Transportowy Dozór Techniczny
ul. Puławska 125
02-707 Warszawa
tel.: +48 22 490 29 02
e-mail: info@tdt.gov.pl

POLSKA STULECIE ODZYSKANIA NIEPODLEGŁOŚCI

Warszawa, dn. 29.07.2021 r.

Nr referencyjny postępowania
ZP 7/2021

Znak sprawy: P.290.3.2021.PZ

dotyczy: postępowania o udzielenie zamówienia publicznego: „Dostawa sprzętu sieciowego”, Nr referencyjny postępowania: ZP 7/2021.

Szanowni Państwo,

uprzejmie informuję, iż Zamawiający na podstawie art. 137 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129) zwaną dalej ustawą Pzp, zmienia treść SWZ w następującym zakresie.

1. **Treść SWZ Rozdział 3 Opis przedmiotu zamówienia ustęp 5**

Po ustępie 5 dodaje się zapisy w następującym brzmieniu:

6. Zamawiający dopuszcza zastosowanie ofert równoważnych rozwiązaniu opisanemu w OPZ, pod warunkiem spełnienia przez rozwiązanie równoważne minimalnej funkcjonalności i minimalnych parametrów oraz kryteriów równoważności - opisanych w treści OPZ.

7. Wykonawca, który w ofercie powoła się na zastosowanie rozwiązania równoważnego do opisywanego w treści OPZ, jest **obowiązany wykazać** za pomocą wszelkich środków dostępnych Wykonawcy, że oferowane przez niego rozwiązanie spełnia wymagania określone przez Zamawiającego, w szczególności poprzez wpisanie nazwy rozwiązania równoważnego w treści oferty oraz wykazanie równoważności oferowanego rozwiązania w stosunku do OPZ.

8. Wykazanie równoważności winno odbyć się w szczególności za pomocą przedmiotowych środków dowodowych. Udowodnienie tej okoliczności powinno nastąpić w ofercie.

9. Za rozwiązanie równoważne zostanie uznane rozwiązanie, o nie gorszych parametrach i funkcjonalnościach, niż te opisane przez Zamawiającego w dokumentacji postępowania.

2. **Załącznik numer 1 do SWZ – opis przedmiotu zamówienia po zmianie z dnia 01.06.2021r. pkt. III.2 Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne) pkt 2**

Zapis:

„Specjalizowane urządzenia sieciowe i towarzyszące oprogramowanie musi być dostarczone i wspierane przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 5 lat.”

otrzymuje następujące brzmienie:

Specjalizowane urządzenia sieciowe i towarzyszące oprogramowanie musi być dostarczone i wspierane przez jednego producenta. Producent oferowanego rozwiązania musi być obecny w rynkowych raportach Gartner Magic Quadrant for Enterprise Network Firewalls w części (ćwiartce) Leaders przynajmniej od 4 lat.

3. Ponadto Zamawiajacy dokonuje poniższych zmian SWZ:

Załącznik numer 1 do SWZ – opis przedmiotu zamówienia po zmianie z dnia 01.06.2021r.

Ad. pkt. III Wymagania dotyczące urządzeń

L.p	Tytuł	Miejsce zapisu	Aktualny zapis	Zmieniony zapis
1	Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne)	Pkt III 1.4	Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 lub w co najmniej jeden port konsoli w standardzie USB oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 BASE-T. Wymagane jest dostarczenie wraz z oferowanymi urządzeniami odpowiednich kabli konsolowych, które umożliwiają podłączenie ich do komputera przez port USB 2.0 lub 3.0.	Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 lub w co najmniej jeden port konsoli w standardzie USB oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 BASE-T. Wymagane jest dostarczenie wraz z oferowanymi urządzeniami odpowiednich kabli konsolowych, które umożliwiają podłączenie ich do komputera przez port USB 2.0 lub 3.0. lub równoważny Urządzenia muszą być wyposażone w co najmniej jeden port konsoli szeregowej RJ45 oraz w co najmniej jeden port konsoli w standardzie USB oraz w co najmniej jeden dedykowany port zarządzający 10/100/1000 BASE-T. Razem z urządzeniem należy dostarczyć kabel konsolowy oraz kabel Ethernet.
2	Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne)	Pkt III 1.5	Urządzenia firewall muszą posiadać budowę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów pamięci przetwarzających ruch sieciowy (tzw. Data Plane).	Urządzenia firewall muszą posiadać budowę z odseparowanymi zasobami. Procesory zarządzające oraz pamięć (tzw. Management Plane) muszą być oddzielne od procesorów i /lub pamięci przetwarzających ruch sieciowy (tzw. Data Plane). lub równoważny Urządzenia firewall muszą posiadać separację logiczną zasobów służących do przetwarzania ruchu od zasobów służących do zarządzania urządzeniem.
3	Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne)	Pkt III 1.6	Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI.	Nadmierne obciążenie ruchem sieciowym (Data Plane) urządzenia nie może blokować funkcjonowania części zarządzającej (Management Plane). Nie może powodować problemów z konfigurowaniem czy monitorowaniem urządzenia, dostępem do interfejsu GUI i CLI. lub równoważny Urządzenia firewall muszą posiadać dedykowane zasoby procesora (CPU) do funkcji zarządzania urządzeniem lub możliwość ustawienia dedykowanego procesora do funkcji zarządzania urządzeniem.
4	Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne)	Pkt III 1.7	Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN.	Urządzenia firewall muszą wspierać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4000 znaczników VLAN. lub równoważne Urządzenia firewall muszą wspierać protokół Ethernet z obsługą VLAN poprzez znakowanie zgodne z IEEE 802.1q. Pod-interfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
5	Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne)	Pkt III 1.22	Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF i CSV. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Sposób realizacji możliwy jest również jako	Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF i CSV. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu. Sposób realizacji możliwy jest również jako rozwiązanie równoważne przez dostarczenie dodatkowego,

			rozwiązanie równoważne przez dostarczenie dodatkowego, lokalnego systemu logowania który powinien mieć takie same możliwości w każdej lokalizacji objętej postępowaniem. Po odzyskaniu połączenia z punktem centralnym musi być możliwe zsynchronizowanie lokalnych logów i raportów z lokalnych systemów z centralnym systemem zarządzania. W przypadku rozwiązania z dodatkowym lokalnym systemem logowania w każdej lokalizacji, musi zostać zapewniony poziom redundancji zasilania i dysków, który umożliwi kontynuację pracy nawet w wypadku awarii jednego z tych komponentów.	lokalnego systemu logowania który powinien mieć takie same możliwości w każdej lokalizacji objętej postępowaniem. Po odzyskaniu połączenia z punktem centralnym musi być możliwe zsynchronizowanie lokalnych logów i raportów z lokalnych systemów z centralnym systemem zarządzania. W przypadku rozwiązania z dodatkowym lokalnym systemem logowania w każdej lokalizacji, musi zostać zapewniony poziom redundancji zasilania i dysków, który umożliwi kontynuację pracy nawet w wypadku awarii jednego z tych komponentów. lub równoważny Urządzenia firewall muszą umożliwiać tworzenie raportów dostosowanych do wymagań Zamawiającego, zapisania ich na urządzeniu i uruchamiania w sposób ręczny lub automatyczny w określonych interwałach czasowych. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV lub XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika na przestrzeni wskazanego zakresu czasu. Równoważnie dopuszczona jest realizacja za pomocą lokalnego systemu logowania, który zostanie zainstalowany w każdej lokalizacji objętej postępowaniem. W przypadku przerw w łączności WAN, po odzyskaniu połączenia z głównym systemem zarządzania (centralnym) musi być dokonywana synchronizacja lokalnych logów i raportów z systemem centralnym. W przypadku rozwiązania z dodatkowym lokalnym systemem logowania w każdej lokalizacji musi on posiadać te same wymagania serwisowe co centralny system zarządzania.
6	Wymagania wspólne dla wszystkich urządzeń firewall. (Wymagania minimalne)	Pkt III 1.27	Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa	Urządzenia firewall muszą posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. lub równoważne Urządzenia firewall muszą obsługiwać NAT64.
7	Wymagania urządzenia Centralne – 2 szt. (para HA)	Pkt III 2.3	Urządzenie musi być wyposażone w dysk systemowy SSD minimum 220 GB potrzeby systemu operacyjnego i logów. Dysk musi mieć możliwość wymiany bez potrzeby rozkręcania urządzenia.	Urządzenie musi być wyposażone w dysk systemowy SSD minimum 220 GB potrzeby systemu operacyjnego i logów. Dysk musi mieć możliwość wymiany bez potrzeby rozkręcania urządzenia. lub równoważne Urządzenie musi być wyposażone w przestrzeń na logi i system operacyjny w postaci innej niż obrotowy dysk twardy (HDD) o wielkości minimum 200 GB. Zamawiający wymaga, aby wymiana uszkodzonego urządzenia umożliwiała odesłanie urządzenia (RMA) bez nośnika danych (dysku).
8	Centralny System zarządzania	Pkt IV 1.2	Zamawiający eksploatuje obecnie system Palo Alto Networks Panorama (PAN-PRA-25) w wersji wirtualnej z aktywnym kontraktem gwarancyjnym do dnia 2021-07-31 i dopuszcza migrację/wymianę posiadanej licencji na rzecz zamawianego Centralnego Systemu Zarządzania Urządzeniami Firewall przy przedłużeniu kontraktu gwarancyjnego.	Dokonuje się wykreślenia zapisu
9	Centralny System zarządzania	Po treści pkt Pkt IV 1.5d dodaje się pkt IV 1.5e o następującej treści: Wymiana uszkodzonego urządzenia umożliwia odesłanie urządzenia (RMA) bez nośników danych (dysków).		
10	Wymagania dotyczące Dostawy i Usługi wdrożenia	Pkt V 11	Wykonawca będzie zobowiązany do przeniesienia logów systemowych z aktualnie użytkowanych urządzeń firmy PALOALTONETWORKS tj.PA-3020, PA-500 i PA-	Wykonawca będzie zobowiązany do przeniesienia logów systemowych z aktualnie użytkowanych urządzeń firmy PALOALTONETWORKS tj.PA-3020, PA-500 i PA-200 oraz centralnego sytemu zarządzania

	Systemu		200 oraz centralnego sytemu zarządzania PAN-PRA-25 do nowych urządzeń lub zachowanie tych logów w miejscu wyznaczonym przez Zamawiającego	PAN-PRA-25 do nowych urządzeń lub zachowanie tych logów w miejscu wyznaczonym przez Zamawiającego lub równoważne: Wykonawca będzie zobowiązany do przeniesienia logów systemowych z aktualnie użytkowanych urządzeń firmy PALOALTONETWORKS tj. PA-3020, PA-500 i PA-200 w miejsce (do zasobu dyskowego) wyznaczonego przez Zamawiającego.
11	**Wymagania dotyczące Dostwy i Usługi wdrożenia Systemu**	Pkt V 12	Wykonawca zobowiązany jest zachować polityki bezpieczeństwa wdrożone w aktualnych rozwiązaniach i przenieść je do nowych urządzeń w uzgodnieniu z Zamawiającym.	Wykonawca zobowiązany jest zachować polityki bezpieczeństwa wdrożone w aktualnych rozwiązaniach i przenieść je do nowych urządzeń w uzgodnieniu z Zamawiającym. lub równoważne Wykonawca w ramach wdrożenia urządzeń firewall przeniesie obecne polityki z eksploatowanego aktualnie przez Zamawiającego klastra firewalli Palo Alto Networks oraz urządzeń oddziałowych. Proces wdrażania firewalli nie może spowodować przerwy dłuższej niż 60 minut. Wdrożenie musi się odbyć w przerwie serwisowej, której datę i godzinę wskaże Zamawiający na etapie uzgodnień z Wykonawca. Szczegółową konfiguracje obecnych reguł i polityk w obecnie używanych przez Zamawiającego firewallach Palo Alto, Zamawiajacy przekaże Wykonawcy wyłonionego w ranach niniejszego postępowania na etapie realizacji wdrożenia.
12	Wymagania - Szkolenia	Dokonuje się zmiany treści pkt IX.1 *„Wykonawca jest zobowiązany do dostarczenia w formie voucherów szkoleniowych :* *- podstawowego autoryzowanego przez producenta dostarczonych urządzeń szkolenia dla dwóch administratorów Zamawiającego oraz* *- zaawansowanego autoryzowanego przez producenta dostarczonych urządzeń szkolenia dla jednego administratora Zamawiającego.”* W następujący sposób: Wykonawca zapewni Zamawiającemu oficjalne/autoryzowane szkolenia producenta dla administratorów (w formie voucherów szkoleniowych) w zakresie każdego rodzaju oferowanego urządzenia. Szkoleniem należy objąć 4 osoby w wymiarze nie krótszym niż 80 godzin zegarowych dla każdej z osób.		

Na podstawie art. art. 137 ust. 2 ustawy Pzp, Zamawiający udostępnia dokonaną zmianę treści SWZ na stronie internetowej prowadzonego postępowania, na której udostępniona jest SWZ i jest ona wiążąca.

Załączniki:

Załącznik nr 1 Opis przedmiotu zamówienia - po zmianie z dnia 29.07.2021r.

Załącznik nr 2 Formularz ofertowy po zmianie z dnia 29.07.2021r.