

CUPT/DO/OZ/241/13/3/KR/16

Warszawa, dnia 29 listopada 2016 r.

**Do wszystkich uczestników  
postępowania**

**Dotyczy:** postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na „Dostawę i wdrożenie systemu zabezpieczeń sieciowych wraz z licencjami i wsparciem technicznym” 13/2016/ZAM.

Stosownie do treści art. 38 ust. 1 i 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych t.j. Dz. U. z 2015 r. poz. 2164 z późn. zm.), Zamawiający – Centrum Unijnych Projektów Transportowych informuje, że do niniejszego postępowania wpłynęły pytania dotyczące treści Specyfikacji Istotnych Warunków Zamówienia. Poniżej przedstawiono treść pytań, a także udzielone odpowiedzi.

**Pytanie 1**

**Wymaganie zamawiającego:**

8. Urządzenia zabezpieczeń sieciowych muszą być wyposażone w co najmniej 8 interfejsów optycznych (SFP) każde, w tym co najmniej 2 interfejsy w każdym urządzeniu obsadzone wkładkami SFP.

**Pytanie:**

Czy zamawiający dopuszcza zastosowanie urządzeń posiadających 4 interfejsy SFP oraz 2 SFP+?

**Odpowiedź:**

Zamawiający podtrzymuje zapisy SIWZ.

**Pytanie 2**

**Wymaganie zamawiającego:**

10. Każde z oferowanych urządzeń zabezpieczeń sieciowych musi posiadać wbudowany twardy dysk o pojemności minimum 120 GB (HDD lub SSD).

**Pytanie:**

Czy zamawiający dopuszcza zastosowanie urządzeń nie posiadających dysków twardych? Brak dysków twardych w przypadku posiadania centralnego systemu logowania i raportowania jest zaletą.

**Odpowiedź:**

Zamawiający podtrzymuje zapisy SIWZ.

**Pytanie 3****Wymaganie zamawiającego:**

14. Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu.

**Pytanie:**

Czy zamawiający dopuszcza zastosowanie urządzeń nie posiadających możliwości tworzenia wirtualnych routerów?

**Odpowiedź:**

Zamawiający podtrzymuje zapisy SIWZ.

**Pytanie 4****Wymaganie zamawiającego:**

18.

1) System zabezpieczeń sieciowych, zgodnie z ustaloną polityką, musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa.

2) System musi umożliwiać utworzenie minimum 20 stref bezpieczeństwa.

3) System musi umożliwiać utworzenie minimum 2000 polityk zabezpieczeń firewall.

**Pytanie:**

Czy zamawiający dopuszcza zastosowanie urządzeń obsługujących maksymalnie 1000 polityk zabezpieczeń oraz 406 zon?

**Odpowiedź:**

Zamawiający podtrzymuje zapisy SIWZ.

**Pytanie 5****Wymaganie zamawiającego:**

24. System zabezpieczeń musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

**Pytanie:**

Czy zamawiający dopuszcza zastosowanie urządzenia bez możliwości inspekcji ruchu SSH, za to z możliwością wykrywania i blokowania ruchu SSH ?

**Odpowiedź:**

Zamawiający podtrzymuje zapisy SIWZ.