Załącznik nr 2 do SIWZ

Pieczątka firmowa Wykonawcy

Nr postępowania: ZP/240/055/D/16

OFERTA

Zamawiający:
Politechnika Gdańska
ul. G. Narutowicza 11/12
80-233 Gdańsk

Nawiązując do ogłoszenia o postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie przetargu nieograniczonego na **dostawę wraz z usługą wdrożenia urządzeń do transmisji danych cyfrowych dla Centrum Usług Informatycznych Politechniki Gdańskiej,**

my niżej podpisani:

imię ..... nazwisko .....

imię ..... nazwisko .....

działający w imieniu i na rzecz:

Pełna nazwa Wykonawcy:	
Adres Wykonawcy:	
Regon nr:	NIP nr:
Nr telefonu:	Nr faksu:
e-mail do kontaktu:	
Nazwa banku:	Nr rachunku bankowego:

1. **Oferuję (oferujemy)** realizację przedmiotu zamówienia, zgodnie z wymogami Specyfikacji Istotnych Warunków Zamówienia:

   za cenę brutto: ..... PLN,

   słownie:
   ..... .
2. **Oświadczam (oświadczamy)**, że oferowane urządzenia do transmisji danych cyfrowych spełniają wymagania podstawowe określone przez Zamawiającego w Załączniku nr 1 do SIWZ – Szczegółowym opisie przedmiotu zamówienia.
3. **Oświadczam (oświadczamy)**, że oferowane urządzenia do transmisji danych cyfrowych spełniają wymagania dodatkowe określone przez Zamawiającego w Załączniku nr 1 do SIWZ – Szczegółowym opisie przedmiotu zamówienia, będące podstawą oceny ofert, zgodnie z poniższą tabelą:

L.p.	Kryterium	Wymagania dodatkowe	TAK/NIE*
1	Rozbudowa urządzenia	Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego posiadające budowę modularną zapewniającą co najmniej trzy sloty pozwalające na ich wyposażenie w moduły co najmniej: a) 8-portowe 10/100/1000BASE-T RJ45, b) 4-portowe 1GE SFP, c) 4-portowe 10GE SFP+, d) 2-portowe 40GE QSFP+.	
2	URL filtering oraz Identyfikacja użytkownika	1. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które posiada bazę znanych aplikacji większą niż 7000 pozycji oraz wspiera rozpoznawanie minimum 260.000 widgetów WEB 2.0. 2. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które do automatycznego wykrywania i klasyfikowania aplikacji korzysta z lokalnego cache w celem optymalizacji tego mechanizmu. 3. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które do filtrowania URL pozwala na kategoryzację względem ryzyka danego adresu. 4. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które wspiera obsługę nagłówków pozwalających na identyfikację użytkownika np. X-forwarded.	
3	Zaawansowane funkcjonalności eliminacji ataków zero-day	1. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym które poza modułem umożliwiającym analizę podejrzanych plików w wydzielonym środowisku emulacyjnym, realizuje funkcję dostarczania bezpiecznych plików poprzez usunięcie z nich zawartości aktywnej. 2. Administrator musi mieć możliwość utworzenia listy adresatów oraz nadawców poczty e-mail, którzy mają być wykluczeni z inspekcji plików.	
4	Zaawansowane funkcjonalności administrowania	1. Urządzenie do korelacji zdarzeń i raportowania wyposażone w mechanizm który umożliwia administratorowi tworzenie własnych reguł korelacji. 2. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego którego system zarządzania: 2.1 dokonuje weryfikacja poprawności konfiguracji przez jej zainstalowaniem, 2.2 umożliwia wersjonowanie konfiguracji i pozwala na pracę na kilku (minimum 5) zapisanych konfiguracjach, 2.3 zmiany w konfiguracji reguł bezpieczeństwa przeprowadza w trybie off-line oraz umożliwia wdrażanie spójnej polityki bezpieczeństwa na wszystkich posiadanych i obsługiwanych urządzeniach jednocześnie, 2.4 ma możliwość automatycznego wycofania zmian w trakcie wdrażania spójnej polityki bezpieczeństwa jeśli na jednym z urządzeń nowa polityka nie zostanie poprawnie zainstalowana, 3. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego którego system zarządzania umiejscowiony jest poza zamawianymi urządzeniami (np. na dedykowanej maszynie wirtualnej) 4. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego którego system zarządzania posługuje się bazę obiektów dla stosu IPv4 oraz IPv6 charakteryzującą się tym, że dla danego obiektu możemy przypisać jednocześnie adres IPv4 oraz IPv6 5. Urządzenie pełniące funkcję bramy bezpieczeństwa sieciowego które posiada wbudowane narzędzie diagnostyczne tcpdump dostępne z poziomu konsoli CLI zamawianych urządzeń.	

5	Integracja z posiadanymi przez zamawiającego systemami zarządzania firmy Check Point:	1. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym którego zarządzanie politykami bezpieczeństwa oraz konfiguracja urządzenia jest realizowane z poziomu posiadanego przez zamawiającego rozwiązania Check Point Security Management Server R77.30 2. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym które korelację zdarzeń i raportowanie realizuje z poziomu posiadanego przez Zamawiającego rozwiązania Check Point SmartEvent 3. Urządzenie wyposażone w system zarządzania konfiguracją oraz politykami bezpieczeństwa który integruje się w pełni z posiadanym przez zamawiającego rozwiązaniem Check Point Security Management Server R77.30 4. Urządzenia dające możliwość wykorzystania posiadanych przez zamawiającego licencji do uruchomienia funkcjonalności opisanych w OPZ	

* wpisać „TAK" lub „NIE"

4. **Oświadczam (oświadczamy),** że zamówienie zrealizuję (zrealizujemy) w terminie 21 dni od dnia zawarcia umowy.
5. **Oświadczam (oświadczamy),** że udzielam (udzielamy) 36 miesięcznej gwarancji na urządzenia do transmisji danych cyfrowych, liczonej od daty podpisania protokołu odbioru bez zastrzeżeń.
6. **Oświadczam (oświadczamy),** że w cenie oferty zostały uwzględnione wszystkie koszty niezbędne do prawidłowego, pełnego i terminowego wykonania przedmiotu zamówienia, w tym koszty dostawy, uruchomienia i wdrożenia urządzeń do transmisji danych cyfrowych, wykupienia subskrypcji i przeszkolenia personelu Zamawiającego.
7. **Oświadczam (oświadczamy),** że zapoznałem (zapoznaliśmy) się ze Specyfikacją Istotnych Warunków Zamówienia, nie wnoszę (nie wnosimy) do jej treści zastrzeżeń i uznaję (uznajemy) się za związanego (związanych) określonymi w niej postanowieniami i zasadami postępowania.
8. **Oświadczam (oświadczamy),** że zapoznałem (zapoznaliśmy) się z postanowieniami wzoru umowy, który stanowi załącznik nr 8 do SIWZ. Nie wnoszę (wnosimy) do jego treści zastrzeżeń. Zobowiązuję (zobowiązujemy) się, w przypadku wyboru mojej (naszej) oferty do zawarcia umowy na określonych w nim warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego.
9. **Oświadczam (oświadczamy),** że uważam (uważamy) się za związanego (związanych) niniejszą ofertą na czas wskazany w Specyfikacji Istotnych Warunków Zamówienia, czyli przez okres 60 dni od upływu terminu składania ofert.
10. **Oświadczam (oświadczamy),** że zamówienie zrealizuję (zrealizujemy) przy udziale podwykonawców, którzy będą realizować wymienione części (zakres) zamówienia:
    a) .....,
    b) .....
11. **Oświadczam (oświadczamy),** że akceptuję (akceptujemy) warunki płatności określone we wzorze umowy.
12. **Oświadczam (oświadczamy),** że wadium o wartości: **32000** zł, wniosłem (wnieśliśmy) w dniu ..... w formie (wpisać w jakiej) ..... .
13. **Oświadczam (oświadczamy),** że tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, które nie mogą być udostępnione, stanowią informacje zawarte w ofercie na stronach nr ..... . Do oferty załączam (załączamy) …….. , w których wykazuję (wykazujemy), że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.
14. Ofertę niniejszą składam (składamy) na ..... ponumerowanych stronach.
15. Załącznikami do niniejszej oferty, stanowiącymi jej integralną część są:

    1. .....
    2. .....
    3. .....
    4. .....
    5. .....
    6. .....

7. .....
8. .....
9. .....
10. .....

....., dn. .....

.....

(podpis i pieczątka osoby uprawnionej
do reprezentowania Wykonawcy)