któregoś z renomowanych producentów) oraz realizacji zamówienia w sposób zgodny z prawem, co może wyrządzić odwołującemu szkodę w postaci utraconego zysku z realizacji zamówienia objętego postępowaniem.

Izba ustaliła i zważyła, co następuje.

Izba stwierdziła, że nie zachodzą przesłanki do odrzucenia odwołania, o których stanowi przepis art. 528 ustawy Pzp.

Zamawiający prowadzi postępowanie o udzielenie zamówienia publicznego z zastosowaniem przepisów ustawy Prawo zamówień publicznych wymaganych przy procedurze, której wartość szacunkowa zamówienia przekracza kwoty określone w przepisach wydanych na podstawie art. 3 ustawy Prawo zamówień publicznych.

Krajowa Izba Odwoławcza stwierdziła, że odwołujący posiada interes w uzyskaniu przedmiotowego zamówienia, kwalifikowanego możliwością poniesienia szkody w wyniku naruszenia przez zamawiającego przepisów ustawy, o których mowa w art. 505 ust. 1 ustawy Pzp, co uprawniało go do złożenia odwołania.

Zamawiający złożył pisemną odpowiedź na odwołanie (I) z 14 września 2023 roku, w której oświadczył, iż uwzględnia częściowo zarzut nr 2 w zakresie wniosku nr 5 i 6, w pozostałym zakresie wniósł o oddalenie odwołania.

Odwołujący, pismem z 14 września 2023 roku, wniósł o przeprowadzenie dowodów

z dokumentów:

1/ dokumentu Magic Quadrant for Network Firewalls z tłumaczeniem;

- na okoliczność, iż rynek liderów urządzeń firewall jest ograniczony do producentów Checkpoint, Palo Alto i Fortinet,

2/ e-mail (…) z 14 września 2023 z wyceną Arrow rozwiązania Checkpoint;

- na okoliczność, iż dystrybutor Arrow odmówił wyceny rozwiązania Checkpoint z uwagi na niespełnienia przez rozwiązanie Checkpoint wymagań przedmiotowych OPZ;

3/ e-mail (…) z 14 września 2023 z wyceną Arrow rozwiązania Fortinet (plik Excel) dla:

a/ konfiguracji określonej w OPZ;

b/ konfiguracji określonej w OPZ z uwzględnieniem zmian zgodnych z żądaniami odwołania;

- na okoliczność, iż zaskarżone wymagania OPZ podrażają cenę rozwiązania Fortinet ponad z kwoty 2.348.946,36 Euro netto do kwoty 5.889.419,52 Euro netto (wg cen katalogowych producenta).

Odwołujący, na posiedzeniu w dniu 15 września 2023 roku, w związku z wyjaśnieniami zamawiającego z 14 września 2023 r. oświadczył, że wycofuje żądanie opisane w odwołaniu w punkcie 1. Odnośnie żądania nr 3 i dokonaną przez zamawiającego zmianą specyfikacji
w OPZ oświadcza, że żądanie zostało spełnione przez zamawiającego w związku z tym,
w tym zakresie odwołanie powinno podlegać umorzeniu. Analogiczne w zakresie żądania 5, natomiast cofa żądanie 6.

Tym samym do merytorycznego rozpoznania na rozprawę zostały skierowane zarzuty, których żądania zostały opisane w pkt 2 i 4 odwołania.

Zamawiający, pismem z 15 września 2023 r., wniósł o przeprowadzenie dowodów
z dokumentów, tj. zrzuty ze strony sprzedawców zaawansowanych systemów bezpieczeństwa dla systemu ofertowanego przez producenta Fortinet w wersji FortiGate_4401F Firewall wraz z cenami sprzedaży,

- na okoliczność, że wycena dostarczona przez odwołującego przedstawia ceny katalogowe, które są o około 72% wyższe od faktycznych cen sprzedaży.

Odwołujący, pismem z 18 września 2023 roku, w odpowiedzi na wniosek dowodowy zamawiającego z dnia 15 września 2023 roku, przedstawił dodatkowe stanowisko w sprawie.

Zamawiający, pismem z 20 września 2023 roku, odniósł się do stanowiska odwołującego (odpowiedź na odwołanie II), wnosząc o oddalenie odwołania.

Na rozprawie, w dniu 21 września 2023 roku, odwołujący zmodyfikował żądanie (nr 2) precyzując, iż „*W odniesieniu do żądania nr 2 rozszerza żądanie o kolejne żądanie ewentualne, tj. uchylenie z punktu 29e wymagań co do wartości przepustowości przy jednoczesnym zamieszczeniu w SWZ w postaci warunku przedmiotowego, tj. wyników testów spełnienia przez zaoferowaną konfigurację parametrów, o których mowa na str. 10-11 pisma Zamawiającego z 20.09.2023 r., określenia wartości tych parametrów oraz zdefiniowania dopuszczalnych architektur dla oferowanych rozwiązań przy założeniu, że będą one obejmować co najmniej architektury NGFW producentów wymienionych w aktualnej klasyfikacji GARTNER LEADERS – dotyczy OPZ*”.

Uwzględniając dokumentację z przedmiotowego postępowania o udzielenie zamówienia publicznego, jak również biorąc pod uwagę oświadczenia i stanowiska stron, złożone w pismach procesowych, jak też podczas rozprawy Izba stwierdziła,

iż odwołanie nie zasługuje na uwzględnienie.

W zakresie zarzutów skierowanych do merytorycznego rozpoznania na rozprawie odwołujący wskazał, co następuje.

(żądanie nr 2)

Wymaganie pkt 29) e) część Specyfikacja komponentu zabezpieczającego OPZ.

Treść wymagania:

„*Zamawiający dopuszcza, aby wymagane funkcjonalności komponentu zabezpieczającego (z wyjątkiem funkcji wykrywania aplikacji, obsługi IPS, AV i NAT) zostały zrealizowane poprzez dostarczenie urządzenia albo zespołu urządzeń wraz z odpowiednim oprogramowaniem (zwanych dalej łącznie elementem dodatkowym) pod warunkiem, że spełnione zostaną łącznie niżej określone wymagania:*

(…)

e) dla ewentualnych urządzeń w funkcji Inspekcji SSL/TLS, wymaganych jest co najmniej 4 interfejsów 100Gbps i wkładek o przepustowości 100 Gbps (transmisja na odległość min. 10km)

(Zamawiający nie dopuszcza zastosowania w tym celu żadnego z podstawowych interfejsów 100Gbps, tzn. w takim wypadku każdy komponent zabezpieczający musi być wyposażony w 4 dodatkowe, w stosunku do wymagań SWZ interfejsy 100Gbps)”

Powyższe wymaganie dotyczy elementu dodatkowego odpowiadającego za funkcjonalność opisaną w pkt 28 tj. funkcjonalność deszyfracji SSL/TLS w sytuacji, gdy oferowany firewall nie posiada własnej funkcjonalności deszyfracji SSL/TLS zgodnej z opisem z pkt 28. Tylko urządzenia firewall NGFW Palo Alto zapewniają deszyfrację SSL/TLS zgodn

z opisem z pkt 28 (dowód: matryca przeglądu oferowanych przez producentów urządzeń firewall NGFW cech technicznych urządzeń z dokumentami źródłowymi – na okoliczność spełnienia wymagania wyłącznie przez urządzenia firewall NGFW Palo Alto).

W wymaganiu z pkt 28 zamawiający oczekuje wydajności deszyfracji SSL/TLS na poziomie 20Gbps, zarówno w sytuacji, gdy deszyfrację zapewnia sam firewall jak również, gdy zapewnia ją element dodatkowy: „*Bez względu na użyte rozwiązanie, wymaga się wydajności minimum 20 Gbps przepustowości dla inspekcji SSL/TLS (ang. SSL Inspection Throughput) oraz obsługę 75 wirtualnych instancji (analogicznie do NGFW)*".

Pomimo, iż pkt 28 definiuje minimalną wydajność przepustowości na poziomie 20 Gbps
w pkt 29 wymaga się zastosowania dodatkowych interfejsów dla elementu dodatkowego
w postaci 4 interfejsów po 100 Gbps:

„*e) dla ewentualnych urządzeń w funkcji Inspekcji SSL/TLS, wymaganych jest co najmniej 4 interfejsów 100Gbps i wkładek o przepustowości 100 Gbps (transmisja na odległość min. 10km)*

(Zamawiający nie dopuszcza zastosowania w tym celu żadnego z podstawowych interfejsów 100Gbps, tzn. w takim wypadku każdy komponent zabezpieczający musi być wyposażony w 4 dodatkowe, w stosunku do wymagań SWZ interfejsy 100Gbps)"

Przedmiotowe wymaganie jest nadmiarowe, gdyż 4 interfejsy i wkładki po 100Gbps zapewniają łącznie 400 Gbps przepustowość, czyli dwudziestokrotnie krotnie większą niż wymagana przepustowość dla SSL/TLS (tą określono na 20 Gbps w pkt 28). Jest to zatem przypadek zbędnego przewymiarowania wymagania w zakresie przepustowości interfejsów zmuszających wykonawców oferujących urządzenia innych producentów niż Palo Alto do uwzględnienia w cenie oferty kosztów zakupu 4 interfejsów i wkładek po 100 Gbps, podczas gdy interfejsy o mniejszej przepustowości zapewniłyby prawidłowe działanie SSL/TLS na poziomie wymaganych 20Gpbs. Wymaganie jest przeskalowane wyłącznie w celu zwiększenia kosztów zastosowania elementu dodatkowego, a więc promuje natywne szyfrowanie SSL/TLS przez urządzenia Palo Alto NGFW (dowód: kalkulacja cen zakupu 4 interfejsów i wkładek pod 100 Gbps, kalkulacja cen zakupu 4 interfejsów i wkładek pod 10 Gbps, kalkulacja cen zakupu 4 interfejsów i wkładek pod 25 Gbps – na okoliczność różnicy
w cenie zakupu i wpływu na cenę oferty). Z tej przyczyny odwołujący wniósł o zmianę wymagania poprzez obniżenie minimalnej przepustowości interfejsów.

Zamawiający w „odpowiedzi na odwołanie I" wskazał, iż w swej argumentacji odwołujący nie bierze pod uwagę okoliczności, iż zgodnie z zapisami OPZ zamawiający wymaga dostarczenia w pełni redundantnego Systemu o całkowitej przepustowości 60Gbps. Mając na uwadze powyższe, wykonawca, który zaoferuje rozwiązanie oparte na urządzeniu bez wbudowanej inspekcji SSL/TLS musi dostarczyć dwa równorzędne komponenty zabezpieczające i dwa równorzędne elementy dodatkowe. Należy również wziąć pod uwagę, iż dopuszczane przez OPZ rozwiązanie w zakresie realizacji inspekcji SSL/TLS, opisane
w punkcie 28 OPZ, może być realizowane także przez zespół połączonych ze sobą urządzeń.

Schemat połączenia komponentu zabezpieczającego z urządzeniem dodatkowym zamawiający zilustrował stosownym rysunkiem.

Uwzględnienie warunku redundancji podwaja wymagania na liczbę interfejsów, gdyż komponent zabezpieczający musi być dodatkowo wpięty do elementu dodatkowego zapasowego komponentu zabezpieczającego. Przebieg ruchu pomiędzy komponentem zabezpieczającym i elementem dodatkowym wygląda następująco:

•Komponent zabezpieczający wysyła 20 Gbps ruchu szyfrowanego do elementu dodatkowego

•Element dodatkowy rozszyfrowuje ruch i wysyła go do komponentu zabezpieczającego.

Należy zaznaczyć, że realna wielkość ruchu rozszyfrowanego może być wyższa niż wspomniane wyżej 20Gbps

•Komponent zabezpieczający dokonuje analizy ruchu (np. sprawdza, czy są tam wirusy)

•Komponent zabezpieczający przesyła ruch do elementu dodatkowego celem powtórnego zaszyfrowania

•Element dodatkowy szyfruje ruch i wysyła go do komponentu zabezpieczającego

•Komponent zabezpieczający wysyła zaszyfrowany ruch do miejsca docelowego Opisane czynności dzieją się równolegle.

Proces ten zamawiający zobrazował odpowiednim rysunkiem.

Z powyższej analizy i przedstawionego rysunku wynika, że:

a.interfejsy o przepustowości 10Gbps nie są wystarczające do przesłania 20Gbps ruchu zaszyfrowanego.

b.propozycja z wykorzystaniem do tego celu interfejsów o przepustowości 25Gbps także jest nie do zaakceptowania przez zamawiającego z uwagi na to, że przełączniki sieciowe zamawiającego nie są wyposażone w interfejsy 25Gbps, ale są wyposażone w interfejsy 100Gbps z wkładkami o przepustowości 100Gbps (transmisja na odległość min 10km).

Zamawiający zwrócił uwagę jak kłopotliwe jest zastosowanie rozwiązania z elementem dodatkowym:

•wymaga więcej miejsca i doprowadzenia dodatkowego zasilania

•powoduje zwiększenie potencjalnych punktów awarii

•zwiększa skomplikowanie topologii (wymaga większej liczby połączeń sieciowych)

•zwiększa koszty utrzymania w kontekście planowanej eksploatacji urządzeń

•zmniejsza bezpieczeństwo Systemu (ruch nieszyfrowany opuszcza komponent zabezpieczający).

Pomimo opisanych powyżej wad zastosowania rozwiązania z elementem dodatkowym zamawiający dopuszcza go jako alternatywne rozwiązanie z uwagi na zwiększenie potencjalnej liczby otrzymanych ofert stanowiąc zabezpieczenie zamawiającego przed potencjalnie wygórowanymi warunkami cenowymi rozwiązania ze zintegrowanym elementem dodatkowym. Zamawiający wyjaśnił, że wymaganie zastosowania do połączenia komponentu zabezpieczającego z elementem dodatkowym interfejsu 100Gbps uzasadnione jest również rozwiązaniami, na których oparta jest obecnie infrastruktura sieciowa u zamawiającego. Zmiana powyższego parametru na opisany przez odwołującego wiązałaby się z istotną

i kosztowną reorganizacją całej infrastruktury sieciowej zamawiającego, co jest rozwiązaniem nieproporcjonalnym. Zamawiający wskazuje, iż powyższy parametr jest również wymagany dla rozwiązania, w którym NGFW jest urządzeniem, w którym wykonywane jest deszyfrowanie SSL/TLS i ponowne zaszyfrowanie – tj. bez elementu dodatkowego. Również w przypadku zastosowania rozwiązania bez elementu dodatkowego urządzenie będzie łączyć się

z infrastrukturą sieciową zamawiającego za pomocą interfejsu 100 Gbps (patrz OPZ, Specyfikacja komponentu zabezpieczającego pkt 3).

Biorąc pod uwagę powyższe powody zamawiający uważa, że zastosowanie do połączenia komponentu zabezpieczającego z elementem dodatkowym interfejsu 100Gbps jest w pełni uzasadnione i nie zgadza się na proponowane przez odwołującego zmiany w OPZ.

Odwołujący, w odpowiedzi na wniosek dowodowy zamawiającego z dnia 15 września 2023 roku zwrócił uwagę, iż:

1)firma ENBITCOM jak również firma ALLFIREWALLS nie są autoryzowanymi dystrybutorami producenta FORTINE zatem asortyment powyższych firm nie spełnia wymagania tytułu Wymagania dotyczące Systemu OPZ pkt 2 w treści: „*Wszystkie elementy oferowanego Systemu muszą pochodzić z oficjalnych kanałów dystrybucyjnych producentów, zapewniających w szczególności realizację uprawnień gwarancyjnych. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu*

z autoryzowanego kanału sprzedaży z krajów obszaru UE”,

2)ceny urządzeń oferowanych przez ENBITCOM i ALLFIREWALLS nie posiadają konfiguracji opisanej w SIWZ, szczególności asortyment ALLFIREWALLS określa ceny minimalne, z uwagi na to, iż urządzenia wymagają doposażenia;

3)ceny ENBITCOM jak również firma ALLFIREWALLS są cenami tylko za urządzenia

i nie obejmują wsparcia producenta dla sprzętu;

4)ceny ENBITCOM jak również firma ALLFIREWALLS nie obejmują cen niezbędnego oprogramowania i wsparcia;

5)ceny ujęte w wycenach ARROW (złożone do akt postępowania odwoławczego) są cenami katalogowymi producenta, gdzie przy zakupie możliwe jest uzyskanie upustów; nie mniej wyceny te zostały zgłoszone przez odwołującego jako na okoliczność różnicy pomiędzy wyceną zgodną z OPZ a wyceną zgodną z OPZ uwzględniającą żądania odwołania.

Odwołujący wskazał, że zamawiający w piśmie z 14 września 2023 roku podnosi konieczność zapewnienia dla dodatkowych urządzeń w funkcji Inspekcji SSL/TLS dodatkowych 4 interfejsów, które i tak są wymagane przy realizacji rozszywania/dekrypcji ruchu SSL na komponencie NGFW. Niezależnie czy ruch jest szyfrowany (gdy dekrypcja następuje na zewnętrznym komponencie- firewalle inne niż Palo Alto) czy nie (gdy dekrypcja następuje na komponencie NGFW- firewalle Palo Alto) owe 20 Gbps ruchu musi być przekazane do innych systemów filtrujących, (np. DLP). Idąc tym torem rozumowania zamawiający musiał już przewidzieć interfejsy do komunikacji z zewnętrznymi komponentami, do których ma zamiar przekazywać rozszyfrowany ruch z komponentu NGFW, gdyż

w przeciwnym wypadku funkcjonalność nie będzie produkcyjnie wykorzystywana.

Rynkowe rozwiązania NGFW „na swoje potrzeby” (czyli na potrzeby własne NGFW) potrafią dokonywać dekrypcji ruchu, natomiast w przypadku niniejszego postępowania zamawiający wymaga szczególnego trybu pracy NGFW, który oprócz dekrypcji na własne potrzeby dodatkowo wysyła ruch do innych systemów (podano tylko przykładowo jakich, bez konkretnych wymagań systemowych). Na tle dalszych wymagań OPZ ten szczególny tryb pracy NGFW jest realizowany przez tylko jednego producenta Palo Alto Networks. Przedstawiony na stronie 10 pisma z 14 września 2023 roku przez zamawiającego schemat dekrypcji odpowiada modelowi pracy NGFW Palo Alto zamieszczonemu w oficjalnej dokumentacji Palo Alto (źródło: (). Tryb dekrypcji oferowany przez urządzenia Palo Alto jest wyjątkową funkcjonalnością tego konkretnego producenta, jednakże w zderzeniu z operatorskimi standardami technologicznymi jakie przywołuje

zamawiający taki tryb dekrypcji nie posiada zdolności do zaspokojenia potrzeb zamawiającego, albowiem:

a)producent (Palo Alto Networks) nie podaje dla tego parametru wydajności w kartach katalogowych, zwłaszcza w zestawieniu z innymi wymaganiami wydajnościowymi (np. Threat Prevention + IPSec + SSL VPN);

b)uruchomienie trybu dekrypcji rażąco wpływa na zasoby wydajność urządzenia/systemu NGFW, tym samym inne wydajności są niemożliwe do równoległego zrealizowania;

c)zamawiający nie podaje rodzaju ruchu i parametrów ruchu, ani nie wymaga konkretnych scenariuszy testowych mających na celu weryfikację wydajności urządzenia.

Biorąc powyższe pod uwagę, można uznać, że wymaganie tego specjalnego trybu pełni funkcję wskazującą na konkretnego producenta i paradoksalnie samo w sobie podnosi cenę ograniczając konkurencję.

Kolejnym nieprawdziwym założeniem w odpowiedzi zamawiającego jest powołanie się na kwestie bezpieczeństwa przekazywania rozszyfrowanego ruchu – niezależnie czy dekrypcja następuje na komponencie NGFW, czy też poza nim, co do zasady i z definicji tej funkcjonalności, ruch rozszyfrowany będzie przekazywany do zewnętrznych komponentów
w każdym z przypadków (o ile nie jest realizowany na NGFW) gdyż dotyczy obu podejść,
tj. zarówno przypadku gdy ruch jest przekazywany do komponentu zewnętrznego (np. DLP), jak i w przypadku gdy funkcjonalność dekrypcji jest realizowana na zewnętrznym systemie
- w obu ruch w formie jawnej będzie podlegał inspekcji przez przykładowy system DLP.

W kwestii interfejsów, pomimo posiadania przez zamawiającego tylko interfejsów 100Gbps – niezależnie już od tego czy przewidział wysyłkę ruchu do systemów zewnętrznych,
w preferowanym systemie można zastosować dedykowane kable, które pozwolą na przejście z 100Gbps na 10x 10Gbps. 8 interfejsów 10Gbps zapewni przepustowość 80 Gbps czyli o 20 Gbps niż przepustowość wymagana przez zamawiającego dla całego urządzenia 60 Gbps (https://lightoptics.co.uk/products/cfp-cxp-cpak-100g-sr10-10x10g-mtp-mtp-to-10x-lc-duplexduplex-multimode-om4?variant=42452594393346).

Ruch dedykowany do deszyfrowania byłby przekazywany do zewnętrznego systemu dekrypcji, tam rozszyfrowywany, kolejno do wirtualnej instancji NGFW celem inspekcji /NGFWAV/IPS itd., a następnie trafiał do analizy przez zewnętrzne systemy (np. DLP, SWG itd.), kolejno do szyfracji i dalej do Internetu lub serwerów. Architektura ta pozwoli w sposób rzeczywisty zapewnić odpowiednie skalowanie, gdyż ruch podlegający deszyfracji będzie skanowany przez NGFW w formie nie wymagającej dodatkowej inspekcji SSL.

Jako wzorcowe alternatywne rozwiązanie należy wskazać przykład projekt budowy Ogólnopolskiej Sieci Edukacyjnej NASK. Ze schematu ruchu w sieci NASK (odwołujący powołał odpowiednią grafikę) wynika, iż w celu zapewnienia adekwatnej wydajności nie przewidziano dekrypcji SSL za pomocą firewalli NGFW. Co więcej wszelkie aspekty wydajności sieci NASK są przedmiotem szczegółowych testów przewidzianych w opisie przedmiotu zamówienia dla postępowania, które przeprowadził NASK (dowód: opz postępowania dotyczącego projekt budowy Ogólnopolskiej Sieci Edukacyjnej NASK).

W przedmiotowym postępowaniu zauważalny jest brak regulacji OPZ w zakresie testów wydajności, w tym dekrypci SSL. Podczas wykorzystania funkcjonalności dekrypcji w trybie chain na rozwiązaniu NGFW zasoby rozwiązania są współdzielone z innymi funkcjonalnościami. W przypadku zgodnego ze sztuką rozwiązań telekomunikacyjnych rozdzielenia funkcjonalności, gdzie deskrypcja jest realizowana na osobnym podsystemie – zasoby te są dedykowane i izolowane, co pozwala na zagwarantowanie wydajności, zarówno dla funkcji filtrujących ruch jak i dla funkcji odpowiedzialnych za deszyfrację. W kartach katalogowych producentów firewalli podawane są wartości dla jednoczesnych wydajności (np. IPSec VPN i SSL VPN i IPS), przykładowo, że przy dekrypcji 20 Gbps ruchu SSL będzi możliwość korzystania z 60 Gbps threat prevention i ruchu IPSec. Niestety wydajności są podawane niezależnie od siebie, tzn. testowane w osobnych scenariuszach (źródło: https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US /resources/datasheets/pa-5450-series).

W przypadku dostarczenia zewnętrznego i dedykowanego komponentu realizującego dekrypcję SSL takie podejście w tym obszarze będzie możliwe. Jeśli natomiast zakładamy realizację dekrypcji SSL na module NGFW, wówczas inne wydajności z racji współdzielenia zasobów są nieprzewidywalne i skrajnie nieosiągalne, a udowodnienie ich osiągnięcia nie może w takich systemach polegać tylko na informacji z karty katalogowej, kluczowe tutaj jest określenie ruchu oraz docelowych systemów współpracujących, których zamawiający nie wyspecyfikował. Tym samym zamawiający preferuje gorsze rozwiązanie (Palo Alto), gdzie wydajności mogą nie być zachowane a jednocześnie upośledza rozwiązania z dedykowanymi zasobami (np. Fortinet), gdzie realizacja poszczególnych funkcjonalności będzie bardziej przewidywalna. Zmiana pkt 29 d) OPZ dokonana w dniu 14 września 2023 stanowi potwierdzenie połączenia przez zamawiającego w wymaganiach dotyczących funkcjonalności NGFW parametrów wydajności NGFW z funkcjonalnościami deszyfrującymi. Wymagania musiałyby być zdublowane, co nie jest uzasadnione, ponieważ kluczową funkcjonalność można uzyskać

bez ich powielania – przepisanie w/w parametrów ma za zadanie eskalację wymagań dla modułu dodatkowego realizującego dekrypcję SSL.

Reasumując, odwołujący wskazał, iż:

1)Firewall typu NGFW nie powinien być elementem przekierowującym do service chain. Wg dobrych praktyk (patrz projekt NASK), przekierowanie powinno nastąpić przez strukturę sieciową: switche L3 / routery do deszyfratora SSL, który prześle ruch do service chain. Wymagane jest tu 20Gbs, więc 8 x 10G w zupełności wystarczy do przyjęcia ruchu, przesłania przez service chain, zaszyfrowania i odesłania dalej do NGFW. Wydzielony VDOM NGFW może być składnikiem service chain. Interfejsy 100G na switchach zamawiającego można rozdzielić na 10 x 10G za pomocą dostępnych wkładek/kabli. Zamawiający może określić rodzaj tych wkładek i mogą one być częścią oferty.

2)Zamawiający jako podmiot świadczący usługi cyfrowe powinien w sposób odpowiedzialny planować budowę infrastruktury. Wymagania wskazujące na jednego producenta Palo Alto Networks skutkują uprzywilejowaną pozycją tej firmy w przetargu, ale nie gwarantują wdrożenia funkcjonalności inspekcji SSL. Dobre praktyki stosowane w innych projektach publicznych np. ochrona Internetu dla szkół (NASK PIB - Operator OSE) zakładają rozszyfrowanie ruchu przez dedykowany element i przesłanie go przez elementy bezpieczeństwa, w tym NGFW.

3)Niezbędnym elementem postępowania powinno być doprecyzowanie testów wydajnościowych wykonanych w laboratorium producenta lub specjalizowanej firmy wynajętej przez wykonawcę. Rodzaj oczekiwanych protokołów, aplikacji, pasmo, ilość nowych sesji L4, L7, SSL na sekundę, ilość równoległych sesji L4, L7, SSL, sposób rozdzielenia ilości transakcji http per sesja SSL oraz maksymalne zużycie zasobów poszczególnych komponentów (CPU, RAM) musi być określone w OPZ, aby zamawiający zagwarantował sobie pozytywne wdrożenie projektu.

4)Systemy NGFW są zoptymalizowane do skanowania ruchu przetwarzanego wewnątrz urządzenia. Rozszyfrowanie w celu wysłania, ponowne odebranie i zaszyfrowanie ruchu wymagają typowych funkcji proxy obciążających w sposób mało przewidywalny urządzenie NGFW, które wykonuje szereg innych zadań. Zagwarantowanie wydajności systemu 60Gbps przy jednoczesnym 20Gbps SSL forward proxy nie jest możliwe bez testów.

5)Uwzględnienie przez Izbę odwołania w zakresie żądania pkt 2) odwołania oznaczać będzie, iż wykonawcy będą musieli uwzględnić w wycenie oferty okoliczność, iż zamawiający dysponuje wkładkami 100Gbps, co będzie wymagało zastosowania odpowiednich łączy zapewniających zastosowanie interfejsów i wkładek o niższej przepustowości.

Zamawiający w odpowiedzi na odwołanie II, dodatkowo wskazał, iż odwołujący w piśmie z 14 września 2023 r. przedstawił argumenty bazując na informacjach o producentach urządzeń Network Firewall wskazanych w raporcie Gartnera. Jednocześnie sposób przedstawienia tych informacji stoi w wyraźnej sprzeczności z zapisami SWZ. W efekcie, zawarta w piśmie sugestia, jakoby dokumentacja przetargowa dopuszczała jedynie rozwiązanie oferowane przez jednego producenta – jest nieprawdziwa jako niepowiązana logicznie z zapisami SWZ. Po pierwsze, parametr związany z pozycją producenta w raporcie Gartnera jest jedynie parametrem punktowanym, a nie wymaganym – jak zdaje się sugerować odwołujący. W efekcie nieuprawnionym jest branie pod uwagę jedynie 3 producentów ocenionych jako „Leaders", gdyż są to producenci, których rozwiązania otrzymałyby 15 punktów. Odwołujący pominął ocenę 7 innych producentów, którzy zostali wskazani w części „Visionaries" i „Challengers", a których rozwiązania otrzymałyby 8 punktów oraz pozostałych licznych producentów, których rozwiązania również byłyby dopuszczone w przetargu. Po drugie, odwołujący zdaje się sugerować, że rozwiązania zaproponowane przez producenta Check Point Software Technologies nie spełniają wymagań zawartych w dokumentacji przetargu, a tym czasem z korespondencji mailowej dołączonej do pisma z 14 września 2023 r. nie wynika jednoznacznie, że rozwiązania oferowane przez tego producenta nie spełniają wymagania OPZ. W komentarzu zawartym w mailu wskazano jedynie na wyższą (nie określoną bliżej) cenę urządzenia spełniającego wymagania. Wskazano również, że w rozwiązaniu Check Pointa nie ma możliwości, aby rozszyfrowany ruch po wysłaniu do zewnętrznego urządzenia powrócił do urządzenia Check Pointa w celu zaszyfrowania i przesłania dalej do celu. Powyższa charakterystyka rozwiązania Check Point nie wyklucza możliwości uzyskania wymaganego parametru przy zastosowaniu dodatkowych elementów dołożonych do systemu. Należy zwrócić uwagę, że również w przypadku rozwiązania oferowanego przez producenta Fortinet – możliwe jest jego wykorzystanie dla dostawy systemu objętego zamówieniem poprzez dołożenie dodatkowych elementów umożliwiających osiągnięcie parametrów wymaganych w postępowaniu. W tym wypadku odwołujący nie kwestionuje takiej możliwości. Tym samym nie sposób przyjąć za prawdziwą sugestii odwołującego jakoby rozwiązania producenta Check Point w sposób jednoznaczny nie mogły być brane pod uwagę przy realizacji przedmiotu zamówienia.

Również producent Fortinet – dostarcza rozwiązanie spełniające wymagania OPZ. Należy podkreślić, że wskazując ceny katalogowe, bez stosowanych każdorazowo upustów, odwołujący sztucznie zawyżył również wartość różnicy pomiędzy wariantami rozwiązań oferowanych przez tego producenta. Jak wynika z wycen przedstawionych przez zamawiającego we wniosku dowodowym z 15.09.2023 r., różnica pomiędzy cenami katalogowymi, a faktycznymi cenami sprzedaży wynosi na ogół ponad 70 %. Odwołujący dodatkowo zawyżył różnicę pomiędzy Fortinet FortiGate-3501F, a

Fortinet FortiGate 4401F, dodając do wyceny wersji 4401F dodatkowe zbędne licencje ze wsparciem u każdego potencjalnego użytkownika (vide: odpowiedź na zarzut nr 4 w piśmie z 14.09.2023 r. oraz poniżej).

Podsumowując, sugestia zawarta w piśmie odwołującego, jakoby tylko jeden produkt spełniał wymagania OPZ jest nieprawdziwa i oparta na założeniach nie uwzględniających zapisów dokumentacji przetargowej.

Odnosząc się do twierdzeń odwołującego zawartych w piśmie z 19.09.2023 r. w zakresie przedstawionych przez zamawiającego informacji o cenach – wyjaśniam, że wskazane tam firmy ENBITCOM i ALLFIREWALLS s sprzedawcami sprzętu IT, a nie dystrybutorami. Tym samym, na podstawie przedstawionej wyceny nie sposób jednoznacznie przesądzić, z jakich kanałów dystrybucyjnych pozyskują ten sprzęt. W szczególności mogą to być kanały oficjalne, a tym samym, twierdzenie odwołującego jest nieuprawnione. Należy też wskazać, że firma Arrow, na którą powołuje się odwołujący jest dystrybutorem i zwykle nie sprzedaje sprzętu dla użytkownika końcowego. W odpowiedzi na zarzut odwołującego, iż przedstawione przez odwołującego wyceny nie zawierają wszystkich niezbędnych elementów zamówienia, należy podkreślić, że wyceny przedstawione przez obydwie Strony mają charakter uproszczony i nie zawierają wszystkich szczegółowych informacji pozwalających określić, czy dany produkt zawiera wycenę wszystkich elementów składowych niezbędnych do realizacji przedmiotu zamówienia zgodnie z jego opisem.

Uzupełnienie stanowiska zamawiającego co do żądania nr 2) z odwołania.

W odpowiedzi na twierdzenia odwołującego zawarte w punkcie III pisma z 19.09.2023 r., zamawiający podtrzymuje swoje dotychczasowe stanowisko i wyjaśnia, co następuje.

W opinii zamawiającego stanowisko prezentowane w piśmie z 19.09.2023 r. stanowi kolejną próbę forsowania przez odwołującego swoich rozwiązań, bez uwzględnienia obiektywnych potrzeb zamawiającego. Świadczy o tym schemat opisany w p.III.7. pisma odwołującego. Schemat ten zawiera szereg urządzeń, których zamawiający nie potrzebuje. Zamawiający zwraca także uwagę, że ustawa „Prawo Telekomunikacyjne" zobowiązuje zamawiającego do stosowania najnowocześniejszych rozwiązań, powoływanie się w tym kontekście na rzeczywiście bardzo dobre rozwiązania stosowane w NASK, które jednak były opracowane co najmniej 5 lat temu, jest co najmniej ryzykowne. Analizując dynamikę zmian na rynku cyberbezpieczeństwa można z dużą dozą prawdopodobieństwa założyć, że gdyby projekt ten był realizowany dzisiaj to część projektu uwzględniłaby bardziej nowoczesne komponenty dostępne obecnie na rynku. Natomiast dla zamawiającego najbardziej istotny jest fakt proponowania przez odwołującego wspomnianego w p.III.6 kabla typu breakout, który, jak rozumie zamawiający, ma rozwiązać problem kompatybilności proponowanego przez odwołującego rozwiązania z posiadaną przez zamawiającego infrastrukturą sieciową. Tak nie jest, interfejsy 100GE zamawiającego nie dopuszczają na wspomniane w p.III.6 rozszycie portu 100GE w trybie 10x10GE. Dlatego zamawiający w pełni podtrzymuje swoje stanowisko, które zawarł w odpowiedzi na odwołanie I, t.j. braku zgody na modyfikację punktu 29 e) OPZ zgodnie z żądaniem odwołującego.

Zamawiający nie zgadza się z argumentacją odwołującego dotyczącą faworyzowania któregokolwiek z producentów (w szczególny sposób jest to przywołane w p. III.1, III.3, III.4, III.9, III.10 pisma odwołującego z 19.09.2023 r.). Opis przedmiotu zamówienia jest sformułowany w taki sposób, iż dopuszcza różne sposoby realizacji oczekiwanej i pożądanej funkcji. Opis funkcji jest w kilku miejscach wręcz bardzo ogólny, co zresztą zauważa sam odwołujący w p. III.4.c pisma „c) Zamawiający nie podaje rodzaju ruchu i parametrów ruchu, ani nie wymaga konkretnych scenariuszy testowych mających na celu weryfikację wydajności urządzenia". Zamawiający określił w swoich wymaganiach, że dopuszcza inne rozwiązania, ale wymaga dostarczenia „opisu współpracy proponowanej integracji z dostarczanymi funkcjami bezpieczeństwa (IPS/AV/Anty-Spyware)". Niejako odwołujący w piśmie wpisał się
w narrację zamawiającego wskazując jeden z możliwych sposobów realizacji funkcji (wskazał to w p.III.7. Architektura forsowana przez zamawiającego nie jest jedyną możliwą, przykładowo, jeśli zastosować zewnętrzny system ruch mógłby wyglądać następująco").

Zamawiający nie ma oczywiście pełnej wiedzy co do szczegółów realizacji zadania, które opisał odwołujący (np. niejasne jest to jakie przełączniki ma na myśli odwołujący i czy będą one częścią oferty, oraz jakie będą one miały parametry – zamawiający dysponując określoną infrastrukturą musi uwzględnić w takiej sytuacji konieczność zapewnienia jakości działania
i dostępność funkcji nie gorszą niż na używanych dotychczas rozwiązaniach). Nie jest również jasne w oparciu o jakie kryteria odwołujący chce przekierować ruch do deszyfratora – chcemy jednoznacznie wskazać, że urządzenia NGFW są urządzeniami potrafiącymi przekierowywać ruch nie tylko w oparciu o informacje L3/L4 jak wskazał odwołujący, ale w oparciu o inne parametry niedostępne dla tych przełączników (np. gdy ruch SSL będzie odbywał się
z wykorzystaniem innych niż standardowy -443- portów TCP/IP). Nie zmienia to jednak faktu, iż odwołujący w niniejszym piśmie w p.III.7 sam obalił tezę, że zamawiający wskazał jeden sposób realizacji zadania.

Idąc dalej - w p. III.1 odwołujący słusznie zauważył „Zamawiający musiał już przewidzieć interfejsy do komunikacji z zewnętrznymi komponentami, do których ma zamiar przekazywać rozszyfrowany ruch z komponentu NGFW, gdyż w przeciwnym wypadku funkcjonalność nie będzie produkcyjnie wykorzystywana". Zamawiający na potrzeby wykazania, iż

potrzeba zapewnienia dodatkowych interfejsów jest uzasadniona wskazuje jeden z możliwych sposobów realizacji – potencjalnie najprostszy nie wymagający ani funkcji deszyfracji SSL wbudowanej w firewall ani rozbudowanej konfiguracji deszyfratora (wystarczające byłyby dodatkowe interfejsy wymagane przez zamawiającego).

Przykładowy scenariusz ruchowy:

1.Ruch sieciowy wchodzi do firewalla. Firewall na podstawie informacji dotyczących ruchu – np. wykrywanie ruchu HTTPS - określa który ruch będzie przesłany do deszyfracji (wymagane 20Gbps)

2.Ruch zaszyfrowany (20Gbps) jest przekierowany do deszyfratora

3.Deszyfrator odszyfrowuje ruch i wysyła dane zdeszyfrowane z powrotem do firewalla

4.Firewall przeprowadza inspekcję z wykorzystaniem wbudowanych silników bezpieczeństwa

5.Firewall wysyła (z wykorzystaniem dostępnych interfejsów opisanych w wymaganiach podstawowych) ruch do analizy z wykorzystaniem zewnętrznych systemów bezpieczeństwa typu IPS, DLP, itd.

6.Firewall przyjmuje ruch sprawdzony przez zewnętrzne systemy bezpieczeństwa

7.Firewall przesyła otrzymany ruch po inspekcji do ponownego zaszyfrowania (20Gbps)

8.Deszyfrator szyfruje otrzymany ruch i wysyła w postaci zaszyfrowanej ponownie do firewalla

9.Ruch zaszyfrowany przez deszyfrator (20Gbps) wchodzi do firewalla

10.Firewall przesyła ruch zaszyfrowany na zewnątrz do odbiorców

Zamawiający zwraca tutaj uwagę, że bez względu na to czy funkcja deszyfracji jest realizowana bezpośrednio na firewallu czy też z wykorzystaniem zewnętrznego deszyfratora, wymagania dotyczące interfejsów niezbędnych do komunikacji z zewnętrznymi systemami bezpieczeństwa są niezmienne. W przypadku realizacji funkcji deszyfracji w urządzeniu NGFW, firewall operuje już na ruchu zdeszyfrowanym (bo sam deszyfruje) i przekierowanie ruchu do poszczególnych zewnętrznych systemów bezpieczeństwa może być realizowany wbudowanymi interfejsami. W przypadku, gdy deszyfracja będzie realizowana na zewnętrznym komponencie to ruch ten musi zostać z firewalla wysłany oraz odebrany
w bardzo jasno zdefiniowanej relacji ruchowej tj. do/z deszyfratora. Do obsługi tego ruchu wymagane są dodatkowe interfejsy. Te interfejsy w ocenie zamawiającego będą potrzebne
w każdym scenariuszu z zastosowaniem zewnętrznych deszyfratorów.

Odpowiadając na zarzut z p.III.2 zamawiający ponownie podkreśla, że jego intencją jest wykorzystanie posiadanych już obecnie rozwiązań. Zamawiający informuje, że w pierwszej kolejności rozwiązanie ma wykorzystywać dodatkowe systemy IPS (Snort, Suricata) oraz systemy bezpieczeństwa firmy Juniper. Zamawiający przewiduje również, iż paleta wykorzystywanych zewnętrznych systemów bezpieczeństwa będzie się powiększać w trakcie eksploatacji rozwiązania.

Biorąc pod uwagę zarzuty odwołującego o możliwe dodatkowe obciążenie firewalli opisane w p.III.4.a-c zamawiający informuje, iż według jego wiedzy żaden z producentów nie podaje
w kartach katalogowych specyficznych informacji dotyczących wydajności urządzeń
z włączonymi funkcjami bezpieczeństwa – jak podał odwołujący w p.III.4.a przykład dla Threat Prevention + IPSec + SSL VPN. Zamawiający ma tego świadomość i zakłada, że wykonawcy jako firmy posiadające odpowiednie certyfikacje i dostęp do informacji zastrzeżonych poszczególnych producentów będą mogli właściwie dobrać urządzenia,

Odpowiadając na zarzuty z p. III.4.b-c zamawiający ma świadomość, że „uruchomienie trybu deskrypcji rażąco wpływa na zasoby wydajność urządzenia/systemu NGFW" stąd też, aby nie dopuścić do kanibalizacji tych zasobów zmienił wymaganie 28 OPZ dotyczące komponentu zabezpieczającego. Zamawiający zrezygnował też z testowania urządzeń – opisanie scenariusza testów w przypadku, gdy zamawiający dopuszcza różne sposoby realizacji systemu w powiązaniu ze zmienną charakterystyką ruchu (sezonowo) jak też różnymi zestawami parametrów dotyczących samego SSL (klucze, uwierzytelnienie, itp.) jest praktycznie niemożliwe, a same wyniki ów mogą być trudne do porównania. Jednocześnie wprowadzenie wymogu testów powoduje również znaczące zwiększenie kosztów zarówno pieniężnych jak i ludzkich w zakresie ich przygotowania i przeprowadzenia.

Dodatkowo zamawiający wyjaśnił, iż wziął pod uwagę szereg innych uwarunkowań, które to nie zostały uwzględnione w Opisie Przedmiotu Zamówienia, gdyż ich ujęcie mogłoby spowodować znaczące ograniczenie konkurencji lub doprowadzić wręcz do sytuacji, w której wymagania spełniałoby tylko jedno rozwiązanie, lub też koszt realizacji wszystkich wymagań spowodowałby przekroczenie budżetu. Żeby pokazać jeden z takich aspektów, który mógłby wpłynąć na ograniczenie zamawiający wskazuje tylko na jeden z czynników związany
z wykorzystaniem zewnętrznego deszyfratora. Zgodnie z opisem przykładowego scenariusza ruchowego, o który mowa powyżej, firewall w przypadku zastosowania zewnętrznego deszyfratora obsługuje dodatkowe 40Gbps ruchu, które należałoby uwzględnić
w wymaganiach i tym samym podnieść parametry wymagane w opisie komponentu zabezpieczającego. Podobna kwestia dotyczy liczby obsługiwanych sesji – zarówno w ujęciu globalnym jak i określanym jako liczba sesji na sekundę. Zamawiający mając na względzie,

że oba rozwiązania, zarówno z jak i bez zewnętrznego szyfratora wprowadzają dodatkowe obciążenie dla Firewalla postanowił, iż ten aspekt nie będzie brany pod uwagę.

Odpowiadając na zarzuty z p. III.5 zamawiający przyznaje, iż kwestie bezpieczeństwa przekazywania rozszyfrowanego ruchu są w rozumieniu jego przesyłania - w formie już zdeszyfrowanej - takie same dla obu porównywanych modeli wdrożenia. Jednocześnie zamawiający podtrzymuje argumentację dotyczącą pozostałych kwestii związanych
z wykorzystaniem zewnętrznego deszyfratora.

W kwestii interfejsów – odwołujący w p.III.1 i p.III.6 kwestionuje zarówno potrzebę stosowanie dodatkowych interfejsów jak również wykazuje, że możliwe jest zastosowanie wkładek i kabli typu breakout produkowanych również przez firmy trzecie.

Kwestia dodatkowych interfejsów jest dla zamawiającego bezdyskusyjna co zostało wykazane powyżej. Jeżeli zaś chodzi o dobór wkładek/kabli to zamawiający stoi na stanowisku, iż dopuszcza stosowanie takich komponentów, które są zatwierdzone do stosowania przez producenta komponentu zabezpieczającego zgodnie z wymaganiem opisanym w OPZ w punkcie 13 Wymagań dotyczących systemu. W rozumieniu zamawiającego wszystkie wkładki muszą pochodzić od tego samego producenta lub być udokumentowane jako dopuszczone w tzw. tabelach kompatybilności. Ponadto zamawiający informuje, że połączenia pomiędzy urządzeniami będą realizowane pomiędzy lokalizacjami zamawiającego (wdrożenie w modelu rozproszonym z połączeniami skrośnymi między lokalizacjami) oznacza to że w przypadku zastosowania kabli typu breakout wykonawca zobowiązany będzie dodatkowo do zagwarantowania połączenia wspomnianego kabla breakout z przełącznikami zamawiającego w obu lokalizacjach celem zapewnienia łączności za pomocą infrastruktury zamawiającego. Natomiast przełączniki sieciowe zamawiającego nie pozwalają na rozszycie portów 100GE w trybie 10x10GE. Dodatkowo zamawiający zaznaczył, że przeciąganie kabli typu breakout pomiędzy halami zamawiającego, co może być wymagane w przypadku dostarczenia rozbudowanego elementu dodatkowego, jest absolutnie niemożliwe.

W p. III.8 odwołujący wskazał, że jako „wzorcowe alternatywne rozwiązanie należy wskazać przykład projekt budowy Ogólnopolskiej Sieci Edukacyjnej NASK".

Zamawiający informuje, iż na etapie przygotowania projektu przeanalizował różnego rodzaju modele wdrożeniowe i model, na który powołuje się odwołujący jest mu znany. Realizacja bardzo dużych projektów – a do takich należy przywołany projekt OSE realizowanych przez NASK - zazwyczaj przewiduje zastosowanie specjalizowanych rozwiązań do realizacji określonych funkcji (osobno deszyfracja, WAF, itp.). Zmniejsza to liczbę urządzeń, złożoność topologii i upraszcza zarządzanie. Projekt realizowany przez NASK był projektem ogólnopolskim o budżecie ok. 600 mln zł i jego skala jest niewspółmiernie większa niż projekt realizowany przez zamawiającego. Dla wskazania dysproporcji pomiędzy projektami można przytoczyć tylko kilka faktów:

- W załączonym dokumencie OPZ NASK w p.2.3.2. znajduje się informacja,

iż „Sumaryczna ilość ruchu z sieci Internet do szkół wyniesie 1 058 Gbps, a ze szkół do sieci Internet 385 Gbps (wartości szacowane na rok 2025)". Oznacza to, że systemy bezpieczeństwa były projektowane by obsłużyć ruch 1443Gbps podczas gdy projekt realizowany przez zamawiającego zakłada ruch 60Gbps, czyli 24 razy mniejszy,

- W załączonym dokumencie OPZ NASK w p.3.2.1 opisane są funkcje, które były wymagane w projekcie NASK – w sumie było ich 18. Są tą m.in. funkcje LoadBalancing (równoważenie obciążenia), Monitorowanie urządzeń pod względem obciążenia, Inżynieria ruchu Dystrybucja tożsamości do system SWG, Funkcjonalność WAF, Funkcjonalność SSL VPN*, Dekrypcja i ponowna enkrypcja ruchu szyfrowanego*, FW*, Funkcjonalność IPS*, Funkcjonalność AV* Funkcjonalność Kontroli aplikacji*, DNS resolver, DNS Firewall - ochrona antimalware, DNS Firewall – filtracja treści Kategoryzacja URL, filtrowanie treści, AV dla http. Zamawiający wskazuje, że jego projekt obejmuje tylko 6 (oznaczone *) z 18 funkcjonalności. Zakres funkcjonalny projektu jest zatem zdecydowanie mniejszy – tym samym w większości wdrożeń projekty te cechują się zwykle unifikacją i integracją funkcji w możliwie najmniejszej liczbie urządzeń,

- W załączonym dokumencie OPZ NASK w p.3.3.1 wskazano w tabeli m.in. „Wymaganie na skalowanie Systemu inspekcji ruchu SSL/TLS". Z analizy wynika, że wymagania dla węzłów regionalnych budowanych w ramach projektu OSE w kwestii deszyfracji dramatycznie przewyższają wymagania postawione w projekcie prowadzonym przez ACK Cyfronet. Należy podkreślić, że wymagania dla średniej wielkości województw (lubelskie i podkarpackie) 3,5-krotnie przekraczają wymagania postawione w niniejszym projekcie, zaś wymagania dla województwa małopolskiego są już na poziomie 112 Gbps czyli wymagania zamawiającego są 5,5 razy mniejsze.

Tym samym zamawiający wskazuje na nieporównywalny zakres projektów, wymagania wydajnościowe jak też funkcjonalne. Nie bez znaczenia jest też fakt, że stosowanie urządzeń dedykowanych dla każdej z funkcji jest po prostu rozwiązaniem z natury rzeczy droższym zarówno w kwestii nabycia jak i utrzymania. Warto też wskazać, że wzorując się wprost na projekcie NASK zamawiający musiałby nabyć rozwiązanie składające się z trzech komponentów (lub nawet czterech, jeżeli uznamy, że funkcja ochrony DNS powinna być przeniesiona z firewalla na dedykowane

urządzenie) – co z kolei prowokowałoby do dyskusji w zakresie właściwego wydatkowania środków publicznych. O ile zatem zamawiający przyznaje, że projekt NASK jest ciekawym źródłem referencyjnym dla podmiotów prowadzących bardzo duże projekty, o tyle wykazuje, iż prowadzony przez niego projekt nie spełni kryteriów projektu określanego jako bardzo duży. Tym samym nie możemy zgodzić się, że model referencyjny wskazany przez odwołującego jest modelem, który może być bez refleksji przypisywany jako właściwy dla zamawiającego.

Ponadto zamawiający wskazuje, że projekt OSE prowadzony przez NASK był realizowany w roku 2018, zaś same założenia do projektu musiały być przygotowane wcześniej. Analizując dynamikę zmian na rynku cyberbezpieczeństwa można z dużą dozą prawdopodobieństwa założyć, że gdyby projekt ten był realizowany dzisiaj to część projektu uwzględniłaby bardziej nowoczesne komponenty dostępne obecnie na rynku. Zamawiający wskazuje tym samym, że starał się opisać wymagania według wiedzy o potrzebach i własnej ekspertyzy technicznej uwzględniając stan na połowę 2023 roku, opisać w sposób możliwie otwarty, przejrzysty, niedyskryminujący.

Odpowiadając na zarzuty z p. III.9 zamawiający informuje, iż kwestia ta została przez niego wyjaśniona – zamawiający zrezygnował też z testowania urządzeń z powodów związanych z dopuszczeniem szeregu różnych sposobów realizacji zadania.

Jednocześnie zamawiający informuje, iż zmiana p.29.d OPZ, na który powołuje się odwołujący miała na celu doprecyzowanie wymagania – zamawiający nie podziela zdania odwołującego, iż wymagania te są nadmiarowe. Wymagania odzwierciedlają podzbiór wymagań już określonych dla NGFW, tym samym zamawiający nie widzi tutaj powodów dla postawionego zarzutu eskalacji wymagań. Zresztą sam odwołujący to przyznał akceptując zmiany dokonane przez zamawiającego.

W odniesieniu do p.III.10 pt. „Reasumując"

W p.III.10.1 - odwołujący w sposób autorytatywny wskazuje konkretne rozwiązanie techniczne i próbuje udowodnić wyższość rozwiązań technologicznych, którymi najprawdopodobniej dysponuje w ofercie. Zamawiający informuje, że dopuszcza techniczną realizację postawionych wymagań z wykorzystaniem zewnętrznego deszyfratora i urządzeń sieciowych (zwraca jednak uwagę na to, że na schemacie w p.III.7 odwołujący wykorzystuje dodatkowe urządzenia sieciowe, których zamawiający najprawdopodobniej nie posiada). Jednocześnie zamawiający jest jednak świadom, że zewnętrzny tzw. offload protokołu SSL ma wiele zalet, ale ma też wiele wad. Dlatego też zamawiający dopuszcza inne opcje realizacji wymagań zamawiającego.

W p.III.10.2. odwołujący ponownie wskazuje na domniemane preferowanie jednego z producentów. Zamawiający wielokrotnie wskazywał, że jego celem jest uzyskanie określonej funkcjonalności. Wskazywał też, że dopuszcza różne sposoby realizacji. Co więcej – w kilku punktach specyfikacji sam odwołujący zauważa, że niektóre parametry są pominięte, czy też poszczególne komponenty zostały opisane ogólnie bez nadmiernego wnikania w cechy szczegółowe. Celem zamawiającego jest pozyskanie określonego rozwiązania spełniającego jego wymagania techniczne, charakteryzującego się możliwie wysoką niezawodnością oraz nie obarczonego nadmiarowymi kosztami utrzymania. Zarówno w p.10.1 jak i 10.2 odwołujący wskazuje projekt OSE jako jedyną wykładnię właściwego projektowania i planowania środowisk bezpieczeństwa. Jak wykazał zamawiający projekt ten ani skalą w rozumieniu wymagań wydajnościowych, ani funkcjonalnie nie jest porównywalny z projektem realizowanym przez zamawiającego.

W p.III.10.3 i p.III.10.4 odwołujący ponownie w sposób autorytatywny stara się wykazać, iż przeprowadzenie testów wydajnościowych jest jedynym właściwym działaniem pozwalającym zamawiającemu na zweryfikowanie parametrów urządzeń, kwestionując jednocześnie inne środki dowodowe. Należy tutaj nadmienić, iż wymaganie dotyczące deszyfracji SSL jest dzisiaj powszechne i dotyczy wielu postępowań publicznych dotyczących rozwiązań klasy NGFW – można by zatem dokonać domniemania, że wszystkie takie postępowania, w których nie były przeprowadzone testy były przeprowadzone w sposób w którym „Zamawiający nie zagwarantował sobie pozytywnego wdrożenia projektu" - co jest oczywistą nieprawdą. Zamawiający podjął decyzję by nie przeprowadzać procedury testowej jako nadmiarowej.

(żądanie nr 4)

Odwołujący w odwołaniu wskazał, co następuje.

Wymaganie pkt 31 c) część Specyfikacja komponentu zabezpieczającego OPZ.

Treść wymagania:

„Komponent zabezpieczający musi zapewniać realizację funkcjonalności zdalnych sesji VPN (ang. remote access VPN) dla użytkowników w zakresie opisanym poniżej:

c) Zestawianie tuneli SSL VPN z wykorzystaniem klienta VPN dostarczonego przez producenta urządzenia NGFW dla co najmniej 30000 użytkowników"

Dodatkowo w pkt e) i f) wymaga się, aby

„f) Komponent zabezpieczający musi zapewniać realizację połączeń VPN

z wykorzystaniem klientów instalowanych na stacjach roboczych (ang. desktop clients). Aplikacje te muszą być kompatybilne z oferowanym urządzeniem i pochodzić od tego samego producenta.

g) Aplikacje klienckie instalowane na stacjach klienckich nie mogą wymagać dodatkowych licencji instalowanych na tych stacjach i muszą być udostępnione przez Wykonawcę lub producenta. Jeżeli dostęp do strony umożliwiającej pobranie oprogramowania wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników. W czasie trwania wsparcia technicznego Wykonawca musi zapewnić dostęp do aktualizacji i nowych wersji aplikacji klienckich, jak również zapewnić wsparcie dla samego oprogramowania klienckiego".

Wymaganie z pkt c) w świetle wymagań pkt e) i f) należy rozumieć w ten sposób, że w cenie oferty należy uwzględnić koszt licencji dla 30.000 użytkowników, jeżeli producent zaoferowanego urządzenia uzależnia liczbę użytkowników korzystających z połączenia VPN od wniesienia opłat licencyjnych. Zamawiający oczekuje (pkt f)) także wsparcia dla licencji dostępowym w całym okresie świadczenia wsparcia technicznego przez wykonawcę co podraża koszt oferty o ile dany producent nalicza opłaty za wsparcie w danym przypadku. Ponieważ polityka producentów urządzeń jest w tym zakresie różna i nie koresponduje
z oczekiwaniami zamawiającego w pkt 31 konieczne jest przeformułowanie przedmiotowego wymagania w sposób zapewniający identyczne warunki sporządzenia oferty przez wykonawców oferujących urządzenia różnych producentów (dowód: macierz porównawcza warunków dostępu producentów firewall - na okoliczność różnorodności typów i warunków dostępu VPN do firewall NGFW).

Odwołujący zwrócił uwagę na fakt, iż zamawiający oczekuje dostępu dla 30.000 użytkowników co jest wartością wielokrotnie przekraczającą liczbę personelu zamawiającego z uwzględnieniem współpracowników zamawiającego mogących uzyskać dostęp do systemów powiązanych z oferowanym rozwiązaniem. W efekcie wymagania pkt c), e) i f) prowadzą do preferowania rozwiązania Palo Alto z uwagi na brak opłat za dostęp VPN.

Wobec powyższego odwołujący wnosi o zmianę pkt 31 c) część Specyfikacja komponentu zabezpieczającego OPZ.

Zamawiający w odpowiedzi na odwołanie I podkreślił, że sposób interpretacji zapisów OPZ dokonany przez odwołującego jest całkowicie błędny, niezgodny z wymaganiami zamawiającego określonymi szczegółowo w przywołanych punktach 31 c), e) i f) OPZ, tym samym zarzut odwołującego należy uznać za całkowicie bezpodstawny. Zamawiający w pkt. 31 c) wymaga zapewnienia dla komponentu zabezpieczającego funkcjonalności zestawienia tuneli SSL VPN dla co najmniej 30 000 sesji użytkowników. Wymóg ten definiuje wydajność komponentu zabezpieczającego, której wartość podyktowana jest rzeczywistymi potrzebami zamawiającego, a wynikającymi z konieczności zapewnienia dostępu wszystkich stacji klienckich w tym samym czasie. Liczba stacji klienckich wynika z estymacji liczby tych stacji pracujących na infrastrukturze ACK Cyfronet AGH. Liczby tej nie determinuje jedynie liczba pracowników zamawiającego, ale również między innymi liczba osób prowadzących badania naukowe z wykorzystaniem infrastruktury ACK (superkomputery, z których korzystają naukowcy całej Polski). W pkt 31 e) zamawiający określa minimalną wymaganą przez zamawiającego charakterystykę techniczną ruchu VPN, która to charakterystyka w żaden sposób nie odnosi się do przywołanych przez odwołującego, a rzekomo wymaganych licencji. Pkt. f) wskazuje, że zamawiający wymaga, dla zapewnienia poprawności działania połączeń VPN, aby oferowane rozwiązanie zapewniało dostępność autoryzowanego oprogramowania umożliwiającego zestawienie połączenia VPN dla stacji klienckich (Aplikacje klienckie).

Z przywołanych zapisów OPZ wynika jednoznacznie, iż zamawiający nie wymaga dostarczenia przez wykonawców żadnych licencji w tym zakresie, czego potwierdzeniem jest treść pkt 33 g) „*Aplikacje klienckie instalowane na stacjach klienckich nie mogą wymagać dodatkowych licencji instalowanych na tych stacjach i muszą być udostępnione przez Wykonawcę lub producenta*".

Odwołujący za pismem procesowym z 18 września 2023 r. wskazał, iż stanowisko zamawiającego jest niekonsekwentne i jego przyjęcie wywoływałoby sprzeczność wewnętrzną w OPZ. Zamawiający w piśmie z dnia 14 września 2023 roku stwierdził „*Z przywołanych zapisów OPZ wynika jednoznacznie, iż Zamawiający nie wymaga dostarczenia przez Wykonawców żadnych licencji w tym zakresie, czego potwierdzeniem jest treść pkt 33 g)*

„Aplikacje klienckie instalowane na stacjach klienckich nie mogą wymagać dodatkowych licencji instalowanych na tych stacjach i muszą być udostępnione przez Wykonawcę lub producenta".

Jest to wypowiedź sprzeczna z treścią wymagań OPZ 31 ppkt d).

Ponieważ dostęp VPN może być realizowany na podstawie licencji darmowych lub płatnych (różniących się oferowanymi funkcjonalnościami) odwołujący oczekuje jednoznacznego określenia oczekiwań zamawiającego w tym zakresie bowiem ma to wpływ na wycenę oferty (konieczność uwzględnienia kosztu licencji dla 30.000 użytkowników i wsparcia).

Zamawiający w odpowiedzi na odwołanie II wskazał, iż podtrzymuje swoje dotychczasowe stanowisko i wyjaśnia, że nie ma sprzeczności we wskazanych zapisach OPZ. Dokumentacja zamówienia określa wyraźnie, iż oferowany system musi posiadać funkcjonalność zdalnych sesji VPN dla estymowanej liczby 30 000 użytkowników. W ramach tej liczby – dostęp dla wszystkich użytkowników musi być realizowany na tych samych zasadach, a zatem nie jak sugerował

odwołujący – z wyróżnieniem pewnej liczby użytkowników, dla których dostęp miałby być realizowany na innych zasadach. Jednocześnie zamawiający nie wymaga wsparcia producenckiego realizowanego bezpośrednio u każdego z użytkowników. Tym samym, zamawiający wyraźnie określa żądane funkcjonalności. Należy jednak zwrócić uwagę, że odwołujący nie potrafi określić wyraźnie jakiej funkcjonalności zamawiający rzekomo nie sprecyzował. Odwołujący ogranicza się do stwierdzenia, że nie wie, czy ma zastosować licencje darmowe, czy płatne, co wskazuje na model rynkowy, a nie na konkretne parametry funkcjonalności.

Krajowa Izba Odwoławcza odnosząc się do ww. zarzutów odwołania (łącznie 2 i 4),
w całości podziela stanowisko prezentowane przez zamawiającego uznając je za własne.
W związku z tym, iż stanowisko to zostało już powołane powyżej, Izba stwierdziła, że nie ma potrzeby powielania go w dalszej części uzasadnienia. Ponadto, Izba stwierdziła,
co następuje.

W ocenie Izby zarzuty odwołania są bezzasadne, albowiem zamawiający opisał przedmiot zamówienia w sposób, który gwarantuje spełnienie jego uzasadnionych potrzeb. Zamawiający jako gospodarz postępowania, w granicach przepisów prawa, opisuje przedmiot zamówienia w sposób, który zagwarantuje spełnienie jego uzasadnionych potrzeb, nawet gdyby powodowało to, że nie wszystkie produkty występujące na rynku w danej branży będą w stanie spełnić wymogi wynikające z tego opisu. W sytuacji, gdy opis przedmiotu zamówienia jest podyktowany uzasadnionymi potrzebami zamawiającego, a nie zamiarem faworyzowania konkretnego wykonawcy i dyskryminowania innych wykonawców, nie jest możliwe skuteczne ingerowanie w określony przez zamawiającego opis przedmiotu zamówienia (vide: wyrok Krajowej Izby Odwoławczej z dnia 28 marca 2023 r., sygn. akt KIO 704/23).

Zamawiający wskazał, że jest wiodącym w Polsce Centrum Superkomputerowym
i sieciowym. W ramach swojej infrastruktury informatycznej zamawiający udostępniania moc obliczeniową i infrastrukturę teleinformatyczną oraz świadczy inne usługi informatyczne wyższym uczelniom, podmiotom realizującym badania naukowe oraz innym jednostkom edukacyjnym. Akademickie Centrum Komputerowe Cyfronet AGH od kilkunastu lat w swoich zasobach posiada najszybsze superkomputery w Polsce. W obecnej edycji listy TOP500 (https://top500.org) najszybszych superkomputerów świata z Polski są jedynie 3 z tego
1. (Athena-poz. 123) i 3.(Ares- poz. 362) znajdują się u zamawiającego. W chwili obecnej zamawiający przygotowuje się do montażu najnowszego superkomputera o mocy obliczeniowej wielokrotnie większej od posiadanych obecnie. Nastąpi to w ciągu kilku tygodni. Trwa również dostawa urządzeń do modernizacji miejskiej sieci komputerowej do standardu 400/100GE. Zakup objęty przedmiotem zamówienia ma pozwolić na skuteczną ochronę całej opisanej powyżej infrastruktury teleinformatycznej zamawiającego, w tym również tej będącej w fazie instalacji, przed zagrożeniami dla systemów informatycznych powodowanymi postępującą transformacją cyfrową, wzrostem zainteresowania pracą zdalną oraz wzrastającą aktywnością różnych grup przestępczych (cyberbezpieczeństwo).

Ocena uzasadnionych potrzeb zamawiającego w kontekście przedmiotu zamówienia musi być dokonywana przy uwzględnieniu opisanych powyżej okoliczności wskazujących na skalę działalności zamawiającego oraz zakres usług, które są i będą oferowane w oparciu
o przedmiot zamówienia. W szczególności należy w tym miejscu podkreślić, że infrastruktura zamawiającego estymowana jest dla około 30 000 użytkowników. Skalę uzasadnionych potrzeb zamawiającego determinuje również fakt, że zamawiający świadczy część usług jako operator publicznej sieci telekomunikacyjnej w rozumieniu Prawa telekomunikacyjnego, a tym samym, zobowiązany jest do spełniania szczególnych wymogów w zakresie bezpieczeństwa zgodnie z ustawą Prawo telekomunikacyjne z dnia 16 lipca 2004 r. (tj. Dz.U. z 2022 r. poz. 1648), dalej jako „Prawo telekomunikacyjne".

Zgodnie z art. 175 ust. 1 ustawy Prawo telekomunikacyjne, dostawca publicznie dostępnych usług telekomunikacyjnych, a jeżeli jest to konieczne – także operator publicznej sieci telekomunikacyjnej, są obowiązani podjąć środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów
w związku ze świadczonymi usługami. Podjęte środki powinny zapewniać poziom bezpieczeństwa odpowiedni do stopnia ryzyka, przy uwzględnieniu najnowocześniejszych osiągnięć technicznych oraz kosztów wprowadzenia tych środków.

Przepis art. 99 ust. 4 ustawy Pzp, stanowi, iż przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję, w szczególności przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów.

Jak wskazuje się w doktrynie (Prawo zamówień publicznych – Komentarz, pod redakcją
H. Nowaka, M. Winiarza, wydanie II, Warszawa 2023), opis przedmiotu zamówienia odpowiadać powinien uzasadnionym i rzeczywistym potrzebom zakupowym zamawiającego związanym z realizacją przypisanych mu zadań. Sporządzając

opis przedmiotu zamówienia, zamawiający powinien mieć na uwadze zasady udzielania zamówień publicznych, w tym zasadę proporcjonalności wyrażoną w art. 16 pkt 3 i 99 ust. 2 Pzp oraz zasadę efektywności wyrażoną w art. 17 ust. 1 Pzp. Niedopuszczalne jest zatem w świetle art. 99 ust. 4 Pzp zaburzenie konkurencji pomiędzy wykonawcami, mające swoją genezę w przygotowanym opisie przedmiotu zamówienia, polegające albo na preferencji w opisie konkretnego wykonawcy lub produktu, albo na niemającym uzasadnieniu wyeliminowaniu wykonawcy lub produktu. Poprzez niedopuszczalne preferowanie należy rozumieć wszystkie zabiegi, przy użyciu dowolnych sposobów opisu przedmiotu zamówienia, które w sposób nieuzasadniony preferują lub wprost wskazują na konkretnego wykonawcę lub konkretny produkt. Skutkiem takiego zapisu jest niemożność złożenia oferty zgodnej z tak sformułowanym opisem przedmiotu zamówienia przez wykonawcę innego niż preferowany lub zaproponowania innego niż preferowany produkt. Zapisami eliminującymi określone produkty (i określonych wykonawców) będą zaś takie, które w sposób inny niż odpowiadający zobiektywizowanym
i rzeczywistym potrzebom zakupowym zamawiającego związanym z realizacją przypisanych mu zadań, prowadzą do niemożności złożenia oferty przez określone grupy wykonawców
(i zaproponowania określonych grup produktów).

Przyjmując powyższe twierdzenia za prawidłowe, przedkładając na stan faktyczny przedmiotowej sprawy Izba stwierdziła, że zamawiający nie dopuścił się naruszenia przepisów wskazywanych przez odwołującego, tj. art. 16 pkt 1 i 3 w zw. z art. 99 ust. 1 i 4 ustawy Pzp.

Zamawiający dokonując opisu przedmiotu zamówienia, kierował się uzasadnionymi potrzebami, ale również możliwościami organizacyjno-technicznymi oraz zasobem sprzętowym, jaki już posiada.

Ponadto Izba stwierdziła, że opis przedmiotu zamówienia dokonany przez zamawiającego nie ogranicza konkurencji w sposób dyskryminujący wykonawców, którzy mogą zaoferować rozwiązanie równoważne rozwiązaniu przyjętemu przez zamawiającego. Specyfika tzw. przetargów informatycznych, charakteryzuje się bowiem dużą różnorodnością opcji, dedykowanych konkretnym projektom. Okoliczność, iż sposób osiągnięcia zamierzonego przez zamawiającego celu determinuje zaproponowanie przez wykonawców znanych
i dostępnym im rozwiązań w inny sposób niż to, które opisał w dokumentach zamówienia zamawiający nie oznacza jeszcze, że zamawiający dopuścił się naruszenia zasad opisanych przez Ustawodawcę w art. 16 pkt 1 i 3 ustawy Pzp.

Opis przedmiotu zamówienia jest sformułowany w taki sposób, iż dopuszcza różne sposoby realizacji oczekiwanej i pożądanej funkcji. Opis funkcji jest w kilku miejscach wręcz bardzo ogólny, co zresztą zauważa sam odwołujący w swoim stanowisku. Zamawiający określił
w swoich wymaganiach, że dopuszcza inne rozwiązania, ale wymaga dostarczenia „*opisu współpracy proponowanej integracji z dostarczanymi funkcjami bezpieczeństwa (…)*".

Co istotne, z punktu widzenia przedmiotowej sprawy, odwołujący nie twierdził, że nie może zaoferować rozwiązania opisanego przez zamawiającego jako wzorcowe. Podnosił jedynie, że rozwiązanie odwołującego może być dużo droższe, powołując w tym zakresie odpowiednie dowody (e-mail). Jednakże w ocenie Izby fakt, iż rozwiązanie preferowane przez odwołującego będzie rozwiązaniem droższym nie oznacza, że postępowanie prowadzone jest z naruszeniem zasady uczciwej konkurencji oraz równego traktowania wykonawców i jest prowadzone
w sposób nieproporcjonalny.

Dynamika rynku informatycznego, kontakty handlowe, dedykowane określonym wykonawcom warunki współpracy z producentami określonych rozwiązań dają bowiem duże pole do ustalania cen produktów na poziomie konkurencyjnym.

Zdaniem Izby, opis przedmiotu zamówienia ustanowiony przez zamawiający
w przedmiotowym postępowaniu nie wyłącza jego konkurencyjności, a uzasadnione potrzeby zamawiającego mierzone przez pryzmat jego możliwości technicznych tłumaczą niezasadność podnoszonych zarzutów odwołania.

Nadto, argumentacja odwołującego ukierunkowana na sposób oceny zaproponowanych przez wykonawców rozwiązań zdaje się wykluczać wiedzę i znajomość przedmiotu rzeczy przez zamawiającego. Zamawiający znając bowiem rozwiązania dostępne na rynku jest
w posiadaniu wiedzy, a co za tym idzie świadomy jest możliwości oceny zaproponowanych mu, na etapie składania ofert, rozwiązań. Zamawiający jako gospodarz postępowania ustala takie warunki oceny, które dadzą mu pewność, iż wybrane rozwiązanie techniczne spełni jego wszystkie oczekiwania.

Biorąc pod uwagę powyższe, orzeczono jak w sentencji.

O kosztach postępowania orzeczono stosownie do wyniku sprawy na podstawie art. 575 ustawy Pzp oraz § 8 ust. 2 pkt 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 wysokości wpisu od odwołania (Dz. U. poz. 2437), uwzględniając koszty poniesione przez zamawiającego, tytułem dojazdu na posiedzenie i rozprawę (15 oraz 21 września 2023 r.) w kwocie 997,10 zł oraz wynagrodzenia pełnomocnika w kwocie 3 600,00 zł.

Przewodniczący:……