

Sygn. akt: KIO 3390/24

WYROK

Warszawa, dnia 15 października 2024 r.

Krajowa Izba Odwoławcza – w składzie:

Przewodniczący:

Monika Szymanowska

Protokolant:

Aldona Karpińska

po rozpoznaniu na rozprawie w dniu 10 października 2024 r. odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 16 września 2024 r. przez odwołującego Innergo Systems Sp. z o.o. w Warszawie w postępowaniu prowadzonym przez zamawiającego Komendę Główną Państwowej Straży Pożarnej w Warszawie przy udziale uczestnika po stronie zamawiającego A. K. prowadzącego działalność gospodarczą pod firmą Sieciowe Systemy Informatyczne A. K. w Oławie

orzeka:

1. umarza postępowanie odwoławcze w zakresie zarzutu dotyczącego naruszenia

art. 99 ust. 1-6 oraz art. 16 pkt 1-3 p.z.p. z pkt III ppkt: 1, 4, 7, 11, 15, 17, 18 petitum odwołania,

2. częściowo uwzględnia odwołanie i nakazuje zamawiającemu modyfikację

dokumentacji postępowania poprzez:

- 2.1. podanie kryteriów równoważności dla dostawy rozwiązania innego niż funkcjonujące u zamawiającego poprzez określenie wymaganych parametrów technicznych i funkcjonalnych lub poprzez określenie, że w przypadku dostawy rozwiązania innego niż funkcjonujące u zamawiającego, wykonawca musi

dostarczyć równoważne rozwiązanie oparte na urządzeniach spełniających wymagania określone w postępowaniu dla urządzeń typ 4 (końcowy węzeł komunikacyjny) (pkt III ppkt 2),

- 2.2. zmianę pkt 2.1 ppkt 25 OPZ poprzez dopuszczenie, aby usługa sandbox realizowana była w formie maszyny wirtualnej lub w formie minimum dwóch centralnych urządzeń, w różnych lokalizacjach, typu sandbox na poziomie Komendy Głównej PSP na potrzeby całej sieci zamawiającego (pkt III ppkt 5),

- 2.3 dopuszczenie zaoferowania dowolnej architektury systemów wirtualnych realizujących wymagane funkcjonalności w ramach oferowanego systemu i realizację funkcjonalności, o których mowa w pkt 1 ppkt 20, pkt 1 ppkt 22 i 23 oraz w pkt 2.1 ppkt 2, pkt 2.2 ppkt 2, pkt 2.3 ppkt 2, pkt 2.4 ppkt 2 oraz pkt 2.5 ppkt 2 OPZ z poziomu systemu zarządzania (pkt III ppkt

6), tj. w szczególności:

- a. usunięcie wymagań pkt 1 ppkt 20, pkt 1 ppkt 22 i 23 oraz w pkt 2.1 ppkt

- 2, pkt 2.2 ppkt 2, pkt 2.3 ppkt 2, pkt 2.4 ppkt 2 oraz pkt 2.5 ppkt 2 OPZ, gdyż funkcjonalności są wystarczająco zapewnione w ramach wymagań pkt 3 OPZ „System Centralnego Zarządzania i Monitorowania NG Firewall i SD-WAN”,

- b. dopuszczenie, aby System Centralnego Zarządzania i Monitorowania

mógł być zrealizowany za pomocą jednej lub więcej niż jednej dedykowanej maszyny wirtualnej, zachowując wysoki poziom integracji takich maszyn wirtualnych za pomocą natywnych dla danego producenta mechanizmów integracyjnych,

2.4. usunięcie wymogu pasywnego chłodzenia (budowa bez użycia wentylatorów) dla urządzeń typ nr 3, 4 i 5, tj. wymagań pkt 2.3 ppkt 9, pkt 2.4 ppkt 9, pkt 2.5 ppkt 9 OPZ (pkt III ppkt 10),

2.5. zmianę wymagania pkt 2.1 ppkt 19 OPZ poprzez wykreślenie wymagania konkretnych kategorii dla określonych typów zagrożeń i dopuszczenie innej kategoryzacji URL, tj. nadanie wymaganiu brzmienia: „wymagane jest posiadanie oddzielnych kategorii URL.” (pkt III ppkt 12),

2.6. usunięcie wymagania pkt 2.1 ppkt 20 OPZ (wymagany sposób określenia ryzyka przypisanego URL) (pkt III ppkt 13),

2.7. w zakresie kryteriów oceny ofert (pkt III ppkt 19):

a. zmniejszenie wagi kryteriów: KPml - Blokowanie zagrożeń

z wykorzystaniem algorytmów uczenia maszynowego, aktualizowanych dynamicznie przez producenta i KPas - Możliwość sprawdzania wpływu nowo pobranych aktualizacji sygnatur wykrywających aplikacje (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – dla każdego z ww. z 15 punktów do 7,5 punktów,

b. zmianę kryterium KPkk - Posiadanie konceptu konfiguracji kandydackiej

na poziomie API, GUI oraz CLI na „KPkk-Posiadanie konceptu konfiguracji kandydackiej na poziomie systemu centralnego zarządzania - waga 30 punktów” wraz z uszczegółowieniem kiedy kryterium zostanie spełnione,

oraz odpowiednie dostosowanie pozostałych postanowień ogłoszenia i SWZ, w tym wzorów do liczenia punktacji w kryteriach oceny ofert,

3. w pozostałym zakresie oddała odwołanie,

4. kosztami postępowania odwoławczego w części 1/2 obciąża zamawiającego

Komendę Główną Państwowej Straży Pożarnej w Warszawie oraz w części 1/2 obciąża odwołującego Innergo Systems Sp. z o.o. w Warszawie i:

4.1. zalicza na poczet kosztów postępowania kwotę 22 200,00 zł (dwadzieścia dwa tysiące dwieście złotych) stanowiącą uiszczony wpis od odwołania i uzasadnione koszty stron postępowania odwoławczego,

4.2. zasądza od zamawiającego Komendy Głównej Państwowej Straży Pożarnej w Warszawie na rzecz odwołującego Innergo Systems Sp. z o.o. w Warszawie kwotę 11 100,00 zł (jedenaście tysięcy sto złotych) tytułem zwrotu części kosztów postępowania odwoławczego.

Na orzeczenie – w terminie 14 dni od dnia jego doręczenia – przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Warszawie -Sądu Zamówień Publicznych.

Przewodniczący:

Sygn. akt: KIO 3390/24

Uzasadnienie

Zamawiający – Komenda Główna Państwowej Straży Pożarnej ul. Podchorążych 38, 00-463 Warszawa, prowadzi postępowanie o udzielenie zamówienia publicznego pn. „Dostawa urządzeń infrastruktury sieci SD-WAN dla platformy chmurowej integracji danych Komendy Głównej Państwowej Straży Pożarnej”, o ogłoszeniu o zamówieniu opublikowanym w dniu 4 września 2024 r. w Dzienniku Urzędowym Unii Europejskiej pod numerem 172/2024 529292-2024, dalej zwane „postępowaniem”.

Postępowanie na dostawę, o wartości powyżej kwoty określonej w przepisach wydanych na podstawie art. 3 ust. 3 ustawy z dnia 11 września 2019. Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320) dalej zwanej „p.z.p.”, jest prowadzone przez zamawiającego w trybie przetargu nieograniczonego.

W dniu 16 września 2024 r. odwołanie wobec treści dokumentacji postępowania wniósł wykonawca Innergo Systems Sp. z o.o. ul. św. Jacka Odrowąża 15, 03-310

Warszawa (dalej zwany „odwołującym”). We wniesionym środku zaskarżenia odwołujący postawił zamawiającemu następujące zarzuty naruszenia (pisownia oryginalna):

- art. 99 ust. 1, 2, 4 oraz ust. 5 i 6 oraz art. 16 pkt 1, 2 i 3 Pzp przez opisanie przedmiotu zamówienia w sposób niejednoznaczny, nieuwzględniający wszystkich okoliczności koniecznych dla sporządzenia oferty, a także nieproporcjonalny do przedmiotu zamówienia i nieuzasadniony obiektywnymi potrzebami Zamawiającego, a zarazem ograniczający konkurencję i naruszający zasady proporcjonalności, przejrzystości, równego traktowania wykonawców i uczciwej konkurencji oraz określenie kryteriów równoważności w sposób wyłącznie pozornie dopuszczający możliwość zaoferowania rozwiązań równoważnych i naruszający zasady uczciwej konkurencji i równego traktowania wykonawców, w zakresie w jakim:

1. w przypadku dostawy rozwiązania innego niż funkcjonujące u Zamawiającego,

wymagana jest wymiana urządzeń posiadanych przez Zamawiającego wraz z zapewnieniem serwisu gwarancyjnego oraz wsparcia i pakietu subskrypcji na okres 60 miesięcy (str. 4 OPZ), podczas gdy aktualnie posiadane przez Zamawiającego rozwiązanie posiada aktualnie krótszy okres wsparcia i subskrypcji licencji;

2. Zamawiający nie określił poprawnie kryteriów równoważności w przypadku dostawy

rozwiązania innego niż funkcjonujące u Zamawiającego (str. 4-5 OPZ), tj. nie podał wymagań technicznych ani funkcjonalnych, co uniemożliwia precyzyjne ustalenie wymagań oczekiwanych dla rozwiązania równoważnego i powoduje pozorność dopuszczonej równoważności;

3. W pkt 1 OPZ „Ogólne wymagania na sprzęt i oprogramowanie urządzeń brzegowych

typu NG Firewall”, ppkt 46 oraz 48 lit. a., określił, że jeżeli oprogramowania klienta Remote Access VPN dla laptopów z systemem klienckim Windows wymaga licencji – należy dostarczyć licencję na maksymalną wydajność oraz maksymalną wspieraną ilość dla oferowanego modelu urządzeń, podczas gdy jest to wymaganie nadmierne i nieuzasadnione potrzebami Zamawiającego, a do tego powoduje niezasadne preferowanie rozwiązania określonego producenta;

4. Zamawiający określił wymagania dotyczące funkcjonalności zdalnego dostępu

w sposób niejasny i nie pozwalający na jednoznaczne ustalenie oczekiwanego rozwiązania poprzez określanie nakładających się wymagań dotyczących zdalnego dostępu oraz różnicowanie funkcjonalności w nieuzasadniony sposób, a także w sposób nadmierny, nie uwzględniający odmiennych sposobów licencjonowania niż stosowane w preferowanym rozwiązaniu oraz powodujący oderwane od obiektywnych potrzeb preferowanie rozwiązania określonego producenta (co dotyczy w szczególności wymagań dla urządzeń typu nr 3, wymagań ogólnych pkt 1 ppkt 4648 OPZ oraz pkt 2.1 ppkt 29 i 2.3 ppkt 10 OPZ);

5. W pkt 2.1 OPZ „Wymagania dodatkowe dla urządzeń Typ nr 1 – 4 sztuki (2 pary HA)”

ppkt 25, wymagane jest, aby zewnętrzny Sandbox producenta był zlokalizowany w Polsce, podczas gdy jest to wymaganie nadmierne i nieuzasadnione potrzebami Zamawiającego, a do tego powoduje niezasadne preferowanie rozwiązania określonego producenta, zaś alternatywne wymaganie w przypadku braku dostępności polskiej lokalizacji takiego systemu jest tylko pozornie równoważne;

6. Zamawiający wymaga, aby funkcjonalności opisane w pkt 1 ppkt 20, pkt 1 ppkt

22 i 23 oraz w pkt 2.1 ppkt 2, pkt 2.2 ppkt 2, pkt 2.3 ppkt 2, pkt 2.4 ppkt 2 oraz pkt 2.5 ppkt 2 – realizowane były jako funkcjonalności dostępne na poziomie urządzeń, podczas gdy mając na uwadze całość opisu przedmiotu zamówienia, nie jest to uzasadnione i prowadzi do preferencyjnego traktowania rozwiązania określonego producenta;

7. W pkt 2.1 dla urządzeń Typ nr 1 wymagane jest (pkt 1 lit. a i c.): minimum 12 portów

Ethernet RJ45 wspierających 10G/5G/2.5G/1GE/100Mbps oraz 4 porty Ethernet SFP28, podczas gdy jest to wymaganie nadmierne i nieuzasadnione potrzebami Zamawiającego, a do tego powoduje niezasadne preferowanie rozwiązania określonego producenta;

8. W pkt 2.2 OPZ dla urządzeń Typ nr 2 wymagane jest (pkt 1 lit. a i b.): minimum

4 portów Ethernet RJ45 wspierających 1GE/100Mbps oraz minimum 8 portów Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps, podczas gdy jest to

wymaganie nadmierne i nieuzasadnione potrzebami Zamawiającego, a do tego powoduje niezasadne preferowanie rozwiązania określonego producenta;

9. Dla urządzeń Typ 1-5 (pkt 2.1 ppkt 4 lit. g. oraz pkt. 2.2 ppkt 3 lit. g, pkt 2.3 ppkt

3 lit. g., pkt 2.4 ppkt 3 lit. g., pkt 2.5 ppkt 3 lit. g. OPZ), określono zbyt wysokie parametry liczby sąsiedztw IKE, co jest nadmierne i nieuzasadnione potrzebami Zamawiającego, a do tego powoduje niezasadne preferowanie rozwiązania określonego producenta;

10. Dla urządzeń Typ nr 3, 4 i 5 (pkt 2.3 ppkt 9, pkt 2.4 ppkt 9, pkt 2.5 ppkt 9 OPZ) wymagany jest brak użycia wentylatorów (fan-less desing lub inaczej: funkcjonalność pasywnego chłodzenia), podczas gdy jest to wymaganie nadmierne i nieuzasadnione potrzebami Zamawiającego, a do tego powoduje niezasadne preferowanie rozwiązania określonego producenta;

11. W pkt 1 ppkt 30 OPZ wymagana jest obsługa formatu BSD, podczas gdy brak jest obiektywnego uzasadnienia dla takiego wymagania;

12. W pkt 2.1 ppkt 19 OPZ wymagane jest posiadanie oddzielnych kategorii URL dla poszczególnych

wymienionych typów zagrożeń, co jest wymaganiem nadmiernym i wskazującym na rozwiązanie jednego producenta;

13. W pkt 2.1 ppkt 20 OPZ wymagane jest określenie ryzyka przypisanego URL w określony sposób (co najmniej wysokie/średnie/niskie), co jest wymaganiem nadmiernym i wskazującym na rozwiązanie jednego producenta;

14. W pkt 2.1 ppkt 22 OPZ wymagane jest zapewnienie obsługi plików PKG na MacOS, co jest wymaganiem nadmiernym i wskazującym na rozwiązanie jednego producenta;

15. W pkt 3 ppkt 2 OPZ wymagany jest jeden centralny, zunifikowany system zarządzania, logowania i raportowania, co jest wymaganiem w sposób nieuzasadniony ograniczającym konkurencję;

16. W pkt 3 ppkt 3 OPZ wymaga się, aby system umożliwiał zarządzanie co najmniej 1000 urządzeń NG Firewall sprzętowymi, co jest wymaganiem nadmiernym i niezasadnie ograniczającym konkurencję;

17. Wymaganie pkt 3 ppkt 4 OPZ jest niejasne i niejednoznaczne w zakresie, w jakim określa, że „W tym celu moduły odpowiedzialne za zbieranie logów muszą zostać zrealizowane z wykorzystaniem protokołu konsensusu posiadającego mocne gwarancje spójności (tzw. consensus protocol). Każdy z węzłów musi obsługiwać przestrzeń dyskową o pojemności nie mniejszej niż 22 TB oraz minimum 20 000 logów na sekundę.”, jak również prowadzi do nieuzasadnionego ograniczenia możliwych do zaoferowania rozwiązań;

18. W pkt 3 ppkt 12 OPZ wymagane jest tworzenie dynamicznych raportów w czasie rzeczywistym dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-

down”, co w sposób niezasadny ogranicza konkurencyjność postępowania i wskazuje na rozwiązanie jednego producenta

- art. 239 ust. 2 i art. 16 pkt 1-3 Pzp przez ustanowienie kryteriów oceny ofert, które z naruszeniem zasad uczciwej konkurencji, równego traktowania wykonawców i zasady przejrzystości, preferują rozwiązania jednego producenta, uniemożliwiając złożenie ofert opartych o rozwiązania konkurencyjnych producentów i powodują praktyczną niemożliwość złożenia oferty konkurencyjnej i uzyskania zamówienia, ze względu na przyjęte proporcje kryteriów preferujących jednego producenta a kryteriów pozostałych – w zakresie kryteriów oceny ofert określonych w rozdz. XII pkt 2, 3 i 5 SWZ.

Wobec powyższego odwołujący wniósł o uwzględnienie odwołania oraz nakazanie zamawiającemu „dokonania zmiany warunków zamówienia, w sposób uwzględniający argumentację odwołania zawarta w uzasadnieniu, tj.:

1. Określenia okresu zapewnienia wsparcia i pakietu subskrypcji urządzeń posiadanych

u Zamawiającego, wymaganego w przypadku dostawy rozwiązania innego niż funkcjonujące u Zamawiającego, jako obowiązujących do tej samej daty, do której obowiązują okresy wsparcia i subskrypcji, którymi obecnie dysponuje Zamawiający dla posiadanego rozwiązania;

2. Podania kryteriów równoważności dla dostawy rozwiązania innego niż funkcjonujące

u Zamawiającego poprzez określenie wymaganych parametrów technicznych i funkcjonalnych lub poprzez określenie, że w przypadku dostawy rozwiązania innego niż funkcjonujące u Zamawiającego, Wykonawca musi dostarczyć równoważne rozwiązanie oparte na urządzeniach spełniających wymagania określone w Postępowaniu dla urządzeń typ 4 (Końcowy Węzeł Komunikacyjny);

3. Zmianę OPZ w pkt 1 ppkt 46 poprzez określenie rzeczywistej i realnej

(odpowiadającej obiektywnym potrzebom Zamawiającego) liczby użytkowników, dla których ma zostać zapewniony dostęp zdalny, tj. pomiędzy 2000 a 5000 użytkowników;

4. Zmianę OPZ poprzez określenie spójnych wymagań dotyczących funkcjonalności

zdalnego dostępu, odpowiadających realnym potrzebom Zamawiającego i jednolitych dla całego systemu oraz doprecyzowanie opisu przedmiotu zamówienia umożliwiając realne zaoferowanie rozwiązań innych niż preferowanego producenta poprzez

a. Określenie czy połączenia mają być skoncentrowane do urządzeń Typ nr 3 (czyli Węzły VPN), a jeśli nie – to wskazanie takich urządzeń, dla których ma być zapewniony dostęp zdalny, dla których jest to uzasadnione;

b. Określenie spójnych wymagań dla funkcjonalności zdalnego dostępu do systemu dla użytkowników zdalnych, bez różnicowania poziomu tej funkcjonalności dla różnych urządzeń;

c. Zapewnienie równego traktowania Wykonawców oferujących rozwiązania o różnym modelu licencjonowania;

przykładowo poprzez zastąpienie dotychczasowym wymagań dotyczących zdalnego dostępu zawartych w treści OPZ, spójnie określonym dla całego systemu wymaganiem, zgodnie, z którym: „Urządzenia Firewall będą wspierały możliwość podłączenia się do sieci SD-WAN dla użytkowników zdalnych. Urządzenia Typ nr 3 są przewidziane do obsługi połączeń

zdalnych Remote VPN dla 3000 użytkowników zdalnych jednocześnie w całym systemie. Funkcjonalność Remote VPN będzie jednolita dla całej sieci i będzie dostarczała funkcjonalności takich, jak określone w pkt 2.3 („Wymagania dodatkowe dla urządzeń Typ nr 3”) ppkt 10 lit. a-g. OPZ”.

5. Zmiany OPZ w pkt 2.1 ppkt 25 poprzez określenie, że wymagane jest, aby „zewnętrzny Sandbox producenta był zlokalizowany na terenie Unii Europejskiej”;

6. Dopuszczenia zaoferowania dowolnej architektury systemów wirtualnych realizujących wymagane funkcjonalności w ramach oferowanego systemu i realizacji funkcjonalności, o których mowa w pkt 1 ppkt 20, pkt 1 ppkt 22 i 23 oraz w pkt 2.1 ppkt 2, pkt 2.2 ppkt 2, pkt 2.3 ppkt 2, pkt 2.4 ppkt 2 oraz pkt 2.5 ppkt 2 OPZ z poziomu systemu zarządzania, tj. w szczególności:

a. usunięcia wymagań pkt 1 ppkt 20, pkt 1 ppkt 22 i 23 oraz w pkt 2.1 ppkt 2, pkt 2.2 ppkt 2, pkt 2.3 ppkt 2, pkt 2.4 ppkt 2 oraz pkt 2.5 ppkt 2 OPZ, gdyż funkcjonalności są wystarczająco zapewnione w ramach wymagań pkt 3 OPZ „System Centralnego Zarządzania i Monitorowania NG Firewall i SD-WAN”;

b. dopuszczenia, aby System Centralnego Zarządzania i Monitorowania mógł być zrealizowany za pomocą jednej lub więcej niż jednej dedykowanej maszyny wirtualnej, zachowując wysoki poziom integracji takich maszyn wirtualnych za pomocą natywnych dla danego producenta mechanizmów integracyjnych.

7. Usunięcie (pkt 2.1 ppkt 1 lit. a i c. OPZ) wymagania posiadania przez urządzenia

Typu nr 1: minimum 12 portów Ethernet RJ45 wspierających

10G/5G/2.5G/1GE/100Mbps oraz 4 portów Ethernet SFP28;

8. Usunięcie (pkt 2.2. ppkt 1, lit. a. i b. OPZ) wymagania posiadania przez urządzenia

Typu nr 2: minimum 4 portów Ethernet RJ45 wspierających 1GE/100Mbps oraz minimum 8 portów Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps;

9. Określenie wymagań dla parametru liczby sąsiedztw IKE dla urządzeń Typ nr 1-5

w sposób realnie odzwierciedlający potrzeby Zamawiającego opisane w warunkach zamówienia, tj. zmiana parametru dla każdego z typów urządzeń do wartości 1000 sąsiedztw IKE (IPSec);

10. Usunięcia wymogu pasywnego chłodzenia (budowa bez użycia wentylatorów) dla urządzeń Typ nr 3,4 i 5, tj. wymagań pkt 2.3 ppkt 9, pkt 2.4 ppkt 9, pkt 2.5 ppkt 9 OPZ;

11. Usunięcie wymogu obsługi formatu BSD (pkt 1 ppkt 30 OPZ) lub modyfikację na „obsługę formatu Syslog”;

12. Usunięcie wymagania pkt 2.1 ppkt 19 OPZ (oddzielne kategorie URL dla wymienionych typów zagrożeń);

13. Usunięcie wymagania pkt 2.1 ppkt 20 OPZ (wymagany sposób określenia ryzyka przypisanego URL);

14. Usunięcie z wymagania pkt 2.1 ppkt 22 OPZ wymogu obsługi plików typu PKG dla MacOS;

15. Modyfikacja pkt 3 ppkt 2 OPZ w sposób dopuszczający, aby system zarządzania (NMS) oraz system logowania mogły być zrealizowane jako dwie osobne maszyny wirtualne, które ściśle współpracują ze sobą za pomocą natywnych mechanizmów producenta rozwiązania;

16. Modyfikacja pkt 3 ppkt 3 OPZ poprzez doprecyzowanie, że na dzień dostawy system ma umożliwiać podłączenie 572 urządzeń NG Firewall oraz posiadać możliwość rozbudowy do co najmniej 1000 podłączonych urządzeń w przyszłości;

17. Modyfikacja pkt 3 ppkt 4 OPZ poprzez usunięcie wymagania dostarczenia więcej niż jednego modułu odpowiedzialnego za zbieranie i dopuszczenie swobodnego doboru architektury rozwiązania przez Wykonawców oraz doprecyzowanie wymagania poprzez określenie oczekiwanej pojemności systemu logowania i raportowania (dla całego systemu);

18. Modyfikacja pkt 3 ppkt 12 OPZ poprzez wprowadzenie opisu funkcjonalnego i umożliwienie realizacji funkcjonalności w dobrany przez Wykonawcę sposób, np. za pomocą interaktywnego interfejsu/dashboard, tj. nadanie wymaganiu w pkt 3 ppkt 12 OPZ brzmienia: „Zamawiający wymaga, aby system miał możliwość analizy danych z funkcjonalnością „drill-down” (pozyskiwania coraz większej ilości informacji o danym zdarzeniu).”;

19. Modyfikacja kryteriów pozacenowych oceny ofert poprzez wykreślenie kryteriów (rozdział XII pkt 2 i 5 SWZ):

a. KPml - Blokowanie zagrożeń z wykorzystaniem algorytmów uczenia maszynowego, aktualizowanych dynamicznie przez producenta.

- b. KPas - Możliwość sprawdzania wpływu nowo pobranych aktualizacji sygnatur wykrywających aplikacje (przed ich zatwierdzeniem na urzędzeniu) na istniejące polityki bezpieczeństwa.

oraz modyfikację kryteriów oraz wagi im przypisanych (rozdział XII pkt 3 i 4 SWZ) w następujący sposób:

- c. KPkk-Posiadanie konceptu konfiguracji kandydackiej na poziomie systemu centralnego zarządzania - 30%
- d. KPg-Obecność producenta oferowanego rozwiązania w najnowszym rynkowym

raporcie „Gartner Magic Quadrant for SD-WAN” w części (tzw. Ćwiartce) „Leaders” – 20%

oraz odpowiednie dostosowanie pozostałych postanowień ogłoszenia i SWZ, w tym wzorów do liczenia punktacji.”

W uzasadnieniu środka zaskarżenia odwołujący wskazał co następuje. Zamawiający prowadzi postępowanie na zakup i wdrożenie urządzeń, które mają służyć do zbudowania spójnego i zintegrowanego systemu komunikacyjnego dla Państwowej Straży Pożarnej na terenie całego kraju. W ramach zamówienia, oczekiwana jest dostawa i wyposażenie 553 lokalizacji PSP w urządzenia w ilości 605 sieci SD-WAN w celu stworzenia systemu opartego na technologii SD-WAN. Mimo, że pozornie opis przedmiotu nie zawiera wskazania na konkretnego producenta oczekiwanego rozwiązania, to w rzeczywistości szereg postanowień Załącznika nr 1 do SWZ (OPZ) preferuje rozwiązania producenta Palo Alto do tego stopnia, że zestawienie wszystkich wymagań OPZ powoduje, że nie jest możliwe zaoferowanie rozwiązań innego producenta z realną szansą na uzyskanie zamówienia. Przy czym, wymagania te dotyczą różnych aspektów przedmiotu zamówienia, a nawet jeśli teoretycznie zamawiający dopuszcza zastosowanie wymagań alternatywnych, to są one opisane w sposób nadmierny, powodujący konieczność zaoferowania rozwiązania przewymiarowanego, o zdecydowanie wyższym koszcie, przez co oferta taka nie ma realnych szans na uzyskanie zamówienia. Powoduje to pozornie przewidzianych w opisie przedmiotu zamówienia postanowień dopuszczających rozwiązania równoważne, podczas gdy faktycznie – mając na uwadze całość OPZ – nie jest możliwe zaoferowanie rozwiązań konkurencyjnych do produktów Palo Alto.

Dodatkowo, opis przedmiotu zamówienia został sformułowany nie w oparciu o potrzeby zamawiającego i wymagania funkcjonalne mające na nie odpowiedzieć, ale został on sporządzony w oparciu o dostępne rozwiązanie Palo Alto. Porównanie wymagań określonych w OPZ z właściwościami i cechami produktów Palo Alto nie pozostawia wątpliwości, że opis przedmiotu zamówienia został sporządzony w celu zakupu rozwiązań tego konkretnego producenta, tylko pozornie zachowując konkurencyjność i obiektywność postawionych wymagań.

W związku z tym, opis przedmiotu zamówienia zawiera wymagania dotyczące sposobu zapewnienia określonych funkcjonalności zgodnie z tym, jak jest to realizowane przez preferowanego producenta, zarówno w zakresie architektury i parametrów, jak

i sposobu licencjonowania rozwiązania. Powoduje to niezasadne ograniczenie swobody Wykonawców w doborze rozwiązań i sposobów realizacji określonych funkcji i celów systemów stosownie do właściwości oferowanego rozwiązania konkurencyjnego do Palo Alto. Producenci przewidują bowiem różne rozwiązania pozwalające na osiągnięcie tych samych efektów funkcjonalnych i zaspokojenia potrzeb zamawiającego. Natomiast opis przedmiotu zamówienia w sposób niezasadny ogranicza tę swobodę powodując, że nie jest możliwe zaoferowanie rozwiązań konkurencyjnych lub też wymaga to przewymiarowania rozwiązania w sposób uniemożliwiający realne konkurowanie o udzielenie zamówienia. Szczegółowe zarzuty odwołania wskazują szereg takich wymagań.

W opisie przedmiotu zamówienia zawarto wymaganie kompatybilności z urządzeniami i systemem zarządzania posiadanymi przez zamawiającego: „Dostarczone urządzenia muszą być w pełni kompatybilne z urządzeniami zamawiającego, w tym z systemem zarządzania, tak aby można było zaimplementować polityki bezpieczeństwa oraz konfigurację polityk routingu na dostarczone urządzenia bez konieczności ich modyfikacji. Kompatybilność musi obejmować obszary, takie jak:

- kompatybilność sprzętowa: zgodność na poziomie fizycznym, w tym złącza, interfejsy i protokoły komunikacyjne.
- kompatybilność programowa: zgodność z systemami operacyjnymi, oprogramowaniem zarządzającym oraz politykami bezpieczeństwa.
- kompatybilność operacyjna: możliwość implementacji polityk bezpieczeństwa i routingu bez konieczności modyfikacji dostarczonych urządzeń.”

Powyższe wymaganie jest możliwe do spełnienia tylko i wyłącznie przez dostawę rozwiązań Palo Alto. Chociaż pozornie zamawiający nie wskazuje z nazwy, iż oczekuje dostawy produktów określonego producenta, nie ma technicznej możliwości, aby wymaganie to mogło być spełnione przez jakiegokolwiek rozwiązania konkurencyjne. Oznacza to, że faktycznie nastąpiło wskazanie w warunkach zamówienia konieczności zaoferowania produktów określonego producenta. Przy czym, należy mieć na uwadze, że zamawiający sformułował wymaganie kompatybilności w odniesieniu do systemu, który zakupiony został w postępowaniu prowadzonym w zeszłym roku (postępowanie na dostawę i wdrożenie urządzeń firewall nr sprawy BF-IV.2370.8.2023). W ramach tego postępowania zamawiający zakupił urządzenia i system zarządzania, o znacznie mniejszej wartości (cena wybranej oferty to 1 207 860,00 PLN brutto, podczas gdy wartość tego zamówienia to nie mniej niż ponad 13 mln zł) i parametrach niższych niż wymagane od aktualnie zamawianych urządzeń (nie wspominając już o skali zamówienia). Urządzenia firewall Palo Alto PA 1420 są urządzeniami niższej klasy i nie spełniają wymagań dla żadnego z typów urządzeń zamawianych obecnie. Podane jako

funkcjonujące u zamawiającego modele urządzeń Palo Alto PA 1420 nie spełniają wymagań, które są stawiane wobec urządzeń opisanych w tym

postępowaniu jako Typ nr 1 lub 2, ani nie są też urządzeniami zamawianymi jako Typ nr 3 – czyli są urządzenia dużo mniej ważne niż kluczowe elementy architektury zamawiane w ramach tego postępowania. Poddaje to w wątpliwość zasadność i efektywność decyzji zamawiającego o podporządkowaniu całości zamawianego systemu (wymóg kompatybilności) akurat temu rozwiązaniu. Jest to kierunek integracji przeciwny do przyjętego w ramach rozbudowy systemów informatycznych, gdzie to urządzenia mniej ważne integruje się z kluczowymi komponentami (urządzenia dostępowe do szkieletowych, urządzenia końcowe do systemów centralnych itd.).

O tym, którego producenta rozwiązanie jest preferowane i oczekiwane obecnie podyktowane jest przez niewielki stosunkowo (w porównaniu do skali urządzeń zamawianych obecnie) system złożony z klastra dwóch urządzeń firewall i systemu zarządzania, który funkcjonuje u zamawiającego. W postępowaniu, w którym dokonano zakupu rozwiązania posiadanego przez zamawiającego, nie zawarto informacji o tym, iż będzie on stanowił punkt odniesienia dla przyszłego postępowania na dostawę urządzeń tworzących całą, ogólnokrajową sieć objętą obecnym postępowaniem. Wręcz przeciwnie, w toku postępowania w odpowiedzi na pytania wykonawców (w tym odwołującego), wskazujące na to, że wymagania opisu przedmiotu zamówienia w odniesieniu do systemu zarządzania są nieadekwatne, a do tego ograniczają konkurencję – zamawiający w odpowiedzi informował o tym, że system zarządzania ma charakter pomocniczy i nie jest kluczowy z punktu widzenia potrzeb zamawiającego. Tymczasem, aktualnie, to właśnie wobec zakupionego wówczas systemu zarządzania wymagana jest kompatybilność całości dostarczanego rozwiązania, co uniemożliwia zaferowanie rozwiązań konkurencyjnych producentów. W postępowaniu o udzielenie zamówienia na obecnie funkcjonujące u zamawiającego rozwiązanie złożono oferty wyłącznie w oparciu o urządzenia Palo Alto, gdyż wymagania opisu przedmiotu zamówienia nie pozwalały na zaferowanie urządzeń innych producentów.

Automatycznie zatem, jakkolwiek konkurencja w zakresie możliwości zaferowania rozwiązań innego producenta jest utrudniona, przez wymaganie dostarczenia rozwiązania równoważnego polegającego na wymianie już funkcjonującego u zamawiającego rozwiązania, czyli wymagania dostawy, wdrożenia, migracji i konfiguracji przez jakiegokolwiek wykonawcę reprezentującego konkurencyjnego producenta dodatkowego systemu, który funkcjonuje u zamawiającego. Już powyższe powoduje zakłócenie zasad uczciwej konkurencji i równego traktowania wykonawców i utrudnia złożenie prawdziwie konkurencyjnej oferty, która nie oferowałaby produktów Palo Alto. Jednakże, dodatkowo, opis przedmiotu zamówienia zawiera szereg wymagań, które w ich zestawieniu uniemożliwiają zaferowanie produktów innych niż preferowane Palo Alto, a przewidziana możliwość wymiany systemu funkcjonującego u zamawiającego i zaferowania rozwiązań

innego producenta jest tylko pozornie równoważna, gdyż określone wymagania dla takiej sytuacji, powodują, że równoważność ta jest zaburzona na niekorzyść jakiegokolwiek konkurencyjnego rozwiązania, powodując że nawet jeśli teoretycznie oferta może zostać złożona, to nie ma realnych szans, aby być konkurencyjna cenowo wobec rozwiązań Palo Alto. Szczegółowe zarzuty odwołania obejmują kluczowe z tych wymagań.

W związku z brzmieniem art. 99 ust. 1, 2 i 4 p.z.p., aktualny pozostaje dorobek orzecznictwa i doktryny dotyczący art. 29 ust. 1 poprzednio obowiązującej ustawy Prawo zamówień publicznych z 2004 r., zgodnie z którym przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty. Jednocześnie, wszystkie stawiane wymagania powinny być uzasadnione potrzebami zamawiającego i zapewniać konkurencyjność postępowania, która jest wartością korzystną również dla zamawiającego ze względu na dopuszczenie szerszego zakresu możliwych do zaferowania rozwiązań oraz konkurencji cenowej między wykonawcami. Zgodnie z orzecznictwem Krajowej Izby Odwoławczej, naruszeniem norm art. 99 p.z.p., jest nie tylko posługiwanie się w opisie przedmiotu zamówienia nazwami własnymi produktów bez dopuszczenia zaferowania rozwiązań równoważnych, ale także takie ustalenie wymagań czy zestawienia parametrów, które prowadzi do wyeliminowania możliwości zaferowania rozwiązań odpowiadających w pozostałym zakresie uzasadnionym potrzebom funkcjonalnym zamawiającego. Jakiegokolwiek wymagania, które mogą prowadzić do ograniczenia konkurencji przez preferowanie określonych rozwiązań lub eliminowanie szeregu innych produktów lub wykonawców, powinny znajdować uzasadnienie w potrzebach zamawiającego - obiektywnych i proporcjonalnych do ograniczenia konkurencji, które powodują, co potwierdza m.in. wyrok Krajowej Izby Odwoławczej z dnia 14 grudnia 2021 r., sygn. KIO 3466/21. Zamawiający nie może stosować jedynie pozornego dopuszczenia konkurencyjności postępowania i sporządzając opis przedmiotu zamówienia powinien mieć na względzie, że także pośrednie preferowanie określonego rozwiązania lub uniemożliwianie złożenia ofert konkurencyjnych ze względu nie na bezpośredni zakaz, ale na odpowiednie ukształtowanie warunków zamówienia, także stanowi naruszenie przepisów ustawy i jest działaniem niedopuszczalnym. Za reprezentatywny w powyższym zakresie należy uznać wyrok Krajowej Izby Odwoławczej z dnia 14 lutego 2022 r., sygn. akt KIO 248/22.

Zamawiający dopuścił się naruszeń ww. przepisów oraz zasad określonych w art. 16 p.z.p., stwarzając warunki uniemożliwiające realną i uczciwą konkurencję między wykonawcami oraz w sposób nieuzasadniony preferując rozwiązanie jednego, wybranego przez siebie producenta. Szczegółowo przejawia się to w zestawieniu licznych wymagań SWZ, z których nawet te pozornie nieistotne, wpływają na wyeliminowanie konkurencji w stosunku do produktów Palo Alto.

I. Zarzut nr 1 i 2 – wymagania w sytuacji dostawy rozwiązania innego niż funkcjonujące u zamawiającego.

W OPZ przewidziano, że w sytuacji, w której wykonawca decyduje się na zaferowanie rozwiązania innego niż Palo Alto,

oczekuje się, że taki wykonawca: dodatkowo, na własny koszt, dostarczy, skonfiguruje i wdroży równoważne rozwiązanie oparte na urządzeniach pracujących jako para wysokiej dostępności (HA) w trybach Active/Standby i Active/Active, wyposażone w system centralnego zarządzania i monitorowania NG Firewall. Zamawiający określił przy tym wymagania, jakie ma spełniać takie rozwiązanie, jednakże nie są to prawidłowe kryteria równoważności, gdyż po pierwsze nie opisują rozwiązania równoważnego, a po drugie: nie pozwalają na faktyczne ustalenie, jakie rozwiązanie jest oczekiwane, gdyż zamawiający opisując równoważność nie posłużył się jednoznacznymi kryteriami technicznymi czy funkcjonalnymi.

Zgodnie z OPZ, takie rozwiązanie równoważne musi obejmować:

- odpowiednią ilość licencji i oprogramowania, przeniesienie i implementację wszystkich polityk i konfiguracji z pełnym odwzorowaniem funkcjonalności i bezpieczeństwa,
- zapewnić serwis gwarancyjny oraz wsparcie na okres co najmniej 60 miesięcy, - zapewnić pełne wsparcie techniczne przez okres 60 miesięcy w trybie 24/7/365 z czasem reakcji do 2 godzin od zgłoszenia oraz maksymalnie 6 godzin na usunięcie awarii dla całego dostarczonego rozwiązania opisanego w niniejszym postępowaniu,
- zapewnić certyfikowane szkolenia dla personelu zamawiającego wraz ze wsparciem technicznym opisanym poniżej z uwagi na doświadczenie i samodzielne utrzymanie systemu przez personel zamawiającego.

Rozwiązanie funkcjonujące u Zamawiającego zawiera m.in.:

- klastery dwóch urządzeń firewall nowej generacji Palo Alto PA 1420 wraz z pakietem subskrypcji Core Security: zaawansowane zapobieganie zagrożeniom, zaawansowane filtrowanie adresów URL, zaawansowany Wildfire, zabezpieczenia DNS i SD-WAN (PAN-PA-1420-BND-CORESEC-5YR) na okres 60 miesięcy,
- wsparcie premium (PAN-SVC-BKLN-1420-5YR) na okres 60 miesięcy,
- oprogramowanie do centralnego zarządzania Panorama dla 100 urządzeń (PAN-PRA-100) ze wsparciem na okres 60 miesięcy,
- licencje na wirtualne systemy (10 szt.) dla 2 urządzeń,
- subskrypcje GlobalProtect z funkcją HIP (dla 2000 urządzeń końcowych) dla 2 urządzeń Palo Alto PA- 1420 pracujących w klastrze HA na okres 60 miesięcy.

Powyższy opis wymagań nie zawiera żadnych parametrów ani określenia funkcjonalności, które pozwalałyby na jednoznaczne ustalenie, jakie rozwiązanie zamawiający uzna za równoważne. Opis wymaganego do dostarczenia rozwiązania jest niejasny i ogólnikowy, do tego stopnia, że wykonawca nie ma możliwości ustalenia, jakie są

oczekiwania i jakie urządzenia i oprogramowanie powinien dostarczyć bez ryzyka narażenia się na zarzut niezgodności z warunkami zamówienia. Zamawiający opisał posiadane rozwiązanie, które wykonawca ma zastąpić nie za pomocą kryteriów równoważności zawierających wymagane parametry techniczne i funkcjonalne, ale przez wskazanie urządzeń i licencji obecnie posiadanych – nie wiadomo, w jakim zakresie wykonawca ma zapewnić ich równoważność, a jest oczywiste, że nie jest możliwe dostarczenie rozwiązania innego producenta zgodnego w zakresie wszystkich parametrów i właściwości posiadanych urządzeń. Powoduje to, że możliwość zaoferowania rozwiązania innego producenta niż Palo Alto (dopuszczenie rozwiązania równoważnego) jest pozorna i w praktyce zamawiający nie dopuszcza takiej możliwości eliminując realną konkurencję w postępowaniu. Dlatego też, żądaniem odwołującego jest podanie kryteriów równoważności dla dostawy rozwiązania innego niż funkcjonujące u zamawiającego poprzez określenie wymaganych parametrów technicznych i funkcjonalnych lub poprzez określenie, że w przypadku dostawy rozwiązania innego niż funkcjonujące u zamawiającego, wykonawca musi dostarczyć równoważne rozwiązanie oparte na urządzeniach spełniających wymagania określone w postępowaniu dla urządzeń typ 4 (Końcowy Węzeł Komunikacyjny) – jako najbardziej odpowiadające pod względem parametrów wydajności.

Opisując co ma obejmować rozwiązanie oferowane zamiast tego, które funkcjonuje u zamawiającego, podano wymóg: serwisu gwarancyjnego oraz wsparcia na okres co najmniej 60 miesięcy oraz pełne wsparcie techniczne przez okres 60 miesięcy. Jest to wymaganie przekraczające obecne właściwości posiadanego rozwiązania, a tym samym – nie jest ono równoważne do rozwiązania, które wykonawca ma zastąpić w ramach realizacji zamówienia. Obecnie funkcjonujące rozwiązanie zostało zakupione w wyniku rozstrzygnięcia postępowania na dostawę i wdrożenie urządzeń firewall (nr sprawy BF-IV.2370.8.2023), które zostało rozstrzygnięte w lipcu 2023 r. Jeśli rozwiązanie obecnie funkcjonujące zostało zakupione i wdrożone u zamawiającego w roku poprzednim, to na dzień składania ofert, a także na dzień zastąpienia dotychczasowego rozwiązania, okres wsparcia, serwisu, gwarancji subskrypcji licencji nie będzie już wynosić 60 miesięcy, ale odpowiednio krócej. Jest to oczywiście pominięcie przez zamawiającego faktu, że dostawa ma polegać na zastąpieniu funkcjonującego systemu, a nie dostawa urządzeń o takich samych parametrach, jak zakupione w poprzednim roku. Jest to kolejny element utrudniający złożenie oferty zawierającej rozwiązanie konkurencyjnego producenta do Palo Alto, a na wypadek złożenia takiej oferty – zwiększający jej cenę, aby uniemożliwić wybór takiej oferty jako najkorzystniejszej. Wykonawca wnosi zatem o określenie okresu zapewnienia wsparcia i pakietu subskrypcji urządzeń posiadanych u zamawiającego, wymaganego w przypadku dostawy rozwiązania innego niż funkcjonujące, jako obowiązujących do tej samej daty, do

której obowiązują okresy wsparcia i subskrypcji, którymi obecnie dysponuje zamawiający dla posiadanego rozwiązania.

II. Zarzut nr 3 i 4 – dostęp zdalny VPN.

Dla realizacji funkcjonalności dostępu zdalnego VPN, przewidziano w architekturze zamawianego rozwiązania osobny typ urządzeń – koncentratory VPN (Typ nr 3). Z OPZ wynika, że jest to wyłączna funkcja tych urządzeń. Mimo to, w wymaganiach ogólnych dla wszystkich urządzeń zawarto wymagania dotyczące dostępu zdalnego (pkt 1 ppkt 4648 OPZ). Również w ramach wymagań szczegółowych dla urządzeń Typ nr 1 (pkt 2.1 ppkt 29) i Typu nr 3 (pkt 2.3 ppkt 10) zawarto wybiórcze wymagania szczegółowe dotyczące zdalnego dostępu. Skoro urządzenia Typ nr 3 mają mieć zaawansowaną funkcję zdalnego dostępu, to określanie tych wymagań dla wszystkich urządzeń Firewall jest nadmiarowe i nieadekwatne do potrzeb oraz przewidzianej architektury, w której realizować tę funkcję mają urządzenia określonego typu.

Oprócz tego, taki sposób formułowania wymagań wprowadza różne wymagania dla różnych urządzeń w systemie, który ma być jednolity. Jest to niezrozumiałe z perspektywy funkcjonalnej, a skutkuje wyłącznie utrudnieniem złożenia konkurencyjnej oferty producentów, którzy stosują model licencjonowania tej funkcjonalności per użytkownik. O ile opisanie wymagań tej funkcji zdalnego dostępu dla urządzeń Typ nr 3 ma sens, gdyż to one będą terminowały urządzenia VPN, o tyle dla urządzeń Typ 1 jest to zbędne i powoduje wyłącznie ograniczenie konkurencji. Poza tym, zamawiający w pkt 1 ppkt 46 (a zatem wymaganie wobec wszystkich urządzeń), określił, że wymaga licencji na maksymalną wspieraną ilość dla oferowanego modelu urządzeń – wymaganie takie oderwane jest całkowicie od realnych i obiektywnych potrzeb zamawiającego, gdyż maksymalne wspierane liczby użytkowników wielokrotnie przewyższają realne zapotrzebowanie zamawiającego (np. urządzenie Typu 1 z portfolio producenta Fortinet - FortiGate 2600F posiada pojemność 100 000 połączeń klienckich IPsec, podczas gdy liczba użytkowników zdalnych w ramach Straży nie przekroczy nawet 10 000). Jednocześnie, jest to wymaganie ewidentnie preferujące rozwiązanie Palo Alto, gdzie model licencjonowania jest niezależny od liczby użytkowników końcowych – dla wykonawców oferujących Palo Alto, gdzie funkcjonalność jest licencjonowana per węzeł, liczba użytkowników nie ma znaczenia dla oferowanej ceny, natomiast wykonawcy oferujący rozwiązania producentów, gdzie wymagany jest zakup licencji dla użytkowników/urządzeń końcowych muszą ponosić koszty licencji nadmiarowych, wielokrotnie przewyższających realne zapotrzebowanie, jakie może mieć zamawiający. Dla zobrazowania, przyjmując przykładowe urządzenia producenta konkurencyjnego do Palo Alto – Fortinet, dostarczenie licencji w pełnej pojemności dla urządzeń wszystkich typów oznacza:

- urządzenie przykładowo odpowiadające urządzeniom Typu nr 2 posiada pojemność 100 000 użytkowników zdalnych,
- urządzenie Typu nr 4 – 16 000 użytkowników zdalnych,
- wymagane ilości urządzeń to 32 urządzenia Typu 2 (16 par) oraz 533 urządzenia Typu 4, sumarycznie oznacza to, że w obecnym brzmieniu wymagań OPZ, wykonawca rozwiązań klasy Fortinet (o wysokich parametrach w zakresie liczby wspieranych połączeń zdalnych), musiałby dostarczyć zamawiającemu 12 700 000 licencji na dostęp zdalny (ok. 1/3 populacji Polski), i to nie licząc urządzeń Typu 1 i 3, dla których również maksymalne ilości wskazują na konieczność zakupu kolejnych setek tysięcy licencji. Jest to wymaganie rażąco wygórowane i powodujące faktyczną eliminację z konkurencji o uzyskanie zamówienia producentów stosujących model licencjonowania per użytkownik (czyli inny niż Palo Alto).

Zaznaczyć przy tym trzeba, że faktyczne zapotrzebowanie po stronie zamawiającego to liczby rzędu 2000-5000 użytkowników korzystających z dostępu zdalnego. Liczba pracowników zamawiającego to liczbą rzędu 30 000, ale tylko niewielki procent z nich faktycznie korzysta i ma techniczną i formalną możliwość oraz potrzebę wykorzystywania dostępu zdalnego na urządzeniach mobilnych. Z treści OPZ wynika, że zamawiający dysponuje aktualnie licencjami GlobalProtect w ilości 2000 użytkowników dostępu zdalnego, co stanowi punkt odniesienia dla oznaczenia tych potrzeb zamawiającego.

III. Zarzut nr 5 – dotyczy funkcji Sandbox.

Dla urządzeń Typu 1 zamawiający określił wymagania dla funkcji Sandbox, przy czym dopuścił on wykorzystanie systemów chmurowych, gdzie jest to funkcja wspólna dla całego systemu. W pkt 2.1 ppkt 25 Zamawiający wymaga: „Zewnętrzny sandbox producenta musi być zlokalizowany w Polsce. W przypadku braku dostępności polskiej lokalizacji takiego systemu należy dostarczyć lokalne urządzenia typu sandbox do zainstalowania w sieci Zamawiającego w ilości odpowiadającej ilości urządzeń NG Firewall zawartych w ofercie.” Wymaganie, aby Sandbox producenta (system chmurowy producenta) był zlokalizowany w Polsce jest arbitralne i nieadekwatne do przedmiotu zamówienia. Nie ma żadnych względów przemawiających za niedopuszczeniem lokalizacji Sandbox producenta na terenie Unii Europejskiej, poza preferowaniem rozwiązania oferowanego przez Palo Alto. Na podstawie obecnych przepisów ustawy o Krajowym Systemie Cyberbezpieczeństwa przetwarzanie danych w ramach Unii Europejskiej jest wystarczającym wymaganiem z uwagi na zgodność przepisów polskich i unijnych. Również ze względu na spójność polityki cyberbezpieczeństwa w całej Unii Europejskiej producenci tego typu usług wdrażają najczęściej jeden wspólny punkt przetwarzania danych dla całego regionu UE, zamiast tworzyć osobne infrastruktury w każdym kraju osobno. Wymaganie na przetwarzanie danych w Polsce jest również nieuzasadnione ze względu na rodzaj danych, które w tym wypadku mają być przetwarzane. Przetwarzanie w chmurze producenta w konkretnym Państwie

z punktu widzenia prawa polskiego nie jest niczym uzasadnione a wręcz narusza przepisy traktatowe o UE uniemożliwiając umiejscowienia go w ramach Europejskiego Obszaru Gospodarczego. Jeżeli zamawiający obawia się przesyłania plików do chmury producenta to powinien oczekiwać od wszystkich dostawców zaoferowania systemów lokalnych a nie krajowych. Brak więc uzasadnienia dla wymagania przetwarzania takich plików w Polsce.

Jednocześnie podane rozwiązanie na wypadek braku dostępności polskiej lokalizacji takiego systemu nie stanowi realnej alternatywy – jest nadmiernie wygórowane i generuje koszty powodujące brak realnej alternatywy dla wymagania polskiej lokalizacji. Zamawiający w przypadku systemu chmurowego zlokalizowanego w Polsce określa jeden wspólny system/usługę realizującą funkcję Sandbox dla całej sieci, natomiast w przypadku systemu chmurowego poza Polską (nawet jeśli znajduje się w innym państwie UE) wymaga lokalnych urządzeń i liczbie równej liczbie urządzeń NG Firewall czyli ponad 550 dodatkowych fizycznych urządzeń (mimo, że wymaganie dotyczy tylko urządzeń Typu 1). Sam koszt dostarczenia tylu systemów Sandbox wielokrotnie przewyższy koszt dostarczenia samych urządzeń Firewall, więc w praktyce wymaganie w sposób nieuzasadniony i naruszający uczciwą konkurencję eliminuje każdego producenta, który nie ma lokalizacji Sandbox w Polsce. Odwołujący wnosi zatem o zmianę wymagania pkt 2.1 ppkt 25 i określenie, że: „Zewnętrzny system Sandbox producenta musi być zlokalizowany na terenie Unii Europejskiej”.

IV. Zarzut nr 6.

Zamawiający z jednej strony oczekuje dostarczenia centralnego systemu, co jest uzasadnione przy tej skali i liczbie urządzeń. Jednocześnie jednak szereg wymagań określonych dla urządzeń Firewall w zakresie funkcji zarządzania jest powielanych z funkcjonalnościami wymaganymi dla systemu centralnego. Wymagania te są nadmiarowe, bowiem niepotrzebnie powielają na poziomie samych urządzeń funkcje, które są przewidziane i będą realizowane na poziomie centralnego systemu zarządzania.

Wymaganie realizacji tych funkcji na poziomie urządzeń w ramach zamawianego systemu jest wygórowane i nadmiarowe, a z drugiej strony, prowadzi do ograniczenia konkurencji, gdyż dla producentów innych niż Palo Alto, funkcjonalności te na poziomie urządzeń Firewall albo nie są dostępne albo są dodatkowo płatne podwyższając cenę oferty. We wspomnianym wcześniej postępowaniu nr BF-IV.2370.8.2023 na dostawę urządzeń obecnie wykorzystywanych przez zamawiającego również pojawiło się wymaganie tych funkcjonalności jako funkcja urządzeń a nie systemu. W odpowiedzi na pytania o zmianę wymagań i umożliwienie realizacji tych funkcji z poziomu systemu zarządzania, zamawiający odmówił argumentując, że system zarządzania w tamtym postępowaniu miał funkcję tylko pomocniczą i tym uzasadniał potrzebę zapewnienia realizacji tych funkcji za poziomu urządzeń. W aktualnej architekturze systemu, centralny system zarządzania pełni już

kluczową rolę – ma zapewnić spójność, integrację, pojedynczy punkt zarządzania i tworzenia polityki bezpieczeństwa itd., zatem to uzasadnienie stosowane we wcześniejszym postępowaniu przestaje być adekwatne.

Ponieważ postępowanie ma na celu dostarczenie spójnego środowiska, zarządzanego z centralnego punktu. Wymagania dotyczące zaawansowanych funkcji zarządzania z poziomu pojedynczych urządzeń nie znajdują odzwierciedlenia w planowanym projekcie, są realnie niemożliwe do wykorzystania w tak dużej rozproszonej infrastrukturze i sztucznie ograniczają konkurencję.

Dodatkowo, w wymaganiach dla Centralnego Systemu Zarządzania, pkt 3 ppkt 4 OPZ, zamawiający wskazał, że system zarządzania ma pełnić rolę systemu logowania dla zarządzanych firewalli i systemu centralnego raportowania”. Skoro w architekturze rozwiązania przewidziano centralny system logowania i raportowania to wymagania dotyczące dysków lokalnych dla celów logowania na poziomie urządzeń Typ nr 1-5 oraz wymagania dotyczące logowania i raportowania zawarte w pkt 1 OPZ (Wymagania ogólne dla urządzeń Firewall) są nadmiarowe i zbędne, powodując tylko ograniczenie konkurencji i zwiększenie kosztów dostawy rozwiązań konkurencyjnych wobec Palo Alto. Raportowanie i korelacja danych z centralnego poziomu zapewnia szersze spojrzenie i agregację danych, a pozostawienie wymagania raportowania na poziomie poszczególnych urządzeń nie stanowi obiektywnej i realnej potrzeby (nie będzie na pewno wykorzystywane realnie w sieci o skali ponad 570 urządzeń). Taka potrzeba logowania i generowania raportów na pojedynczych urządzeniach nie jest uzasadniona, skoro funkcja ta jest dostępna centralnie z systemu raportowania i korelacji danych. Na pewno zaś, ta potrzeba nie uzasadnia istotnego ograniczenia konkurencji i wzrostu kosztów realizacji zamówienia (zapewnienie dysków w każdym urządzeniu), jakie niesie ze sobą wprowadzenie tego wymagania.

Opis przedmiotu zamówienia powinien mieć charakter funkcjonalny i celowościowy, zaś Wykonawca powinien mieć możliwość zaproponowania dowolnej architektury systemów wirtualnych realizujących poszczególne funkcje (np. funkcję zarządzania, funkcję korelacji logów itp.). W świetle powyższego, jest uzasadnione dopuszczenie realizacji niższej zaprezentowanych funkcjonalności z poziomu systemu zarządzania, który według opisu zamawiającego ma być pojedynczym punktem zarządzania urządzeniami, kreowania polityki bezpieczeństwa i raportowania. a) pkt 1 ppkt. 20 – integracja z systemami uwierzytelniania Cisco ISE oraz Aruba Clearpass - integracje mają sens na wyższych poziomach bo mamy pojedynczy interfejs pomiędzy systemami a nie setki interfejsów; b) pkt 1 ppkt 22 i 23 – wymaganie na dysk lokalny urządzeń firewall oraz funkcje logowania, analizy i korelacji logów i budowania na ich podstawie raportów. (raportowanie i korelowanie zdarzeń ma większy sens na większej liczbie danych – pochodzących z wielu urządzeń, a nie lokalnie na pojedynczych urządzeniach); c) pkt 2.1 ppkt 2, pkt 2.2 ppkt 2, pkt 2.3 ppkt 2., pkt 2.4 ppkt 2.,

pkt 2.5 ppkt 2. – wymaganie na dysk dużej pojemności na cel przechowywania logów – w przypadku centralnego systemu logowania wymaganie tych dysków jest niezasadne, gdyż logi będą przechowywane w systemie centralnym i tam poddawane analizie. Zamawiający przewiduje centralny system logowania o pojemności 22 TB.

W związku z tym, odwołujący wnosi o dopuszczenie zaoferowania dowolnej architektury systemów wirtualnych realizujących wymagane funkcjonalności w ramach oferowanego systemu i realizacji funkcjonalności, o których mowa w pkt 1 ppkt 20, pkt 1 ppkt 22 i 23 oraz w pkt 2.1 ppkt 2, pkt 2.2 ppkt 2, pkt 2.3 ppkt 2, pkt 2.4 ppkt 2 oraz pkt 2.5 ppkt 2 OPZ z poziomu systemu zarządzania, tj. w szczególności: usunięcia wymagań pkt 1 ppkt 20, pkt 1 ppkt 22 i 23 oraz w pkt 2.1 ppkt 2, pkt 2.2 ppkt 2, pkt 2.3 ppkt 2, pkt 2.4 ppkt 2 oraz pkt 2.5 ppkt 2 OPZ, gdyż funkcjonalności są wystarczająco zapewnione w ramach wymagań pkt 3 OPZ „System Centralnego Zarządzania i Monitorowania NG Firewall i SD-WAN”;

dopuszczenia, aby System Centralnego Zarządzania i Monitorowania mógł być zrealizowany za pomocą jednej lub więcej niż jednej dedykowanej maszyny wirtualnej, zachowując wysoki poziom integracji takich maszyn wirtualnych za pomocą natywnych dla danego producenta mechanizmów integracyjnych.

V. Zarzut nr 7-8 - wymagania dotyczące portów dla urządzeń Typ nr 1 i 2.

Dla każdego z typów urządzeń zamawiający określił w jaki sposób przewiduje podłączenie urządzeń do pozostałych elementów sieci, uzasadniając zapotrzebowanie na porty określonego rodzaju i w określonej liczbie: dla urządzeń typu 1 – 2x SFP+ 10GE + 2x QSFP+ 40GE na potrzeby HA, 8x SFP+ 10GE na potrzeby LAN; dla urządzeń typu 2 - 2x SFP+ 10GE na potrzeby HA, 8x SFP+ 10GE lub 1GE na potrzeby LAN. Jednocześnie, w wymaganiu opisującym porty, jakie muszą posiadać urządzenia Typ nr 1 i 2, znalazły się porty, które nie będą wykorzystywane do przewidzianych w architekturze połączeń. A do tego, trudno uzasadnić realne zapotrzebowanie na ich wymaganie, szczególnie, że są to porty niestandardowe lub o niższej przepustowości.

Powyższe dotyczy: dla urządzeń Typu 1: 12 portów 10G/5G/2,5G/1GE/100Mbps oraz 4 porty Ethernet SFP28; dla urządzeń Typu 2: 4 porty Ethernet RJ45 1GE/100Mbps oraz 8 portów Ethernet RJ-45 5G/2,5G/1GE/100Mbps. Urządzenia SD-WAN mają być dodatkowym elementem sieci lokalnej, dedykowanym do połączeń SD-WAN, nie będą więc agregować innych połączeń lokalnych lub zdalnych ponad te, które można określić na tym etapie – tych pomiędzy routerem brzegowym obecnym w lokalizacjach a łączami WAN. Nie istnieje więc realna potrzeba wykorzystywania w przyszłości dodatkowych połączeń, szczególnie bazujących na portach o prędkościach niższych niż już teraz planowane do wykorzystania w ramach budowy połączeń (przykładowo – jeżeli teraz wykorzystywane będzie połączenie do LAN o przepustowości 4x10G=40G, to nawet w przypadku potrzeby zwiększenia tej przepustowości nie realizuje się tego w oparciu o porty o niższej

przepływności np. 1G. Racjonalnym rozwiązaniem jest wówczas dołożenie dodatkowego łącza tej samej przepustowości, tworząc łącza agregowane lub migrowanie łącza do wyższej przepustowości.

Natomiast, wymaganie tych portów dla urządzeń Typ 1 i 2, skutecznie ogranicza konkurencję i preferuje urządzenia Palo Alto – rodzaj i liczba tych nadmiarowych portów występuje akurat w tych urządzeniach tego producenta, które odpowiadają wymaganiom OPZ dla Typu 1 i 2. Poddaje to w wątpliwości, czy opis wymagań został stworzony w oparciu o realne i obiektywne potrzeby zamawiającego co do portów tych urządzeń, czy też stanowi odzwierciedlenie cech preferowanych urządzeń Palo Alto, które dodatkowo nie są możliwe do zapewnienia przez rozwiązania konkurencyjne. Odwołujący wnosi o usunięcie: pkt 2.1 ppkt 1 lit. a i c. OPZ, tj. wymagania posiadania przez urządzenia Typu nr 1: minimum 12 portów Ethernet RJ45 wspierających 10G/5G/2,5G/1GE/100Mbps oraz 4 portów Ethernet SFP28; pkt 2.2. ppkt 1, lit. a. i b. OPZ, tj. wymagania posiadania przez urządzenia Typu nr 2: minimum 4 portów Ethernet RJ45 wspierających 1GE/100Mbps oraz minimum 8 portów Ethernet RJ45 wspierających 5G/2,5G/1GE/100Mbps.

VI. Zarzut nr 9 – wymaganie dotyczące liczby sąsiedztw IKE (IPSec).

W wymaganiach dla urządzeń Typ 1-5 (pkt 2.1 ppkt 4 lit. g. oraz pkt. 2.2 ppkt 3 lit. g, pkt 2.3 ppkt 3 lit.g., pkt 2.4 ppkt 3 lit. g., pkt 2.5 ppkt 3 lit.g. OPZ), określono parametry liczby sąsiedztw IKE (IPSec). Zwraca przy tym uwagę, że dla każdego typu urządzenia wymagana jest różna wydajność, natomiast w zakresie sąsiedztw IKE, ich liczba pozostaje praktycznie taka sama, mimo wyraźnej różnicy w pozostałych parametrach i ich powiązaniu: dla typu 1 – 4000 sąsiedztw IKE (13 Gbps wydajności IPSec VPN), dla typu 2 – 2500 sąsiedztw IKE (6 Gbps wydajności IPSec VPN), dla typu 3 – 2400 sąsiedztw IKE (2,5 Gbps wydajności IPSec VPN), dla typu 4 i 5 – 2400 sąsiedztw IKE (1 Gbps wydajności IPSec VPN).

Wymagana liczba sąsiedztw jest nieproporcjonalnie wysoka w stosunku do przedmiotu zamówienia (poniżej 600 różnych lokalizacji, a nie powyżej 2000, jak wskazywałby oczekiwany parametr). Warto nadmienić, że projekt obejmuje już prawie wszystkie jednostki (węzły centralne, wojewódzkie oraz lokalne) oraz fakt, że sam zamawiający określił wielowarstwową strukturę sieci (węzły Centralne, Pośrednie i Końcowe), w której właśnie w celu lepszej skalowalności sieci nie wykorzystuje się połączeń każdy z każdym, tylko regionalnie agreguje się ruch przez węzły Pośrednie (węzły Końcowe łączą się do pośrednich i dopiero pośrednie kierują ruch w miarę potrzeb do węzłów Centralnych). Wymaganie jest zatem nieadekwatne i wygórowane, a także istotnie ogranicza konkurencję, gdyż wymagane parametry odpowiadają adekwatnym urządzeniom preferowanego Palo Alto. Natomiast pozostali producenci, aby sprostać wygórowanym parametrom liczby sąsiedztw musieliby zaoferować modele urządzeń znacznie przewymiarowanych w stosunku do pozostałych wymagań, w szczególności parametrów

wydajnościowych (np. wydajność Firewall, wydajność ochrony IPS/Antywirus, liczba jednoczesnych sesji itd.). Odwołujący wnosi o określenie wymagań dla parametru liczby sąsiedztw IKE dla urządzeń Typ nr 1-5 w sposób realnie odzwierciedlający potrzeby Zamawiającego opisane w warunkach zamówienia, tj. zmiana parametru dla każdego z typów urządzeń do wartości 1000 sąsiedztw IKE (IPSec).

VII. Zarzut nr 10 – funkcja tzw. pasywnego chłodzenia dla urządzeń Typ nr 3, 4 i 5.

Dla urządzeń Typ nr 3, 4 i 5 (pkt 2.3 ppkt 9, pkt 2.4 ppkt 9, pkt 2.5 ppkt 9 OPZ) wymagane jest chłodzenie bez użycia wentylatorów (fan-less desing lub inaczej: funkcjonalność pasywnego chłodzenia). Przedmiot zamówienia obejmuje dostawę urządzeń Firewall, które są montowane w głównych serwerowniach jednostek, które mają stałe warunki środowiskowe. Wymaganie dotyczące pasywnego chłodzenia (które jest typowo przemysłowym wymaganiem przy instalacji w szafach zewnętrznych, o niekontrolowanych warunkach środowiskowych) jest nieadekwatne i wygórowane.

Dodatkowo zamawiający nie wymaga np. pracy w rozszerzonym zakresie temperaturowym pracy, więc wymaganie dotyczące pasywnego chłodzenia nie ma odzwierciedlenia w pozostałych wymaganiach. Za zasadnością wykluczenia

zastosowania chłodzenia przy użyciu wiatraków nie przemawia także argument dotyczący cichej pracy, gdyż urządzenia będą montowane w głównej szafie serwerowej razem z innymi centralnymi systemami IT/ICT, a nie w pomieszczeniach, gdzie znajdują się biurka pracowników itd. W pomieszczeniach serwerowni znajdują się zapewne inne urządzenia, które korzystają z wentylatorów.

Wskazane wymaganie jest niezasadne, a do tego – istotnie ogranicza konkurencję preferując urządzenia Palo Alto. Należy mieć na uwadze, że wymaganie dotyczące chłodzenia jest związane z parametrami wydajnościowymi, gdyż im urządzenie ma większą wydajność, tym większe zapotrzebowanie na odprowadzanie ciepła, a w konsekwencji konieczność korzystania z chłodzenia z wykorzystaniem wentylatorów, a nie konstrukcji pasywnej. Czyli w sytuacji, gdy aby spełnić pozostałe wymagania zamawiającego, producenci konkurencyjni do Palo Alto zdecydowaliby się na zaoferowanie urządzeń przewymiarowanych, o zwiększonej wydajności (np. aby sprostać wymaganiom opisanym w zarzucie nr 9), to napotykają kolejne ograniczenie wynikające z przedmiotowego wymagania „fan-less design”. Odwołujący wnosi o wykreślenie wymogu pasywnego chłodzenia (budowa bez użycia wentylatorów) dla urządzeń Typ nr 3,4 i 5, tj. wymagań pkt 2.3 ppkt 9, pkt 2.4 ppkt 9, pkt 2.5 ppkt 9 OPZ.

VIII. Zarzut nr 11 – obsługa formatu BSD.

W pkt 1 ppkt 30 OPZ wymagana jest obsługa formatu BSD, który jest formatem przestarzałym i niepotrzebnym w ramach zamawianego systemu. Format BSD został wycofany z RFC wiele lat temu, na co wskazuje określenie „obsoleted”, czyli „wycofany”,

„przestarzały” a zastąpiony przed standard RFC5424 (Protokół Syslog) opracowany w 2009 r. Do tego wymaganie to jest zbędne w ramach zamawianego systemu, gdzie dostarczany jest nowy system logowania, który ma współpracować z nowymi urządzeniami, a całość elementów systemów ma pochodzić od jednego producenta. Wymaganie to nie wynika zatem z obiektywnych potrzeb, a służy wyłącznie ograniczeniu konkurencji i swobody Wykonawców w doborze dostępnych rozwiązań. Odwołujący wnosi o usunięcie przedmiotowego wymagania ewentualnie poprzez modyfikację wymogu na „obsługę formatu Syslog”.

IX. Zarzuty nr 12-14 – wymagania dla urządzeń Typu nr 1.

Wymagania określone w pkt 2.1 ppkt 19, 20 i 22 OPZ są wymaganiami, które nie znajdują obiektywnego uzasadnienia, a prowadzą do istotnego ograniczenia konkurencyjności, zaś w zestawieniu z innymi parametrami OPZ – powodują one wyeliminowanie możliwości zaoferowania rozwiązań innych niż Palo Alto).

Zamawiający opisuje szczegółowo, jakiej kategoryzacji typów oczekuje oraz jaki podział oceny ryzyka stosuje, co wskazuje jednoznacznie na preferowane rozwiązanie, gdyż producenci mogą stosować różne kategorie, a pozwalają na uzyskanie tej samej funkcjonalności – zamawiający opisał wymagania nie w oparciu o swoje potrzeby, ale stosując opis właściwości urządzenia Palo Alto. W szczególności, w pkt 2.1 ppkt 19 wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen – podane przyseregowanie typów zagrożeń jest charakterystyczne dla jednego producenta. Wyklucza to zaoferowanie rozwiązań tych producentów, którzy rozpoznają te same rodzaje zagrożeń, natomiast stosują inne przyseregowanie (np. mają mniej lub więcej kategorii). Wymaganie to również dotyczy wyłącznie urządzeń Typu 1, a nie występuje dla pozostałych typów urządzeń bezpieczeństwa.

Dodatkowo, opisany w ppkt 20 wymagany sposób określania ryzyka odpowiada modelowi kategorii ryzyka, który stosuje Palo Alto. Wymaganie to ogranicza konkurencję, nie dopuszczając rozwiązań realizujących inne sposoby kategoryzacji i/lub oceny ryzyka, w tym przykładowo podstawową, dwustopniową ocenę ryzyka (URL podejrzanym lub bezpiecznym). Ocena ryzyka typu „średni” nie daje żadnej dodatkowej funkcjonalności, gdyż bezpieczeństwo systemu wskazuje na traktowanie takiego ryzyka jako „wysokie”, w celu zwiększenia poziomu bezpieczeństwa systemu. Odwołujący wnosi zatem o wykreślenie z pkt 2.1 OPZ, ppkt 19, 20 i 22.

X. Zarzut nr 15 – wymóg pojedynczego Systemu Zarządzania.

Zgodnie z pkt 3 ppkt 2 OPZ, należy dostarczyć centralny, zunifikowany system zarządzania, logowania zdarzeń i raportowania pochodzący od tego samego producenta co dostarczone urządzenia NG Firewall. Jest to nieuzasadnione, gdyż zgodnie z ppkt 3,

przewidywane jest podłączenie dostarczanego systemu do funkcjonującego systemu Panorama, więc siłą rzeczy całość działającego systemu nie będzie pojedynczym systemem. Jednocześnie tak postawione wymaganie znacząco ogranicza swobodę wykonawców w doborze dostępnych rozwiązań, wśród których cele zamówienia zrealizować można w taki sposób, że system zarządzania (NMS) oraz system logowania stanowiąc będą dwie osobne maszyny wirtualne, ale takie, które ściśle współpracują ze sobą za pomocą natywnych mechanizmów producenta rozwiązania. Zapewniając, że system pozostanie spójny i umożliwiając centralne zarządzanie.

Odwołujący wnosi, aby system zarządzania (NMS) oraz system logowania mogły być zrealizowane jako dwie osobne maszyny wirtualne, które ściśle współpracują ze sobą za pomocą natywnych mechanizmów producenta rozwiązania.

XI. Zarzut nr 16 – liczba zarządzanych urządzeń.

W pkt 3 ppkt 3 OPZ wymaga się, aby System Centralnego Zarządzania umożliwiał zarządzanie co najmniej 1000 urządzeń NG Firewall sprzętowymi. W przedmiocie zamówienia przewidziano dostawę zdecydowanie mniejszej liczby urządzeń, bo 572 NG Firewall. Oznacza to, że wymaganie jest wygórowane w stosunku do aktualnego zapotrzebowania

zamawiającego, i wpływa na niezasadne zróżnicowanie cen w zależności od oferty i modelu licencjonowania producenta. Realnym odzwierciedleniem zapotrzebowania wynikającego z tego zamówienia jest dostawa w ramach postępowania licencji na podłączenie 572 urządzeń NG Firewall oraz zapewnienie, że w przyszłości możliwe będzie rozbudowanie systemu do co najmniej 1000 urządzeń, w zależności od przyszłego zapotrzebowania.

Odwołujący wnosi o zmianę pkt 3 ppkt 3 OPZ poprzez doprecyzowanie, że na dzień dostawy system ma umożliwić podłączenie 572 urządzeń NG Firewall oraz posiadać możliwość rozbudowy do co najmniej 1000 podłączonych urządzeń w przyszłości. XII. Zarzut nr 17 – dotyczy modułu zbierania logów.

Zamawiający wymaga jednego centralnego systemu zbierającego i korelującego logi. Jednocześnie w pkt 3 ppkt 4 OPZ stawia niejasne wymaganie: „W tym celu moduły odpowiedzialne za zbieranie logów muszą zostać zrealizowane z wykorzystaniem protokołów konsensusu posiadającego mocne gwarancje spójności (tzw. consensus protocol). Każdy z węzłów musi obsługiwać przestrzeń dyskową o pojemności nie mniejszej niż 22 TB oraz minimum 20 000 logów na sekundę.” Wymaganie to odnosi się do „modułów zbierania logów”, czyli więcej niż jednego, natomiast przewidziany jest jeden system do zbierania logów. Powoduje to niejasność, co do faktycznych potrzeb i wymagań zamawiającego oraz narzuca wykonawcy określony sposób realizacji architektury systemu, podczas gdy prawidłowo opis przedmiotu zamówienia powinien zawierać wskazanie parametrów

i funkcjonalności, a wykonawca powinien mieć swobodę decyzji, co do tego, jak zamierza je zrealizować na bazie dostępnych na rynku rozwiązań.

Wobec powyższego, odwołujący wnosi o usunięcie wymagania „modułów do zbierania logów” i uzupełnienie opisu przedmiotu zamówienia o jednoznaczne określenie pojemności systemu logowania i raportowania (dla całego systemu), w taki sposób, aby Wykonawca mógł zaproponować, w oparciu o jednego z różnych producentów, optymalne rozwiązanie zapewniające żadaną funkcjonalność i pojemność systemu, bez względu na architekturę wybranego przez siebie rozwiązania (pojedynczy węzeł kolekcjonujący logi lub kilka rozproszonych modułów/węzłów itp.).

XIII. Zarzut nr 18 – dynamiczne raporty.

Zamawiający w pkt 3 ppkt 12 OPZ określił, że system musi umożliwiać tworzenie dynamicznych raportów w czasie rzeczywistym dopasowanych do wymagań zamawiającego z funkcjonalnością „drill-down”. Wymaganie zostało sformułowane w sposób niezasadnie ograniczający konkurencję (preferujący określone produkty) i uniemożliwiający zaoferowanie rozwiązań, które w inny sposób pozwalają na osiągnięcie tej samej funkcjonalności (realizują ten sam cel). Posłużenie się w ww. wymaganiu pojęciem „raport” odnosi się do statycznej formy ekstrakcji podzbioru danych w oparciu o pewne założenia (wybrane filtry, agregacja danych według konkretnych założeń itp.). Raport ma formę zamkniętą i jako taki nie umożliwia interakcji. Wymaganie w obecnej formie ogranicza konkurencję do rozwiązań, w których opisana funkcjonalność jest nazwana „raportem” natomiast uniemożliwia złożenie oferty rozwiązaniom, które realizują tę funkcję w inny sposób (przykładowo interaktywny interfejs/dashboard). Odwołujący wnosi o zmianę tego wymagania i opisanie go w sposób funkcjonalny, tj.: „Zamawiający wymaga, aby system miał możliwość analizy danych z funkcjonalnością „drill-down” (pozyskiwania coraz większej ilości informacji o danym zdarzeniu).”

W przedmiocie zarzutu dotyczącego kryteriów oceny ofert odwołujący wskazał, że obok wymagań obligatoryjnych opisu przedmiotu zamówienia, także kryteria oceny ofert zostały ustalone nie w sposób zmierny do wyboru oferty przedstawiającej najkorzystniejszy stosunek jakości do ceny lub kosztu, ale w sposób preferujący rozwiązania jednego producenta. Kryteria opisane w rozdz. XII pkt 2-3 i 5 SWZ zostały dobrane w taki sposób, że spośród wiodących na rynku producentów rozwiązań objętych przedmiotem zamówienia, tylko rozwiązania Palo Alto mogą uzyskać dodatkową punktację. W kontekście wyżej opisanego zestawienia wymagań OPZ preferujących Palo Alto, powoduje to kolejny poziom, na którym zamawiający ustalił warunki zamówienia w sposób preferujący określone rozwiązanie i powodujący praktyczne wyeliminowanie konkurencji w postępowaniu. Kryteria określone w rozdziale XII pkt 2 i 5 SWZ zostały tak zdefiniowane, że są typowymi właściwościami rozwiązania Palo Alto, pomimo możliwości zaoferowania przez innych

producentów innego rodzaju funkcjonalności korzystnych dla zamawiającego to tylko te jedynie właściwe dla Palo Alto są punktowane.

Analogicznie w przypadku kryterium z rozdziału XII pkt 3 SWZ, także ono preferuje w sposób nieuzasadniony rozwiązanie Palo Alto, przy czym w tym przypadku znajduje uzasadnienie argumentacja przedstawiona powyżej dotycząca właściwości każdego z urządzenia a nie systemu zarządzania. Wnosimy zatem aby to kryterium związane było z systemem centralnego zarządzania nie na poziomie API, GUI oraz CLI. To pozwoli osiągnąć rezultat oczekiwany przez zamawiającego a jednocześnie nie będzie stanowiło naruszenia zasady uczciwej konkurencji i równego traktowania wykonawców. Nawet, gdyby wykonawcy mogli – po zmianie eliminujących wymagań technicznych objętych pozostałymi zarzutami odwołania – złożyć ofertę opartą o rozwiązania innego producenta niż Palo Alto, to nie byłoby w stanie uzyskać punktów dodatkowych w ramach ww. kryteriów, tj. aż w wysokości 45 pkt, które uzyska preferowane rozwiązanie Palo Alto. Różnica ta powoduje, że aby mieć realne szanse konkurencji o uzyskanie zamówienia, wykonawca musiałby zaoferować odpowiednią niższą cenę, co jest oderwane od rynkowej wartości tego typu rozwiązań. Oznacza to, że nawet jeśli kryteria te są tylko fakultatywne, to ich zestawienie w sposób, który jest możliwy do spełnienia przez preferowanego producenta, a nie pozwalała na uzyskanie punktów konkurencyjnym producentom, prowadzi do faktycznego uniemożliwienia pozostałym wykonawcom uzyskania zamówienia, pozostawiając jedynie pozory konkurencyjności. W związku z tym, iż odwołujący żąda wykreślenia dwóch podkryteriów i modyfikacji jednego z nich, koniecznym stała się także zmiana wagi im przypisanych.

Działając w imieniu i na rzecz zamawiającego odpowiedź na odwołanie w formie pisemnej wniósł pełnomocnik strony

wskazując, iż zamawiający dokona modyfikacji OPZ zmieniając treść (pisownia oryginalna): „Wstęp”, „Opis stanu obecnego”, „Główne cele”, „Wymagania stawiane sieci SD-WAN”, „Zakres zamówienia”, Rozwiązanie równoważne...”, „Opis Techniczny: Pkt 1. Ogólne wymagania na sprzęt i oprogramowanie urządzeń brzegowych typu NG Firewall, ppkt.30, Pkt 1 ppkt 46 i 48 wymagania dotyczące zdalnego dostępu, Pkt 2. Wymagania precyzujące sprzęt i oprogramowanie ze względu na wydajność, rodzaj i ilość portów wej./wyj.;, Pkt 2.1. Wymagania dodatkowe dla urządzeń Typ nr 1 – 4 sztuki (2 pary HA), ppkt. 5, ppkt.25, Pkt 2.2. Wymagania dodatkowe dla urządzeń Typ nr 2 – 32 sztuki (16 par HA) (urządzenia obsługujące Pośrednie Węzły Komunikacyjne (PWK)), ppkt.4, Pkt 2.3. Wymagania dodatkowe dla urządzeń Typ nr 3 – 3 sztuki. (urządzenia obsługujące Węzły VPN), ppkt.10, Pkt 2.4. Wymagania dodatkowe dla urządzeń Typ nr 4 – 533 sztuk (urządzenia obsługujące Końcowe Węzły Komunikacyjne (KWK)), ppkt.4, Pkt 2.5. Wymagania dodatkowe dla urządzeń Typ nr 5 – 33 sztuki (urządzenia zapasowe dla Końcowe Węzły Komunikacyjne (KWK)), ppkt.4, Pkt 3. System Centralnego

Zarządzanie i Monitorowania NG Firewall i SD-WAN, ppkt. 2, ppkt. 4, ppkt. 12, wnosząc o „umorzenie postępowania w ww. zakresie z uwagi na to, że stało się zbędne”, w pozostałym zakresie wniesiono o oddalenie odwołania – zgodnie z uzasadnieniem wskazanym w odpowiedzi na odwołanie z dnia 7 października 2024 r.

Wobec spełnienia przesłanek art. 525 ust. 1-3 p.z.p. Izba dopuściła do udziału w postępowaniu odwoławczym wykonawcę A. K. prowadzącego działalność gospodarczą pod firmą Sieciowe Systemy Informatyczne A. K. Plac Zamkowy 24a, 55-200 Oława (dalej zwanego „przystępującym”), który zgłosił przystąpienie po stronie zamawiającego. Przystępujący przedstawił swoje stanowisko procesowe w formie pisemnej – pismo z dnia 30 września 2024 r., wnosząc o oddalenie odwołania w całości jako bezzasadnego.

Krajowa Izba Odwoławcza – po przeprowadzeniu rozprawy w przedmiotowej sprawie, po zapoznaniu się ze stanowiskami przedstawionymi w odwołaniu, odpowiedzi na odwołanie, stanowiskiem przystępującego, konfrontując je z zebranych w sprawie materiałem procesowym, w tym z dokumentacją postępowania o udzielenie zamówienia publicznego oraz po wysłuchaniu oświadczeń i stanowisk złożonych do protokołu w toku rozprawy – ustaliła i zważyła, co następuje:

Skład orzekający stwierdził, że odwołanie dotyczy materii określonej w art. 513 p.z.p. i podlega rozpoznaniu zgodnie z art. 517 p.z.p., a odwołujący wykazał, że posiada legitymację materialną do wniesienia środka zaskarżenia zgodnie z wymaganiami art. 505 ust. 1 p.z.p. Izba stwierdziła również, że nie została wypełniona żadna z przesłanek określonych w art. 528 p.z.p., których stwierdzenie skutkowałoby odrzuceniem odwołania i odstąpieniem od badania meritum sprawy.

Postępowanie odwoławcze w zakresie zarzutu naruszenia przez zamawiającego art. 99 ust. 1-6 oraz art. 16 pkt 1-3 p.z.p. z pkt III petitum odwołania, w przedmiocie żądań modyfikacji dokumentacji zawartych w ppkt: 1, 4, 11, 15, 17 i 18 zostało umorzono, ponieważ w dniu 8 października 2024 r. dokonano zmian SWZ w sposób czyniący zadość żądaniom odwołania (tak pkt II stanowiska procesowego odwołującego z 09.10.2024 r.). W powyższym zakresie Izba zastosowała art. 568 pkt 2 p.z.p. uznając, że dalsze postępowanie stało się zbędne z powodu dokonania zmiany treści dokumentacji postępowania, która wyczerpuje żądania odwołania. Odwołanie stało się w tej części bezprzedmiotowe, a wydanie merytorycznego rozstrzygnięcia zbędne (utraciło rację bytu), bowiem cel wniesienia odwołania został zrealizowany. Zatem wynik procesu nie powinien mieć charakteru rozstrzygnięcia merytorycznego, a powinien być jedynie jego formalnym zakończeniem.

W przeciwieństwie do pozostałych zarzutów, gdzie dokonano zmiany SWZ, jednakże nie w sposób określony w odwołaniu. Odwołujący w tym zakresie podtrzymał zarzuty

wskazując, że modyfikacja dokumentacji nie powoduje utraty aktualności jego argumentacji faktycznej i prawnej. Co istotne, Izba nie uwzględniła wniosku zamawiającego o umorzenie postępowania odwoławczego w tym przedmiocie, ponieważ zamawiający nie wykazał, aby wydanie rozstrzygnięcia merytorycznego było zbędne. Niezależnie od tego, czy od nowej czynności zamawiającego wykonawcy będzie przysługiwało prawo do wniesienia odrębnego odwołania (co zazwyczaj powoduje wycofanie zarzutów dotyczących zmodyfikowanej SWZ), to stwierdzenie, że postępowanie odwoławcze staje się bezprzedmiotowe zależne jest od sposobu dokonania zmiany SWZ, a nie opiera się na samym fakcie dokonania takiej zmiany, co forsował zamawiający w odpowiedzi na odwołanie. W rozpoznawanym sporze modyfikacja dokumentacji postępowania nie spowodowała bezprzedmiotowości rozstrzygnięcia o podtrzymanych przez odwołującego zarzutach odwołania, pozostawiając je aktualnymi (oświadczenie odwołującego z pkt III stanowiska procesowego z 09.10.2024 r.), zamawiający także nie wykazał okoliczności przeciwnej, uznając, że zmiana SWZ niejako automatycznie powoduje zbędność postępowania odwoławczego, z czym nie sposób się zgodzić.

Poważne wątpliwości budzi natomiast stanowisko przystępującego, który stwierdził, że doszło do braku substratu zaskarżenia. Umknęło bowiem uczestnikowi, że z chwilą dokonania zmiany SWZ zmienia się stan sprawy (art. 552 ust. 1 p.z.p.), a częściowo zmodyfikowane postanowienia dokumentacji postępowania powinny być rozpoznane w odniesieniu do stanu ustalonego w toku postępowania odwoławczego, a więc stanu po dokonaniu modyfikacji. („Natomiast co do zarzutów odnoszących się do częściowo zmodyfikowanych postanowień - o ile pozostają aktualne, mimo zmiany ich brzmienia i nie zostały przez odwołującego cofnięte - to powinny one zostać rozpoznane w odniesieniu do stanu ustalonego w toku postępowania odwoławczego, a więc stanu po dokonaniu modyfikacji SIWZ, a nie stanu nieobowiązującego - z zastrzeżeniem, że przy rozpoznaniu takiego zarzutu nie dokonuje się oceny i rozstrzygnięcia w zakresie samej modyfikacji, ponieważ do tego służy odwołanie od tej czynności, ale jej znaczenia dla rozpatrywanego zarzutu, odnoszącego się do kwestionowanej w odwołaniu treści SIWZ.” – wyrok Sądu Okręgowego w Warszawie z 22.10.2020 r. sygn. akt: XXIII Ga 1308/20).

W przedmiocie zarzutu naruszenia przez zamawiającego art. 99 ust. 1-6 oraz art. 16 pkt 1-3 p.z.p. z pkt III ppkt 7, na

posiedzeniu z udziałem stron i uczestników postępowania odwoławczego zamawiający uwzględnił odwołanie w tej części, a przystępujący nie zdecydował się na wniesienie sprzeciwu do czasu zamknięcia posiedzenia, co wyczerpuje przesłanki art. 522 ust. 4 p.z.p. Dodatkowo Izba wskazuje, że nie uwzględniła wniosku odwołującego o umorzenie postępowania odwoławczego dot. pkt III ppkt: 1, 4, 11, 15, 17 i 18 na podstawie art. 522 ust. 4 p.z.p., ponieważ niezależnie od oceny odwołującego, że doszło

do „faktycznego uwzględnienia odwołania”, uwzględnienie środka zaskarżenia wymaga złożenia oświadczenia przez zamawiającego, a takiego w postępowaniu nie złożono.

Skład orzekający – uwzględniając zgromadzony materiał dowodowy przedłożony przez strony, po dokonaniu ustaleń na podstawie aktualnej na dzień wyrokowania treści dokumentacji postępowania o udzielenie zamówienia publicznego, w szczególności w oparciu o postanowienia ogłoszenia o zamówieniu i SWZ, mając na względzie zakres sprawy określony przez okoliczności podniesione w odwołaniu, uwzględniając odpowiedź na odwołanie, stanowisko procesowe przystępującego, dodatkowe stanowisko procesowe odwołującego, a także oświadczenia złożone w toku rozprawy – stwierdził, że sformułowane przez odwołującego zarzuty znajdują częściowe potwierdzenie w ustalonym stanie faktycznym i prawnym. Tym samym rozpoznawane odwołanie zasługiwało na uwzględnienie w części, co skutkowało nakazaniem zamawiającemu dokonania zmiany dokumentacji postępowania zgodnie z punktem 2 tenoru sentencji wyroku.

Skład orzekający stwierdził, że w postępowaniu doszło do naruszenia przez zamawiającego art. 99 ust. 4 w zw. z art. 99 ust. 5 i 6 w zw. z art. 16 pkt 1 p.z.p. poprzez ukształtowanie zaskarżonej treści dokumentacji postępowania dotyczącej zarzutów z pkt III ppkt 2, 5, 6, 10, 12 i 13 w sposób prowadzący do uprzywilejowania producenta Palo Alto Networks, a tym samym eliminujący produkty innych wykonawców, co w konsekwencji doprowadziło do przygotowania postępowania w sposób naruszający zasadę zapewnienia zachowania uczciwej konkurencji i równego traktowania wykonawców, w tym ukształtowane przez zamawiającego kryteria równoważności nie pozwalają na zaoferowanie urządzeń innych producentów. Izba nie podzieliła stanowiska odwołującego dotyczącego zarzutów wskazanych pkt III ppkt 3, 8, 9, 14 i 16 odwołania, dzieląc w tym zakresie argumentację przedstawioną przez zamawiającego. Częściowo uwzględniono także zarzut naruszenia przez zamawiającego art. 239 ust. 2 i art. 16 pkt 1-3 p.z.p. przez ustanowienie kryteriów oceny ofert, które z naruszeniem zasad uczciwej konkurencji, równego traktowania wykonawców i zasady przejrzystości, preferują rozwiązanie jednego producenta, uniemożliwiając złożenie ofert opartych o rozwiązania konkurencyjnych producentów i powodując praktyczną niemożliwość złożenia oferty konkurencyjnej i uzyskania zamówienia, ze względu na przyjęte proporcje kryteriów preferujących producenta Palo Alto Networks – w zakresie kryteriów oceny ofert określonych w rozdz. XII pkt 2, 3 i 5 SWZ.

W ramach uwag natury ogólnej Izba wskazuje, że określenie wymagań dotyczących przedmiotu zamówienia należy do zamawiającego, który jest gospodarzem postępowania i przyszłym odbiorcą przedmiotu umowy, jest on zatem uprawniony do skonstruowania przedmiotu zamówienia stosownie do własnych potrzeb, które powinny być obiektywne i uzasadnione, a zarazem niedyskryminujące. Zamawiający ma prawo tak ukształtować dokumentację postępowania, aby uwzględniła jego wymagania i zapewniła uzyskanie

oczekiwanego efektu gwarantującego zaspokojenie określonych celów. Niemniej, jeżeli zamawiający decyduje się na przeprowadzenie postępowania w trybie konkurencyjnym, jakim jest przetarg nieograniczony, to musi na rynku istnieć co najmniej dwóch wykonawców/producentów, którzy spełnią wymagania SWZ i są zdolni do złożenia oferty w przetargu (co najmniej dwa różne produkty/urządzenia pochodzące od różnych dostawców spełniają wymagania SWZ). W przeciwnym razie zastosowanie trybu konkurencyjnego byłoby fikcyjne i mielibyśmy do czynienia z zamówieniem z wolnej ręki. Zatem o ile uzasadnione potrzeby zamawiającego mogą być obiektywną barierą, która nie pozwoli na złożenie ofert przez wszystkie podmioty działających na danym rynku, to takie sformułowanie przedmiotu zamówienia (w tym kryteriów równoważności), które ogranicza konkurencję do jednego dostawcy, będącego producentem rozwiązania wzorcowego (Palo Alto Networks), nie może zostać uznane za prawidłowe, kiedy zamawiający wybiera tryb przetargu nieograniczonego. Ten bowiem wybór potwierdza założenie, że w postępowaniu nie mamy ustanowionego monopolu jednego produktu od konkretnego producenta, a postępowanie prowadzone jest w rzeczywistym trybie konkurencyjnym.

Jeżeli zamawiający nie jest w stanie wykazać chociażby jednego podmiotu, oprócz producenta Palo Alto Networks, tj. urządzeń z rozwiązania podstawowego, który spełniłby wskazane w SWZ wymagania, w tym zastosowane przez zamawiającego kryteria równoważności (zarzut z pkt III ppkt 2 petitum odwołania), to wprost wpisuje się to w naruszenie art. 99 ust. 4 p.z.p. Norma ta jest jedną z głównych zasad związanych z procesem formułowania przedmiotu zamówienia, zakazującą opisywania go w sposób, który mógłby utrudniać uczciwą konkurencję, w szczególności przez scharakteryzowanie produktów dostarczanych przez konkretnego wykonawcę, jeżeli prowadzi to do uprzywilejowania niektórych wykonawców lub produktów, jak miało miejsce w rozpoznawanym sporze, gdzie uprzywilejowano produkty Palo Alto Networks i określono kryteria równoważności niepozwalające na złożenie ofert przez innych dostawców. Co istotne, w omawianej normie ustawodawca posłużył się sformułowaniem „mógłby utrudniać uczciwą konkurencję”. Powyższe powoduje, że na odwołującym ciąży jedynie obowiązek uprawdopodobnienia, że opis przedmiotu zamówienia może utrudniać uczciwą konkurencję, zaś ciężar dowiedzenia, że do takiego utrudnienia – pomimo prawdopodobieństwa jego wystąpienia – nie doszło lub nie może dojść, zostaje przerzucony na zamawiającego. Uprawdopodobnienie jest środkiem zastępczym dowodu wskazującym na wiarygodność (prawdopodobieństwo) twierdzenia o danym fakcie. W piśmiennictwie uprawdopodobnienie określane jest jako ułatwione postępowanie dowodowe zmierzające do uwiarygodnienia twierdzeń, środek zastępczy dowodu niedający pewności, lecz przymiot wiarygodności. Nie wymaga się zatem pełnego udowodnienia utrudnienia uczciwej konkurencji, a za wystarczające należy uznać wykazanie realnego prawdopodobieństwa takiego utrudnienia.

Jest to zwłaszcza aktualne w świetle okoliczności, że możliwość utrudnienia konkurencji często opiera się na

okolicznościach negatywnych (brak możliwości złożenia oferty przez inne podmioty/brak możliwości zaoferowania innych produktów niż uprzywilejowane). Prawdopodobieństwo naruszenia prawa stało się rzeczywiste, kiedy zamawiający nie był w stanie wskazać ani jednego rozwiązania, oprócz producenta Palo Alto Networks, które można byłoby zaoferować w przetargu. Zamawiający powołał się na producentów Cisco i Fortinet (bez wskazania na konkretne urządzenia przez nich dostarczane), ale za takim głośliwym stwierdzeniem nie stały żadne środki dowodowe, zaś odwołujący – posiadający status partnerski ww. producentów, co zdaniem Izby potwierdza jego wiedzę i dostęp do informacji pozwalających na zweryfikowanie spełnienia przez rozwiązania każdego z nich zakwestionowanych wymagań OPZ – zaprzeczył jakoby Cisco i Fortinet posiadali w swojej ofercie urządzenia, które łącznie mogłyby spełnić wymagania SWZ dla poszczególnych typów urządzeń kupowanych w postępowaniu. Zatem żaden z tych producentów nie oferuje urządzeń, które spełniają wymagania SWZ, a zamawiający nie wykazał okoliczności przeciwnej. Dodatkowo odwołujący przedłożył oświadczenia producenta Juniper Networks Poland Sp. z o.o. w Warszawie i Exclusive Networks Poland S.A. w Krakowie, że pośród rozwiązań przez nich oferowanych nie występują modele urządzeń jednocześnie spełniające wszystkie wymagania OPZ. Wobec zaniechania jakiegokolwiek inicjatywy dowodowej przez zamawiającego i treści oświadczeń przedstawionych przez odwołującego, które Izba uznała za wiarygodne, należało uznać, że nie wykazano żadnych urządzeń, oprócz produktów Palo Alto Networks, które spełniają zaskarżone wymagania SWZ, w tym nie wskazano, ani nie wykazano produktów, które spełniają kryteria równoważności określone w modyfikacji SWZ z dnia 8 października 2024 r.

W związku z tym, że zamawiający nie wykazał już pierwszego elementu ukształtowania dokumentacji postępowania w sposób zapewniający możliwość przeprowadzenia postępowania konkurencyjnego – możliwości złożenia oferty w przetargu na jakiegokolwiek inne urządzenia niż oferowane przez Palo Alto Networks, to tym samym wszelkie dalej idące zarzuty, tj. dotyczące poszczególnych cech technicznych/parametrów kupowanych produktów stały się niejako a priori uzasadnione, ponieważ w przypadku każdego z tych zarzutów elementem kluczowym będzie brak sporeństwa przez zamawiającego ciężarowi wykazania, że opis przedmiotu zamówienia pozwala na złożenie oferty nie tylko na rozwiązania producenta Palo Alto Networks. Bezprzedmiotowym jest szczegółowe opisywanie poszczególnych zarzutów i techniczna nad nimi deliberacja, skoro w obecnym stanie rzeczy i tak konieczne jest usunięcie spornej treści SWZ oraz zastąpienie jej przez zamawiającego brzmieniem, które nie będzie ograniczało konkurencji do produktów jednego producenta, a tym samym spełniało wymogi ustawy p.z.p.

Wymagania utrudniające uczciwą konkurencję, o których mowa powyżej, powodujące uprzywilejowanie produktów Palo Alto Networks, zawarto w zarzucie z pkt III ppkt 2, 5, 6, 10, 12 i 13. Natomiast argumentacja zamawiającego, że wymogi te zostały postawione w odpowiedzi na jego określone uzasadnione potrzeby nie spowoduje, że ofertę w przetargu będzie w stanie złożyć jakikolwiek inny podmiot niż ofertujący urządzenia Palo Alto Networks, a przynajmniej nic takiego nie udowodniono. Stanowisko instytucji zamawiającej zdaje się bardziej wpywać w próbę uzasadnienia trybu niekonkurencyjnego, a nie faktycznego wykazania, że zaskarżone wymagania SWZ nie dyskryminują innych produktów, a ustanowione kryteria równoważności nie mają charakteru pozornego, zatem nie mogło spowodować oddalenia odwołania w tym zakresie. Należy także zwrócić uwagę, że niezależnie, iż na właściwym rynku dany, pojedynczy wymóg mógłby zostać spełniony przez jakieś urządzenie, nie oznacza to, że będzie ono możliwe do zaoferowania w postępowaniu, bowiem oferta, aby nie zostać odrzucona, powinna łącznie spełniać wszystkie wymogi SWZ, a nie pojedyncze parametry.

Warto także dodać, że zamawiający kilkakrotnie podnosił, że zaskarżony wymóg powoduje jedynie zwiększenie ceny oferty, a nie dyskryminuje inne urządzenia niż oferowane przez Palo Alto Networks. Problemem z weryfikacją i ewentualnym podzieleniem tego stanowiska był jego bardzo ogólny, a zarazem głośliwy charakter. Aby skutecznie powołać się na fakt, że dana cecha techniczna jest obiektywnie możliwa do spełnienia przez innego producenta, tylko powoduje wzrost ceny oferty, to po pierwsze zamawiający musiałby wskazać producenta, który spełniłby sporne wymagania SWZ, po drugie określić konkretne urządzenie, które ten producent miałby zaoferować i zmodyfikować w celu podolania wymaganiom zamawiającego, a po trzecie podać koszt takiej modyfikacji (choćby w ogólnym przybliżeniu, żeby zweryfikować czy jakakolwiek konkurencja byłaby faktycznie realna, a cena modyfikacji nie byłaby zaporowa, tylko na pozór rozszerzająca konkurencję, przy takiej wysokości, że dalej byłby faktyczny monopol Palo Alto Networks). W odpowiedzi na odwołanie ograniczono się do subiektywnego stwierdzenia zamawiającego, że określone cechy techniczne nie są dyskryminujące, a jedynie zmierzają do optymalizacji ceny oferty, pozostawiając to jako nieweryfikowalną hipotezę, bez żadnych skonkretyzowanych, uchwytnych podstaw. Zastosowana forma przedstawienia stanowiska powoduje, że nie poddaje się ono żadnej weryfikacji, a tym bardziej nie było możliwe jego podzielenie. W szczególności, że jak już wcześniej wspomniano, zamawiający nie był w stanie wskazać żadnych urządzeń, żadnych producentów, którzy mogliby przystąpić do przetargu, więc jego hipotezy dotyczące ceny urządzeń nie mogły zostać uznane za wiarygodne.

Oprócz powyższego, jedynie dodatkowo należy zaznaczyć, że w zakresie zmiany pkt 2.1 ppkt 25 OPZ poprzez dopuszczenie, aby usługa sandbox realizowana była w formie maszyny wirtualnej lub w formie minimum dwóch centralnych urządzeń, w różnych

lokalizacjach, typu sandbox na poziomie Komendy Głównej PSP na potrzeby całej sieci zamawiającego (pkt III ppkt 5), skład orzekający uwzględnił stanowisko wyrażone przez zamawiającego na rozprawie, gdzie przyznano, że taka treść SWZ będzie spełniała jego wymagania, więc taką zmianę nakazano w sentencji. Co do pkt III ppkt 12, Izba uwzględniła zmianę żądania przez odwołującego zawartą w jego piśmie procesowym z dnia 9 października 2024 r., zaś co do pkt III ppkt 13 nakazano usunięcie wymagania, zgodnie z żądaniem, usuwając określony sposób określania ryzyka przypisanego URL obecnie preferujący model stosowany przez producenta Palo Alto Networks, przy pozostawieniu wymagania posiadania przez wykonawcę sposobu określania ryzyka (dopuszczając inne sposoby kategoryzacji ryzyka, co wynika z zarzutu).

Izba nie uwzględniła zarzutu z pkt III ppkt 3 odwołania, ponieważ oparto go na wadliwym założeniu, że pkt 1 ppkt 46 OPZ jest oderwany od obiektywnych potrzeb zamawiającego, a maksymalne wspierane liczby użytkowników wielokrotnie przewyższają jego realne zapotrzebowanie (zdaniem odwołującego liczba użytkowników nie przekroczy nawet 10.000), co się nie potwierdziło. Zarzut i żądanie modyfikacji SWZ, poprzez określenie liczby użytkowników pomiędzy 2.000 a 5.000, nie znalazł uzasadnienia w świetle argumentacji zamawiającego, że kwestionowane wymaganie zostało określone na podstawie obiektywnych potrzeb wynikających z bieżących i przyszłych wymagań operacyjnych Komendy Głównej Państwowej Straży Pożarnej, jak również planowanego rozwoju infrastruktury w jednostkach Ochotniczej Straży Pożarnej. Obecna liczba użytkowników systemów informatycznych, którzy mogą wymagać dostępu zdalnego, wynosi około 13.000, a w związku z planowanym rozszerzeniem infrastruktury o jednostki OSP, liczba użytkowników dostępu VPN może być znacząco wyższa. Nieprawidłowo założono w odwołaniu, że skoro zamawiający dysponuje aktualnie licencjami GlobalProtect w ilości 2.000 użytkowników dostępu zdalnego, stanowi to punkt odniesienia dla oznaczenia potrzeb zamawiającego, co się nie potwierdziło. Dodatkowo odwołujący nie wykazał, aby był to parametr graniczny, uniemożliwiający mu złożenie oferty w postępowaniu.

Tożsamo Izba stwierdziła w zakresie zarzutu z pkt III ppkt 9 odwołania, dotyczącego liczby sąsiedztw IKE (IPSec). Odwołujący podnosił, że wymagana liczba sąsiedztw jest nieproporcjonalnie wysoka w stosunku do przedmiotu zamówienia (poniżej 600 różnych lokalizacji, a nie powyżej 2.000, jak wskazywałby oczekiwany parametr), co czyni wymóg nieadekwatnym i wygórowanym, żądając określenia wymagań dla parametru liczby sąsiedztw IKE dla urządzeń typ 4 i 5 w sposób realnie odzwierciedlający potrzeby zamawiającego opisane w warunkach zamówienia, tj. zmiana parametru dla każdego z tych typów (4 i 5) urządzeń do wartości 1.000 sąsiedztw IKE (IPSec). Takie stanowisko nie mogło doprowadzić do zmiany SWZ, ponieważ zaskarżony wymóg jest podyktowany planem rozbudowy infrastruktury SD-WAN o kolejne urządzenia do zapewnienia redundancji, które

mogą pracować w trybie active-active oraz wybrane jednostki OSP (których jest obecnie ok. 17.000 na terenie kraju, w tym ok. 5.500 w KSRG). Zatem spełnienie oczekiwania odwołującego dotyczącego zmniejszenia ilości do 1.000 nie zapewniłoby obsługi infrastruktury po rozbudowie, a żądana ilość 1.000 nie byłaby adekwatna do ilości lokalizacji. Innymi słowy, nie było podstaw do stwierdzenia, że w OPZ postawiono nieadekwatny i wygórowany wymóg, skoro sporne wymaganie posiada uzasadnione podstawy. Jednocześnie odwołujący nie wykazał, żeby był to parametr graniczny, uniemożliwiający mu złożenie oferty w przetargu, przynajmniej, że są modele innych producentów niż Palo Alto Networks spełniające ww. wymaganie.

Podobnie skład orzekający stwierdził w zakresie pkt 3 ppkt 3 OPZ (pkt III ppkt 16 odwołania), w którym wymaga się, aby system umożliwiał zarządzanie co najmniej 1.000 urządzeń NG Firewall, co zdaniem odwołującego jest wymaganiem nadmiernym i niezasadnie ograniczającym konkurencję, ponieważ przewidziano dostawę 572 urządzeń. Odwołujący wniósł o zmianę SWZ poprzez doprecyzowanie, że na dzień dostawy system ma umożliwiać podłączenie 572 urządzeń NG Firewall oraz posiadać możliwość rozbudowy do co najmniej 1.000 podłączonych urządzeń w przyszłości. Uzasadnioną potrzebą zamawiającego, w związku z już wyżej zaznaczoną, planowaną rozbudową infrastruktury o jednostki PSP i OSP, jest zakup systemu, który będzie umożliwiał podłączenie wskazanej w OPZ liczby urządzeń. W przyszłości skala rozbudowy może znacznie przewyższać 1.000 urządzeń, czyniąc żądanie odwołującego niezasadnym. Jak również, już teraz kupowane urządzenia muszą spełniać parametry w zakresie wydajnościowej i ilościowej możliwości podłączenia tych urządzeń, bez ponoszenia dodatkowych nakładów finansowych, czyniąc to obiektywnie uzasadnioną potrzebą zakupową zamawiającego. W szczególności także, iż odwołujący w tym zakresie nie zdecydował się na wykazanie, że jest to wymóg graniczny, uniemożliwiający mu przystąpienie do przetargu.

W zakresie zarzutu z pkt III ppkt 8 odwołania dot. pkt 2.2 OPZ, gdzie żądano zmiany lit. b poprzez usunięcie wymagania posiadania przez urządzenia typu 2 portów Ethernet RJ45 wspierających 5G/2.5 G, skład orzekający podzielił argumentację zamawiającego, że użycie znaku „/” w tym wypadku oznacza alternatywę. Odwołujący oparł zarzut na wadliwym sposobie wykładni SWZ, który powodowałby konieczność zaferowania urządzeń o standardzie niszowym. Takie rozumienie byłoby nie do zaakceptowania na kanwie pozostałych wymagań zamawiającego i celu, jaki zamówienie ma spełniać. Mając zatem na uwadze całokształt SWZ nie ma podstaw, aby podzielić stanowisko odwołującego i usiłować wyklądać znak „/” inaczej niż alternatywę, co czyni zarzut nieuzasadnionym.

Zarzutu z pkt III ppkt 14 odwołania, tj. dotyczący wniosku o usunięcie wymagania pkt 2.1. ppkt 22 OPZ dot. obsługi plików typu PKG dla MacOS, został oddalony, ponieważ w odwołaniu nie zawarto jakiegokolwiek uzasadnienia dla postawionego żądania. Na str.

23 odwołania (pkt XVIII zarzuty nr 12-14) nie wskazano żadnych okoliczności faktycznych uzasadniających nakazanie zamawiającemu wnioskowanej przez odwołującego modyfikacji SWZ.

W przedmiocie zarzutu naruszenia przez zamawiającego art. 239 ust. 2 i art. 16 pkt 13 Pzp – przez ustanowienie kryteriów oceny ofert, które z naruszeniem zasad uczciwej konkurencji, równego traktowania wykonawców i zasady przejrzystości, preferują rozwiązania jednego producenta, uniemożliwiają złożenie ofert opartych o rozwiązania konkurencyjnych producentów i powodują praktyczną niemożliwość złożenia oferty konkurencyjnej i uzyskania zamówienia, ze względu na przyjęte proporcje kryteriów preferujących jednego producenta a kryteriów pozostałych – w zakresie kryteriów oceny ofert określonych w rozdz. XII pkt 2, 3 i 5 SWZ, Izba wskazuje co następuje.

W odpowiedzi zamawiającego na odwołanie dotyczącej tego zarzutu (vide str. 17-19 odpowiedzi na odwołanie z 07.10.24 r.) zamawiający nie przedstawił żadnego stanowiska, które pozwałoby przyjąć, że nie zgadza się z argumentami podniesionymi przez odwołującego w zakresie zaskarżenia kryterium określonego w rozdziale XIII pkt 3, tj. KPkk - Posiadanie konceptu konfiguracji kandydackiej na poziomie API, GUI oraz CLI, gdzie odwołujący żądał zmiany SWZ poprzez modyfikację tego kryterium na „KPkk - Posiadanie konceptu konfiguracji kandydackiej na poziomie systemu

centralnego zarządzania – 30%”, zatem zarzut został przez Izbę uwzględniony, zgodnie z żądaniem odwołania. Odpowiadając na odwołanie pominięto konieczność przedstawięcia okoliczności uzasadniających zastosowanie przez zamawiającego zaskarżonego kryterium, dotyczącego rozwiązania producenta Palo Alto Networks. Nie wskazano okoliczności, które pozwoliłyby na zweryfikowanie i podzielenie stanowiska dlaczego obecnie premiowany ww. wymóg jest uzasadniony – przykładowo tak, jak zamawiający wskazał dla pozostałych kryteriów z punktów 2 i 5. Zatem zarzut dotyczący kryterium z punktu 3 nie mógł zostać oddalony i zamawiającemu została nakazana zmiana SWZ zgodnie z żądaniem, co powoduje dalsze konsekwencje dotyczące punktacji za całość kryteriów oceny ofert. Przy tym skład orzekający nakazał także, aby instytucja zamawiająca uszczegółowiła kiedy kryterium zostanie spełnione, ponieważ w SWZ jednolicie, w zakresie każdego kryterium, wskazano sposób obliczenia punktów.

W odpowiedzi na odwołanie zamawiający przedstawił swoje stanowisko w dotyczące zasadności kryterium z punktu 2 (KPml - Blokowanie zagrożeń z wykorzystaniem algorytmów uczenia maszynowego, aktualizowanych dynamicznie przez producenta) i kryterium z punktu 5 (KPas - Możliwość sprawdzania wpływu nowo pobranych aktualizacji sygnatur wykrywających aplikacje (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa)), które – w zakresie uzasadnienia pozostawienia tych kryteriów – Izba podzieliła. Dodatkowo skład orzekający stwierdził, że wprowadzenie do kryteriów oceny

ofert zaproponowanego w odwołaniu kryterium obecności producenta oferowanego rozwiązania w najnowszym rynkowym raporcie „Gartner Magic Quadrant for SD-WAN” w części (tzw. ćwiartce) „Leaders” – 20%, nie znajduje uzasadnionych podstaw.

Jednakże w odpowiedzi na odwołanie zamawiający nie przedstawił właściwego stanowiska w zakresie uzasadnienia zastosowanej punktacji dla kryteriów z punktów 2 i 5, tj. podstaw do przyznania dla tych kryteriów po 15 punktów. W przedmiocie punktacji wskazano jedynie, że stanowisko zamawiającego „uzasadnia dodatkową punktację takiej funkcjonalności w ramach oceny ofert”, co jest dalece niewystarczające, kiedy zarzucono zamawiającemu, że premiowanie tych rozwiązań – producenta Palo Alto Networks (tak dokumenty postępowania na dostawę i wdrożenie firewall, nr sprawy BF-IV.2370.8.2023), w ramach wysokości zastosowanej punktacji prowadzi do faktycznego uniemożliwienia pozostałym wykonawcom uzyskania zamówienia, pozostawiając jedynie pozory konkurencyjności. Odwołujący podnosił, że aby mieć realne szanse konkurowania o uzyskanie zamówienia, wykonawca musiałby zaoferować odpowiednio niższą cenę, oderwaną od rynkowej ceny urządzeń. Zarzut opiera się nie tylko na samym fakcie ustanowieniu danego kryterium, ale także na sposobie przyznania punktacji, która powoduje „praktyczną niemożliwość złożenia oferty konkurencyjnej i uzyskania zamówienia, ze względu na przyjęte proporcje kryteriów preferujących jednego producenta a kryteriów pozostałych”. Niniejsze spowodowało, że nie było uzasadnionych podstaw do pozostawienia punktacji przyznawanej za kryteria 2 i 5 w wysokości po 15 punktów za każde. Zamawiający nie podjął się należytego wykazania zasadności przyznanej punktacji lub wykazania, że określona waga kryteriów nie powoduje pozornej konkurencji, w której przetarg wygrywa producent Palo Alto Networks.

W konsekwencji powyższego, wobec uwzględnienia zarzutu dotyczącego kryterium z punktu 3, co w związku z żądaniem odwołania przyznania nowemu kryterium 30 punktów musiało spowodować zmiany w obecnej punktacji, a także z powodu braku właściwego uzasadnienia przez zamawiającego zaskarżonej punktacji dla kryteriów 2 i 5, Izba orzekła jak w sentencji, wprowadzając nowe kryterium, zgodne z wnioskiem odwołania i zmniejszając punktację dla kryteriów 2 i 5 – dla każdego z 15 punktów do 7,5 punktów.

Ponadto, Izba zaliczyła na poczet materiału dowodowego złożone przez odwołującego dokumenty dotyczące postępowania BF-IV.2370.8.2023, gdzie wszystkie oferty złożono w oparciu o produkty producenta Palo Alto Networks, porównanie wymagań OPZ i dokumentacji Palo Alto Networks oraz zestawienie własne dotyczące wybranych wymagań i ich braku spełnienia przez rozwiązania różnych producentów, które byłyby przydatne dla rozstrzygnięcia, gdyby zamawiający nie uległ już na pierwszy etapie, gdzie nie wykazano, że w zaskarżonej dokumentacji postępowania nie ustanowiono monopolu

produktów producenta Palo Alto Networks. Podobnie Izba stwierdziła w zakresie dokumentów złożonych przez strony, dotyczących usługi sandbox (pkt 2.1 ppkt 25 OPZ).

Krajowa Izba Odwoławcza częściowo uwzględniła odwołanie, gdyż wykazano, że w przedmiotowym stanie faktycznym została wypełniona hipoteza art. 554 ust. 1 pkt 1 p.z.p. – stwierdzone naruszenie przepisów ustawy może mieć istotny wpływ na wynik postępowania o udzielenie zamówienia publicznego.

Mając na uwadze powyższe, orzeczono jak w sentencji.

Rozstrzygnięcie o kosztach postępowania wydano na podstawie art. 575 p.z.p. obciążając strony kosztami zgodnie z zasadą odpowiedzialności za wynik postępowania odwoławczego z uwzględnieniem § 7 ust. 2 pkt 1 i ust. 3 w zw. z § 5 pkt 1 i 2 lit. b rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz. U. z 2020 r. poz. 2437). Izba częściowo uwzględniła obydwie zarzuty odwołania, co powoduje, że strony odpowiadają za koszty po połowie. Na koszty postępowania złożył się uiszczony przez odwołującego wpis (15.000,00 zł) oraz koszty zastępstwa procesowego odwołującego i zamawiającego, na podstawie przedłożonych faktur VAT (po 3.600,00 zł, zgodnie z limitem z § 5 pkt 2 lit. b ww. rozporządzenia). Uwzględniając wynik sporu, Izba zasądziła na rzecz odwołującego od zamawiającego połowę kosztów wpisu (7.500,00 zł); koszty zastępstwa procesowego każda ze stron ponosi we własnym zakresie, bez konieczności krzyżowego zwracania tej samej kwoty (po 1.800,00 zł) stronie przeciwnej.

Przewodniczący:

37