Ogłoszenie nr 560294-N-2020 z dnia 2020-07-09 r.

Miasto Rybnik: Zakup i dostawa Firewall Miejskiej Sieci Szerokopasmowej

OGŁOSZENIE O ZAMÓWIENIU - Dostawy

Zamieszczanie ogłoszenia: Zamieszczanie obowiązkowe

Ogłoszenie dotyczy: Zamówienia publicznego

Zamówienie dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej

Nie

Nazwa projektu lub programu

O zamówienie mogą ubiegać się wyłącznie zakłady pracy chronionej oraz wykonawcy, których działalność, lub działalność ich wyodrębnionych organizacyjnie jednostek, które będą realizowały zamówienie, obejmuje społeczną i zawodową integrację osób będących członkami grup społecznie marginalizowanych

Nie

Należy podać minimalny procentowy wskaźnik zatrudnienia osób należących do jednej lub więcej kategorii, o których mowa w art. 22 ust. 2 ustawy Pzp, nie mniejszy niż 30%, osób zatrudnionych przez zakłady pracy chronionej lub wykonawców albo ich jednostki (w %)

SEKCJA I: ZAMAWIAJĄCY

Postępowanie przeprowadza centralny zamawiający

Nie

Postępowanie przeprowadza podmiot, któremu zamawiający powierzył/powierzyli przeprowadzenie postępowania

Nie

Informacje na temat podmiotu któremu zamawiający powierzył/powierzyli prowadzenie postępowania:

Postępowanie jest przeprowadzane wspólnie przez zamawiających

Nie

Jeżeli tak, należy wymienić zamawiających, którzy wspólnie przeprowadzają postępowanie oraz podać adresy ich siedzib, krajowe numery identyfikacyjne oraz osoby do kontaktów wraz z danymi do kontaktów:

Postępowanie jest przeprowadzane wspólnie z zamawiającymi z innych państw członkowskich Unii Europejskiej

Nie

W przypadku przeprowadzania postępowania wspólnie z zamawiającymi z innych państw członkowskich Unii Europejskiej – mające zastosowanie krajowe prawo zamówień publicznych:

Informacje dodatkowe:

I. 1) NAZWA I ADRES: Miasto Rybnik, krajowy numer identyfikacyjny 27625543000000, ul. Bolesława Chrobrego 2 , 44-200 Rybnik, woj. śląskie, państwo Polska, tel. +48324392302, e-mail zam_pub@um.rybnik.pl, faks +48324224124.

Adres strony internetowej (URL): www.rybnik.eu

Adres profilu nabywcy:

Adres strony internetowej pod którym można uzyskać dostęp do narzędzi i urządzeń lub formatów plików, które nie są ogólnie dostępne

I. 2) RODZAJ ZAMAWIAJĄCEGO: Administracja samorządowa

I.3) WSPÓLNE UDZIELANIE ZAMÓWIENIA *(jeżeli dotyczy)*:

Podział obowiązków między zamawiającymi w przypadku wspólnego przeprowadzania postępowania, w tym w przypadku wspólnego przeprowadzania postępowania z zamawiającymi z innych państw członkowskich Unii Europejskiej (który z zamawiających jest odpowiedzialny za przeprowadzenie postępowania, czy i w jakim zakresie za przeprowadzenie postępowania odpowiadają pozostali zamawiający, czy zamówienie będzie udzielane przez każdego z zamawiających indywidualnie, czy zamówienie zostanie udzielone w imieniu i na rzecz pozostałych zamawiających):

I.4) KOMUNIKACJA:

Nieograniczony, pełny i bezpośredni dostęp do dokumentów z postępowania można uzyskać pod adresem (URL)

Tak

bip.um.rybnik.eu

Adres strony internetowej, na której zamieszczona będzie specyfikacja istotnych warunków zamówienia

Tak

bip.um.rybnik.eu

Dostęp do dokumentów z postępowania jest ograniczony - więcej informacji można uzyskać pod adresem

Nie

Oferty lub wnioski o dopuszczenie do udziału w postępowaniu należy przesyłać:

Elektronicznie

Nie

adres

Dopuszczone jest przesłanie ofert lub wniosków o dopuszczenie do udziału w postępowaniu w inny sposób:

Tak

Inny sposób:

drogą elektroniczną za pośrednictwem https://miniportal.uzp.gov.pl/

Wymagane jest przesłanie ofert lub wniosków o dopuszczenie do udziału w postępowaniu w inny sposób:

Tak

Inny sposób:

forma pisemna

Adres:

Urząd Miasta Rybnika, ul. Bolesława Chrobrego 2, pok. 302, Wydział Zamówień Publicznych

Komunikacja elektroniczna wymaga korzystania z narzędzi i urządzeń lub formatów plików, które nie są ogólnie dostępne

Nie

Nieograniczony, pełny, bezpośredni i bezpłatny dostęp do tych narzędzi można uzyskać pod adresem: (URL)

SEKCJA II: PRZEDMIOT ZAMÓWIENIA

II.1) Nazwa nadana zamówieniu przez zamawiającego: Zakup i dostawa Firewall Miejskiej Sieci Szerokopasmowej

Numer referencyjny: ZP.271.45.2020

Przed wszczęciem postępowania o udzielenie zamówienia przeprowadzono dialog techniczny

Nie

II.2) Rodzaj zamówienia: Dostawy

II.3) Informacja o możliwości składania ofert częściowych

Zamówienie podzielone jest na części:

Nie

Oferty lub wnioski o dopuszczenie do udziału w postępowaniu można składać w odniesieniu do:

Zamawiający zastrzega sobie prawo do udzielenia łącznie następujących części lub grup części:

Maksymalna liczba części zamówienia, na które może zostać udzielone zamówienie jednemu wykonawcy:

II.4) Krótki opis przedmiotu zamówienia *(wielkość, zakres, rodzaj i ilość dostaw, usług lub robót budowlanych lub określenie zapotrzebowania i wymagań)* **a w przypadku partnerstwa innowacyjnego - określenie zapotrzebowania na innowacyjny produkt, usługę lub roboty budowlane:** Przedmiotem zamówienia jest dostawa wraz z uruchomieniem dwóch urządzeń typu firewall na potrzeby Miejskiej Sieci Szerokopasmowej (MSS) na warunkach wskazanych poniżej. Realizacja przedmiotu zamówienia obejmuje: 1) dostawę firewall nowej generacji z licencją IPS – 2 urządzenia, 2) montaż ww. urządzeń, 3) przeniesienie konfiguracji z obecnie działających firewalli CISCO ASA 5540, 4) szkolenie z obsługi dla administratorów MSS, 5) świadczenie usług gwarancyjnych w oparciu o serwis producenta na okres 36-mc, w tym aktualizacja oprogramowania systemowego dostarczonych urządzeń. Architektura urządzenia, obudowa, interfejsy 1) Urządzenie będące dedykowaną platformą sprzętową – Zamawiający nie dopuszcza rozwiązań „serwerowych/wirtualnych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. 2) Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall). 3) Urządzenie wyposażone w min. 8 portów SFP RJ45 oraz min. 4 porty SFP. 4) Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1 000 sieci VLAN. 5) Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band . 6) Urządzenie wyposażone w port USB 3.0. 7) Zasilacz umożliwiający zasilanie prądem przemiennym 230V. 8) Możliwość montażu w szafie rack 19" (dołączone niezbędne elementy montażowe). 9) Wysokość urządzenia 1U. Parametry wydajnościowe 1) Przepustowość urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie min. 2 Gbps dla pakietów wielkości 1024B. 2) Przepustowość urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) wraz z uruchomionym silnikiem IPS (Intrusion Prevention System) na poziomie min. 2 Gbps dla pakietów wielkości 1024B. 3) Min. 350 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 20 000 nowych połączeń na sekundę. 4) Możliwość połączenia VPN do 400 urządzeń z maksymalną sumaryczną przepustowością min 1 Gbps dla pakietów 1024B TCP. 5) Przepustowość dekrypcji ruchu szyfrowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048B) wynosi min. 1 Gbps. 6) Maksymalna ilość „wirtualny/logiczno firewalla" – 5, przy dostawie urządzenia należy dostarczyć 2 dla każdego urządzenia. Funkcjonalność urządzenia 1) Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. 2) Możliwość uruchomienia urządzenia w trybie firewall'a L3, jak i w trybie transparentnym. 3) Urządzenie

obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP) . 4) Urządzenie umożliwia separację ruchu w warstwie L3 w ramach jednej instancji firewalla poprzez tworzenie osobnych tablic routingu. 5) Urządzenie umożliwia utworzenia min. 2 tablic rutingu. 6) Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory. 7) Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT). 8) Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby. 9) Urządzanie zapewnia możliwość obsługi użytkowników zdalnych VPN (RA VPN). 10) Urządzenie zapewnia funkcjonalności: a) systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control), b) systemu IPS, c) systemu ochrony przed malware, d) systemu filtracji ruchu w oparciu o URL, 11) Wraz z urządzeniem należy dostarczyć licencję/subskrybcję systemu IPS na min. 3 lata. 12) System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów: a) wiedza o użytkownikach – uwierzytelnienie, b) wiedza o urządzeniach – pasywne skanowanie ruchu, c) wiedza o urządzeniach mobilnych, d) wiedza o aplikacjach wykorzystywanych po stronie klienta, e) wiedza o podatnościach, f) wiedza o bieżących zagrożeniach, g) baza danych URL. 13) System posiada otwarte API dla współpracy z systemami zewnętrznymi. 14) Rozwiązanie współpracuje z systemami SIEM (Security Information and Event Management). 15) System wykrywania aplikacji AVC zapewniający: a) możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji, b) możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług, c) wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji, d) współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach. 16) System IPS zapewniający: a) możliwość pracy w trybie in-line, b) możliwość pracy w trybie pasywnym (IDS), c) możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym: - złośliwe oprogramowanie, - skanowanie sieci, - ataki na usługę VoIP, - próby przepełnienia bufora, - ataki na aplikacje P2P, - zagrożenia dnia zerowego, d) możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna), e) wiele sposobów wykrywania zagrożeń w tym: - sygnatury ataków opartych na exploitach, - reguły oparte na zagrożeniach, - mechanizm wykrywania anomalii w protokołach, - mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego, f) możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu, g) mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives), h) możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń, i) wiele możliwości reakcji na zdarzenia w tym takie, jak: - tylko monitorowanie, - blokowanie ruchu zawierającego zagrożenia, - zastąpienie zawartości pakietów, - zapisywanie pakietów, j) możliwość detekcji ataków i zagrożeń opartych na protokole IPv6, k) możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o: - systemach operacyjnych, - serwisach, - otwartych portach, aplikacjach , - zagrożeniach, l) możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych, m) możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp., n) możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji, o) możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego, p) mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne, q) możliwość definiowania wyjątków dla sygnatur z określeniem

adresów IP źródła, przeznaczenia lub obu jednocześnie, r) obsługę reguł system wykrywania włamań Snort, s) możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS, t) mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise), u) mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa. 17) System filtracji URL zapewniający: a) kategoryzację stron – w co najmniej 80 kategoriach, b) bazę URL o wielkości nie mniejszej niż 280 mln URL, c) bazę URL producenta rozwiązania. 18) Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym: a) pliki systemowe, b) pliki graficzne, c) pliki PDF, d) pliki wykonywalne, e) pliki multimedialne, f) pliki pakietu Office, g) pliki skompresowane. 19) Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download. 20) Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez: a) sprawdzenie reputacji plików w systemie globalnym, b) sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze), c) statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu. 21) Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach: a) pliki wolne od złośliwego kod, b) pliki zawierające złośliwy kod, c) pliki podejrzane, d) pliki o własnej, zdefiniowanej przez użytkownika kategorii. 22) Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna). Zarządzanie urządzeniem Wraz z urządzeniem Wykonawca zobowiązany jest dostarczyć dedykowaną platformę zarządzającą opartą na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym. Platforma zarządzająca może mieć formę maszyny wirtualnej pracującej pod kontrolę Kernel Based Virtual Machines (KVM) i spełnia następujące wymagania: 1) umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym, 2) jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego, 3) zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria, 4) ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm, 5) ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami, 6) zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany, 7) zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS, 8) zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją, 9) ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci, 10) daje możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszenie reakcji na zagrożenia poprzez automatyczną priorytetyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta, 11) ma możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora, 12) zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS, 13) ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej, 14) zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania, 15) zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu, 16) zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP, 17) zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze, 18) zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika, 19) zapewnia

informowanie o zagrożeniach poprzez: a) wysłanie e-maila, b) wyslanie trap SNMP, c) przesłanie informacji do serwera Syslog, d) uruchomienie skryptu użytkownika, e) wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane łącze. 20) posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy: a) aktualnego stanu danego urządzenia, b) podglądu historii dostępnych zasobów, c) możliwość eliminacji powtarzających się alarmów (tzw. Black Listing). 21) ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym, 22) ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników: a) dozwolone porty i protokoły, b) dozwolone aplikacje według różnych kategorii, c) dozwolone kategorie stron internetowych (URL filtering), d) dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej, e) sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne. 23) w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia. 24) posiada wbudowany edytor reguł IPS w formacie Snort oraz własnych detektorów aplikacji w języku LUA, 25) posiada wbudowane narzędzie do obsługi informacji o zagrożeniach z wielu źródeł poprzez STIX/TAXII, importu przez URL oraz uploadu z lokalnego komputera. Zgodnie z art. 30 ust 5 ustawy wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy, usługi lub roboty budowlane spełniają wymagania określone przez Zamawiającego.

II.5) Główny kod CPV: 32420000-3

Dodatkowe kody CPV:

Kod CPV
32410000-0

II.6) Całkowita wartość zamówienia *(jeżeli zamawiający podaje informacje o wartości zamówienia)*:

Wartość bez VAT: 150000,00

Waluta:

PLN

(w przypadku umów ramowych lub dynamicznego systemu zakupów – szacunkowa całkowita maksymalna wartość w całym okresie obowiązywania umowy ramowej lub dynamicznego systemu zakupów)

II.7) Czy przewiduje się udzielenie zamówień, o których mowa w art. 67 ust. 1 pkt 6 i 7 lub w art. 134 ust. 6 pkt 3 ustawy Pzp: Nie

Określenie przedmiotu, wielkości lub zakresu oraz warunków na jakich zostaną udzielone zamówienia, o których mowa w art. 67 ust. 1 pkt 6 lub w art. 134 ust. 6 pkt 3 ustawy Pzp:

II.8) Okres, w którym realizowane będzie zamówienie lub okres, na który została zawarta umowa ramowa lub okres, na który został ustanowiony dynamiczny system zakupów:

miesiącach: 2 *lub* **dniach:**

lub

data rozpoczęcia: *lub* **zakończenia:**

II.9) Informacje dodatkowe:

SEKCJA III: INFORMACJE O CHARAKTERZE PRAWNYM, EKONOMICZNYM, FINANSOWYM I TECHNICZNYM

III.1) WARUNKI UDZIAŁU W POSTĘPOWANIU

III.1.1) Kompetencje lub uprawnienia do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów

Określenie warunków:

Informacje dodatkowe

III.1.2) Sytuacja finansowa lub ekonomiczna

Określenie warunków:

Informacje dodatkowe

III.1.3) Zdolność techniczna lub zawodowa

Określenie warunków: - Wykonawca spełni warunek, jeżeli wykaże, że wykonał w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy to w tym okresie, co najmniej jedno zamówienie polegające na dostawie i skonfigurowaniu firewalla o wartości minimum 70.000 zł brutto. W przypadku zamówień, których wartość została wyrażona w umowie w innej walucie niż PLN należy dokonać przeliczenia tej waluty na PLN przy zastosowaniu średniego kursu NBP na dzień zakończenia zamówienia (w przypadku zamówień rozliczanych wyłącznie w walutach innych niż PLN). Warunek musi być spełniony: 1) przez Wykonawcę samodzielnie lub 2) przez minimum jeden podmiot udostępniający wiedzę i doświadczenie (podwykonawcę) samodzielnie; 3) w przypadku Wykonawców występujących wspólnie, samodzielnie przez minimum jednego z Wykonawców występujących wspólnie. Nie jest dopuszczalne łączenie (sumowanie) wyżej wymaganego doświadczenia w ramach doświadczenia różnych podmiotów zaangażowanych w realizację zamówienia. W sytuacji, gdy Wykonawca polega na doświadczeniu grupy Wykonawców, której był członkiem (np. Konsorcjum), doświadczenie będzie oceniane w zależności od konkretnego zakresu udziału tego Wykonawcy, a więc jego faktycznego wkładu w prowadzenie działań, które były wymagane od tej grupy w ramach zamówienia publicznego wykazanego na potwierdzenie spełniania warunku udziału w postępowaniu. - Wykonawca spełni warunek, jeżeli skieruje do realizacji zamówienia publicznego osobę, która będzie pełniła funkcję specjalisty systemów zabezpieczeń posiadającą certyfikat Cisco Certified Network Professional.

Zamawiający wymaga od wykonawców wskazania w ofercie lub we wniosku o dopuszczenie do udziału w postępowaniu imion i nazwisk osób wykonujących czynności przy realizacji zamówienia wraz z informacją o kwalifikacjach zawodowych lub doświadczeniu tych osób: Tak

Informacje dodatkowe:

III.2) PODSTAWY WYKLUCZENIA

III.2.1) Podstawy wykluczenia określone w art. 24 ust. 1 ustawy Pzp

III.2.2) Zamawiający przewiduje wykluczenie wykonawcy na podstawie art. 24 ust. 5 ustawy Pzp Nie Zamawiający przewiduje następujące fakultatywne podstawy wykluczenia:

III.3) WYKAZ OŚWIADCZEŃ SKŁADANYCH PRZEZ WYKONAWCĘ W CELU WSTĘPNEGO POTWIERDZENIA, ŻE NIE PODLEGA ON WYKLUCZENIU ORAZ SPEŁNIA WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ SPEŁNIA KRYTERIA SELEKCJI

Oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu

Tak

Oświadczenie o spełnianiu kryteriów selekcji

Nie

III.4) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW , SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI, O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 3 USTAWY PZP:

III.5) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI, O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 1 USTAWY PZP

III.5.1) W ZAKRESIE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU:

1. Wykonawca, którego oferta zostanie najwyżej oceniona, zostanie wezwany do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów potwierdzających spełnianie przez Wykonawcę warunków udziału w postępowaniu, tj. 1) wykaz dostaw wykonanych w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane na formularzu zgodnym z treścią załącznika nr 5 do SIWZ, oraz załączeniem dowodów określających czy te dostawy zostały wykonane należycie, przy czym dowodami o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy. 2) wykaz osób, skierowanych przez Wykonawcę do realizacji zamówienia publicznego na formularzu zgodnym z treścią załącznika nr 6 do SIWZ, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości lub kierowanie robotami budowlanymi, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami. 2. Wykonawca, którego oferta zostanie najwyżej oceniona, na wezwanie Zamawiającego zobowiązany będzie złożyć oświadczenia i dokumenty podmiotu, na zdolności lub sytuację którego Wykonawca powoływał się w celu wykazania spełniania warunków udziału w postępowaniu. Wykonawca zobowiązany będzie złożyć dokumenty tego podmiotu potwierdzające spełnianie warunków udziału w postępowaniu w zakresie zdolności lub sytuacji, na których Wykonawca polegał w celu wykazania spełniania tych warunków.

III.5.2) W ZAKRESIE KRYTERIÓW SELEKCJI:

III.6) WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW SKŁADANYCH PRZEZ WYKONAWCĘ W POSTĘPOWANIU NA WEZWANIE ZAMAWIAJACEGO W CELU POTWIERDZENIA OKOLICZNOŚCI, O KTÓRYCH MOWA W ART. 25 UST. 1 PKT 2 USTAWY PZP

III.7) INNE DOKUMENTY NIE WYMIENIONE W pkt III.3) - III.6)

1. Formularz oferty. 2. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia. 3. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenie o niepodleganiu wykluczeniu oraz spełnianiu warunków udziału w postępowaniu, składa każdy z Wykonawców wspólnie ubiegających się o

zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia. 4. Pełnomocnictwo złożone w formie oryginału lub notarialnie poświadczonej kopii w sytuacji: 1) Wykonawców wspólnie ubiegających się o udzielenie zamówienia - pełnomocnictwo do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia. Pełnomocnik może być ustanowiony do reprezentowania Wykonawców w postępowaniu albo do reprezentowania w postępowaniu i zawarcia umowy. 2) podpisania oferty względnie innych dokumentów składanych wraz z ofertą przez osobę, dla której prawo do ich podpisania nie wynika wprost z dokumentu stwierdzającego status prawny Wykonawcy (np. wypisu z Krajowego rejestru sądowego) – pełnomocnictwo do podpisania oferty. 5. Wykonawca, w terminie 3 dni od zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5, przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. Zamawiający zamieści informacje, o których mowa w art. 86 ust. 5 ustawy w pliku o nazwie „Zbiorcze zestawienie ofert" na swojej stronie internetowej www.bip.um.rybnik.eu.

SEKCJA IV: PROCEDURA

IV.1) OPIS

IV.1.1) Tryb udzielenia zamówienia: Przetarg nieograniczony

IV.1.2) Zamawiający żąda wniesienia wadium:

Nie

Informacja na temat wadium

IV.1.3) Przewiduje się udzielenie zaliczek na poczet wykonania zamówienia:

Nie

Należy podać informacje na temat udzielania zaliczek:

IV.1.4) Wymaga się złożenia ofert w postaci katalogów elektronicznych lub dołączenia do ofert katalogów elektronicznych:

Nie

Dopuszcza się złożenie ofert w postaci katalogów elektronicznych lub dołączenia do ofert katalogów elektronicznych:

Nie

Informacje dodatkowe:

IV.1.5.) Wymaga się złożenia oferty wariantowej:

Nie

Dopuszcza się złożenie oferty wariantowej

Nie

Złożenie oferty wariantowej dopuszcza się tylko z jednoczesnym złożeniem oferty zasadniczej:

Nie

IV.1.6) Przewidywana liczba wykonawców, którzy zostaną zaproszeni do udziału w postępowaniu

(przetarg ograniczony, negocjacje z ogłoszeniem, dialog konkurencyjny, partnerstwo innowacyjne)

Liczba wykonawców

Przewidywana minimalna liczba wykonawców

Maksymalna liczba wykonawców

Kryteria selekcji wykonawców:

IV.1.7) Informacje na temat umowy ramowej lub dynamicznego systemu zakupów:

Umowa ramowa będzie zawarta:

Czy przewiduje się ograniczenie liczby uczestników umowy ramowej:

Nie

Przewidziana maksymalna liczba uczestników umowy ramowej:

Informacje dodatkowe:

Zamówienie obejmuje ustanowienie dynamicznego systemu zakupów:

Nie

Adres strony internetowej, na której będą zamieszczone dodatkowe informacje dotyczące dynamicznego systemu zakupów:

Informacje dodatkowe:

W ramach umowy ramowej/dynamicznego systemu zakupów dopuszcza się złożenie ofert w formie katalogów elektronicznych:

Przewiduje się pobranie ze złożonych katalogów elektronicznych informacji potrzebnych do sporządzenia ofert w ramach umowy ramowej/dynamicznego systemu zakupów:

IV.1.8) Aukcja elektroniczna

Przewidziane jest przeprowadzenie aukcji elektronicznej *(przetarg nieograniczony, przetarg ograniczony, negocjacje z ogłoszeniem)* Nie

Należy podać adres strony internetowej, na której aukcja będzie prowadzona:

Należy wskazać elementy, których wartości będą przedmiotem aukcji elektronicznej:

Przewiduje się ograniczenia co do przedstawionych wartości, wynikające z opisu przedmiotu zamówienia:

Należy podać, które informacje zostaną udostępnione wykonawcom w trakcie aukcji elektronicznej oraz jaki będzie termin ich udostępnienia:

Informacje dotyczące przebiegu aukcji elektronicznej:

Jaki jest przewidziany sposób postępowania w toku aukcji elektronicznej i jakie będą warunki, na jakich wykonawcy będą mogli licytować (minimalne wysokości postąpień):

Informacje dotyczące wykorzystywanego sprzętu elektronicznego, rozwiązań i specyfikacji technicznych w zakresie połączeń:

Wymagania dotyczące rejestracji i identyfikacji wykonawców w aukcji elektronicznej:

Informacje o liczbie etapów aukcji elektronicznej i czasie ich trwania:

Czas trwania:

Czy wykonawcy, którzy nie złożyli nowych postąpień, zostaną zakwalifikowani do następnego etapu:

Warunki zamknięcia aukcji elektronicznej:

IV.2) KRYTERIA OCENY OFERT

IV.2.1) Kryteria oceny ofert:

IV.2.2) Kryteria

Kryteria	Znaczenie
Cena	60,00
Gwarancja i serwis	40,00

IV.2.3) Zastosowanie procedury, o której mowa w art. 24aa ust. 1 ustawy Pzp (przetarg nieograniczony)

Tak

IV.3) Negocjacje z ogłoszeniem, dialog konkurencyjny, partnerstwo innowacyjne

IV.3.1) Informacje na temat negocjacji z ogłoszeniem

Minimalne wymagania, które muszą spełniać wszystkie oferty:

Przewidziane jest zastrzeżenie prawa do udzielenia zamówienia na podstawie ofert wstępnych bez przeprowadzenia negocjacji

Przewidziany jest podział negocjacji na etapy w celu ograniczenia liczby ofert:

Należy podać informacje na temat etapów negocjacji (w tym liczbę etapów):

Informacje dodatkowe

IV.3.2) Informacje na temat dialogu konkurencyjnego

Opis potrzeb i wymagań zamawiającego lub informacja o sposobie uzyskania tego opisu:

Informacja o wysokości nagród dla wykonawców, którzy podczas dialogu konkurencyjnego przedstawili rozwiązania stanowiące podstawę do składania ofert, jeżeli zamawiający przewiduje nagrody:

Wstępny harmonogram postępowania:

Podział dialogu na etapy w celu ograniczenia liczby rozwiązań:

Należy podać informacje na temat etapów dialogu:

Informacje dodatkowe:

IV.3.3) Informacje na temat partnerstwa innowacyjnego

Elementy opisu przedmiotu zamówienia definiujące minimalne wymagania, którym muszą odpowiadać wszystkie oferty:

Podział negocjacji na etapy w celu ograniczeniu liczby ofert podlegających negocjacjom poprzez zastosowanie kryteriów oceny

ofert wskazanych w specyfikacji istotnych warunków zamówienia:

Informacje dodatkowe:

IV.4) Licytacja elektroniczna

Adres strony internetowej, na której będzie prowadzona licytacja elektroniczna:

Adres strony internetowej, na której jest dostępny opis przedmiotu zamówienia w licytacji elektronicznej:

Wymagania dotyczące rejestracji i identyfikacji wykonawców w licytacji elektronicznej, w tym wymagania techniczne urządzeń informatycznych:

Sposób postępowania w toku licytacji elektronicznej, w tym określenie minimalnych wysokości postąpień:

Informacje o liczbie etapów licytacji elektronicznej i czasie ich trwania:

Czas trwania:

Wykonawcy, którzy nie złożyli nowych postąpień, zostaną zakwalifikowani do następnego etapu:

Termin składania wniosków o dopuszczenie do udziału w licytacji elektronicznej:

Data: godzina:

Termin otwarcia licytacji elektronicznej:

Termin i warunki zamknięcia licytacji elektronicznej:

Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, albo ogólne warunki umowy, albo wzór umowy:

Wymagania dotyczące zabezpieczenia należytego wykonania umowy:

Informacje dodatkowe:

IV.5) ZMIANA UMOWY

Przewiduje się istotne zmiany postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy: Nie

Należy wskazać zakres, charakter zmian oraz warunki wprowadzenia zmian:

IV.6) INFORMACJE ADMINISTRACYJNE

IV.6.1) Sposób udostępniania informacji o charakterze poufnym *(jeżeli dotyczy):*

Środki służące ochronie informacji o charakterze poufnym

IV.6.2) Termin składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu:

Data: 2020-07-23, godzina: 09:00,

Skrócenie terminu składania wniosków, ze względu na pilną potrzebę udzielenia zamówienia (przetarg nieograniczony, przetarg ograniczony, negocjacje z ogłoszeniem):

Nie

Wskazać powody:

Język lub języki, w jakich mogą być sporządzane oferty lub wnioski o dopuszczenie do udziału w postępowaniu

> język polski

IV.6.3) Termin związania ofertą: do: okres w dniach: 30 (od ostatecznego terminu składania ofert)

IV.6.4) Przewiduje się unieważnienie postępowania o udzielenie zamówienia, w przypadku nieprzyznania środków, które miały być przeznaczone na sfinansowanie całości lub części zamówienia: Nie

IV.6.5) Informacje dodatkowe:

ZAŁĄCZNIK I - INFORMACJE DOTYCZĄCE OFERT CZĘŚCIOWYCH