WOF.261.3.8.2019.WM

Lublin, dnia 29 października 2019 r.

ODPOWIEDZI NA ZAPYTANIA ORAZ ZMIANA TREŚCI SIWZ

DOTYCZY: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego na **dostawę sieciowych urządzeń zabezpieczających oraz przeprowadzenie instruktażu z niezbędnych konfiguracji,** w ramach realizacji projektu „Poprawa komunikacji pomiędzy Regionalną Dyrekcją Ochrony Środowiska w Lublinie a społeczeństwem poprzez narzędzia informatyczne – e – drzwi do ochrony środowiska" RPLU.02.01.00-06-0023/16.

Uprzejmie informuję, że w/w postępowaniu wpłynęły zapytania o następującej treści:

1. Certyfikat ISO 9001 podmiotu serwisującego - czy zamawiający dopuszcza złożenie oferty na rozwiązanie, którego podmiot serwisujący nie posiada ISO 9001, ale jest autoryzowanym wsparciem producenta rozwiązania?

   Odpowiedź:

   W oparciu o art. z art. 38 ust. 4 ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych (t j. Dz. U. z 2019 r., poz. 1834) Zamawiający zmienia zapisy załącznika nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, w punkcie 9 (strona 3), który otrzymuje brzmienie:

   „ *9. Na wezwanie Zamawiającego, Wykonawca dostarczy:*

   - *oświadczania producenta lub autoryzowanego dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (adres strony internetowej serwisu i numer infolinii telefonicznej),*

- *oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań,*
- *w przypadku udzielanego instruktarzu, od prowadzącego instruktarz - certyfikat powiązany z dostarczonymi urządzeniami*".

2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN - Czy zamawiający dopuszcza zaoferowanie produktu nie posiadającego funkcji monitorowania na porcie SPAN?

Odpowiedź:

W oparciu o art. z art. 38 ust. 4 ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych (t j. Dz. U. z 2019 r., poz. 1834) Zamawiający zmienia zapisy załącznika nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia - dotyczy URZĄDZENIE BRZEGOWE TYP-1, w lp.1 (Wymagania ogólne, strona 4),
oraz URZĄDZENIE BRZEGOWE TYP-2, w lp.1 (Wymagania ogólne, strona 11),
które otrzymują brzmienie:

„*Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym pochodzącymi od producenta dostarczonego sprzętu.*

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT oraz transparentnym.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- *firewall,*
- *ochrony w warstwie aplikacji,*
- *protokołów routingu dynamicznego*".

3. Odnośnie pkt 9. Obsługa routingu i łączy WAN - Czy zamawiający dopuszcza zaoferowanie produktu, który obsługuje Protokoły RIPv2, OSPF oraz BGP (bez protokołu PIM)?

Odpowiedź:

W oparciu o art. z art. 38 ust. 4 ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych (t j. Dz. U. z 2019 r., poz. 1834) Zamawiający zmienia zapisy załącznika nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia - dotyczy URZĄDZENIE BRZEGOWE TYP-1, w lp. 9 (Obsługa routingu i łączy WAN, strona 6) oraz URZĄDZENIE BRZEGOWE TYP-2, w lp. 9 (Obsługa routingu i łączy WAN, strona 13), które otrzymują brzmienie:

„ *- routingu statycznego,*

- Policy Based Routingu,

- protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF oraz BGP.

System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN".

4. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora - Czy zamawiający dopuszcza zaoferowanie produktu, który oferuje minimum 1800 sygnatur bazy kontroli aplikacji?

Odpowiedź:

Nie. Zamawiający nie dopuszcza produktu, który oferuje minimum 1800 sygnatur bez bazy kontroli aplikacji.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur – Czy zamawiający dopuszcza zaoferowanie produktu, który nie daje możliwości definiowania wyjątków oraz własnych sygnatur?

   Odpowiedź:
   Nie. Zamawiający nie dopuszcza produktu, który nie daje możliwości definiowania wyjątków oraz własnych sygnatur.

6. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL - Czy zamawiający dopuszcza zaoferowanie produktu, który nie ma możliwości nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL?

   Odpowiedź:
   Nie. Zamawiający nie dopuszcza produktu, który nie ma możliwości nadpisywania kategorii oraz tworzenia wyjątków - białe/czarne listy dla adresów URL.

7. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API – Czy zamawiający dopuszcza zaoferowanie produktu, który nie ma możliwości zarządzania przez systemy firm trzecich poprzez API?

   Odpowiedź:
   Nie. Zamawiający nie dopuszcza produktu, który nie ma możliwości zarządzania przez systemy firm trzecich poprzez API.

8. Czy zamawiający dopuszcza wykreślenie ze specyfikacji zdania: „Zamawiający będąc użytkownikiem sprzętu firmy Fortinet, zabezpieczającego połączenia brzegowe sieci, wymaga aby dostarczone urządzenia były z nim w pełni kompatybilne."- To zdanie jednoznacznie wyklucza możliwość zaproponowania rozwiązania alternatywnego dla

produktów firmy FORTINET. Urządzenie, które chcemy zaproponować posiada w sobie możliwość zarządzania wszystkim zakupionymi modelami z punktu jednej konsoli, bez konieczności posiadania dodatkowych narzędzi jak ._ -FortiAnalyzer czy Fortilvlanager.

Odpowiedź:

W oparciu o art. z art. 38 ust. 4 ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych (t j. Dz. U. z 2019 r., poz. 1834) Zamawiający zmienia zapisy załącznika nr 1 do SIWZ – Szczegółowy opis przedmiotu zamówienia, w punkcie 10 (strona 3), który otrzymuje brzmienie:

„ 10. Zamawiający wymaga aby dostarczone urządzenia obsłużyły istniejącą strukturę sieciową oraz strefę DMZ, a także realizowały zabezpieczenia IDS/IPS, Antywirus, Web Filtering, Anyspam. Zamawiający będąc użytkownikiem sprzętu firmy Fortinet, zabezpieczającego połączenia brzegowe sieci, wymaga aby dostarczone urządzenia były z nim kompatybilne. Wdrożenie urządzeń polegać ma na zastąpieniu istniejących rozwiązań sieciowych we wszystkich lokalizacjach Zamawiającego nowymi urządzeniami odpowiednio skonfigurowanymi, z zachowaniem istniejących parametrów sieciowych oraz odpowiednim zabezpieczeniu sieci. Uruchomione rozwiązanie umożliwiać ma obsługę redundancji połączenia z siecią Internet przy użyciu drugiego łącza bez ponoszenia dodatkowych kosztów na sprzęt albo licencje i oprogramowanie. Zamawiający wymaga wykonania rejestracji urządzeń oraz dostarczonych serwisów na stronach producenta (w porozumieniu z przedstawicielem Zamawiającego) oraz przekazania niezbędnych danych dostępowych Zamawiającemu.”

Pozostałe zapisy Specyfikacji Istotnych Warunków Zamówienia pozostają bez zmian.

Regionalny Dyrektor Ochrony Środowiska w Lublinie
dr inż. Arkadiusz Iwaniuk

Fundusze Europejskie Program Regionalny | Rzeczpospolita Polska | lubelskie Smakuj życie! | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

główny specjalista
29 PAŹ. 2019

Naczelnik Wydziału Organizacyjno - Finansowego
Justyna Woźniak