Warszawa, 07 czerwca 2023 r.

KOMENDA GŁÓWNA
PAŃSTWOWEJ STRAŻY POŻARNEJ

BF-IV.2370.8.2023.23

do uczestników postępowania

Dotyczy: postępowania o udzielenie zamówienia publicznego, prowadzonym w trybie przetargu nieograniczonego na dostawę i wdrożenie urządzeń firewall nr sprawy: BF-IV.2370.8.2023.

W związku z wątpliwościami Wykonawców dotyczącymi specyfikacji warunków zamówienia (SWZ), zgodnie z art. 135 ust. 2 ustawy z dnia 11 września 2019 roku – Prawo zamówień publicznych (Dz.U. z 2022 r., poz. 1710 z późn. zm.) zwanej dalej „ustawą", Zamawiający wyjaśnia co następuje.

Zapytanie nr 1 z 29.05.2023

Pytanie 1:
Dotyczy Załącznika nr 2 do SWZ – wzór umowy:
Zgodnie z § 4 ust. 1 wzoru umowy, „WYKONAWCA dostarczy do siedziby ZAMAWIAJĄCEGO przedmiot umowy na własny koszt i ryzyko wraz z ubezpieczeniem od zniszczenia i kradzieży". Wykonawca zwraca się z prośbą o wyjaśnienie, czy Zamawiający oczekuje wykupienia przez Wykonawcę dodatkowego ubezpieczenia przedmiotu umowy od ryzyka zniszczenia i kradzieży, a jeżeli tak to na jaki okres, czy też intencją Zamawiającego jest stwierdzenie, że do czasu odbioru przedmiotu umowy przez Zamawiającego ryzyka takie jak zniszczenie i kradzież obciążają Wykonawcę.

Odpowiedź:
Zamawiający odstępuje od wymogu ubezpieczenia przedmiotu umowy do czasu jego dostarczenia do siedziby Zamawiającego. Intencją Zamawiającego jest ustalenie, że do chwili podpisania protokołu odbioru wszelkie ryzyka takie jak zniszczenie i kradzież obciążają Wykonawcę.
W związku z tym Zamawiający modyfikuje treść § 4 ust. 1 wzoru umowy.
Zamawiający dokonał zmian w zapisach § 4 ust.1 umowy.

Pytanie 2:
Dotyczy Załącznika nr 2 do SWZ – wzór umowy:
Zgodnie z § 7 ust. 1 wzoru umowy, „Strony ustalają, że w przypadku zwłoki w realizacji przedmiotu umowy, w stosunku do terminu, o którym mowa w § 3 ust. 1 - WYKONAWCA zapłaci ZAMAWIAJĄCEMU karę umowną w wysokości 0,3 % wynagrodzenia brutto określonego w § 5 ust. 1, za każdy rozpoczęty dzień zwłoki". Również w §7 ust. 4 i 6 powiązano kary umowne z kwotami wynagrodzenia brutto. Czy Zamawiający wyrazi zgodę na powiązanie kar z kwotą netto wynagrodzenia a nie kwotą brutto? Kwota brutto obejmuje podatek VAT, a ten nie jest przychodem Wykonawcy co de facto oznacza, że w relacji do wysokości przychodu potencjalne kary są wyższe niż wskazane w umowie.
Odpowiedź:
Zamawiający nie wyraża zgody na wprowadzenie zmian. Zamawiający podtrzymuje zapisy SWZ.

Pytanie 3:
Dotyczy Załącznika nr 2 do SWZ – wzór umowy:
Zgodnie z § 7 ust. 2 wzoru umowy, „Jeżeli zwłoka w wykonaniu przedmiotu umowy przez WYKONAWCĘ przekroczy 7 dni, ZAMAWIAJĄCY może odstąpić od umowy, z wyłączeniem przypadków siły wyższej". Ustalenie podstawy do odstąpienia przez Zamawiającego od umowy przy zaledwie 7-dniowym uchybieniu terminowi realizacji zamówienia przez Wykonawcę stanowi zbyt rygorystyczne ustalenie warunków kontraktowych, stanowiące przejaw wykorzystania dominującej pozycji Zamawiającego w postępowaniu o udzielenie zamówienia publicznego. Czy Zamawiający wyrazi zgodę na zmianę okresu 7-dniowego na 14-dniowy.

Odpowiedź:
Mając na względzie nieprzewidywalne zdarzenia wynikające z wydłużonych łańcuchów dostaw, Zamawiający wyraża zgodę na wydłużenie terminu, o którym mowa w § 7 ust. 2 wzoru umowy, do 14 dni.
Zamawiający dokonał zmian w zapisie § 7 ust 2 umowy.

Pytanie 4:
Dotyczy Załącznika nr 2 do SWZ – wzór umowy:
Zgodnie z § 7 ust. 7 wzoru umowy: „ZAMAWIAJĄCY może na zasadach ogólnych dochodzić odszkodowania przewyższającego kary umowne". Czy Zamawiający dopuści zmianę § 7 ust. 7 umowy poprzez dodanie postanowienia, z którego wynikało będzie, że całkowita odpowiedzialność Wykonawcy z tytułu Umowy zostanie ograniczona do wartości 40% wynagrodzenia netto i wyłączona jest odpowiedzialność z tytułu utraconych korzyści.

Odpowiedź:
Zamawiający nie wyraża zgody na wprowadzenie zmian. Zamawiający podtrzymuje zapisy SWZ.

Pytanie 5:
Dotyczy Załącznika nr 2 do SWZ – wzór umowy:
Zgodnie z § 10 ust. 7 wzoru umowy, „Czas naprawy (przywrócenia funkcjonalności) przedmiotu umowy (produktów, oprogramowania i funkcjonalności) nie może przekroczyć 1 (jednego) dnia roboczego od dnia zgłoszenia".
Wykonawca wskazuje, że termin 1-dniowy na dokonanie naprawy jest niewystarczający wobec charakteru przedmiotu zamówienia. Na czas skutecznej naprawy wpływa wiele czynników, w tym okres reakcji producenta, dostępność części, dostępność wykwalifikowanych techników, lokalizacja urządzenia. Wobec powyższego Wykonawca zwraca się z pytaniem, czy Zamawiający wyrazi zgodę na określenie, że „Czas naprawy (przywrócenia funkcjonalności) przedmiotu umowy (produktów, oprogramowania i funkcjonalności) nie może przekroczyć 3 (trzech) dni roboczych od dnia zgłoszenia"

Odpowiedź:
Zamawiający wyraża zgodę na zmianę z (1) jednego dnia roboczego na (3) dni robocze. Zamawiający dokonał zmian w zapisach § 10 ust.7 umowy.

Zapytanie nr 2 z dnia 29.05.2023

Pytanie 1:
Dotyczy Załącznik nr 1 do SWZ – OPZ, część II Minimalne wymagania dla urządzeń NG firewall, pkt. 19:
„Urządzenia firewall muszą zapewniać możliwość automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie min. z systemami:

a) Microsoft Active Directory,
b) Microsoft Exchange
c) Terminal Services d. Syslog e. Cisco ISE".
Z uwagi na fakt, że integralną częścią postępowania jest dostarczenie centralnej konsoli zarządzającej (systemu zarządzania urządzeniami – wymagania części IV OPZ), prosimy o dopuszczenie rozwiązania, w którym wszystkie wyżej wymienione integracje będą możliwe z poziomu tego systemu centralnego, co ułatwia znacząco zarządzanie i konfigurację integracji systemów.

Odpowiedź:
Zamawiający podtrzymuje wymaganie by już na poziomie urządzenia firewall były funkcjonalności automatycznego i transparentnego ustalenia tożsamości użytkowników sieci i integrować się w tym zakresie min. z systemami:

a. Microsoft Active Directory,
b. Microsoft Exchange
c. Terminal Services
d. Syslog
e. Cisco ISE

System zarzadzania jest dla Zamawiającego elementem pomocniczym w zarzadzaniu urządzeniami, a nie integralną częścią funkcjonalności Firewalla, dotychczasowe doświadczenia Zamawiającego ujawniły słabe strony proponowanego w pytaniu rozwiązania, w którym firewall bez systemów pomocniczych, zarzadzania traci ważne cechy bezpieczeństwa i funkcjonalności.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 2:
Dotyczy Załącznik nr 1 do SWZ – OPZ, część II Minimalne wymagania dla urządzeń NG firewall, pkt. 21:
„Urządzenia firewall muszą pozwalać na lokalne zbieranie (na dysk urządzenia) i analizowanie logów, korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach, filtrowaniu url, deszyfracji SSL, połączeniach VPN."
Dotyczy Załącznik nr 1 do SWZ – OPZ, część II Minimalne wymagania dla urządzeń NG firewall, pkt. 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, CSV i XML. Na urządzeniu musi być również dostępne tworzenie raportów o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni wskazanego okresu czasu."
Dotyczy Załącznik nr 1 do SWZ – OPZ, część III Wymagania dodatkowe dla urządzeń NG Firewall, pkt. 2:
„Musi być wyposażone w zasób dyskowy (inny niż obrotowy HDD) minimum 200 GB na potrzeby systemu operacyjnego i logów".
Dotyczy Załącznik nr 1 do SWZ – OPZ, część II Minimalne wymagania dla urządzeń NG firewall, pkt. 47:
„W przypadku potrzeby wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby dyski zostały wymontowane z urządzenia i pozostały w jego siedzibie w celu bezpiecznej utylizacji".
Dotyczy Załącznik nr 1 do SWZ – OPZ, część III Wymagania dodatkowe dla urządzeń NG Firewall, pkt 3:
„W przypadku procedury wymiany serwisowej urządzenia (tzw. RMA) Zamawiający wymaga, aby zasób dyskowy został wymontowany z urządzenia i pozostał w jego siedzibie w celu bezpiecznej utylizacji"

W świetle zapisów w części IV – zarządzania urządzeniami firewall, w których Zamawiający oczekuje dostarczenia centralnego systemu zarządzania i raportowania, które mogą być dostarczone w formie kilku komponentów, zwracamy się z prośbą o rezygnację z wyżej wymienionych zapisów w kontekście urządzeń Firewall. Z części IV OPZ wynika, że Zamawiający oczekuje dostarczenia centralnej konsoli, zapewniającej wszystkie funkcjonalności zarządzania, logowania, korelacji logów etc. wymienionych w powyższych zapisach. Z uwagi na fakt, że centralny system zarządzania jest elementem nadrzędnym nad samymi urządzeniami, funkcjonalności te na poziomie samych urządzeń nigdy nie będą wykorzystywane, co powoduje, że są nadmiarowe w stosunku do ich wykorzystania w sieci Zamawiającego. W środowiskach o wysokim poziomie bezpieczeństwa centralizacja wyżej wymienionych funkcji jest bardzo pożądana i zapewnia więcej możliwości dla operatorów niż podobne funkcje zaimplementowane bezpośrednio na urządzeniach. W kontekście centralnego systemu zarządzania i logowania wymaganie na dużą przestrzeń dyskową poszczególnych urządzeń staje się zbędne, więc w celu optymalizacji kosztowej prosimy o usunięcie również zapisów dotyczących wymagania na lokalną przestrzeń dyskową oraz konieczność pozostawienia dysków u Zamawiającego przy wymianie RMA (zasoby te realnie nie będą wykorzystywane przy centralnym systemie zarządzania i logowania).

Odpowiedź:
Zamawiający podtrzymuje wymaganie by już na poziomie urządzenia firewall były dostępne w/w funkcjonalności. System zarzadzania jest dla Zamawiającego elementem pomocniczym w zarzadzaniu urządzeniami, a nie integralną częścią funkcjonalności Firewall-a, dotychczasowe doświadczenia Zamawiającego ujawniły słabe strony proponowanego w pytaniu rozwiązania, w którym firewall bez systemów pomocniczych, w tym systemu zarzadzania, traci ważne cechy bezpieczeństwa i funkcjonalności. Każda awaria systemu zarzadzania wpływa na działanie wymienionych funkcjonalności i jej konfiguracja jest rozproszona, co może skutkować niespójnością konfiguracji, gdyż tylko poprzez procesy walidacji konfiguracji kilku współpracujących narzędzi możliwa jest stabilna praca komponentów urządzenia firewall wraz z dodatkowymi potrzebnymi systemami zarzadzania, co w rozumieniu Zamawiającego jest nie do przyjęcia.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 3:
Dotyczy Załącznik nr 1 do SWZ – OPZ, część II Minimalne wymagania dla urządzeń NG firewall, pkt. 29:
„Urządzenia firewall muszą pozwalać na selektywne wysyłanie logów w zależności od ich rodzaju. Konieczna jest obsługa Syslog za pomocą transportu UDP, TCP, SSL oraz obsługa formatów IETF oraz BSD" Prosimy o dopuszczenie rozwiązania, w którym wykorzystywany jest wyłącznie format logów IETF, z uwagi na jego szeroką implementację w rozwiązaniach różnych producentów i kompatybilność z rozwiązaniami typu SIEM. Dodatkowo zwracamy uwagę, że w świetle wymagań części IV OPZ dotyczących centralnej konsoli zarządzania i analizy logów, serwerem syslog dla tego rozwiązania będzie właśnie wspomniany centralny system zarządzania pochodzący od tego samego producenta, co powoduje, że inne niż wspierane przez danego producenta formaty nie będą realnie wykorzystywane.

Odpowiedź:
Zamawiający podtrzymuje wymaganie na obsługę formatów IETF oraz BSD. Zamawiający używa też innych serwerów SYSLOG, w związku z tym istnieje potrzeba wykorzystania obu formatów, komunikatów SYSLOG-a.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 4:
Dotyczy Załącznik nr 1 do SWZ – OPZ, część III Wymagania dodatkowe dla urządzeń NG Firewall, pkt. 1:
„Urządzenie musi być wyposażone w minimum:

a) minimum 4 porty Ethernet RJ45 wspierających 100Mbps/1GE;
b) minimum 4 porty Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps;
c) minimum 4 porty Ethernet RJ45 wspierających 5G/2.5G/1GE/100Mbps z zasilaniem PoE z budżetem 150W mocy oraz możliwością udostępnienia na porcie 50W mocy;
d) minimum 2 portów Ethernet SFP (akceptujących moduły 1GE SFP)
e) minimum 8 portów Ethernet SFP+ (akceptujących moduły 10GE SFP+ oraz 1GE SFP)
f) minimum 1 port dla celów połączenia urządzeń w HA: minimum 1x 10GE SFP+ (lub szybszy) oraz minimum 2x 1GE (SFP lub RJ45) (lub szybszy). Porty te muszą być traktowane jako dodatkowe względem wymaganych powyżej. Nie dopuszcza się liczenia jako HA, portów wymaganych wcześniej".
Pragniemy zwrócić uwagę, że urządzenia firewall są urządzeniami mającymi centralne miejsce w sieci; najczęściej są podłączone do przełączników agregacyjnych lub szkieletowych w sieci lokalnej, szczególnie dla urządzeń o wydajności podanej w wymaganiach OPZ (czasami zdarza się obsługa PoE dla bardzo małych urządzeń firewall, będących jedynym urządzeniem w sieci lokalnej). Funkcjonalność Power over Ethernet (PoE) to funkcjonalność charakterystyczna dla urządzeń dostępowych, które za pomocą portów z tą funkcją zapewniają zasilanie urządzeniom końcowym. Obsługa PoE na części portów Firewalla znacząco ogranicza więc konkurencję, jednocześnie będąc funkcjonalnością całkowicie zbędną w poprawnie zaprojektowanej sieci, gdzie urządzenia są podłączane do sieci za pomocą przełączników dostępowych. Dodatkowo, w połączeniach z przełącznikami szkieletowymi/agregacyjnymi wykorzystywane są połączenia światłowodowe (Zamawiający sam wskazuje w części III konieczność dostarczenia wkładek SFP+ 10G typu SR do podłączenia sieci LAN). Prosimy więc o usunięcie z podpunktu c wymagania dotyczącego zasilania PoE na portach Ethernet. Dodatkowo prosimy o dopuszczenie rozwiązania równoważnego, w którym część z wymaganych portów Ethernet RJ-45 będzie zrealizowana za pomocą portów SFP z modułem SFP typu Base-T.

Odpowiedź:
Zamawiający podtrzymuje wymaganie dotyczące dostępności portu z zasilaniem PoE, port taki pozwala na niezależne podpięcie modemu GSM (bez dodatkowych zasilaczy i poprzez port RJ-45) za pomocą którego w przypadku ataku np. DDOS pozwoli na tylne wejście do zarządzania urządzeniem nawet w przypadku uszkodzeń w wyniku potencjalnego ataku na infrastrukturę sieci LAN/WAN. Fakt bezpośredniego podłączenia urządzenia do FIREWALL-a pozwala na niezawodność alternatywnej możliwości zarządzania, reagowania na zagrożenia w przytoczonych sytuacjach. Zamawiający dopuszcza rozwiązanie równoważne, w którym część z wymaganych portów Ethernet RJ-45 będzie zrealizowana za pomocą portów SFP z modułem SFP typu Base-T.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 5:
Dotyczy Załącznik nr 1 do SWZ – OPZ, część III Wymagania dodatkowe dla urządzeń NG Firewall, pkt. 10:
„Bezpośrednio w GUI urządzenia musi istnieć możliwość uruchomienia/aktywowania nowej aktualizacji sygnatur oraz powrotu do starszej wersji sygnatur, gdyby taka potrzeba zachodziła"
Pragniemy zwrócić uwagę, że powrót do starszej wersji sygnatur jest procedurą bardzo rzadko wykorzystywaną, z uwagi na fakt inkrementalnego podejścia do aktualizacji tych baz przez producentów. W związku z tym prosimy o dopuszczenie rozwiązania, w którym powrót do starszej wersji sygnatur jest możliwy w inny sposób niż z poziomu GUI (np. ręczny upload odpowiedniej bazy).

Odpowiedź:
Zamawiający podtrzymuje tą dodatkową funkcjonalność, która dla Zamawiającego będzie w przypadku użycia prostszym procesem, ponieważ do przeprowadzenia w GUI a nie ręczny upload przygotowanej bazy, czyli sposób podatny na błąd administratora podmiany odpowiedniej bazy.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 6:
Dotyczy Załącznik nr 1 do SWZ – OPZ, część III Wymagania dodatkowe dla urządzeń NG Firewall, pkt. 17:
„Wymagane jest posiadanie oddzielnych kategorii URL dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen" Prosimy o dopuszczenie rozwiązania, w którym kategoria C2C znajdują się w części związanej z malware jako, że malware jest głównym wektorem nawiązywania komunikacji C2C.

Odpowiedź:
Zamawiający podtrzymuje wymaganie by można było w oddzielnych kategoriach URL konfigurować zabezpieczenia dla zagrożeń typu malware, phishing, C2C oraz dla ostatnio zarejestrowanych domen. Wielu atakujących próbuje łączyć ruch C2C z innymi typami legalnego ruchu, takimi jak HTTP/HTTPS lub DNS. Celem jest uniknięcie wykrycia. Konfiguracja w kategorii URL pozwala na gradualną konfigurację tego obszaru.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 7:
Dotyczy Załącznik nr 1 do SWZ – OPZ, część III Wymagania dodatkowe dla urządzeń NG Firewall, pkt. 19:
„Urządzenie musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sandbox" plików różnych typów (Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG, PKG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, HTA) w celu ochrony przed zagrożeniami typu „zero-day". Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym. Interwał aktualizacyjny to maksymalnie 2 godziny" Prosimy o dopuszczenie rozwiązania wspierającego następujące typy plików – m.in. Windows Portable Executable (m.in. exe, dll), MacOS (MachO, DMG), Linux ELF, pdf, MS Office, JAR, APK, JS, VBS, PowerShell Script, HTA.

Odpowiedź:
Zamawiający podtrzymuje wymaganie na przesyłanie do systemu typu Sandbox PKG OS X Installer File, ponieważ stanowią one podatność na zainfekowanie.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 8:
Dotyczy Załącznik nr 1 do SWZ – OPZ, część IV Zarządzanie urządzeniami firewall, pkt. 5:
„System zarządzania, logowania i raportowania musi zapewniać narzędzia dla szybkiej i skutecznej analizy informacji w tym co najmniej:
a) umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych,
b) tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego,
c) zapisywanie stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób,
d) tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down"."
Prosimy o potwierdzenie, że Zamawiający zaakceptuje rozwiązanie, w którym pojęcie „dynamicznego raportu" będzie spełnione za pomocą odpowiednich widoków w interfejsie zarządzania, z możliwością zarządzania przez operatora elementami tego widoku.

Odpowiedź:
Zamawiający podtrzymuje wymaganie dotyczące możliwości dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down".

Przedstawiona propozycja nie jest dynamicznym raportem, jest statycznie utworzonym widokiem prezentującym raport.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 9:
Dotyczy Specyfikacja Warunków Zamówienia (SWZ) – część XIV Opis kryteriów oceny ofert, pkt 3, Kryterium nr 2:
Prosimy o dopuszczenie rozwiązania, w którym opisane wyżej mechanizmy ML będą wykorzystywane tylko na poziomie modułu antywirusowego, gdyż analiza w oparciu o ML opiera się w zdecydowanej większości na analizie plików (wykonywalnych, skryptów itp.). Filtrowanie URL opiera się wyłącznie na danych związanych z adresem URL, który sam w sobie jest informacją niewystarczającą do określenia czy treść znajdująca się pod danym adresem jest złośliwa.

Odpowiedź:
Zamawiający podtrzymuje wymaganie dla uczenia maszynowego ML zgodnie z zapisem by: było w akcji dynamicznej aktualizacji przez producenta, wykrywanie za pomocą algorytmów lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach antywirusowych oraz funkcji filtrowania URL. W wymaganiu Zamawiający wyjaśnił, że tego typu uczenie maszynowe pozwala znacznie zmniejszyć opóźnienie wynikające z czasu na analizę przez system sandbox oraz ryzyka typu „pacjent ZERO". Przedmiotowe wymaganie zwiększa dodatkowo możliwości odparcia zagrożenia używając też w korelacji filtrowania URL.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 10:
Dotyczy Specyfikacja Warunków Zamówienia (SWZ) – część XIV Opis kryteriów oceny ofert, pkt 3, Kryterium nr 3:
Kryterium zostanie uznane za spełnione, jeżeli zaoferowane urządzenia będą posiadały koncept konfiguracji kandydackiej (na poziomie API, GUI, oraz CLI), którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
Konfiguracja kandydacka musi być wspierana przez minimum 7 dni oraz posiadać możliwość:
- edytowania jej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami,
- blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.

Z uwagi na fakt, że integralną częścią postępowania jest centralny system zarządzania, który z definicji jest systemem nadrzędnym nad urządzeniami w kontekście interfejsu zarządzania, prosimy o dopuszczenie rozwiązania, w którym powyższa funkcjonalność jest spełniona na poziomie centralnego systemu zarządzania i na poziomie interfejsów, które ten system zarządzania posiada (przykładowo, systemy zarządzania w formie wirtualnej -a taką formę wymaga Zamawiający – nie będą posiadały interfejsu CLI)

Odpowiedź:
Zamawiający podtrzymuje wymaganie dla Konfiguracji kandydackiej dostępnej na urządzeniu firewall.
System zarzadzania jest dla Zamawiającego elementem pomocniczym w zarządzaniu urządzeniami a nie integralną częścią funkcjonalności Firewall-a, dotychczasowe doświadczenia Zamawiającego ujawniły słabe strony proponowanego w pytaniu rozwiązania, w którym firewall bez systemów pomocniczych, w tym zarządzania, traci ważne cechy bezpieczeństwa oraz funkcjonalności, w tym związane z administrowaniem.
Zamawiający podtrzymuje zapisy SWZ.

Zapytanie nr 3 z dnia 29.05.2023

Pytanie 1:
Dotyczy SWZ, Rozdział VII. Informacja o podmiotowych i przedmiotowych środkach dowodowych ust.3
Zamawiający wymaga aby *„3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia podmiotowe środki dowodowe, wymienione w ust. 1 pkt 2 lit. a-e (tj. na potwierdzenie braku podstaw wykluczenia), składa każdy z Wykonawców występujących wspólnie."*
Pragniemy zauważyć, iż w przywołanym ust. 1 pkt. 2 nie występuje pkt. e). Prosimy o potwierdzenie, iż prawidłowe brzmienie ust 3. to „W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia podmiotowe środki dowodowe, wymienione w ust. 1 pkt 2 lit. a-d (tj. na potwierdzenie braku podstaw wykluczenia), składa każdy z Wykonawców występujących wspólnie."

Odpowiedź:
Tak potwierdzamy, że w Rozdziale VII ust. 3 w wyniku omyłki pisarskiej zapisano ust.1 pkt 2 lit. a-e winno być ust.1 pkt 2 lit. a-d.

Pytanie 2:
Dotyczy SWZ, Rozdział VII. Informacja o podmiotowych i przedmiotowych środkach dowodowych ust. 4
Zamawiający wymaga aby *„4. W przypadku podmiotu, na którego zdolnościach lub sytuacji Wykonawca polega na zasadach art. 118 Ustawy, Wykonawca składa podmiotowe środki dowodowe, wymienione w ust. 1 pkt 2 lit. a, c-e i f (tj. na potwierdzenie braku podstaw wykluczenia), w odniesieniu do każdego z tych podmiotów."*
Pragniemy zauważyć, iż w przywołanym ust. 1 pkt. 2 nie występuje pkt. e – f. Prosimy o potwierdzenie, iż prawidłowe brzmienie ust 4. to „W przypadku podmiotu, na którego zdolnościach lub sytuacji Wykonawca polega na zasadach art. 118 Ustawy, Wykonawca składa podmiotowe środki dowodowe, wymienione w ust. 1 pkt 2 lit. a, c, d (tj. na potwierdzenie braku podstaw wykluczenia), w odniesieniu do każdego z tych podmiotów.

Odpowiedź:
Tak potwierdzamy, że w Rozdziale VII ust. 4 w wyniku omyłki pisarskiej zapisano ust.1 pkt 2 lit. a, c-e i f winno być ust.1 pkt 2 lit. a, c, d.

Pytanie 3:
Dotyczy Załącznik nr 1 do SWZ, Opis przedmiotu zamówienia, pkt. V. Warunki gwarancji i wdrożenia

a) Ile godzin wsparcia merytorycznego o którym wspomniano w ww. punkcie wymaga Zamawiający?
b) Czy wsparcie merytoryczne w ramach prowadzonego projektu może byś świadczone zdalnie?
c) Z jakimi parametrami SLA ma być świadczone wsparcie merytoryczne.

Odpowiedź:

a) Zamawiający wymaga wsparcia merytorycznego Wykonawcy w okresie 60 m-cy w reżimie 24/7/365.
b) tak, wsparcie merytoryczne może być prowadzone zdalnie.
c) wsparcie merytoryczne w zakresie przyjmowania przez Wykonawcę zgłoszeń serwisowych powinno być świadczone w reżimie 24/7/365. Czas reakcji na zgłoszenie serwisowe powinno wynosić nie więcej niż 6 godzin w reżimie 24/7/365. Wsparcie merytoryczne w zakresie rozwiązywania bieżących problemów i awarii rozumianych jako czas naprawy przedmiotu umowy nie może przekroczyć 3 dni roboczych.

Pytanie 4:
Dotyczy Załącznika nr 2 do SWZ – Umowa
Prosimy o informację, czy Zamawiający wyraża zgodę na otrzymanie faktury VAT oraz wszelkich załączników do niej w formie elektronicznej, w rozumieniu przepisów o podatku VAT (ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług)?

W sytuacji, w której Zamawiający dopuszcza taką możliwość prosimy o dodanie postanowienia w brzmieniu:
"*Zamawiający wyraża zgodę na otrzymanie faktury VAT oraz wszelkich załączników do niej w formie elektronicznej, w rozumieniu przepisów o podatku VAT (ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług). Faktura VAT oraz wszelkie załączniki do niej będą wysyłane na adres: [...]*"

Odpowiedź:
Zamawiający dopuścił składanie faktur elektronicznych zgodnie z ustawą z dnia 9 listopada 2018 roku o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno – prawnym.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 5:
Dotyczy Załącznika nr 2 do SWZ – Umowa, § 7. Kary umowne, ust. 1
Prosimy o zmianę zapisów dotyczących naliczania kary umownej od „wartości netto" a nie od „wartości brutto". Zważywszy, że odszkodowanie wypłaca się zawsze od kwoty netto (podatek VAT nie jest składnikiem wynagrodzenia wykonawcy) właściwą praktyką jest formułowanie zapisów dotyczących kar w oparciu o wynagrodzenie netto (bez VAT).

Odpowiedź:
Zamawiający nie wyraża zgody na zmianę zapisów § 7 ust.1 wzoru umowy.
Zamawiający podtrzymuje zapisy SWZ.

Pytanie 6:
Dotyczy Załącznika nr 2 do SWZ – Umowa, § 7. Kary umowne
Zdaniem Wykonawcy Zamawiający nakłada na Wykonawcę kary, które są rażąco wygórowane. Zwracamy się z prośbą o modyfikację zapisów istotnych postanowień umowy w § 7 i proponujemy brzmienie:
1. Strony ustalają, że w przypadku zwłoki w realizacji przedmiotu umowy, w stosunku do terminu, o którym mowa w § 3 ust. 1 - WYKONAWCA zapłaci ZAMAWIAJĄCEMU karę umowną w wysokości 0,2 % wynagrodzenia netto określonego w § 5 ust. 1, za każdy rozpoczęty dzień zwłoki.
[.....]
4. Zrealizowanie przez ZAMAWIAJĄCEGO prawa do odstąpienia od umowy rodzi po stronie WYKONAWCY obowiązek zapłaty ZAMAWIAJĄCEMU kary umownej w wysokości 5% wynagrodzenia netto określonego w § 5 ust. 1.
5.Za każdorazowe przekroczenie przez WYKONAWCĘ czasu naprawy przedmiotu umowy, o którym mowa w § 10 ust. 7, WYKONAWCA zapłaci ZAMAWIAJĄCEMU karę umowną w wysokości 500 zł za każdy taki przypadek.
6.Łączna wysokość naliczonych WYKONAWCY kar umownych z jednego lub kilku tytułów nie może przekroczyć limitu 20 % wynagrodzenia netto, o którym mowa w § 5 ust. 1.

Odpowiedź:
Zamawiający nie wyraża zgody na zmianę zapisów § 7 wzoru umowy.
Zamawiający podtrzymuje zapisy SWZ.

Zapytanie nr 4 z dnia 01.06.2023

Pytanie 1:
Dotyczy: Załącznik nr 2 do SWZ - Umowa, § 10, Wymagania gwarancji i serwisu, pkt 7
Czy Zamawiający jako awarie rozumie zdarzenie, w którym uszkodzeniu uległ lub błędnie działa jeden (lub więcej) komponent wdrożonego rozwiązania w sposób całkowicie uniemożliwiający Zamawiającemu wykorzystanie go zgodnie z jego przeznaczeniem?

Odpowiedź:
Zamawiający jako awarie rozumie zdarzenie, w którym uszkodzeniu uległ lub błędnie działa jeden (lub więcej) komponent wdrożonego rozwiązania w sposób całkowicie uniemożliwiający Zamawiającemu wykorzystanie go zgodnie z jego przeznaczeniem.
Dodatkowo Zamawiający uznał za konieczne dokonanie zmiany treści § 10 ust. 6 oraz modyfikuje treść § 10 ust. 7 wzoru umowy, które otrzymują następujące brzmienie:
„6.Przyjmowanie przez Wykonawcę zgłoszeń serwisowych będzie realizowane w trybie 24/7/365 (24 godziny dziennie, 7 dni w tygodniu, 365 dni w roku) z czasem reakcji na zgłoszenie serwisowe do 6 godzin. Wraz z dostawą WYKONAWCA dołączy oświadczenie z danymi kontaktowymi (adres, numery telefonu i faksu, adresy WWW oraz email), na które ZAMAWIAJĄCY będzie zgłaszać usterki i awarie. WYKONAWCA będzie pośredniczył w przekazywaniu zgłoszeń do producenta urządzeń. Za moment zgłoszenia usterki uważa się telefoniczne lub elektroniczne przekazanie informacji o usterce lub awarii.
7. Czas naprawy (przywrócenia funkcjonalności) przedmiotu umowy (produktów, oprogramowania i funkcjonalności) nie może przekroczyć 3 (trzech) dni roboczych od dnia zgłoszenia serwisowego. Usunięcie awarii oznacza przywrócenie przez WYKONAWCĘ produktu (składowej przedmiotu umowy) do pełnej sprawności lub dostarczenie produktu zamiennego (model i parametry identyczne lub lepsze jak urządzenie, które uległo awarii), które przywróci funkcjonalność przedmiotu umowy."
Zamawiający dokonał zmian w zapisach § 10 umowy ust.6, 7.

Pytanie 2:
Dotyczy: Załącznik nr 2 do SWZ - Umowa, § 10
Wymagania gwarancji i serwisu, pkt 7. Oferent nie jest właścicielem i nie może modyfikować kodu źródłowego dostarczonego rozwiązania. W związku z tym nie ma wpływu na czas naprawy usterki oprogramowania. Jednocześnie producent oferowanego rozwiązania gwarantuje czas naprawy lub wymiany jedynie dla dostarczonego sprzętu. Czy w związku z tym Zamawiający może ograniczyć wymagany czas naprawy do sprzętu.

Odpowiedź:
Analogicznie jak w pytaniu poprzednim Zamawiający jako awarie rozumie zdarzenie, w którym uszkodzeniu uległ lub błędnie działa jeden (lub więcej) komponent wdrożonego rozwiązania w sposób całkowicie uniemożliwiający Zamawiającemu wykorzystanie go zgodnie z jego przeznaczeniem i również dotyczy to awarii/usterek oprogramowania, które całkowicie uniemożliwiają funkcjonowanie wdrożonego rozwiązania zgodnie z jego przeznaczeniem.
Wobec powyższego Zamawiający uznał za konieczne dokonanie zmiany treści §10 ust. 6 oraz modyfikuje treść § 10 ust. 7 wzoru umowy, wydłużając czas naprawy (przywrócenia funkcjonalności) przedmiotu umowy (produktów, oprogramowania i funkcjonalności) do 3 dni roboczych.
Zamawiający dokonał zmian w zapisach § 10 ust.6, 7 umowy.

Pytanie 3:
Czy Zamawiający wyrazi zgodę, aby przedmiotowe środki dowodowe w postaci kart katalogowych oferowanych rozwiązań zostały złożone przez Wykonawcę w języku angielskim bez tłumaczenia.

Odpowiedź 3:
Zamawiający dopuszcza możliwość, aby przedmiotowe środki dowodowe w postaci kart katalogowych oferowanych rozwiązań zostały złożone przez Wykonawcę w języku angielskim bez tłumaczenia.
Zamawiający dokonał zmian w zapisach SWZ.

Opublikowane wyjaśnienia są wiążące i dotyczą wszystkich uczestników postępowania.

Jednocześnie zamawiający informuje, że zmiany do SWZ zostały opublikowane na stronie prowadzonego postępowania w dniu 07 czerwca 2023 roku, nr pisma BF-IV.2370.8.2023.24

KOMENDANT GŁÓWNY
PAŃSTWOWEJ STRAŻY POŻARNEJ
z up.

nadbryg. Krzysztof Hejduk
Zastępca Komendanta Głównego