Centrum Usług Informatycznych we Wrocławiu
ul. Namysłowska 8, 50-304 Wrocław

Wrocław, 29.08.2023r.

Dotyczy: postępowania prowadzonego w trybie podstawowym pn.: **„Rozbudowa systemu ochrony sieci**", sygnatura sprawy CUI-ZZ.3200.10.2023

Zamawiający, na podstawie art. 284 ust. 6 ustawy Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710) – dalej ustawa Pzp, przekazuje odpowiedzi na wnioski o wyjaśnienie treści SWZ:

Pytanie nr 1:

W nawiązaniu do OPZ, rozdział Architektura Systemu, punkt 1:

Czy Zamawiający uzna ten punkt za spełniony, jeżeli zaoferowany system będzie posiadał architekturę, która w zakresie interfejsów fizycznych obejmuje 2 wbudowane porty RJ45 (1GbE) oraz osiem slotów na dodatkowe karty rozszerzeń, umożliwiające na uzyskanie następującej maksymalnej konfiguracji: 66x 1GbE RJ45 (jedna karta to 8 portów), 32x 1GbE SFP (jedna karta to 4 porty) , 32x 10GbE SFP+ (jedna karta to 4 porty), 8x 100/40/25 QSFP28 (jedna karta to 2 porty) ?

Jeżeli powyższy system zostanie zaakceptowany, to w jakiej dokładnie konfiguracji kart rozszerzeń ? Zwracamy uwagę, że rozwiązanie modularne pozwoli na zaoferowanie konfiguracji portów, która będzie lepiej dostosowana do potrzeb Zamawiającego i będzie odzwierciedlać siatkę połączeń planowanych do uruchomienia, bez potrzeby zakupu portów „na zapas".

Odpowiedź:

Tak, Zamawiający uzna ten punkt za spełniony. W związku z powyższym Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulegają następujące wymagania Załącznika nr 1 do Umowy – OPZ, rozdział Architektura Systemu pkt. 1:

Było:

1.System realizujący funkcję Firewall dysponuje co najmniej 42 fizycznymi interfejsami komunikacyjnymi w ramach których można wyróżnić:

- ***16 portami Gigabit Ethernet RJ-45,***
- ***8 gniazdami SFP 1 Gbps.***
- ***2 gniazdami SFP+ 10 Gbps.***
- ***12 gniazdami SFP+ pozwalającymi na pracę w trybach 25 SFP28 / 10 GE SFP+ / GE SFP***
- ***4 gniazdami QSFP 40Gbps***

Jest:

1.System realizujący funkcję Firewall dysponuje interfejsami komunikacyjnymi w ramach których można wyróżnić:

a) dla rozwiązań bez kart rozszerzeń:

- ***8 portów Gigabit Ethernet RJ-45,***
- ***12 gniazd SFP+ pozwalającymi na pracę w trybach 25 SFP28 / 10 GE SFP+ / GE SFP,***
- ***4 gniazda QSFP 40Gbps.***

b) dla rozwiązań z kartami rozszerzeń:

- ***8 portówi Gigabit Ethernet RJ-45***
- ***3 moduły z portami 4 x 10GB SFP+***
- ***2 moduły z portami 2 x 100/40/25G QSFP28***

Na podstawie przedstawionych przez Wykonawca danych minimalna konfiguracja to 2 wbudowane porty RJ45 (1GbE) oraz osiem slotów na dodatkowe karty rozszerzeń w konfiguracji co najmniej:

- ***1x8 RJ45,***
- ***3x4 SFP+,***
- ***2x2 QSFP28.***

Pytanie nr 2:

W nawiązaniu do OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Parametry wydajnościowe:

Czy w zakresie szeregu parametrów wydajnościowych Zamawiający zaakceptuje system, który charakteryzuje się następującymi parametrami:
a) 32mln jednoczesnych połączeń

b) 615k nowych połączeń na sekundę
c) 145Gbps firewall (316Gbps dla pakietów 1518bajtów UDP)
d) 51,5Gbps NGFW (firewall + kontrola aplikacji + IPS)
e) 30Gbps (firewall + kontrola aplikacji + URL filtering + IPS + anti-virus + pozostałe mechanizmy ochrony przed atakami)
f) 49Gbps VPN IPSec AES-128
g) liczba tuneli IPSec VPN nie mniej niż 55k

Odpowiedź:

Tak, Zamawiający zaakceptuje system o wskazanych parametrach. W Załączniku nr 1 do Umowy – OPZ, Zamawiający odniósł się wprost do parametru dot. jednoczesnych połączeń oraz nowych połączeń na sekundę.

W związku z powyższym Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulega zapis Załącznika nr 1 do Umowy – OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Parametry wydajnościowe, pkt. 1:

Było:

1.W zakresie Firewall'a obsługa nie mniej niż 12 mln. jednoczesnych połączeń oraz 740 tys. nowych połączeń na sekundę.

Jest:

1.W zakresie Firewall'a obsługa nie mniej niż 12 mln. jednoczesnych połączeń oraz 615 tys. nowych połączeń na sekundę.

Pytanie nr 3:

W nawiązaniu do OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Funkcje Systemu Bezpieczeństwa, punkt 10:

Czy w ramach dwuskładnikowego uwierzytelniania Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania systemu, który można zintegrować z rozwiązaniami firm trzecich? Jeżeli tak to czy Zamawiający wymaga dostarczenia rozwiązania firmy trzeciej w zakresie dostawy tokenów sprzętowych ?

Odpowiedź:

Tak, Zamawiający wymaga rozwiązania sprzętowego lub programowego, czyli Wykonawca musi dostarczyć co najmniej 2 tokeny. Zamawiający dopuszcza rozwiązania firm trzecich.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulega zapis Załącznika nr 1 do Umowy – OPZ, rozdział Podstawowe Funkcje systemu ochrony, sekcja Funkcje Systemu Bezpieczeństwa, punkt 10:

Było:

10.Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Urządzenie musi umożliwiać obsługę minimum 18000 tokenów sprzętowych lub programowych (tokeny (za wyjątkiem 2 szt wymienionych wyżej) nie są przedmiotem zamówienia

Jest:

10.Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. Urządzenie musi umożliwiać obsługę minimum 18000 tokenów sprzętowych lub programowych (tokeny (za wyjątkiem 2 szt wymienionych wyżej) nie są przedmiotem zamówienia). Tokeny mogą pochodzić od firm trzecich niż oferowany system.

Pytanie nr 4:

W nawiązaniu do OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Funkcje Systemu Bezpieczeństwa, punkt 12:

Czy Zamawiający zaakceptuje system, który nie posiada funkcji lokalnego serwera DNS ?

Odpowiedź:

Tak, Zamawiający zaakceptuje system, który nie posiada funkcji lokalnego serwera DNS.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. wykreśla całą dotychczasowa treść pkt. 12 w Załączniku nr 1 do Umowy – OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Funkcje Systemu Bezpieczeństwa. Dotychczasowy pkt. 13 przyjmuje numer 12.

Pytanie nr 5:

W nawiązaniu do OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Routing, punkt 2:

Czy Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania systemu, który zapewnia obsługę Policy Based Routing, w ramach którego umożliwia tworzenie reguł opartych o: interfejs, źródłowy i docelowy adres IP, docelowy port, protokół ?

Odpowiedź:

Tak, Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania systemu, który zapewnia obsługę Policy Based Routing, w ramach którego umożliwia tworzenie reguł opartych o: interfejs, źródłowy i docelowy adres IP, docelowy port lub protokół.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulega zapis Załącznika nr 1 do Umowy – OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Routing, pkt. 2:

Było:

2.Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, interfejsu, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).

Jest:

2.Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, adresu docelowego, interfejsu, protokołu sieciowego).

Pytanie nr 6:

W nawiązaniu do OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Routing, punkt 7:

Czy Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania rozwiązania, w którym system weryfikuje dostępność danego adresu IP, a w przypadku wykrycia braku dostępności umożliwi np. zerwanie sesji BGP, a w konsekwencji usunięcie powiązanych wpisów w tablicy routingu?

Odpowiedź:

Tak, Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania rozwiązania, w którym system weryfikuje dostępność

danego adresu IP, a w przypadku wykrycia braku dostępności umożliwi np. zerwanie sesji BGP, a w konsekwencji usunięcie powiązanych wpisów w tablicy routingu.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulega zapis Załącznika nr 1 do Umowy – OPZ, rozdział Podstawowe funkcje systemu ochrony, sekcja Routing, pkt. 7:

Było:

7.Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Jest:

7.Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu, także np. poprzez zerwanie sesji BGP.

Pytanie nr 7:

W nawiązaniu do OPZ, rozdział Ochrona Sieci, sekcja Ochrona przed malware, punkt 3:

Określenie poziomu zagnieżdżenia archiwum ma zapobiegać sytuacjom, w których nadmiernie zagnieżdżone archiwa zużywają zasoby systemu bezpieczeństwa. Czy Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania rozwiązania równoważnego, które umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum?

Odpowiedź:

Tak, Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania rozwiązania równoważnego, które umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulega zapis Załącznika nr 1 do Umowy – OPZ, rozdział Ochrona Sieci, sekcja Ochrona przed malware, pkt. 3:

Było:

3.System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości

Jest:

3.System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub poprzez konfigurację maksymalnego czasu potrzebnego na dekompresję archiwum.

Pytanie nr 8:

W nawiązaniu do OPZ, rozdział Ochrona Sieci, sekcja Kontrola aplikacji, punkt 5:

Czy Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania systemu, który pozwala na tworzenie wyjątków oraz własnych kategorii aplikacji na podstawie URL?

Odpowiedź:

Tak, Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania systemu, który pozwala na tworzenie wyjątków oraz własnych kategorii aplikacji na podstawie URL.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulega zapis Załącznika nr 1 do Umowy – OPZ, rozdział Ochrona Sieci, sekcja Kontrola aplikacji, pkt. 5:

Było:

5.Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.

Jest:

5.Administrator systemu ma możliwość definiowania wyjątków oraz własnych kategorii aplikacji na podstawie URL.

Pytanie nr 9:

W nawiązaniu do OPZ, rozdział System logowania dla Firewall, sekcja Wymagania ogólne:

W ramach systemu do centralnego logowania, raportowania i korelacji Zamawiający wspomina o logowaniu zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Czy Zamawiający zaakceptuje system, który współpracuje jedynie z rozwiązaniami Producenta (czyt. gromadzi i koreluje zdarzenia pochodzące z systemu zabezpieczeń będącego przedmiotem zamówienia, ale nie jest kompatybilny z rozwiązaniami innych producentów)?

Odpowiedź:

Tak, Zamawiający zaakceptuje system, który współpracuje jedynie z rozwiązaniami Producenta czyt. gromadzi i koreluje zdarzenia pochodzące z systemu zabezpieczeń będącego przedmiotem zamówienia.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulega zapis Załącznika nr 1 do Umowy – OPZ, rozdział System logowania dla Firewall, sekcja Wymagania ogólne w zakresie:

Było:

- **W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, pochodzącego od tego samego Producenta co platforma Firewall, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń..**

Jest:

- **W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, pochodzącego od tego samego Producenta co platforma Firewall, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa.**

Pytanie nr 10:

W nawiązaniu do OPZ, rozdział System logowania dla Firewall, sekcja Logowanie, punkt 5:

Czy Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania systemu zabezpieczeń, który w ramach komunikacji z oferowanym systemem centralnego logowania nie wykorzystuje do komunikacji UDP/514 oraz TCP/514, lecz wewnętrzny bezpieczny system komunikacji, a jednocześnie umożliwia eksport logów to innych systemów zbierania logów między innymi z wykorzystaniem UDP/514 oraz TCP/514?

Odpowiedź:

Tak, Zamawiający uzna ten punkt za spełniony w przypadku zaoferowania systemu zabezpieczeń, który w ramach komunikacji z oferowanym systemem centralnego logowania nie wykorzystuje do komunikacji UDP/514 oraz TCP/514, lecz wewnętrzny bezpieczny system komunikacji, a jednocześnie umożliwia eksport logów to innych systemów zbierania logów między innymi z wykorzystaniem UDP/514 oraz TCP/514.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. zmianie ulega zapis Załącznika nr 1 do Umowy – OPZ, rozdział System logowania dla Firewall, sekcja Logowanie, pkt. 5:

Było:

5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

Jest:

5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514 lub inny wewnętrzny bezpieczny system komunikacji.

Pytanie nr 11:

W nawiązaniu do OPZ, rozdział System logowania dla Firewall, sekcja Korelacja logów, punkt 3:

Czy Zamawiający zaakceptuje system, który nie pozwala na wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne?

Odpowiedź:

Tak, Zamawiający zaakceptuje system, który nie pozwala na wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne.

Zamawiający na podstawie art. 256 ustawy Prawo zamówień publicznych zmienia treść SWZ tj. wykreśla całą dotychczasowa treść pkt. 3 w Załączniku nr 1 do Umowy – OPZ, rozdział System logowania dla Firewall, sekcja Korelacja logów

Pytanie nr 12:

Szanowni Państwo z uwagi na fakt zadania pytań do SWZ zwracamy się z prośbą o wydłużenie terminu składnia ofert do dnia 30 sierpnia 2023

Odpowiedź:

Zamawiający przedłużył termin składnia ofert na dzień 01.09.2023 roku godz. 10.00.

W załączeniu:
Załącznik nr 1 do Umowy – OPZ po zmianach. W przypadku rozbieżności jaką właściwą przyjmuje się treść z odpowiedzi na udzielone pytanie.

Pozostałe zapisy SWZ pozostają bez zmian.

Zastępca Dyrektora
Centrum Usług Informatycznych
we Wrocławiu
Dariusz Dauksz

Dokument podpisano podpisem elektronicznym

Sporządziła: Magdalena Anuszkiewicz

Informacje na temat przetwarzania danych osobowych przez CUI znajdują się na stronie BIP CUI