DYREKTOR
BIURA ŁĄCZNOŚCI I INFORMATYKI
KOMENDY GŁÓWNEJ POLICJI

Warszawa, dnia 22.10.2015 r.

de-1305/15

Zapytanie ofertowe
do spr. 116/UM/BŁiI/WTWSPR/2015

1. Zamawiający:
   Komenda Główna Policji
   02-624 Warszawa ul. Puławska 148/150
   NIP 521-31-72-762

2. Opis przedmiotu zamówienia:

   Modernizacja, budowa redundancji oraz doposażenie węzła CPZ – załącznik nr 1 (projekt umowy wraz z OPZ)

3. Termin realizacji zamówienia:
   Wykonawca zobowiązuje się do dostarczenia Przedmiotu umowy do dnia 15 grudnia 2015 r. od daty zawarcia umowy, przy użyciu własnych środków transportu i na własny koszt.

4. Osoba wyznaczona do porozumiewania się z wykonawcami:
   Łukasz Pachocki, (022) 605 59 96

5. Kryteria wyboru ofert:
   Cena 100%

6. Wymagania, jakie powinni spełniać wykonawcy zamówienia:
   Projekt umowy wraz z załącznikami

7. Projekt umowy lub istotne postanowienia umowy, które zostaną zawarte w jej treści*:
   Projekt umowy wraz z załącznikami

8. Wymagania dotyczące zabezpieczenia należytego wykonania umowy, sposób oraz formę jego wniesienia*:
   Projekt umowy wraz z załącznikami

9. Warunki gwarancji i rękojmi (o ile nie zawiera ich projekt umowy)*:
   Projekt umowy wraz z załącznikami

10. Wykonanie usługi zostanie potwierdzone protokołem przez przedstawiciela Zamawiającego.
    Protokoły odbioru jakościowy i ilościowy

11. Sposób przygotowania oferty:

Oferta w formie pisemnej powinna zawierać następujące informacje:
- **cenę jednostkową netto (bez podatku VAT) i brutto (z podatkiem VAT, cena powinna uwzględniać wszystkie koszty) w złotych;**
- **potwierdzenie zaakceptowania punktów 1 – 11 wraz z załącznikami**
- **okres ważności oferty.**

12. Miejsce i termin złożenia oferty:
Ofertę należy przesłać faksem do Wydziału Technicznego Wsparcia Systemu Powiadamiania Ratunkowego Biura Łączności i Informatyki KGP na numer 226015747 lub adres e-mail: violetta.jankowska@policja.gov.pl do dnia 29.10.2015 r. godz. 15^{00}.

p.o. ZASTĘPCA DYREKTORA
BIURA [illegible]

.....
(podpis, pieczątka dyrektora biura, KGP)

[illegible]

Załączniki:
1. Projekt umowy

* - wypełnić jeżeli dotyczy;

Egz. Nr - ___

U M O W A nr 116/UM/WTWPSR/BŁiI/15

zawarta w Warszawie w dniu _____ 2015 r. pomiędzy:

Skarbem Państwa - Komendantem Głównym Policji z siedzibą w Warszawie przy ul. Puławskiej 148/150, zwanym w treści Umowy **„Zamawiającym"**, reprezentowanym przez:

1. ..... – Dyrektora Biura Łączności i Informatyki Komendy Głównej Policji

a

Firmą_____ z siedzibą _____ przy ul. _____ wpisaną do _____ , NIP _____ REGON _____, reprezentowaną przez:

..... - .....

zwanych dalej łącznie **„Stronami".**

Umowa (zwana dalej „**Umową**") zostaje zawarta *na podstawie rozeznania cenowego dotyczącego zamówienia o wartości nie przekraczającej równowartości kwoty 30.000 euro, zgodnie z art. 4 pkt 8 ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (Dz. U. z 2013 r., poz. 907 z późn. zm.) i § 46 zarządzenie nr 17 Komendanta Głównego Policji z dnia 13 lipca 2015 r. w sprawie planowania i udzielania zamówień publicznych w Komendzie Głównej Policji.*

§ 1
Przedmiot umowy

1. Przedmiotem umowy jest „Modernizacja, budowa redundancji oraz doposażenie węzła CPZ".
2. Szczegółowy opis Przedmiotu umowy określa Załącznik nr 1 do Umowy.
3. Na Przedmiot umowy, o którym mowa w ust. 1, składają się następujące czynności:
   1) sprzedaż i dostarczenie przez Wykonawcę do siedziby Zamawiającego Przedmiotu umowy zgodnie z Załącznikiem nr 1;
   2) udzielenie gwarancji i zapewnienie serwisu gwarancyjnego Przedmiotu umowy na zasadach określonych w Umowie i Załączniku nr 3;
   3) dostarczenie pełnej dokumentacji (w języku polskim lub angielskim) standardowo sporządzanej przez producentów sprzętu oraz kart gwarancyjnych do Przedmiotu umowy;
   4) sprzedaż i dostarczenie przez Wykonawcę do siedziby Zamawiającego licencji do oprogramowania zgodnie z Załącznikiem nr 1.
4. Specyfikację ilościowo-cenową określa Załącznik nr 4.
5. Ilekroć w dalszych postanowieniach Umowy mowa jest o sprzęcie, serwerach, urządzeniach, koncentratorach VPN, oprogramowaniu, licencjach, bez bliższego oznaczenia, należy przez to rozumieć Przedmiot umowy określony w Załączniku nr 1.
6. Postanowienia Umowy obowiązują z dniem jej zawarcia.

7. Na podstawie Umowy Wykonawca zobowiązuje się przenieść na Zamawiającego własność Przedmiotu umowy i wydać mu go na zasadach określonych w Załączniku nr 2 do Umowy, a Zamawiający zobowiązuje się Przedmiot umowy odebrać i zapłacić Wykonawcy wynagrodzenie, o którym mowa w § 5 ust. 1.

§ 2
Organizacja umowy

1. W celu bezpośredniego nadzoru nad realizacją Przedmiotu umowy, Zamawiający na Koordynatora wyznacza nw. przedstawiciela:
   ..... - Biuro Łączności i Informatyki KGP
2. W celu bezpośredniego nadzoru nad realizacją Przedmiotu umowy, Wykonawca na Koordynatora wyznacza nw. przedstawiciela:
   ..... – dane teleadresowe, stanowisko
3. Koordynator, o których mowa w ust. 1 i 2, odpowiednio ze strony Zamawiającego i Wykonawcy, odpowiadają za nadzór nad wykonaniem Przedmiotu umowy zgodnie z wymaganiami, w założonym terminie, w ramach określonego budżetu, przy wykorzystaniu dostępnych zasobów i środków.
4. Koordynatorzy upoważnieni są do podejmowania decyzji i akceptacji zmian dotyczących realizacji Przedmiotu umowy, za wyjątkiem decyzji wymagających formy aneksu.
5. Obie Strony mogą zmienić swoich przedstawicieli w organizacji projektu informując drugą Stronę, z co najmniej 3-dniowym (dni robocze) wyprzedzeniem. Zmiana taka nie wymaga aneksu do Umowy.
6. Dzień roboczy oznacza każdy dzień tygodnia od poniedziałku do piątku w godzinach 8:15- 16:15, z wyłączeniem dni ustawowo wolnych od pracy w Polsce.

§ 3
Wykonanie Umowy

1. Wykonawca zobowiązuje się wykonać Umowę przy zachowaniu najwyższej staranności, uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z zasadami wiedzy i stosowanymi normami technicznymi.
2. Strony zgodnie oświadczają, iż wydanie Przedmiotu Umowy następuje w dniu dostarczenia przez Wykonawcę Sprzętu w miejsce i na zasadach wskazanych w Załączniku nr 2 do Umowy.
3. Zamawiający wymaga, by dostarczony Przedmiot umowy był fabrycznie nowy, wolny od wad fizycznych i prawnych.
4. Wykonawca gwarantuje, iż w stosunku do Przedmiotu umowy nie toczy się żadne postępowanie oraz, że nie jest on obciążony zastawem, zastawem rejestrowym ani zastawem skarbowym ani żadnymi innymi ograniczonymi prawami rzeczowymi.
5. Dostarczony sprzęt posiada „znak CE" – *ConformiteEuropenne*
6. Oferowany Przedmiot umowy pochodzi z autoryzowanego kanału producenta tzn. zakupiony jest w oficjalnym kanale sprzedaży producenta na rynek UE, co oznacza, że będzie nowy i posiadający stosowny pakiet usług gwarancyjnych kierowanych do użytkowników z UE.

§ 4
Termin i warunki dostawy

1. Wykonawca zobowiązuje się do dostarczenia Przedmiotu umowy do dnia 15 grudnia 2015 r. od daty zawarcia umowy, przy użyciu własnych środków transportu i na własny koszt.

2. Za termin dostarczenia Przedmiotu umowy przyjmuje się datę podpisania, bez zastrzeżeń, przez przedstawicieli Wykonawcy i Zamawiającego protokołu odbioru ilościowego, którego wzór stanowi Załącznik nr 6 do Umowy.
3. Przedmiot umowy podlegać będzie odbiorowi. Szczegółowe zasady odbioru Przedmiotu umowy zawiera Załącznik nr 2.
4. Wszystkie czynności związane z odbiorami powinny zakończyć się w terminie wskazanym w ust. 1.
5. Wykonawca ponosi pełną odpowiedzialność za ewentualne uszkodzenia Przedmiotu umowy do czasu jego odbioru przez Zmawiającego na zasadach określonych w Załączniku nr 2 do Umowy.

§ 5
Płatności

1. Wartość Przedmiotu umowy, o którym mowa w § 1, Strony ustalają na kwotę netto ..... zł (słownie zł: ..... i 00/100), co wraz z podatkiem VAT stanowi łącznie ..... brutto (słownie zł: ..... i 00/100). Wartość Przedmiotu umowy brutto obejmuje wszelkie koszty związane z realizacją Umowy z uwzględnieniem podatku od towarów i usług VAT, innych opłat i podatków, opłat celnych, kosztów opakowania oraz ewentualnych upustów i rabatów, skalkulowanych z uwzględnieniem kosztów dostawy (transportu), wniesienia do określonej Umową lokalizacji.
2. Zamawiający opłaci należność za wykonanie Przedmiotu umowy na podstawie prawidłowo wystawionej przez Wykonawcę faktury VAT.
3. Wykonawca wystawi fakturę VAT, wskazując jako płatnika:

Komenda Główna Policji
02-624 Warszawa, ul. Puławska 148/150
NIP 521-31-72-762, REGON 012137497

4. Podstawę do wystawienia faktury VAT stanowi podpisany - bez zastrzeżeń - przez przedstawicieli Zamawiającego i Wykonawcy- Protokół odbioru ilościowego, którego wzór stanowi Załącznik nr 6.
5. Zapłata za realizację Przedmiotu umowy dokonana będzie przelewem bankowym na rachunek Wykonawcy, wskazany na fakturze, w terminie 30 dni od daty doręczenia faktury VAT do siedziby Biura Łączności i Informatyki KGP, ul. Wiśniowa 58, 02-520 Warszawa.
6. Za termin zapłaty przyjmuje się datę obciążenia przez bank rachunku Zamawiającego.
7. Zamawiający upoważnia Wykonawcę do wystawienia faktury VAT bez podpisu Zamawiającego.
8. Wszelkie rozliczenia finansowe między Zamawiającym a Wykonawcą będą prowadzone wyłącznie w złotych polskich.

§ 6
Gwarancja i serwis

1. Warunki gwarancji oraz wymogi określa Załącznik nr 3.
2. Bieg okresu gwarancji na Przedmiot umowy rozpocznie się od daty podpisania – bez zastrzeżeń – protokołu odbioru ilościowego.

§ 7
Kary umowne

1. Wykonawca odpowiada za szkodę wyrządzoną Zmawiającemu, w tym również za szkodę

wyrządzoną przez osoby, którymi Wykonawca posłużył się przy wykonywaniu Umowy, chyba że szkoda została spowodowana działaniem Siły Wyższej, wyłączną winą Zamawiającego lub osoby trzeciej, za którą Wykonawca nie ponosi odpowiedzialności.

2. Wykonawca zobowiązuje się zapłacić Zamawiającemu następujące kary umowne:
   1) 10% wartości brutto Przedmiotu umowy z tytułu niewykonania lub nienależytego wykonania Przedmiotu umowy z powodu okoliczności, za które odpowiedzialność spoczywa na Wykonawcy;
   2) 10% wartości brutto Przedmiotu umowy w razie odstąpienia w całości od Umowy przez Zamawiającego lub Wykonawcę z powodu okoliczności, za które odpowiedzialność spoczywa na Wykonawcy;
   3) 10% wartości brutto Przedmiotu umowy w przypadku odstąpienia przez Zamawiającego lub Wykonawcę od Umowy w części, z przyczyn leżących po stronie Wykonawcy, Wykonawca zobowiązuje się do zapłaty kary umownej w wysokości 10% wartości wynagrodzenia brutto należnego za część Umowy, od której się odstępuje;
   4) 0,15% wartości brutto Przedmiotu umowy, za każdy rozpoczęty dzień opóźnienia w wykonaniu Przedmiotu umowy;
   5) 0,15% wartości brutto Przedmiotu umowy za każdy rozpoczęty dzień opóźnienia w usuwaniu awarii ponad termin określony w Załączniku nr 3.
3. Zapłata kar umownych, o których mowa w ust. 2 pkt 3 i 4, nie zwalnia Wykonawcy z obowiązku wykonania Przedmiotu umowy.
4. Niezależnie od kar umownych, o których mowa w ust. 2, Stronom przysługuje prawo dochodzenia odszkodowania na zasadach ogólnych prawa cywilnego, jeżeli poniesiona szkoda przekroczy wysokość zastrzeżonych kar umownych.
5. Kary umowne podlegają łączeniu.
6. Zamawiający jest uprawniony do potrącenia kar umownych z wynagrodzenia należnego Wykonawcy na podstawie Umowy. Doręczenie Wykonawcy wystawionej przez Zamawiającego noty obciążeniowej, w której określono kwotę naliczonych kar umownych, podstawę ich naliczenia oraz wprowadzono oświadczenie o ich potrąceniu z wynagrodzenia, zastępuje wezwanie do zapłaty oraz oświadczenie Zamawiającego o potrąceniu kar umownych.
8. Prawo naliczenia kar umownych, o których mowa w ust. 2, nie ma zastosowania w przypadku gdy opóźnienie wynika z winy Zamawiającego.
9. Żadna Strona nie będzie odpowiedzialna za niewykonanie lub nienależyte wykonanie swoich zobowiązań w ramach Umowy, jeżeli takie niewykonanie lub nienależyte wykonanie jest wynikiem „Siły Wyższej".
10. W rozumieniu Umowy, „Siła Wyższa" oznacza okoliczności pozostające poza kontrolą Strony i uniemożliwiające lub znacznie utrudniające wykonanie przez tę Stronę jej zobowiązań, których nie można było przewidzieć w chwili zawierania Umowy, ani im zapobiec przy dołożeniu należytej staranności.
11. Za Siłę Wyższą nie uznaje się niedotrzymania zobowiązań przez kontrahenta – dostawcę Wykonawcy.
12. W przypadku zaistnienia „Siły Wyższej", Strona, która powołuje się na te okoliczności, niezwłocznie zawiadomi druga Stronę na piśmie o jej zaistnieniu i przyczynach. W przypadku, gdy na skutek Siły Wyższej nie będzie możliwe niezwłoczne zawiadomienie drugiej Strony, Strona powołująca się na Siłę Wyższą zawiadomi drugą Stronę niezwłocznie po ustaniu przyczyny uniemożliwiającej komunikację.
13. W razie zaistnienia „Siły Wyższej" wpływającej na termin realizacji Umowy, Strony zobowiązują się w terminie 14 (czternastu) dni kalendarzowych od dnia zawiadomienia, o

którym mowa w ust. 11, ustalić nowy termin wykonania Umowy lub ewentualnie podjąć decyzję o odstąpieniu od Umowy za porozumieniem Stron.

§ 8
Zmiany Umowy

1. Strony przewidują możliwość dokonywania zmian w treści Umowy w stosunku do treści oferty Wykonawcy w sytuacji gdy:
   1) powstała możliwość zastosowania nowszych lub korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili zawarcia Umowy, nie powodujących zmiany Przedmiotu umowy i nie powodujących podwyższenia ceny;
   2) powstała możliwość zastosowania nowszych lub korzystniejszych dla Zamawiającego rozwiązań w zakresie modelu/typu sprzętu w przypadku zakończenia produkcji, braku dostępności na rynku pod warunkiem, że będzie posiadał parametry nie gorsze od oferowanego modelu/typu i nie spowoduje podwyższenia ceny;
   3) po zawarciu Umowy doszło do wydłużenia okresu gwarancyjnego przez producenta;
   4) niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest korzystna dla Zamawiającego oraz konieczna w celu prawidłowego wykonania Umowy.
2. Zmiany, o których mowa w ust. 1, wymagają zgody obu Stron i powinny być dokonywane w formie pisemnej pod rygorem nieważności w postaci aneksu.

§ 9
Odstąpienie od Umowy

1. Zamawiający zastrzega sobie prawo do odstąpienia od Umowy, w szczególności w przypadku:
   1) wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy;
   2) niedostarczenia Przedmiotu umowy w terminie, o którym mowa w § 4 ust. 1;
   3) dostarczenia Przedmiotu umowy niespełniającego wymogów określonych w Załączniku nr 1.
2. Odstąpienie powinno nastąpić w formie pisemnej, pod rygorem nieważności takiego oświadczenia i zawierać uzasadnienie.
3. Prawo odstąpienia Zamawiający może wykonać w terminie do 30 dni kalendarzowych od powzięcia wiadomości uzasadniających odstąpienie.
4. Zamawiający zastrzega sobie prawo do odstąpienia od Umowy bez wyznaczania Wykonawcy dodatkowego terminu na wykonanie zobowiązania.
5. W przypadku odstąpienia od realizacji Umowy Wykonawca uprawniony jest do otrzymania wynagrodzenia za wykonane prace oraz świadczone usługi należne do dnia odstąpienia od umowy.
6. Odstąpienie lub wypowiedzenie od Umowy nie powoduje wygaśnięcia roszczeń o zapłatę kar umownych powstałych w czasie obowiązywania Umowy (w tym roszczenia o zapłatę kary umownej z powodu odstąpienia od Umowy)

§ 10

Prawa własności intelektualnej, licencje na Oprogramowanie

1. Wykonawca oświadcza i gwarantuje, że Dokumentacja dostarczona w wykonaniu Umowy, Oprogramowanie oraz inne utwory przekazane Zamawiającemu w trakcie realizacji Umowy ani korzystanie z nich przez Skarb Państwa – Zamawiającego nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów, oraz praw do baz danych.
2. Wykonawca oświadcza i gwarantuje, że Skarb Państwa - Zamawiający w ramach wynagrodzenia brutto, o którym mowa w § 5 ust. 1, uzyskuje prawo do korzystania z Oprogramowania i jego aktualizacji wraz z niezbędną do korzystania z nich Dokumentacją na podstawie niewyłącznych, rozciągających się na całe terytorium Rzeczypospolitej Polskiej i nieograniczonych czasowo licencji, udzielonych przez producenta Oprogramowania lub podmiot przez niego upoważniony, których warunki producent lub podmiot przez niego upoważniony dołączył do Oprogramowania.
3. Licencje, o których mowa w ust. 2, w zakresie nie przewidzianym Umową, udzielone zostaną na warunkach nie gorszych niż stosowane zwykle przez producenta Oprogramowania.
4. Wykonawca oświadcza i gwarantuje, że licencje na Oprogramowanie oraz aktualizacje nie zostaną wypowiedziane (przez Wykonawcę lub inny podmiot, w tym inny niż Wykonawca producent danego Oprogramowania), za wyjątkiem przypadku naruszenia przez Zamawiającego istotnych warunków licencji. W przypadku wypowiedzenia licencji na Oprogramowanie lub aktualizacje, pomimo braku naruszenia przez Zamawiającego istotnych warunków licencji, Wykonawca odpowiadać będzie za wynikłą z tego tytułu szkodę oraz w ramach wynagrodzenia, o którym mowa w § 5 ust. 1, dostarczy odpowiednie oprogramowanie z licencjami odpowiadające warunkom zawartym w Umowie i Załączniku nr 1 do Umowy. W wypadku nie dostarczenia Oprogramowania z licencjami Wykonawca zapłaci karę umowną w wysokości 100 % wynagrodzenia za dane Oprogramowanie z licencjami według cen nabycia.
5. Wykonawca oświadcza i gwarantuje, że w przypadku Oprogramowania, którego nie jest producentem, uzyskał zgodę producenta lub podmiotu upoważnionego przez producenta, na korzystanie z Oprogramowania oraz aktualizacji przez Zamawiającego, w tym na przekazywanie dokumentów zawierających warunki licencji.
6. Udzielenie Zamawiającemu licencji na korzystanie z Oprogramowania następuje bezwarunkowo w chwili podpisania przez Strony Protokołu odbioru ilościowego. Udzielenie Zamawiającemu licencji na korzystanie z aktualizacji następuje nie później niż w momencie zainstalowania aktualizacji.
7. W okresie od dnia dostarczenia Oprogramowania do momentu podpisania przez Strony Protokołu odbioru ilościowego, Wykonawca zapewnia Zamawiającemu prawo korzystania z Oprogramowania w ramach wynagrodzenia, o którym mowa w § 5 ust. 1.
8. Z chwilą udzielenia licencji na korzystanie z Oprogramowania własność nośników, na których utrwalono egzemplarze tego Oprogramowania przechodzi na Skarb Państwa - Zamawiającego. Z chwilą przekazania aktualizacji do Oprogramowania własność nośników, na których utrwalono daną aktualizację przechodzi na Skarb Państwa - Zamawiającego.
9. Dostarczone licencje powinny zapewnić pełną i prawidłową realizację celu Umowy, zamierzonego przez Zamawiającego.

§ 11
Inne postanowienia

1. Przy prowadzeniu korespondencji w sprawach związanych z realizacją Przedmiotu umowy obowiązywać będzie forma pisemna.

2. W razie pilnej potrzeby zawiadomienia mogą być przesyłane faksem z pisemnym potwierdzeniem ich otrzymania.
3. Ustala się następujące adresy, numery faksów i telefonów:

Adres Wykonawcy dla potrzeb korespondencji i składania zawiadomień:

…… Tel:..... faks: …….

Dla Zgłoszeń serwisowych:

……., adres, tel: …… faks……., e-mail: …….

Adres Zamawiającego dla potrzeb składania zawiadomień:

Biuro Łączności i Informatyki KGP
Wydział Technicznego Wsparcia
Systemu Powiadamiania Ratunkowego
ul. Olszewska 6
00-792 Warszawa
Tel. Sekretariat 022 605 62 50
Fax. 022 601 57 47

§ 12
Postanowienia końcowe

1. Wykonawca nie może dokonać cesji na osoby trzecie wierzytelności wynikających z niniejszej Umowy z wyłączeniem cesji na rzecz banku kredytującego Wykonawcę w zakresie Umowy.
2. W sprawach nieuregulowanych Umową stosuje się przepisy Kodeksu Cywilnego, ustawy Prawo Zamówień Publicznych, ustawy o prawie autorskim i prawach pokrewnych
3. Sądem właściwym dla Stron Umowy jest sąd powszechny właściwy dla siedziby Zamawiającego.
4. Umowę sporządzono w 4 (czterech) jednobrzmiących egzemplarzach, z których 3 (trzy) egzemplarze otrzymuje Zamawiający i 1 (jeden) egzemplarz otrzymuje Wykonawca.
5. Załączniki stanowiące integralną część Umowy:
   1) Załącznik nr 1 – Szczegółowy opis Przedmiotu umowy;
   2) Załącznik nr 2 – Zasady odbioru Przedmiotu umowy;
   3) Załącznik nr 3 – Warunki gwarancji;
   4) Załącznik nr 4 – Specyfikacja ilościowo-cenowa;
   5) Załącznik nr 5 – Protokół odbioru jakościowego – wzór;
   6) Załącznik nr 6 – Protokół odbioru ilościowego – wzór
   7) Załącznik nr 7 – zgłoszenie serwisowe – wzór

6. W przypadku zaistnienia jakichkolwiek rozbieżności pomiędzy postanowieniami zawartymi w załącznikach a warunkami ustalonymi w Umowie, wiążące są postanowienia Umowy.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1

umowy nr 116/UM/WTWSPR/BŁiI/2015 z dnia .....

OPIS PRZEDMIOTU ZAMÓWIENIA

CPV: 72268000-1 - usługi dostawy oprogramowania
48821000-9 - serwery sieciowe
32420000-3 – urządzenia sieciowe

1. Wstęp

Przedmiotem zamówienia jest zakup urządzeń oraz licencji oprogramowania na potrzeby „Modernizacji, budowy redundancji oraz doposażenia węzła Centralnego Punktu Zarządzania". Węzeł jest punktem demarkacyjnym łączącym systemy zarządzania systemów i sieci jakie zostały powierzone w administrację Wydziałowi Technicznego Wsparcia Systemu Powiadamiania Ratunkowego, i służy do centralnego zarządzania usługami, systemami, sieciami oraz dostępem do systemów zarządzania dla podmiotów zewnętrznych.

Zamówienie zostało podzielone na zadania.

Celem zadania I jest zakup infrastruktury sprzętowej serwerowej niezbędnej do uruchomienia zarządzania nowych urządzeń w węźle CPZ. Zadanie ma zapewnić stworzenie infrastruktury wirtualnej na potrzeby utrzymania i uruchamiania usług zarządzania.

Celem zadania II jest zakup redundantnej pary firewall'i posiadających funkcjonalności NGFW (Next Generation FireWall) oraz NGIPS (Next Generation Intrusion Prevention Systems) wraz z niezbędnym oprogramowaniem zarządzającym.

Wszystkie urządzenia dostarczone w ramach realizacji zadania muszą spełniać poniższe warunki:

- muszą być dostarczone jako fabrycznie nowe, nie używane w innych projektach, oraz nie starsze niż 4 miesięcy od daty produkcji;
- wszystkie urządzenia muszą pochodzić z oficjalnego kanału dystrybucji na Polskę dla danego producenta;
- dla urządzenia należy dostarczyć wszystkie elementy montażowe wymagane do instalacji urządzenia w szafie rack 19";
- dostarczane systemy operacyjny muszą być wersją najnowszą proponowaną przez producenta rozwiązania, spełniającego warunki zawarte w OPZ;
- zarówno urządzenia jak i jego elementy składowe wraz z systemami operacyjnymi oraz aplikacjami nie mogą znajdować się na aktualnej na czas składania ofert liście elementów producenta przewidzianych do wycofania z produkcji, sprzedaży lub serwisowania.

- urządzenia muszą być objęte 12 miesięcznym serwisem świadczonym pięć dni w tygodniu o ile szczegółowy opis zadania nie mówi inaczej.
- wszelkie koszty dostawy przedmiotu zamówienia pokryje Wykonawca (wyładunek i transport do miejsca wyznaczonego przez Zamawiającego w jego siedzibie w Warszawie).
- zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy) na dzień poprzedzający dzień składania ofert.

Jeżeli w OPZ użyto do opisania przedmiotu zamówienia oznaczeń lub parametrów wskazujących konkretnego producenta, konkretny produkt lub wskazano znaki towarowe, patenty, normy, standardy, aprobaty techniczne lub pochodzenie urządzeń, Zamawiający dopuszcza zastosowanie produktów równoważnych, przez które należy rozumieć produkty o parametrach nie gorszych od przedstawionych w OPZ, kompatybilne (współpracujące) z posiadanym przez Zamawiającego systemem zarządzania, w tym samym zakresie, co produkty określone w OPZ oraz posiadający równoważne funkcje i parametry co produkt opisany w OPZ. W takim wypadku do oferty należy załączyć dokładny opis oferowanych produktów, z którego jasno wynikać będzie zachowanie warunków równoważności.

2. Przedmiot zamówienia

Zadania I

Przedmiotowe zadanie dotyczy zakupu infrastruktury sprzętowej serwerowej niezbędnej do stworzenia platformy serwerowej (wirtualnej) na potrzeby utrzymania i uruchamiania usług zarządzania w CPZ i obejmuje:

- dostawa serwera wraz z wgranym i uruchomionym oprogramowaniem do wirtualizacji - 1 kpl.,

Serwer – 1 szt.

Serwer jest przewidziany jako serwer działający na rzecz środowiska wirtualnego uruchomionego w węźle CPZ dla usług zarządzania nowymi urządzeniami zakupionymi w Zadaniu II. Zamawiający wymaga dostawy serwera o parametrach równych lub lepszych od przedstawionych w poniższej konfiguracji:

1. Obudowa typu RACK 19" wraz z zestawem do zamontowania w szafie teleinformatycznej 19", umożliwiającym pełne wysunięcie obudowy, o wysokości nie przekraczającej 2 U.

2. Płyta główna musi posiadać/spełniać warunki nie gorsze niż:
   - musi być zaprojektowana przez producenta serwera i oznaczona trwale jego logo;
   - dwa fizyczne gniazda do obsługi procesorów wyspecyfikowanych w następnych punktach;
   - 24 sloty do obsługi pamięci DIMM DDR4, pracującej z częstotliwościami 2133 MHz;
   - możliwość wyposażenia serwera w 768 GB RAM;
   - zintegrowana karta graficzna;
   - wewnętrzny slot USB 2.0 umieszczony na płycie głównej serwera, umożliwiający bootowanie lub wewnętrzny slot kart SD wyposażony w kartę o pojemności minimum 16GB z możliwością zainstalowania i uruchamiania z karty dostarczanego w ramach niniejszego postępowania hypervisora wirtualizacyjnego.
3. Serwer musi być wyposażony w dwa procesor 64 bitowe o minimalnych parametrach:
   - liczba rdzeni: 12;
   - liczba wątków 24;
   - liczba kanałów pamięci: 4;
   - obsługa pamięci ECC;
   - wbudowane w procesor wsparcie dla obsługi standardu PCIe 3.0;
   - szybkość zegara: 2,5 GHz;
   - pamięć podręczna procesora cache L3: 30MB;
   - zintegrowany kontroler zarządzania pamięcią;
   - zaoferowany procesor musi wspierać funkcjonalność dynamicznego i automatycznego zwiększenia wydajności serwera dla aplikacji poprzez zwiększenie częstotliwości rdzenia;
   - serwer wyposażony w procesory, które w testach dla serwerów publikowanych na stronach spec.org, w szczególności w teście CINT2006 Rate Base, muszą osiągać wynik minimum 1000 punktów.
4. Serwer musi być wyposażony w Chipset dedykowany przez producenta procesora do pracy w konfiguracjach 2 procesorowych, obsługujący opisane procesory.
5. Serwer musi posiadać zainstalowane dyski HDD w ilości co najmniej dwa dyski typy SAS HotPlug 2,5 cala 10K RPM SFF skonfigurowane w grupę RAID 1 tak by oczekiwany rozmiar dysku były nie mniejsze niż 600 GB. Musi istnieć możliwość instalacji dysków HDD SATA, SAS, SSD oraz możliwość rozbudowy do minimum 16 dysków w serwerze.
6. Serwer musi być wyposażony w minimum 4 sloty PCI-E gen. 3.
7. Serwer musi być wyposażony w sprzętowy kontroler macierzy obsługujący RAID 0, 1, 5, 6, 10 wyposażony w min. 1 GB pamięci cache z zapisem na nieulotną pamięć w przypadku awarii zasilania.
8. Serwer musi być wyposażony w minimum 32 GB pamięci RAM (moduły pamięć RAM minimum 16 GB pamięci RAM DDR4-2133 MHz Registered DIMM).
9. Serwer musi posiadać:
   - min. 4 porty Gigabit Ethernet 10/100/1000 RJ-45 o przepustowości 1Gb/s z możliwością obsługi stosu TCP/IP – TOE;
   - min. 2 porty USB;

- min. 1 porty VGA;
- min. 1 port RJ-45 10/100/1000 dedykowany dla zarządzania.
- dopuszczalne jest stosowanie kart wbudowanych w płytę główną lub w formie modułu rozszerzenia. Zewnętrzne karty PCI-E muszą być identyczne i kompatybilne z zamawianym serwerem oraz zapewnić zgodność z oprogramowaniem do wirtualizacji (dotyczy również kart wbudowanych lub w formie modułu). Muszą być również umieszczone w portach PCI-E 3.0 o przepustowości pozwalających na wykorzystanie pełnej wydajności ich transferu

10. Serwer musi posiadać moduł zdalnego zarządzania (konsoli), pozwalający na:
    - zdalne włączenie, wyłączenie i restart serwera;
    - wykorzystanie zdalnej, graficznej konsoli obsługująca zdalną pracę na serwerze;
    - podgląd logów sprzętowych serwera;
    - przejęcie pełnej konsoli graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS);
    - podłączanie wirtualnych napędów CD i FDD oraz obrazów;
    - rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w slocie PCI;
11. Serwer musi posiadać:
    - minimum dwa zasilacze wymienne podczas pracy serwera, z tego jeden redundantny o mocy zapewniającej bezawaryjną pracę przy pełnej możliwej rozbudowie w dyski, procesory, pamięci itd.;
    - redundantne chłodzenie serwera;
    - szyny ruchome montażowe do szafy 19".
    - dostarczony serwer musi być wstępnie skonfigurowany z uruchomionym i skonfigurowanym RAID 1 oraz osadzonym i uruchomiany oprogramowaniem wirtualizacyjnym.
12. Serwer musi umożliwiać instalację następujących systemów operacyjnych: Microsoft Windows Server 2008, 2012 w wersji Standard i Enterprise, RedHat Linux w wersji standardowej oraz Advanced Platform, VMware vSphere w wersji Advanced, Enterprise, Enterprise Plus.
13. Wszystkie komponenty rozwiązania muszą znajdować się na oficjalnej liście wsparcia HCL danego serwera.
14. Serwer musi być objęty 3 letnią gwarancją z założeniem iż uszkodzone dyski w procesie wymiany pozostają u Zamawiającego.

Zadania II

Przedmiotowe zadanie dotyczy zakupu redundantnej pary firewall'i posiadających funkcjonalności NGFW, NGIPS oraz bramy VPN wraz z niezbędnym oprogramowaniem zarządzającym.

Urządzenie firewall z funkcjonalnością: NGFW, NGIPS bramy VPN – 2 szt.:

Urządzenie pełniące funkcje ściany ogniowej, bramy VPN oraz IPS:

Architektura urządzenia:

1. Rozwiązanie musi być oparte o dedykowany system operacyjny. Nie dopuszcza się rozwiązań gdzie platformą systemową jest system operacyjny ogólnego zastosowania, a na nim zainstalowane oprogramowanie firewall (jako aplikacja).
2. Urządzenie musi pełnić funkcje bramy VPN, ściany ogniowej (firewall) typu Statefull Inspection oraz IPS.
3. Urządzenie wyposażone w:
   - osiem interfejsów Gigabit Ethernet 10/100/1000 (RJ45)
   - dedykowany interfejs Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania
4. Urządzenie obsługuje interfejsy VLAN-IEEE 802.1q na interfejsach fizycznych (minimum 100 sumarycznie).
5. Urządzenie wyposażone w moduł sprzętowego wsparcia szyfrowania 3DES i AES oraz licencje na szyfrowanie 3DES/AES.
6. Urządzenie posiada dedykowany dla zarządzania port konsoli.
7. Urządzenie posiada pamięć Flash o pojemności co najmniej 8GB, umożliwiającej przechowanie co najmniej 3 obrazów systemu operacyjnego i 3 plików konfiguracyjnych.
8. Urządzenie posiada pamięć DRAM o pojemności 8GB, umożliwiającej uruchomienie wszystkich dostępnych dla urządzenia funkcjonalności.
9. Urządzenie zapewnia możliwość budowania systemu wysokiej dostępność w oparciu o dwa urządzenia.
10. Urządzenie posiada zasilacz umożliwiający zasilanie prądem przemiennym 230V.
11. Urządzenie musi mieć metalową obudowę.
12. Urządzenie ma możliwość instalacji w szafie typu rack 19".
13. Urządzenie musi być dostarczone z elementami montażowymi dla szafy rack 19".
14. Urządzenie musi być przystosowane do pracy w zakresie temperatur 0-40 stopni Celsjusza
15. Przepustowość teoretyczna stanowego firewall'a wynosi 1,8Gbps, a dla ruchu rzeczywistego (tzw. ruch multiprotocol) 900 Mbps.
16. Urządzenie posiada wydajność 250 Mbps dla ruchu szyfrowanego protokołami 3DES, AES.

17. Urządzenie umożliwia terminowanie 300 jednoczesnych sesji VPN (IPSec VPN, SSL VPN).
18. Urządzenie umożliwia zestawianie do 300 tuneli SSL VPN w trybie client-based i clientless VPN.
19. Urządzenie obsługuje 250 000 jednoczesnych sesji/połączeń z prędkością zestawiania 20 000 połączeń na sekundę.
20. Urządzenie posiada możliwość agregacji interfejsów fizycznych (IEEE 802.3ad) – 4 łączy zagregowanych. Pojedyncze łącze zagregowane może składać się z 2 interfejsów.

Funkcjonalność urządzenia:

1. Urządzenie musi działać pod kontrolą dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia.
2. Urządzenie pełni funkcję ściany ogniowej śledzącej stan połączeń (tzw. Stateful Inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji.
3. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (tzw. Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory.
4. Urządzenie posiada możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos.
5. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
6. Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access).
7. Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2.
8. Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości 256, 384 i 512 bitów.
9. Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM) i Galois Message Authentication Code (GMAC).
10. Urządzenie musi obsługiwać protokół Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH) dla grup 19,20 i 21.
11. Urządzenie musi obsługiwać protokół DSA w przestrzeni krzywych eliptycznych (ECDSA)
12. Urządzenie zapewnia w zakresie SSL VPN weryfikację uprawnień stacji do zestawiania sesji, poprzez weryfikację następujących cech:
    - OS Check - system operacyjny;
    - File Check - pliki w systemie;
    - Registry Check - wpisy w rejestrze systemu Windows;
    - Certificate Check - zainstalowane certyfikaty;
13. Urządzenie posiada, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym, klienta VPN dla technologii IPSec VPN i SSL VPN.

14. Oprogramowanie klienta VPN (IPSec oraz SSL) ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows (7, XP – wersje 32 i 64-bitowe) i Linux oraz umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC.
15. Oprogramowanie klienta VPN ma możliwość instalacji na urządzeniach mobilnych pracujących z systemami Apple iOS w wersji 6.0 i nowszej oraz Android w wersji 4.0 i nowszej.
16. Oprogramowanie klienta VPN obsługuje protokoły szyfrowania 3DES/AES.
17. Oprogramowanie klienta VPN umożliwia blokowanie lokalnego dostępu do Internetu podczas aktywnego połączenia klientem VPN (wyłączanie tzw. split-tunnelingu).
18. Urządzenie ma możliwość pracy jako transparentna ściana ogniowa warstwy drugiej modelu ISO OSI.
19. Urządzenie obsługuje protokół NTP.
20. Urządzenie współpracuje z serwerami CA.
21. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego. Urządzenie wspiera translację adresów (NAT) dla ruchu multicastowego.
22. Urządzenie zapewnia mechanizmy redundancji, w tym:
    - możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby, active/active dla kontekstów;
    - umożliwia pracę w klastrze.
23. Urządzenie realizuje synchronizację tablicy połączeń pomiędzy węzłami pracującymi w trybie wysokiej dostępności HA.
24. Urządzenie zapewnia możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia.
25. Urządzenie zapewnia funkcjonalność stateful failover dla ruchu VPN.
26. Urządzenie posiada mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
    - Hypertext Transfer Protocol (HTTP),
    - File Transfer Protocol (FTP),
    - Extended Simple Mail Transfer Protocol (ESMTP),
    - Domain Name System (DNS),
    - Simple Network Management Protocol v 1/2/3 (SNMP),
    - Internet Control Message Protocol (ICMP),
    - SQL*Net,
    - inspekcji protokołów dla ruchu voice/video – H.323 (włącznie z H.239), SIP, MGCP, RTSP
27. Urządzenie umożliwia zaawansowaną normalizację ruchu TCP:
    - poprawność pola TCP ACK;
    - poprawność sekwencjonowania segmentów TCP;

- poprawność ustanawiania sesji TCP z danymi;
- limitowanie czasu oczekiwania na segmenty nie w kolejności;
- poprawność pola MSS;
- poprawność pola długości TCP;
- poprawność skali okna segmentów TCP non-SYN;
- poprawność wielkości okna TCP.

28. Urządzenie ma możliwość blokowania aplikacji (np. peer-to-peer, czy „internetowy komunikator") wykorzystujących port 80 do transportu.
29. Urządzenie zapewnia obsługę i kontrolę protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP.
30. Urządzenie ma możliwość inspekcji protokołów HTTP oraz FTP na portach innych niż standardowe.
31. Urządzenie zapewnia wsparcie stosu protokołów IPv6, w tym:
    - listy kontroli dostępu dla IPv6;
    - możliwości filtrowania ruchu IPv6 na bazie nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload;
    - inspekcję protokołu IPv6, pracując w trybie transparentnym;
    - adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover);
    - realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6.
32. Urządzenie obsługuje mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu.
33. Urządzenie umożliwia współpracę z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik.
34. Urządzenie obsługuje routing statyczny i dynamiczny (min. dla protokołów RIP, OSPF i BGP).
35. Urządzenie pozwala na osiągnięcie wysokiej dostępności dla protokołów routingu dynamicznego, tzn. trasy dynamiczne zawarte w tablicy routingu są synchronizowane z urządzenia active na urządzenie standby.
36. Urządzenie umożliwia zbieranie informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL).
37. Urządzenie umożliwia konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie.
38. Urządzenie umożliwia konfigurację reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu.
39. Urządzenie umożliwia pominięcie stanu sesji TCP w scenariuszach wdrożeniowych z asymetrycznym przepływem ruchu.

40. Urządzenie wspiera Proxy dla protokołu SCEP i umożliwia zautomatyzowany proces pozyskiwania certyfikatów przez użytkowników zdalnych dla dostępu VPN.
41. Urządzenie wspiera użytkownika korzystającego z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN, w zakresie obsługi haseł w systemie Microsoft AD, bezpośrednio lub poprzez ACS, dla obsługi sytuacji wygaśnięcia terminu ważności hasła w systemie Microsoft AD, umożliwiając zmianę przeterminowanego hasła.
42. Urządzenie obsługuje IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode. Ponadto urządzenie wspiera protokół IKEv2 (Internet Key Exchange w wersji 2) dla połączeń zdalnego dostępu VPN oraz site-to-site VPN opartych o protokół IPSec.
43. Urządzenie umożliwia rozbudowę poprzez zakup odpowiedniej licencji lub oprogramowania bez konieczności dokonywania zmian sprzętowych, w tym istnieje możliwość wirtualizacji konfiguracji poprzez wirtualne konteksty. Dostarczone urządzenie musi obsługiwać dwa wirtualne konteksty i umożliwiać rozbudowę do co najmniej pięciu wirtualnych kontekstów.

Funkcjonalność urządzenia – NGFW:

1. Urządzenie musi zapewniać funkcjonalności tzw, Next-Generation firewall w zakresie nie mniejszym niż:
   - Możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory;
   - Dostępność systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control - AVC);
   - Dostępność systemu IPS.
2. System musi posiadać otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM;
3. System wykrywania aplikacji AVC musi:
   - posiadać możliwość klasyfikacji ruchu i wykrywania co najmniej 3000 aplikacji sieciowych;
   - zapewniać wydajność co najmniej 850Mbps;
   - pozwalać na tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego z którego korzysta użytkownik oraz wykorzystywanych usług;
   - pozwalać na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji.

Funkcjonalność urządzenia – NGIPS:

1. System IPS musi posiadać możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. Wymagane jest by system tworzył kontekst z wykorzystaniem co najmniej poniższych parametrów
   - Wiedza o użytkownikach – uwierzytelnienie;
   - Wiedza o urządzeniach – pasywne skanowanie ruchu;

- Wiedza o urządzeniach mobilnych;
- Wiedza o aplikacjach wykorzystywanych po stronie klienta;
- Wiedza o podatnościach;
- Wiedza o bieżących zagrożeniach;
- Baza danych URL.

2. System IPS musi:
   - posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system);
   - posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu);
   - posiadać możliwość wykrywania i uniemożliwiać szeroką gamę zagrożeń (np.: złośliwe oprogramowanie, skanowanie sieci, ataki na usługę VoIP, ataki na aplikacje P2P,zagrożenia dnia zerowego, itp.);
   - posiadać możliwość wykrywania modyfikacji znanych ataków (sygnatury) jak i te nowo powstałe, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna);
   - zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
     - sygnatury ataków opartych na exploitach;
     - reguły oparte na zagrożeniach;
     - mechanizm wykrywania anomalii w protokołach;
     - mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego.
   - mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu;
   - posiadać mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives);
   - mieć możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń;
   - posiadać wiele możliwości reakcji na zdarzenia (takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia, zastąpienie zawartości pakietów oraz mieć możliwość zapisywania pakietów);
   - mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6;
   - posiadać 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 – co najmniej powinna być zbierana: informacja o systemach operacyjnych, informacja o serwisach, informacja o otwartych portach, aplikacjach oraz informacji o możliwych zagrożeniach;
   - posiadać 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;
   - zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.;
   - posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji;

- zapewniać możliwość obrony przed atakami skonstruowanymi tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego;
- posiadać możliwość rozpakowywania archiwów (np. zip, rar) celem dokonania analizy zagrożeń;
- posiadać możliwość dekompresji plików celem wykrywania zagrożeń ukrytych w skompresowanych elementach plików Flash i PDF;
- zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne;
- zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie;
- zapewnić w przypadku zarządzania poprzez system centralnego zarzadzania połączenie za pomocą szyfrowanego połączenia;
- zapewniać obsługę reguł Snort.
- zapewniać możliwość wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS;
- zapewniać mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise);
- zapewniać mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa;
- posiadać możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewalla dla uzyskania pełnej widoczności ruchu – w szczególności musi posiadać możliwość pracy w trybie failover firewalla;
- system IPS powinien pozwalać na pracę z przepustowością co najmniej 425Mbps przy jednoczesnym działaniu AVC (nie mniej niż 50% wydajności NGFW);

Zarządzanie i konfiguracja:

1. Urządzenie musi umożliwiać zarządzanie:
   - przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2;
   - przez graficzny interfejs użytkownika z wykorzystaniem dedykowanej aplikacji;
   - programowo przez interfejs API dostępny przy pomocy protokołu https;
   - przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji.
2. Zdalnie dostępne interfejsy zarządzania muszą być dostępne w sieci IPv4 i IPv6.
3. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu o nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.
4. Urządzenie musi umożliwiać konfigurację maksymalnej równoczesnej liczby sesji zdalnego zarządzania.
5. Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4 i IPv6.

6. Urządzenie musi umożliwiać wyeksportowanie konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją.
7. Urządzenie musi mieć możliwość raportowania zdarzeń przy pomocy protokołu SYSLOG. Wymagane jest wsparcie szyfrowanej transmisji wiadomości SYSLOG przy pomocy SSL/TLS.
8. Urządzenie musi wspierać eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow v9 (RFC 3954).
9. Urządzenie musi posiadać możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu RADIUS lub TACACS+.
10. Urządzenie musi umożliwiać uwierzytelnienie i konfigurację poziomu dostępu administratora w oparciu o role (ang. Role Bases Access Control) z wykorzystaniem bazy danych użytkowników zdefiniowanej lokalnie na urządzeniu lub na zewnętrznych serwerach dostępnych przy pomocy protokołów RADIUS lub TACACS+.
11. Dla usług NGFW oraz IPS dopuszcza się zastosowanie dedykowanego scentralizowane systemu zarządzania spełniającego następujące warunki:
    - Platforma zarządzająca musi być oparta na uodpornionym systemie operacyjnym;
    - Platforma zarządzająca musi umożliwiać pracę jako maszyna wirtualna pracując na wykorzystywanym przez Zamawiającego hypervisor VMWare ESXi;
    - Platforma zarządzająca musi obsługiwać dwa urządzenia będące przedmiotem tego postępowania;
    - Platforma zarządzająca musi umożliwiać agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym;
    - Platforma zarządzające musi być dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego.

Serwis i licencjonowanie:

1. Urządzenie musi być objęte co najmniej 36 miesięcznym serwisem świadczonym bezpośrednio przez producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.
2. W ramach w/w serwisu należy uwzględnić subskrybcję sygnatur IPS przez okres 36 miesięcy.
3. System powinien być dostarczony ze wszystkimi niezbędnymi licencjami pozwalającymi na obsługę minimum 25 sesji zdalnego dostępu VPN pozwalające na połączenie przez dedykowanego klienta VPN. W przypadku zastosowania licencji subskrypcyjnych długość subskrypcji powinna być zgodna z długością okresu serwisu, czyli minimum 36 miesięcy.

Załącznik nr 2 do Umowy
Umowy nr .....

Zasady odbioru Przedmiotu umowy

I. Odbiór jakościowy

1. Odbiór jakościowy Przedmiotu umowy w zakresie spełnienia wymagań i funkcjonalności określonego w **Załączniku nr 1 do Umowy** przeprowadzony zostanie przez Koordynatorów do odbioru przedmiotu zamówienia ze strony Zamawiającego, w obecności przedstawicieli Wykonawcy.
2. O przygotowaniu Przedmiotu umowy do odbioru jakościowego Wykonawca powiadomi Wydział Technicznego Wsparcia Systemu Powiadamiania Ratunkowego BŁiI KGP e-mailem na adres: lukasz.pachocki@polcija.gov.pl z co najmniej 2-dniowym wyprzedzeniem, podając:
   - numer niniejszej Umowy,
   - planowaną datę dostarczenia produktu do odbioru jakościowego,
   - numery seryjne produktów.
3. Odbiór jakościowy przeprowadzony zostanie w BŁiI KGP w Warszawie, w ciągu do **1 dni roboczych** w godz. 8,15-16,15 od daty dostarczenia Przedmiotu umowy do odbioru jakościowego.
4. Celem czynności kontrolnych prowadzonych w ramach odbioru jakościowego będzie sprawdzenie jakości oraz zgodności dostarczonego Sprzętu z parametrami/funkcjonalnością zawartymi w Umowie.
5. Wykonawca będzie odpowiedzialny za dostarczenie, wniesienie, rozpakowanie sprzętu do odbioru jakościowego, oraz prezentację parametrów i funkcjonalności wskazanych przez Zamawiającego, wynikających z Umowy.
6. Wykonawca zapewni pełną dokumentację standardowo dostarczoną przez producentów – dokumentacja ta dostarczona będzie w języku polskim lub angielskim.
7. Jeżeli w czasie odbioru jakościowego jakikolwiek produkt nie będzie działał poprawnie lub nie spełni wymagań technicznych czy funkcjonalnych sprzęt przeznaczony do odbioru jakościowego zostanie zwrócony Wykonawcy, a cała procedura odbioru zostanie powtórzona od początku.
8. Odbiór jakościowy zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy protokołu odbioru jakościowego, którego wzór określa Załącznik nr 5 do Umowy.

II. Odbiór ilościowy:

1. Pozytywny wynik odbioru jakościowego warunkuje przystąpienie Stron do odbiorów ilościowych Przedmiotu umowy.
2. Przed przystąpieniem do odbioru ilościowego Wykonawca zobowiązany jest do przygotowania i dostarczenia Zamawiającemu wykazu zawierającego nazwę, typ, producenta produktu, ilość, cenę jednostkową netto produktu, wartość podatku VAT wraz ze stawką podatkową, cenę jednostkową brutto produktu, cenę łączną dla danej ilości produktu oraz numery seryjne.
3. Odbiór ilościowy Przedmiotu umowy zostanie przeprowadzony w miejscu odbioru jakościowego w ciągu do 2 dni roboczych przez Komisję powołaną do odbioru Przedmiotu zamówienia ze strony Zamawiającego, w obecności przedstawicieli Wykonawcy.

4. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowego jest sprawdzenie kompletności dostarczonego produktu i potwierdzenie zgodności z ilością określoną w Umowie.
5. Wykonawca zapewni opakowanie towaru wymagane do zabezpieczenia go przed uszkodzeniem w drodze do miejsca przeznaczenia. Opakowania muszą odpowiadać normom europejskim w zakresie utylizacji i będą własnością Zamawiającego.
6. Wykonawca będzie odpowiedzialny za rozpakowanie dostarczonego produktu.
7. Pozytywny wynik odbioru ilościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowego, którego wzór określa Załącznik nr 6 do Umowy.
8. Pozytywny wynik odbioru ilościowego nie zwalania Wykonawcy od odpowiedzialności za wady ujawnione w terminie późniejszym.
9. Wszystkie protokoły zostaną sporządzone w czterech (4) jednobrzmiących egzemplarzach, z czego jeden (1) otrzymuje Wykonawca, a trzy (3) Zamawiający.

Załącznik nr 3 do Umowy
Umowy nr .....

Warunki gwarancji i serwisu

1. Okres gwarancji na Przedmiot umowy zawarty jest w opisie szczegółowym zadania, przy czym bieg okresu gwarancji rozpocznie się z chwilą podpisania bez zastrzeżeń protokołu odbioru Przedmiotu Umowy.
2. Świadczenie usług gwarancyjnych i serwisowych dostarczonego Sprzętu realizowane będzie zgodnie z zasadami określonymi w Umowie jak również przez producenta oferowanych urządzeń o ile szczegółowy opis zadania nie mówi inaczej.
3. Do dostarczonego sprzętu będą dołączone karty gwarancyjne zawierające numery seryjne urządzenia, termin i warunki ważności gwarancji (zgodnie z umową), adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
4. Wykonawca wraz z dostawą urządzeń przekaże warunki gwarancyjne i serwisowe Sprzętu, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta.
5. Zamawiający oczekuje elastyczności w rozbudowie. Wymaga aby zaproponowany pakiet serwisowy pozwalał i to bez konieczności uzyskania zgody Wykonawcy czy Producenta, na rozbudowę posiadanych urządzeń o kolejne moduły rozszerzeń. Taka rozbudowa nie może powodować utraty praw serwisowych do istniejącej i rozszerzonej konfiguracji danego urządzenia.
6. Zgłoszenia Awarii przyjmowane będą przez całą dobę w układzie 24/5/NBD.
7. Zamawiający nie ponosi żadnych dodatkowych kosztów wynikających z realizacji Umowy innych niż wynagrodzenie przewidziane Umową.
8. Stosowanie praw wynikających z udzielonej gwarancji nie wyklucza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.

Załącznik nr 4 do
Umowy nr .....

Specyfikacja ilościowo - cenowa

(wypełnia Wykonawca przed podpisaniem Umowy)

L.p.	Opis / Nazwa	Ilość	VAT %	Cena jedn. brutto zł.	Wartość netto zł.	Wartość brutto zł.
1.						
2.						
				Razem		

Załącznik nr 5 do Umowy
nr

Protokół odbioru jakościowego - wzór

Miejsce dokonania odbioru: .....
Data dokonania odbioru: .....

Ze strony Wykonawcy:
.....
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)

W ramach odbioru jakościowego, przeprowadzonego w ramach Umowy nr ..... z dnia..... na _____, Koordynatorzy wskazani w Umowie przeprowadzili czynności kontrolne na podstawie zatwierdzonej przez Strony Umowy i potwierdza zgodność jakości dostarczonego produktu z parametrami/funkcjonalnością zawartymi w opisie przedmiotu Umowy.

Wynik odbioru jakościowego:
- Pozytywny*
- Negatywny*

Uwagi:.....

Podpisy Koordynatorów wskazanych do odbioru przedmiotu zamówienia:

1. .....
(Przedstawiciel Zamawiającego)

1.....
(Przedstawiciel Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 6 do Umowy
nr -_

Protokół odbioru ilościowego - wzór

Miejsce dokonania odbioru: .....
Data dokonania odbioru: .....

Ze strony Wykonawcy:
.....
.....
(nazwa i adres)
.....
(osoba upoważniona do udziału w odbiorze)

Ze strony Zamawiającego:
.....
(nazwa i adres)

Przedmiotem odbioru ilościowego przeprowadzonego w ramach przedmiotowej Umowy jest:

Lp.	Nazwa przedmiotu	Jednostka miary	Ilość	Nr seryjny	Wartość jednostkowa [netto]	Wartość łączna [brutto]	Dokumentacja techniczna/ instrukcja obsługi/świadectwo jakości	Uwagi
				Razem:				

Koordynatorzy wskazani w umowie do odbioru przedmiotu zamówienia, przeprowadziła czynności kontrolne i potwierdza kompletność dostarczonego produktu. *
Uwagi:.....

Podpisy:

1. ..... 1.....

(w imieniu Zamawiającego) (Przedstawiciel Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 7 do Umowy
nr

Formularz zgłoszeniowy – wzór

Zgłoszenie serwisowe w ramach realizacji umowy nr .....

Data zgłoszenia:	**Dane kontaktowe Wykonawcy** **.....** **Tel. .....** **Faks: .....** **e-mail: .....**
Dane zgłaszającego usterkę: Firma: ..... Adres: ..... Imię i nazwisko:..... Tel./TEL.FAX:..... .. e-mail:	
Dane urządzeń uszkodzonych: Nazwa:..... Model: ..... Nr seryjny: ..... Ilość :	
Opis uszkodzenia:	
Informacje dodatkowe..... ..... Podpis zgłaszającego	

Załącznik nr 8
Do umowy nr

Kryteria wyboru oferty

Zamawiający dokona oceny wszystkich złożonych, ważnych ofert według ustalonego przez siebie kryterium oceny oferty.

Kryterium, według którego Zamawiający będzie oceniał oferty, wraz z podaniem jego znaczenia (wagi) zawiera poniższa tabela.

Lp.	Nazwa kryterium	Waga	Współczynnik do wyznaczenia liczby punktów uzyskanych przez Wykonawcę	Sposób oceny
1.	K1 - Cena oferty brutto	80 %	80	Minimalizacja
2.	K2 – Termin realizacji zamówienia	20 %	20	Minimalizacja

Sposób obliczenia punktów w odniesieniu do kryterium „K1 - cena oferty brutto":
K1 – waga 80 % (maksymalnie Wykonawca może otrzymać 80 punktów)

Cena wyższa od ceny najniższej oceniona zostanie w następujący sposób:

K1= (cena ofertowa minimalna/cena ofertowa badana) * 80

Sposób obliczenia punktów w odniesieniu do kryterium „K2 – termin realizacji zamówienia":
K2 – waga 20 % (maksymalnie Wykonawca może otrzymać 20 punktów)

Przy ocenie czasu realizacji zamówienia najwyżej będzie punktowana oferta proponująca najkrótszy czas realizacji zamówienia, pozostałe oferty uzyskają odpowiednio mniejszą liczbę punktów zgodnie z poniższym wzorem

K2= (najkrótszy czas realizacji zamówienia/ czas realizacji zamówienia oferty badanej) * 10

Zamawiający odrzuci ofertę jako niezgodną z SIWZ.

Zasady wyboru oferty i udzielenia zamówienia:

Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom określonym w ustawie Pzp i niniejszej SIWZ oraz łącznie uzyska najwyższą liczbę punktów:

K – łączna ilość punktów uzyskana w poszczególnych kryteriach

K = K1 + K2

Istotne informacje dotyczące warunków zamówienia

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Zamawiający nie dopuszcza składania ofert wariantowych,
3. Zamawiający dopuszcza składanie ofert równoważnych

4. Zamawiający wymaga podania łącznej ceny oferowanej do Przedmiotu zamówienia (netto i brutto) wyrażonej w złotych polskich PLN wraz z podaniem pełnej nazwy produktu, typu/modelu i producenta.