Znak sprawy – 24/ ZP/ 2016

POLSKA AKADEMIA NAUK

Specyfikacja Istotnych Warunków Zamówienia

postępowanie o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn. „Odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego"

ZATWIERDZAM:

KANCLERZ
POLSKIEJ AKADEMII NAUK
Tadeusz Latała

Warszawa, dnia 16 grudnia 2016 r.

Specyfikacja istotnych warunków zamówienia zawiera:

I. Nazwę oraz adres Zamawiającego;
II. Tryb udzielenia zamówienia;
III. Opis przedmiotu zamówienia;
IV. Informacje dodatkowe;
V. Termin wykonania zamówienia;
VI. Warunki udziału w postępowaniu;
VII. Wykaz oświadczeń i dokumentów, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełnienia warunków udziału w postępowaniu oraz brak podstaw wykluczenia;
VIII. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami;
IX. Wymagania dotyczące wadium;
X. Termin związania ofertą;
XI. Opis sposobu przygotowania ofert;
XII. Miejsce oraz termin składania i otwarcia ofert;
XIII. Opis sposobu obliczenia ceny;
XIV. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów i sposobu oceny ofert;
XV. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego;
XVI. Wymagania dotyczące zabezpieczenia należytego wykonania umowy;
XVII. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli Zamawiający wymaga od Wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach;
XVIII. Podstawy wykluczenia Wykonawcy z postępowania, o których mowa w art. 24 ust. 5 ustawy Pzp;
XIX. Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia.

<u>Załączniki do SIWZ:</u>
Załącznik nr 1 Wzór formularza ofertowego.
Załącznik nr 2 Wzór oświadczenia - składane na podstawie art. 25a ust. 1 ustawy Pzp dotyczące przesłanek wykluczenia z postępowania.
Załącznik nr 3 Wzór oświadczenia - składane na podstawie art. 25a ust. 1 ustawy Pzp dotyczące spełnienia warunków udziału w postępowaniu.
Załącznik nr 4 Wzór oświadczenia dotyczącego przynależności do grupy kapitałowej
Załącznik nr 5 Szczegółowy opis przedmiotu zamówienia
Załącznik nr 5a Wymagania dla rozwiązania równoważnego
Załącznik nr 6 Wzór umowy

Rozdział I.
Nazwa oraz adres Zamawiającego.

Polska Akademia Nauk
Plac Defilad 1, 00-901 Warszawa
NIP: 5251575083, REGON: 000325713
Tel.: (22) 182 62 30, Faks: (22) 182 70 58
Pon. – Pt. godz. 8^{15} – 16^{15}
Strona internetowa www.pan.pl

Rozdział II.
Tryb udzielenia zamówienia.

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie przetargu nieograniczonego, na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 1126 ze zm.), zwaną dalej „ustawą Pzp".
2. Wartość zamówienia jest mniejsza niż kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 ustawy Pzp.
3. W sprawach nieuregulowanych niniejszą Specyfikacją Istotnych Warunków Zamówienia, zwaną dalej „SIWZ", mają zastosowanie przepisy ww. ustawy.

Rozdział III.
Opis przedmiotu zamówienia.

1. Przedmiotem zamówienia jest przedłużenie pakietu licencji obejmującego: gwarancje, wsparcie techniczne, możliwość aktualizacji oprogramowania dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego oraz subskrypcje bezpieczeństwa w zakresie antywirus, antyspam, IPS, Web filter dla urządzeń typu UTM, w zakresie atywirus, antyspam dla urządzeń zabezpieczających serwery poczty elektronicznej, zakresie antywirus, web security service, IP Reputation Service dla urządzeń monitorujących ruch www wraz z wyrównaniem terminu dla wszystkich urządzeń do 15.02.2018 r. Urządzenia, których termin podlega wyrównaniu posiadają numery seryjne: FG800C3912801356, FG800C3912801722.
2. Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 5 do SIWZ.
3. Zamawiający dopuszcza rozwiązania równoważne. Zgodnie z art. 30 ust. 5 ustawy Pzp Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowany przez niego przedmiot zamówienia spełnia wymagania określone przez Zamawiającego.
4. Szczegółowe wymagania, które muszą zostać spełnione w przypadku zaoferowania rozwiązania równoważnego zawiera załącznik nr 5a do SIWZ.
5. Opis przedmiotu zamówienia wg Wspólnego Słownika Zamówień – CPV:
   48210000-3 - Pakiety oprogramowania dla sieci
   48219000-6 - Pakiety oprogramowania do różnych operacji sieciowych

Rozdział IV.
Informacje dodatkowe.

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Zamawiający nie przewiduje zawarcia umowy ramowej.
3. Zamawiający nie przewiduje udzielania zamówień o których mowa w art. 67 ust. 1 pkt 6 ustawy Pzp.
4. Zamawiający nie dopuszcza składania ofert wariantowych.
5. Zamawiający nie przewiduje rozliczenia w walutach obcych.
6. Zamawiający nie przewiduje aukcji elektronicznej.
7. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
8. Zamawiający nie przewiduje udzielania zaliczek na poczet wykonania zamówienia.
9. Na podstawie art. 36b ustawy Pzp Wykonawca jest zobowiązany umieścić w składanej ofercie informację o części zamówienia, którą zamierza powierzyć podwykonawcom i wskazać nazwy (firmy) podwykonawców.
10. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.

Rozdział V.
Termin wykonania zamówienia

Terminy realizacji zamówienia określono w załączniku Nr 5 do SIWZ.

Rozdział VI.
Warunki udziału w postępowaniu

1. O udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy:
   1) nie podlegają wykluczeniu na podstawie art. 24 ust. 1 pkt 12 – 23 oraz art. 24 ust. 5 ustawy, w podstawach wskazanych w Rozdziale XVIII niniejszej SIWZ;
   2) spełniają warunki udziału w postępowaniu dotyczące:
      a) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów.
      Zamawiający nie określa warunku w tym zakresie.
      b) sytuacji ekonomicznej lub finansowej
      Zamawiający nie określa warunku w tym zakresie.
      c) zdolności technicznej lub zawodowej
      Zamawiający nie określa warunku w tym zakresie
2. Wykonawca może w celu potwierdzenia spełniania warunków, o których mowa w Rozdziale VI ust. 1 pkt. 2 SIWZ w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
3. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów udowodni 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.
4. Zamawiający oceni, czy udostępniane Wykonawcy przez inne podmioty zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu oraz zbada,

czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13–22 i art. 24 ust. 5 ustawy Pzp.

5. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują usługi, do realizacji których te zdolności są wymagane.

Rozdział VII.
Wykaz oświadczeń i dokumentów, potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

1. Do oferty każdy Wykonawca musi dołączyć aktualne na dzień składania ofert oświadczenia w zakresie wskazanym w Załączniku nr 2 i 3 do SIWZ a potwierdzające:
   a. Spełnianie warunków udziału w postępowaniu
   b. brak podstaw do wykluczenia

   Informacje zawarte w oświadczeniach będą stanowić wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.
   Forma dokumentów:
   Oświadczenia muszą być złożone w formie oryginału lub kopii poświadczonej notarialnie.
2. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców oświadczenia o których mowa w Rozdziale VII ust. 1 SIWZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia te mają potwierdzać spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia.
   W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia wymagane jest ustanowienie pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia publicznego albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
3. Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu, zamieszcza informacje o podwykonawcach w oświadczeniu, o którym mowa w Rozdziale VII ust. 1 SIWZ.
4. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia – w zakresie, w jakim powołuje się na ich zasoby - warunków udziału w postępowaniu, zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w Rozdziale VII ust. 1 SIWZ.
5. Zamawiający przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została oceniona jako najkorzystniejsza, do złożenia w terminie 5 dni, aktualnych na dzień złożenia następujących oświadczeń lub dokumentów w celu potwierdzenia braku podstaw wykluczenia Wykonawcy z udziału w postępowaniu, których Zamawiający żąda:
   a) zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.
   b) zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego

dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.

c) odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy.

Forma dokumentów:

- dokumenty, o których mowa w Rozdziale VII ust. 5 SIWZ muszą być złożone w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez Wykonawcę.

6. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy Pzp, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w Rozdziale VII ust. 5 lit. a) - c) SIWZ.
7. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów o których mowa w Rozdziale VII ust. 5 lit. a) - c) SIWZ składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
   a) nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo że zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu (Dokumenty powinny być wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert);
   b) nie otwarto jego likwidacji ani nie ogłoszono upadłości (Dokumenty powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert).
8. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w ust. 7, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby.

W zakresie oświadczeń i dokumentów, o których mowa w ust. 6, 7 i 8 postanowienie dotyczące formy z ust. 5 stosuje się.

9. Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy Pzp, przekaże Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp, którego wzór stanowi Załącznik nr 4 do SIWZ. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z

innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

Forma dokumentów:

Oświadczenie, o którym mowa w Rozdziale VII ust. 8 SIWZ musi być złożone w formie oryginału lub kopii poświadczonej notarialnie.

10. W przypadku wskazania przez wykonawcę dostępności oświadczeń lub dokumentów, o których mowa w Rozdziale VII ust. 5 SIWZ w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, zamawiający pobiera samodzielnie z tych baz danych wskazane przez wykonawcę oświadczenia lub dokumenty. Jeżeli wskazane przez Wykonawcę i pobrane samodzielnie przez Zamawiającego ww. dokumenty są w języku obcym, Zamawiający żąda przedłożenia ich tłumaczenia na język polski.
11. W przypadku wskazania przez wykonawcę oświadczeń lub dokumentów, o których mowa w Rozdziale VII ust. 5 SIWZ, które znajdują się w posiadaniu zamawiającego, w szczególności oświadczeń lub dokumentów przechowywanych przez zamawiającego zgodnie z art. 97 ust. 1 ustawy Pzp, zamawiający w celu potwierdzenia okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 ustawy Pzp, korzysta z posiadanych oświadczeń lub dokumentów, o ile są one aktualne.
12. Jeżeli Wykonawca nie złoży oświadczenia, o którym mowa w Rozdziale VII ust. 1 SIWZ, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, zamawiający wezwie do ich złożenia, uzupełnienia, poprawienia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta Wykonawcy podlegałaby odrzuceniu albo konieczne byłoby unieważnienie postępowania.
13. W przypadku oferowania rozwiązania równoważnego, w celu wykazania, że oferowane dostawy i usługi odpowiadają wymaganiom określonym przez Zamawiającego, Wykonawca zobowiązany jest złożyć wraz z ofertą także dokumenty wymienione w Załączniku nr 5a do SIWZ.
14. Wykonawca oferujący rozwiązanie równoważne zobowiązany jest do złożenia wypełnionego formularza Załącznika nr 5a do SIWZ.

Rozdział VIII.
Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.

1. Z zastrzeżeniem wyjątków określonych w ustawie, wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje pomiędzy zamawiającym oraz wykonawcami będą przekazywane:
   1) pisemnie na adres **Polska Akademia Nauk, Plac Defilad 1,00-901 Warszawa,** lub
   2) faksem na numer **(22) 182 70 58,** lub
   3) drogą elektroniczną na adres e-mail: **zp@pan.pl**
2. Jeżeli Zamawiający lub Wykonawca będą przekazywać oświadczenia, wnioski, zawiadomienia oraz informacje faksem lub drogą elektroniczną, każda ze stron na żądanie drugiej niezwłocznie potwierdzi fakt ich otrzymania.
   W przypadku niepotwierdzenia przez Wykonawcę faktu otrzymania przekazanych przez Zamawiającego zawiadomień, oświadczeń wniosków lub informacji, Zamawiający uzna, że dotarły one do Wykonawcy w dniu i godzinie ich nadania i były czytelne.

3. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa terminu składania ofert, Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu, o którym mowa powyżej, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Zamawiający zamieści wyjaśnienia na stronie internetowej, na której udostępniono SIWZ.
4. Treść zapytań wraz z wyjaśnieniami treści SIWZ będzie zamieszczana na stronie internetowej, na której udostępniono SIWZ.
5. Zamawiający nie ponosi odpowiedzialności z tytułu:
   1) okoliczności wynikających z niewłaściwego zabezpieczenia lub opisania przez Wykonawcę koperty, w której znajduje się składana przez niego oferta lub zmiana oferty;
   2) okoliczności wynikających z niewłaściwego zabezpieczenia przez Wykonawcę informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
   3) nieotrzymania przez Wykonawcę informacji związanych z prowadzonym postępowaniem w przypadku wskazania przez Wykonawcę w ofercie błędnego adresu, numeru telefonu, faxu, adresu e-mail lub numeru sprawy.
6. We wszelkiej korespondencji dotyczącej niniejszego postępowania zaleca się wskazywać na znak sprawy postępowania nadany przez Zamawiającego lub nazwę zamówienia nadaną przez Zamawiającego.

Rozdział IX.
Wymagania dotyczące wadium.

Zamawiający nie wymaga wniesienia wadium.

Rozdział X.
Termin związania ofertą.

1. Wykonawca jest związany ofertą przez okres **30 dni.**
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

Rozdział XI.
Opis sposobu przygotowania ofert.

1. Oferta musi być sporządzona zgodnie ze wzorem Formularza ofertowego, stanowiącym załącznik nr 1 do SIWZ. Do oferty należy dołączyć następujące oświadczenia i dokumenty:
   1) oświadczenia wskazane w Rozdziale VII ust. 1 SIWZ,
   2) wypełniony załącznik nr 5a do SIWZ w przypadku gdy Wykonawca oferuje rozwiązania równoważne opisywanym, wraz z dokumentami opisanymi w załączniku nr 5a do SIWZ.
2. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
3. Oferta powinna zostać przygotowana zgodnie z wymogami zawartymi w SIWZ, w języku polskim i w formie pisemnej.

4. Jeżeli Wykonawcy wspólnie ubiegają się o udzielenie zamówienia, ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i zawarcia umowy. Stosowne pełnomocnictwo w oryginale lub w postaci kopii poświadczonej notarialnie należy dołączyć do oferty.
5. Ofertę należy złożyć w zaklejonym, nienaruszonym opakowaniu **w Polskiej Akademii Nauk, Plac Defilad 1, 00-901 Warszawa, PKiN, piętro 25 pok. 2516.**
6. Opakowanie (koperta) z ofertą powinno być oznakowane w poniższy sposób:
   1) opis zawartości koperty: **„Oferta na odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego" – znak sprawy nr 24/ ZP/ 2016 nie otwierać przed 27 grudnia 2016 r. przed godz. 10.30",**
   2) adresat: **Polska Akademia Nauk, Plac Defilad 1, 00-901 Warszawa, PKiN, Zespół Zamówień Publicznych.**
   3) nadawca: nazwa, dokładny adres i numery telefonów Wykonawcy (dopuszcza się odcisk pieczęci).

   UWAGA: Zamawiający nie ponosi odpowiedzialności za otwarcie oferty przed terminem w przypadku nieprawidłowego oznaczenia koperty.
7. Oferta, której treść nie będzie odpowiadać treści SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt 3 ustawy Pzp, zostanie odrzucona (art. 89 ust. 1 pkt 2 ustawy Pzp). Wszelkie niejasności i wątpliwości dotyczące treści zapisów SIWZ należy wyjaśnić z Zamawiającym przed terminem składania ofert, w trybie przewidzianym w Rozdziale VIII SIWZ. Przepisy ustawy Pzp nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów projektu umowy, po terminie otwarcia ofert.
8. Wskazane jest, aby wszystkie zapisane, zadrukowane strony oferty były kolejno ponumerowane, złączone w sposób uniemożliwiający jej dekompletację.
9. Ofertę należy sporządzić w języku polskim na maszynie do pisania, komputerze lub inną trwałą i czytelną techniką biurową.
10. Wszelkie poprawki, zmiany lub wykreślenia w tekście oferty muszą być parafowane i datowane przez osobę upoważnioną do podpisywania oferty.
11. Oferta i oświadczenia muszą być podpisane przez osobę/osoby uprawnione do reprezentowania i składania oświadczeń woli w imieniu Wykonawcy – zgodnie z wpisem do właściwego rejestru lub w zakresem umocowania wynikającym z właściwego pełnomocnictwa.
12. Jeżeli upoważnienie do podpisywania oferty, oświadczeń, reprezentowania Wykonawcy/Wykonawców w postępowaniu wynika z pełnomocnictwa - winno być ono udzielone (podpisane) przez osobę /osoby uprawnione zgodnie z wpisem do właściwego rejestru, oraz dołączone do oferty. Pełnomocnictwo musi być złożone w formie oryginału lub kopii potwierdzonej notarialnie.
13. Zapis ustępu poprzedzającego stosuje się odpowiednio do dalszych pełnomocnictw.
14. Wymagane w SIWZ dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski.
15. Jeżeli według Wykonawcy oferta będzie zawierała informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, dane te należy umieścić w oddzielnej kopercie wewnątrz oferty, opisanej: „Informacje będące tajemnicą przedsiębiorstwa" oraz wskazać numery stron stanowiących tajemnicę przedsiębiorstwa a także wykazać zasadność utajnienia zgodnie z zasadą wynikającą z art. 8 ust. 3 ustawy Pzp W innym przypadku wszystkie informacje zawarte w ofercie będą uważane za ogólnie dostępne i mogą być udostępnione pozostałym Wykonawcom razem z protokołem postępowania. Zastrzeżenie informacji, danych, dokumentów lub

oświadczeń niestanowiących tajemnicy przedsiębiorstwa w rozumieniu przepisów o nieuczciwej konkurencji powoduje ich odtajnienie.

16. Zaleca się opracowanie pierwszych stron oferty wg załączonego do SIWZ wzoru. Niezastosowanie wzoru określonego w Załączniku nr 1 (Formularz oferty) nie spowoduje jej odrzucenia. Jednakże Zamawiający wymaga, żeby w złożonej ofercie znalazły się wszystkie oświadczenia i informacje zawarte we wzorze oferty.
17. Zgodnie z art. 84 ust. 1 ustawy Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. O wprowadzeniu zmian lub zamiarze wycofania oferty przed ostatecznym terminem składania ofert należy pisemnie zawiadomić Zamawiającego.
18. Zmiany do oferty należy umieścić w oddzielnej, zaklejonej i nienaruszonej kopercie z dopiskiem „ZMIANA". Na kopercie musi znajdować się nazwa Wykonawcy, dokładny adres i numer telefonu Wykonawcy (dopuszcza się odcisk pieczęci).
19. Wykonawca nie może wycofać oferty i wprowadzić zmian w ofercie po upływie ostatecznego terminu składania ofert.

Rozdział XII.
Miejsce oraz termin składania i otwarcia ofert.

1. Miejsce składania ofert – **Polska Akademia Nauk, Plac Defilad 1, 00-901 Warszawa, PKiN, piętro 25 pok. 2516.**
2. Termin składania ofert – **27 grudnia 2016 r. do godz. 10:00,**
3. Oferty złożone po tym terminie zostaną niezwłocznie zwrócone.
4. Miejsce otwarcia ofert – **w siedzibie Zamawiającego w Warszawie, Plac Defilad 1, 00-901 Warszawa, PKiN, (piętro 25 pok. nr 2516),**
5. Termin otwarcia ofert **27 grudnia 2016 r. o godz. 10:30.**

Rozdział XIII.
Opis sposobu obliczenia ceny.

1. Wykonawca w formularzu ofertowym:
   a) Poda wartość zamówienia netto, stawkę podatku VAT, wartość zamówienia brutto;
   b) Dokona obliczenia wartości zamówienia podając w tabeli: cenę jednostkową netto, cenę jednostkową brutto oraz wartość poszczególnych pozycji brutto (wyliczoną poprzez przemnożenie ceny jednostkowej brutto przez ilości określone przez Zamawiającego, wskazane w tabeli).
   c) Cenę oferty stanowi suma iloczynów ilości poszczególnych towarów i ich cen jednostkowych netto powiększona o należny podatek VAT, zgodnie z zasadą obliczenia wynikającą z tabeli zamieszczonej we wzorze formularza oferty.
2. Cena brutto zawiera stawkę podatku VAT, zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2004 r. Nr 54, poz. 535, z późn. zm.).
3. W cenie brutto należy uwzględnić wszystkie koszty jakie mogą powstać w trakcie realizacji zamówienia.
4. Ewentualne rabaty, upusty muszą być wliczone w cenę oferty.
5. Zamawiający wymaga, aby wszystkie ceny były podane z zaokrągleniem do dwóch miejsc po przecinku zgodnie z matematycznymi zasadami zaokrąglania tj.:
   a) ułamek kończący się cyfrą od 1 do 4 zaokrąglić należy w dół,
   b) ułamek kończący się cyfrą od 5 do 9 zaokrąglić należy w górę.

Rozdział XIV.
Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem znaczenia tych kryteriów i sposobu oceny ofert.

1. W przedmiotowym postępowaniu przy wyborze oferty najkorzystniejszej Zamawiający będzie się kierował następującymi kryteriami i ich wagami:
   1) Kryterium ceny – 60 %.
   2) Kryterium termin dostawy produktów – 40 %.

Dla celów porównawczych, przyjmuje się, że 1% = 1 pkt.

2. Zamawiający dokona oceny złożonych ofert, zgodnie z następującymi zasadami:

1) W ramach kryterium „cena" oferta zostanie oceniona na podstawie podanej przez Wykonawcę w ofercie ceny brutto za wykonanie zamówienia podanej w Formularzu oferty. Ocena punktowa w ramach kryterium ceny zostanie dokonana zgodnie ze wzorem:

$$C = \frac{Cmin}{Cbad} \times 60 \text{ pkt},$$

gdzie:
Cmin – oznacza najniższą zaproponowaną cenę,
Cbad – oznacza cenę zaproponowaną w badanej ofercie,
C – liczbę punktów przyznanych badanej ofercie w kryterium cena.

2) W ramach kryterium „termin dostawy produktów" - ocenie będzie podlegał zaproponowany przez Wykonawcę w ofercie termin dostawy produktów opisanych w Załączniku nr 5 do SIWZ a w przypadku gdy Wykonawca zaoferuje rozwiązania równoważne: termin dostawy sprzętu, oprogramowania, licencji, wdrożenia i instalacji sprzętu wraz z oprogramowaniem, przeprowadzenie testów oraz przeszkolenie personelu Zamawiającego (zgodnie z opisem określonym w Załączniku nr 5 do SIWZ).
3) Maksymalny termin realizacji określony przez Wykonawcę wynosi **30 dni kalendarzowych** od daty zawarcia umowy. Skrócenie ww. terminu będzie punktowane w następujący sposób:
   - dla oferowanego terminu dostawy produktów – 4 i mniej dni roboczych: 40 pkt,
   - dla oferowanego terminu dostawy produktów od 5 do 6 dni roboczych: 36 pkt,
   - dla oferowanego terminu dostawy produktów od 7 do 8 dni roboczych: 32 pkt,
   - dla oferowanego terminu dostawy produktów od 9 do 10 dni roboczych: 28 pkt,
   - dla oferowanego terminu dostawy produktów od 11 do 13 dni roboczych: 24 pkt,
   - dla oferowanego terminu dostawy produktów od 14 do 16 dni roboczych: 20 pkt.
   - dla oferowanego terminu dostawy produktów od 17 do 20 dni roboczych: 16 pkt.
   - dla oferowanego terminu dostawy produktów od 21 do 24 dni roboczych: 12 pkt.
   - dla oferowanego terminu dostawy produktów od 25 do 28 dni roboczych: 8 pkt.
   - dla oferowanego terminu dostawy produktów 29 dni roboczych: 4 pkt.
   - dla oferowanego terminu dostawy produktów 30 dni roboczych: 0 pkt.

4) Za ofertę najkorzystniejszą zostanie uznana ta oferta, która po zsumowaniu liczby punktów uzyskanych we wskazanych wyżej kryteriach uzyska największą liczbę punktów, z dokładnością do dwóch miejsc po przecinku – P

$$P = C + Td$$

gdzie:
P - całkowita liczba punktów przyznana ofercie,
C - liczba punktów przyznanych badanej ofercie w kryterium cena,
Id - liczba punktów przyznanych badanej ofercie w kryterium termin dostawy produktów.

3. W przypadku gdy dwie lub więcej ofert uzyska taki sam bilans punktów, zgodnie z art. 91 ust. 4 ustawy Pzp, Zamawiający wybierze ofertę z niższą ceną.

Rozdział XV.
Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.

1. Wykonawcy biorący udział w postępowaniu zostaną powiadomieni o jego wynikach.
2. Po zatwierdzeniu wyboru najkorzystniejszej oferty informacja o wyborze zostanie umieszczona na stronie internetowej Zamawiającego.
3. Zamawiający przystąpi do zawarcia umowy z wybranym Wykonawcą w trybie art. 94 ustawy, z uwzględnieniem zapisów art. 139 ustawy.

Rozdział XVI.
Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

Rozdział XVII.
Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli Zamawiający wymaga od Wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach.

1. Wzór umowy stanowi załącznik nr 6 do niniejszej SIWZ.
2. Zamawiający dopuszcza możliwość zmiany Umowy w zakresie dotyczącym Opisu przedmiotu zamówienia, co do sposobu realizacji zamówienia przez Wykonawcę, w następujących przypadkach:

a) wystąpienia konieczności wprowadzenia zmian, bez których nie byłoby możliwe prawidłowe wykonanie przedmiotu Umowy;
b) wystąpienia konieczności wprowadzenia zmian doprecyzowujących treści Umowy, jeżeli potrzeba ich wprowadzenia wynika z rozbieżności lub niejasności w Umowie, których nie można usunąć w inny sposób, a zmiana będzie umożliwiać usunięcie rozbieżności i doprecyzowanie Umowy w celu jednoznacznej interpretacji jej zapisów;
c) konieczności zrealizowania przedmiotu Umowy przy zastosowaniu innych rozwiązań technicznych/technologicznych niż wskazane w Ofercie Wykonawcy w sytuacji, gdyby zastosowanie przewidzianych rozwiązań groziłoby niewykonaniem lub wadliwym wykonaniem przedmiotu Umowy;

3. Zmiana umowy opisana w ust. 2 powyżej nie spowoduje zmiany ceny zaproponowanej przez Wykonawcę w ofercie.

4. Nie stanowią zmiany Umowy w rozumieniu art. 144 ustawy Pzp następujące przypadki (wymagają jedynie poinformowania drugiej Strony w formie pisemnej z 3 (trzy) dniowym wyprzedzeniem):
   a) zmiana danych teleadresowych Stron;
   b) zmiana danych rejestrowych Stron;
   c) zmiana sposobu prowadzenia korespondencji pomiędzy Stronami.

Rozdział XVIII.
Podstawy wykluczenia Wykonawcy z postępowania, o których mowa w art. 24 ust. 5 ustawy Pzp

Zamawiający przewiduje wykluczenie Wykonawcy na podstawie art. 24 ust. 5 ustawy Pzp, zgodnie z którym z postępowania o udzielenie zamówienia zamawiający może wykluczyć wykonawcę:

1. w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2015 r. poz. 978, 1259, 1513, 1830 i 1844) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2015 r. poz. 233, 978, 1166, 1259 i 1844).
2. Który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych.
3. jeżeli Wykonawca lub osoby, o których mowa w art. 24 ust. 1 pkt 14 ustawy, uprawnione do reprezentowania Wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2–4 ustawy z:
   1) Zamawiającym,
   2) osobami uprawnionymi do reprezentowania Zamawiającego,
   3) członkami komisji przetargowej,
   4) osobami, które złożyły oświadczenie, o którym mowa w art. 17 ust. 2a ustawy

   chyba że jest możliwe zapewnienie bezstronności po stronie Zamawiającego w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu.
4. który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z Zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4 ustawy, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania.
5. będącego osobą fizyczną, którego prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3000 złotych.
6. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za wykroczenie, o którym mowa w pkt 5.
7. wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o

zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną nie niższą niż 3000 złotych.

8. który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co Zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w art. 24 ust. 1 pkt 15 ustawy, chyba że Wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.

Rozdział XIX.
Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia.

Środki ochrony prawnej zostały określone w Dziale VI ustawy. Środki ochrony prawnej przysługują Wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy.

Załącznik nr 1 do SIWZ
wzór

OFERTA
(formularz ofertowy)

Nazwa i adres Wykonawcy:

.....

.....

NIP ..... REGON .....

Adres, na który Zamawiający powinien przesyłać ewentualną korespondencję:

.....

Osoba wyznaczona do kontaktów z Zamawiającym:

.....

Numer telefonu:.....

Numer faksu.....

e-mail .....

W odpowiedzi na ogłoszenie o przetargu nieograniczonym składamy niniejszą ofertę w postępowaniu pn: **„Odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego"** – znak sprawy nr 24/ ZP/ 2016 **oferując wykonanie przedmiotu zamówienia za łączną CENĘ OFERTOWĄ:**

CENA OFERTY NETTO.....zł

(słownie .....zł)

plus podatek VAT (23%) w kwocie ..... zł.

CENA OFERTY BRUTTO.....zł

(słownie .....zł)

Obliczoną zgodnie z poniższą kalkulacją:

Lp.	*Aktualizacja dla produktu*	*Oferowane urządzenie (nazwa, producent, model, rok produkcji) - w przypadku gdy Wykonawca oferuje rozwiązanie równoważne*	*j.m.*	*Ilość*	*Cena jednostkowa netto*	*Cena jednostkowa brutto*	*Wartość brutto*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8 (5 x 7)*
1.	*Pakiet licencji dla FortiAP 220B*		*szt.*	*1*			
2.	*Pakiet licencji dla FortiMail 100C*		*szt.*	*1*			
3.	*Pakiet licencji dla FortiGate 200B*		*szt.*	*2*			
4.	*Pakiet licencji dla FortiGate 40C*		*szt.*	*23*			
5.	*Pakiet licencji dla FortiGate 60C*		*szt.*	*1*			
6.	*Pakiet licencji dla FortiAnalyzer 100C*		*szt.*	*1*			
7.	*Pakiet licencji dla FortiManager - VM*		*szt.*	*1*			
8.	*Pakiet licencji dla FortiAP 223B*		*szt.*	*48*			
9.	*Pakiet licencji dla FortiWeb 400C*		*szt.*	*1*			
10.	*Pakiet licencji dla FortiGate 800C od 19.11.2017 r. do 15.02.2018 r.*		*szt.*	*2*			
	Razem						

1. **OŚWIADCZAMY,** że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
2. **ZOBOWIĄZUJEMY SIĘ** do wykonania zamówienia w terminie określonym w Rozdziale V SIWZ.
3. **AKCEPTUJEMY** warunki płatności określone przez Zamawiającego we wzorze Umowy (minimalny termin płatności: 14 dni od otrzymania faktury przez Zamawiającego).
4. **UWAŻAMY SIĘ** za związanych niniejszą ofertą przez czas wskazany w Specyfikacji Istotnych Warunków Zamówienia, tj. przez okres 30 dni uwzględniając, że termin składania ofert jest pierwszym dniem biegu terminu.

5. **OŚWIADCZAMY,** że termin dostawy produktów wynosi ..... dni.
   Uwaga: maksymalny termin dostawy produktów wynosi 30 dni. W przypadku zaoferowania rozwiązań równoważnych termin ten obejmuje dostawę sprzętu, oprogramowania, licencji, wdrożenia i instalację sprzętu wraz z oprogramowaniem, przeprowadzenie testów oraz przeszkolenie personelu Zamawiającego.
6. **PRZYJMUJEMY** do wiadomości[1], że niewypełnienie pozycji określonych w kolumnie „dane techniczne oferowanego sprzętu" w tabeli Załącznika nr 1 A do SIWZ „Wymagane minimalne parametry techniczne" w sposób wymagany lub udzielenie odpowiedzi negatywnej „nie spełnia'' spowoduje odrzucenie oferty, o ile z treści innych dokumentów stanowiących załączniki do oferty nie będzie wynikało, iż oferowane urządzenia spełniają wymagania określone w ww. tabeli.
7. OŚWIADCZAMY, że *(*niepotrzebne skreślić, a wymagane informacje uzupełnić, jeśli dotyczy)*:
   - nie zamierzamy powierzać wykonania części zamówienia podwykonawcom
   - zamierzamy powierzyć wykonanie następujących części zamówienia niżej wymienionym podwykonawcom:

   .....

Zgodnie z Rozdziałem VII ust. 10 SIWZ wskazuję dostępność poniżej wskazanych oświadczeń lub dokumentów, o których mowa w Rozdziale VII ust. 5 SIWZ w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych (jeżeli dotyczy):

Nazwa oświadczenia lub dokumentu (lub odpowiednie odesłanie do dokumentu wymaganego w SIWZ np. Rozdział VII ust. 5 pkt ... SIWZ):	Adres strony internetowej ogólnodostępnej i bezpłatnej bazy danych

Oferta została złożona na ..... parafowanych i kolejno ponumerowanych stronach.
Do oferty dołączono następujące załączniki:

Załącznik nr 1 – Oświadczenie dotyczące spełniania warunków
Załącznik nr 2 – Oświadczenie dotyczące przesłanek wykluczenia z postępowania

.....
(data, imię i nazwisko oraz podpis upoważnionego przedstawiciela Wykonawcy)

[1] Dotyczy Wykonawcy oferującego rozwiązanie równoważne

Załącznik nr 2 do SIWZ

Zamawiający:
Polska Akademia Nauk
Plac Defilad 1, 00-901 Warszawa
www.pan.pl
NIP: 5251575083, REGON: 000325713
Tel.: (22) 826 37 76, Faks: (22) 826 65 12

Wykonawca:

.....

.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

.....

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy

składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego"** – znak sprawy nr 24/ ZP/ 2016 oświadczam co następuje:

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust 1 pkt 12-23 ustawy Pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 24 ust. 5 ustawy Pzp .

..... *(miejscowość),* dnia ..... r.

.....

(podpis)

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ..... ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 24 ust. 1 pkt 13-14, 16-20 lub art. 24 ust. 5 ustawy Pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze:

.....

.....

.....

.....

..... *(miejscowość),* dnia ..... r.

.....

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODMIOTU, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że następujący/e podmiot/y, na którego/ych zasoby powołuję się w niniejszym postępowaniu, tj.:

.....

(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG) nie podlega/ją wykluczeniu z postępowania o udzielenie zamówienia.

..... *(miejscowość),* dnia ..... r.

.....

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY NIEBĘDĄCEGO PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA:

Oświadczam, że następujący/e podmiot/y, będący/e podwykonawcą/ami:

.....

(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG), nie podlega/ą wykluczeniu z postępowania o udzielenie zamówienia.

..... *(miejscowość),* dnia ..... r.

.....

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

..... *(miejscowość),* dnia ..... r.

.....

(podpis)

Załącznik nr 3 do SIWZ

Zamawiający:
Polska Akademia Nauk
Plac Defilad 1, 00-901 Warszawa
www.pan.pl
NIP: 5251575083, REGON: 000325713
Tel.: (22) 826 37 76, Faks: (22) 826 65 12

Wykonawca:

.....

.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

.....

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy

składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.

Prawo zamówień publicznych (dalej jako: ustawa Pzp),

DOTYCZĄCE SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **„Odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego"** – znak sprawy nr 24/ ZP/ 2016 oświadczam co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY:

Oświadczam, że spełniam warunki udziału w postępowaniu określone przez zamawiającego w .....

(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu).

..... *(miejscowość),* dnia ..... r.

.....

(podpis)

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez zamawiającego w .....

(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu), polegam na zasobach następującego/ych podmiotu/ów:

.....

.....

w następującym zakresie: .....

.....

(wskazać podmiot i określić odpowiedni zakres dla wskazanego podmiotu).

..... *(miejscowość),* dnia ..... r.

.....

(podpis)

OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

..... *(miejscowość),* dnia ..... r.

.....

(podpis)

Załącznik nr 4 do SIWZ

Zamawiający:
Polska Akademia Nauk
Plac Defilad 1, 00-901 Warszawa
www.pan.pl
NIP: 5251575083, REGON: 000325713
Tel.: (22) 826 37 76, Faks: (22) 826 65 12

Wykonawca:

.....

.....

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

.....

.....

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

OŚWIADCZENIE
DOTYCZĄCE PRZYNALEŻNOŚCI DO GRUPY KAPITAŁOWEJ

W związku z ubieganiem się o udzielenie zamówienia publicznego pn. **„Odnowienie subskrypcji oprogramowania/ wsparcia wraz z wyrównaniem terminu do 15.02.2018 r. dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego"** – znak sprawy nr 24/ ZP/ 2016 oświadczam/my, że:

a) należę/my do tej samej grupy kapitałowej (w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. 2015 r., poz. 184 z późn. zm.), wraz z następującymi wykonawcami, którzy złożyli odrębne oferty:*

1) .....
2) .....
3) .....

b) nie należę/my do grupy kapitałowej, wraz z innymi wykonawcami, którzy złoży odrębne oferty*

* niepotrzebne skreślić

Uwaga: w przypadku przynależności do tej samej grupy kapitałowej wykonawca może złożyć, wraz z oświadczeniem dokumenty bądź informacje potwierdzające, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu.

.....	.....	.....
data	imię i nazwisko	podpis wykonawcy lub osoby upoważnionej

Szczegółowy opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest przedłużenie pakietu licencji obejmującego: gwarancje, wsparcie techniczne, możliwość aktualizacji oprogramowania dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego oraz subskrypcje bezpieczeństwa w zakresie antywirus, antyspam, IPS, Web filter dla urządzeń typu UTM, w zakresie atywirus, antyspam dla urządzeń zabezpieczających serwery poczty elektronicznej, zakresie antywirus, web security service, IP Reputation Service dla urządzeń monitorujących ruch www wraz z wyrównaniem terminu dla wszystkich urządzeń do 15.02.2018 r. Urządzenia, których termin podlega wyrównaniu posiadają numery seryjne: FG800C3912801356, FG800C3912801722.

FortiAP 220B - 1 szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Hardware Coverage	Return To Factory
Firmware & General Updates	Web/Online
Enhanced Support	8x5

FortiMail1100C-1 szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Hardware Coverage	Return To Factory
Firmware & General Updates	Web/Online
Enhanced Support	8x5
Virus Definitions Updates	Web/Online
FortiGuard AntiSpam	Web/Online

FortiGate 200B — 2szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Hardware Coverage	Return To Factory
Firmware & General Updates	Web/Online
Enhanced Support	8x5
Virus Definitions Updates	Web/Online
Next Generation Firewall	Web/Online
FortiGuard Web Filtering	Web/Online
FortiGuard AntiSpam	Web/Online

FortiGate 40C - 23szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Hardware Coverage	Return to Factory
Firmware & General Updates	Web/Online
Enhanced Support	8x5
Virus Definitions Updates	Web/Online
Next Generation Firewall	Web/Online
FortiGuard Web Filtering	WebOonline
FortiGuard AntiSpam	Web/Online

FortiGate 60C — 1szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Hardware Coverage	Return to Factory
Firmware & General Updates	Web/Online
Enhanced Support	8x5
Virus Definitions Updates	Web/Online
Next Generation Firewall	Web/Online
FortiGuard Web Filtering	Web/Online
FortiGuard AntiSpam	Web/Online

FortiAnalyzer 100C— 1szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Hardware Coverage	Return To Factory
Firmware & General Updates	Web/Online
Enhanced Support	8x5

FortiManager -VM — 1 szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Firmware & General Updates	Web/Online
Enhanced Support	24x7
Telephone Support	24x7

FortiAP 223B - 48szt.
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Hardware Coverage	Return to Factory
Firware & General Updates	Web/Online
Enhanced Support	8x5

FortiWeb 400C - 1szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 15.02.2017 r.)

Support Type	Support Level
Hardware Coverage	Return to Factory
Firware & General Updates	Web/Online
Enhanced Support	8x5
Virus Definitions Updates	Web/Online
FortiWeb Security Service	Web/Online
IP Reputation	Web/Online

FortiGate 800C – 2szt
Zakres wsparcia produktu do 15.02.2018 r.
(bieżący termin wsparcia upływa 19.11.2017 r.)

Support Type	Support Level
Hardware Coverage	Return to Factory
Firmware & General Updates	Web/Online
Enhanced Support	8x5
Virus Definitions Updates	Web/Online
Next Generation Firewall	Web/Online
FortiGuard Web Filtering	WebOonline
FortiGuard AntiSpam	Web/Online

Dostawa powyższych produktów w terminie maksymalnie **30 dni kalendarzowych** od daty zawarcia umowy.
Skrócenie tego terminu będzie punktowane zgodnie z kryteriami oceny ofert, zgodnie z Rozdziałem XIV SIWZ.
Szczegółowy opis realizacji przedmiotu zamówienia zawierają zapisy we wzorze umowy stanowiącej załącznik nr 6 do SIWZ.

2. Rozwiązanie równoważne
Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązania równoważnego. Rozwiązanie równoważne będzie obejmowało dostawę sprzętu (równoważnego dla wskazanego w pkt A — J Załącznika nr 1a, posiadanego przez Zamawiającego) — w ilościach wskazanych w Załączniku nr 1a, oprogramowania, licencji, zapewnienie wsparcia technicznego i gwarancji producenta oferowanego rozwiązania, wdrożenie i instalację sprzętu wraz z oprogramowaniem, przeprowadzenie testów oraz przeszkolenie personelu Zamawiającego w zakresie podstaw obsługi oprogramowania. Zaoferowane przez Wykonawcę rozwiązanie równoważne musi zapewniać pełną funkcjonalną zamienność produktu z produktem zamawianym, posiadać co najmniej takie same parametry techniczne i funkcjonalne oraz spełniać wymogi dotyczące jakości, gwarancji i serwisów) opisane w tabelach zawartych w Załączniku nr 1a do SIWZ („Wymagane minimalne parametry techniczne", „Wymagania dotyczące spełniania przez oferowane urządzenia równoważne odpowiednich wymogów co do jakości, gwarancji i serwisów").
W przypadku zaoferowania rozwiązania równoważnego, zamówienie zostanie zrealizowane zgodnie z poniższymi warunkami:
a) dostawa sprzętu, oprogramowania, licencji, wdrożenie i instalacja sprzętu wraz z oprogramowaniem, przeprowadzenie testów oraz przeszkolenie personelu Zamawiającego, zostaną dokonane w terminie **30 dni kalendarzowych** od daty zawarcia umowy;
UWAGA: Skrócenie tego terminu będzie punktowane zgodnie z kryteriami oceny ofert, zgodnie z Rozdziałem XIV SIWZ.
b) miejscem dostawy jest siedziba Zamawiającego: Plac Defilad 1, 00-901 Warszawa
c) koszty dostawy (w tym koszty opakowania, transportu, ubezpieczenia) ponosi Wykonawca;

d) sprzęt wchodzący w zakres dostawy zostanie dostarczony Zamawiającemu w opakowaniach zabezpieczających przed uszkodzeniem w czasie transportu;
e) Wykonawca poinformuje Zamawiającego e-mailem na adres: . . . . . lub faxem na nr: .....o dniu planowanej realizacji dostawy co najmniej dwa dni robocze wcześniej przed planowaną datą dostawy;
f) wdrożenie, instalacja i testowanie zaoferowanego rozwiązania w środowisku sprzętowo-programowym Zamawiającego zostaną dokonane w konsultacji z pracownikami Zamawiającego;
g) szkolenie personelu Zamawiającego, w wymiarze ok 40 godzin, odbędzie się w siedzibie Zamawiającego, będzie obejmowało nie więcej niż 5 osób i zostanie przeprowadzone jednorazowo (w jednym terminie dla wszystkich osób);
h) testy zostaną przeprowadzone w siedzibie Zamawiającego, przy współudziale Zamawiającego i będą obejmowały weryfikację równoważności rozwiązania pod kątem wymaganych parametrów technicznych określonych w SIWZ.
i) wsparcie techniczne i licencja będą obejmowały okres 12 miesięcy, liczony od dnia dostawy potwierdzonej protokołem odbioru;
j) realizacja dostawy, wdrożenia, testów i szkolenia dla personelu Zamawiającego zostaną potwierdzone protokołem odbioru, podpisanym przez przedstawicieli obu Stron.

Wymagania dla rozwiązania równoważnego

A. FortiAP 220B 1szt

Wymagane parametry równoważności:

Lp.	Wymagane minimalne parametry techniczne		Dane techniczne oferowanego sprzętu *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent: .....** **Model: .....** **Rok produkcji: .....** *(*należy uzupełnić wszystkie wykropkowane pola)*			
1.	Tryb pracy	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. Ze względu na instniejącą infrastrukturę i uzyskania wymaganego poziomu bezpieczeństwa kontroler sieci wireless ma być uruchomiony w obrębie urządzenia bezpieczeństwa gwarantującego ochronę dla obsługiwanych sieci wireless i przewodowych. W posiadaniu Zamawiającego jest urządzenie klasy UTM – Fortigate 800C.	**Spełnia/Nie spełnia***
2.	Moduł radiowy	Musi być wyposażone w dwa niezależne moduły radiowe, jeden z nich ma pracować w paśmie 5 GHz a/n lub 2,4 GHz b/g/n (do wyboru), drugi natomiast ma zapewniać obsługę zakresu 2,4 GHz b/g/n. Musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID. Wymagana moc nadawania min 17dBm.	*Ilość niezależnych modułów radiowych:* ..... *Ilość jednocześnie rozgłaszanych SSID:* ..... *Moc nadawania:* ..... **Spełnia/Nie spełnia***
3.	Anteny	Minimum 2 anteny wbudowane	*Ilość wbudowanych anten:* ..... **Spełnia/Nie spełnia***
4.	Interfejsy	Minimum 1 interfejs w standardzie 10/100/1000 Base-TX	*Ilość interfejsów w standardzie 10/100/1000 Base-TX:* ..... **Spełnia/Nie spełnia***
5.	Zasilanie	Możliwość zasilania w standardzie PoE 802.3af	**Spełnia/Nie spełnia***
6.	Oprogramowanie	Możliwość aktualizacji firmware minimum przez 12 miesięcy	**Spełnia/Nie spełnia***

B. FortiMail 100C 1szt

Wymagane parametry równoważności:

Lp.		Wymagane minimalne parametry techniczne	Dane techniczne oferowanego sprzętu *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent:**..... **Model**..... **Rok produkcji:** ..... *(*należy uzupełnić wszystkie wykropkowane pola)*			
1.	System	Opcje instalacji w trybie transparentnym, bramki i serwera Obsługa VLAN i interfejsów redundantnych Obsługa adresów IPv6 i IPv4 Wirtualny hosting korzystający z zasobów źródłowych i/lub docelowych adresów IP Obsługa uwierzytelnienia SMTP za pośrednictwem serwerów LDAP, RADIUS,POP3 i IMAP Routnig wiadomości e-mail z użyciem protokołu LDAP Kompleksowy interfejs WebMail do operacji w trybie serwera i zarządzania kwarantanną Zarządzanie kolejką wiadomości Kontrola każdego z użytkowników na podstawie reguł dla danej domeny z użyciem atrybutów LDAP Uwierzytelnianie wiadomości e-mail Tworzenie lokalnej listy reputacji nadawców na podstawie metod sender policy framework, domain keys Identified Mail Kontrola wiadomości przychodzących i wychodzących Wiele domen poczty elektronicznej z możliwością konfiguracji hierarchicznej Kompletna, wielowarstwowa ochrona antywirusowa, antyspamowa, przeciw złośliwemu oprogramowaniu i atakom typu fishing dla nieograniczonej liczby użytkowników.	**Spełnia/Nie spełnia***
2.	Zarządzanie , rejestrowanie, raportowanie	Konta administracyjne dla każdej z domen oparte na rolach Kompleksowe rejestrowanie i raportowanie aktywności i incydentów Rejestr zmian konfiguracji i zdarzeń dotyczących zarządzania Wbudowany moduł raportujący Wsparcie ze strony rozwiązań **służących do centralnego zarządzania i raportowania opisanych w punktach F i G**	**Spełnia/Nie spełnia***

		Obsługa protokołu SNMP z użyciem standardowych i personalizowanych plików MIB Obsługa zewnętrznych lub lokalnych zasobów pamięci masowej , w tym urządzeń iSCSI Obsługa zewnętrznych zdarzeń	
3.	Wydajność	tryb Acticve-Passive Synchronizacja kwarantanny i kolejek wiadomości Wykrywanie usterek urządzneiea i powiadamianie o nich Monitorowanie statusu łącza, przełączeń awaryjnych wraz z obsługą interfejsu nadmiarowego	**Spełnia/Nie spełnia***
4.	Szyfrowanie	Szyfrowanie na podstawie tożsamości w przesyle wiadomosci w trybie Push i Pull Obsługa standardu S/MIME w szyfrowaniu miedzy serwerami pocztowymi Obsługa silnych protokołów szfrujących , w tym HTTPS,SMTPS,SSH,IMAPS i POP3S	**Spełnia/Nie spełnia***
5.	tryb serwera	Usługi poczty e-mail SMTP,IMAP,POP3 Obsługa protokołu SMTP over SSl Obsługa polityk przydziału przestrzeni dyskowej dla użytkowników Bezpieczny dostęp do klienta Webmail Obsługa list użytkowników, grp i pseudonimów Uwierzytelnianie konta na poziomie lokalnym i serwera LDAP Kalendarz WebMail Preferencje dotyczące automatycznego odpowiadamia i przesyłania wiadomości dalej Synchronizacja książki adresowej z sererem LDAP	**Spełnia/Nie spełnia***
6.	Oprogramowanie	oprogramowanie typu antywirus, antyspam licencja minimum na 12 miesięcy Możliwość aktualizacji firmware minimum przez 12 miesięcy	**Spełnia/Nie spełnia***

C. FortiGate 200B 2 szt

Wymagane parametry równoważności:

Lp.	Wymagane minimalne parametry techniczne		Dane techniczne oferowanego sprzętu *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent:**..... **Model**..... **Rok produkcji:** ..... (**należy uzupełnić wszystkie wykropkowane pola)*			
1.	Architektura systemu ochrony	Główne urządzenie ochronne [gateway] musi używać pamięć FLASH. (nie dopuszcza się użycia dysku) Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).	**Spełnia/Nie spełnia***
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.	**Spełnia/Nie spełnia***
3.	Ilość/rodzaj portów	Nie mniej niż **8** portów Ethernet 10/100/1000 Base-TX. Nie mniej niż **4080** interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q	*Liczba portów* Ethernet 10/100/1000 BASE-TX..... *Liczba interfejsów wirtualnych*..... **Spełnia/Nie spełnia***
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: - kontrolę dostępu - zaporę ogniową klasy Stateful Inspection - ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP). Kontrola AV powinna bazować na analizie plików z wykorzystaniem technologii proxy. - poufność danych - IPSec VPN oraz SSL VPN - ochronę przed atakami - Intrusion Prevention System [IPS/IDS] - oraz funkcjonalności uzupełniających: - kontrolę treści – Web Filter [WF] - kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP; POP3, IMAP) - kontrolę pasma oraz ruchu [QoS i Traffic shaping] - kontrolę aplikacji (minimum IM oraz P2P)	**Spełnia/Nie spełnia***
5.	Zasada działania (tryby)	Urządzenie musi dawać możliwość ustawienia jednego z dwóch trybów pracy: - jako router/NAT (3.warstwa ISO-OSI) lub	**Spełnia/Nie spełnia***

		- jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.	
6.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety).	**Spełnia/Nie spełnia***
7.	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. - Nie mniej niż 4000 sygnatur ataków. - Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie - Możliwość wykrywania anomalii protokołów i ruchu	**Spełnia/Nie spełnia***
8.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT.	**Spełnia/Nie spełnia***
9.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.	**Spełnia/Nie spełnia***
10.	Połączenia VPN	Wymagane nie mniej niż: - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site - Dostawca musi udostępniać klienta VPN własnej produkcji - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności - Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) - Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	**Spełnia/Nie spełnia***
11.	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: -haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia -haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP - haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.	**Spełnia/Nie spełnia***

12.	Wydajność	Obsługa nie mniej niż **500 tys** jednoczesnych połączeń i **15 tys** nowych połączeń na sekundę Przepływność nie mniejsza niż **5 Gbps** dla ruchu nieszyfrowanego i **1,5 Gbps** dla VPN (3DES). Obsługa nie mniej niż **2000** jednoczesnych tuneli VPN	*Liczba jednoczesnych połączeń……* *Liczba nowych połączeń……* *Przepływność Gbps dla ruchu nie szyfrowanego……* *Przepływność Gpps dla VPN (3DES)……* *Liczba jednoczesnych tuneli VPN……* **Spełnia/Nie spełnia***
13.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive. System powinien zostać dostarczony w formie klastra urządzeń.	**Spełnia/Nie spełnia***
14.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: - haseł statycznych - haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.	**Spełnia/Nie spełnia***
15.	Zarządzanie	System musi mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym: - Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej - Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości - Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia - Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia - Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) - Zapis i zdalne wykonywanie skryptów na urządzeniach	**Spełnia/Nie spełnia***
16.	Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: - Zbieranie logów z urządzeń bezpieczeństwa - Generowanie raportów - Skanowanie podatności stacji w sieci - Zdalną kwarantannę dla modułu antywirusowego	*……sumaryczna wielkość logów* **Spełnia/Nie spełnia***

		System musi posiadać również funkcję lokalnego logowania i przechowywania logów o sumarycznym rozmiarze min. 63GB.	
17.	Integracja systemu zarządzania	Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów.	**Spełnia/Nie spełnia***
18.	Oprogramowanie	oprogramowanie typu antywirus, antyspam, IPS, Web Filter licencja minimum na 12 miesięcy Możliwość aktualizacji firmware przez minimum na 12 miesięcy	**Spełnia/Nie spełnia***

D. FortiGate 40C 23 szt

Wymagane parametry równoważności:

Lp.	**Wymagane minimalne parametry techniczne**		**Dane techniczne oferowanego sprzętu** *(należy uzupełnić wszystkie wykropkowane pola)* *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent:** ..... **Model:** ..... **Rok produkcji:** ..... *(*należy uzupełnić wszystkie wykropkowane pola)*			
1.	Architektura systemu ochrony	Główne urządzenie ochronne [gateway] musi używać pamięć FLASH. (nie dopuszcza się użycia dysku) Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).	**Spełnia/Nie spełnia***
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.	**Spełnia/Nie spełnia***

3.	Ilość/rodzaj portów	Nie mniej niż 2 porty WAN Ethernet Interfaces 10/100 Base-TX. Nie mniej niż 1 port DMZ Ethernet 10/100 Base-TX Nie mniej niż 5 portów Ethernet 10/100/1000 Base-TX. Nie mniej niż 256 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q Urządzenie musi posiadać SD slot 1 szt.	*Liczba portów WAN* Ethernet Interfaces 10/100 BASE-TX..... *Liczba portów* DMZ Ethernet 10/100 BASE-TX..... *Liczba portów* Ethernet 10/100/1000 BASE-X..... *Liczba interfejsów wirtualnych*..... *Licbaz slotów SD*..... **Spełnia/Nie spełnia***
4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: - kontrolę dostępu - zaporę ogniową klasy Stateful Inspection - ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP). Kontrola AV powinna bazować na analizie plików z wykorzystaniem technologii proxy. - poufność danych - IPSec VPN oraz SSL VPN - ochronę przed atakami - Intrusion Prevention System [IPS/IDS] - oraz funkcjonalności uzupełniających: - kontrolę treści – Web Filter [WF] - kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP; POP3, IMAP) - kontrolę pasma oraz ruchu [QoS i Traffic shaping] - kontrolę aplikacji (minimum IM oraz P2P)	**Spełnia/Nie spełnia***
5.	Zasada działania (tryby)	Urządzenie musi dawać możliwość ustawienia jednego z dwóch trybów pracy: - jako router/NAT (3.warstwa ISO-OSI) - lub jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.	**Spełnia/Nie spełnia***
6.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety).	**Spełnia/Nie spełnia***
7.	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. - Nie mniej niż 4000 sygnatur ataków. - Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie Możliwość wykrywania anomalii protokołów i ruchu	**Spełnia/Nie spełnia***
8.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT.	**Spełnia/Nie spełnia***

9.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.	**Spełnia/Nie spełnia***
10.	Połączenia VPN	Wymagane nie mniej niż: - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site - Dostawca musi udostępniać klienta VPN własnej produkcji - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności - Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	**Spełnia/Nie spełnia***
11.	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: - haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP - haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.	**Spełnia/Nie spełnia***
12.	Wydajność	Obsługa nie mniej niż **80 tys** jednoczesnych połączeń i **3 tys** nowych połączeń na sekundę Przepływność nie mniejsza niż **1 Gbps** dla ruchu nieszyfrowanego i **70 Mbps** dla VPN (3DES). Obsługa nie mniej niż **500** jednoczesnych tuneli VPN	*Liczba jednoczesnych połączeń.....* *Liczba nowych połączeń.....* *Przepływność Gbps dla ruchu nie szyfrowanego.....* *Przepływność Mbps dla VPN (3DES).....* *Liczba jednoczesnych tuneli VPN.....* **Spełnia/Nie spełnia***
13.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive.	**Spełnia/Nie spełnia***

14.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: - haseł statycznych - haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.	**Spełnia/Nie spełnia***
15.	Zarządzanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym: - Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej - Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości - Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia - Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia - Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) Zapis i zdalne wykonywanie skryptów na urządzeniach.	**Spełnia/Nie spełnia***
16.	Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: - Zbieranie logów z urządzeń bezpieczeństwa - Generowanie raportów - Skanowanie podatności stacji w sieci - Zdalną kwarantannę dla modułu antywirusowego System musi posiadać również funkcję lokalnego logowania i przechowywania logów o sumarycznym rozmiarze min. 16GB.	*sumaryczna wielkość logów* .... **Spełnia/Nie spełnia***
17.	Integracja systemu zarządzania	Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów.	**Spełnia/Nie spełnia***
18.	Oprogramowanie	oprogramowanie typu antywirus, antyspam, IPS, Web Filter licencja minimum na 12 miesięcy Możliwosć aktualizacji firmware minimum przez 12 miesięcy.	**Spełnia/Nie spełnia***

E. FortiGate 60C 1szt

Wymagane parametry równoważności:

Lp.	Wymagane minimalne parametry techniczne		Dane techniczne oferowanego sprzętu *(niepotrzebne skreślić, a wymagane pola uzupełnić).*
Oferowane urządzenia: **Producent: .....** **Model: .....** **Rok produkcji: .....** *(*należy uzupełnić wszystkie wykropkowane pola)*			
1.	Architektura systemu ochrony	Główne urządzenie ochronne [gateway] musi używać pamięć FLASH. (nie dopuszcza się użycia dysku) Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizowanego układu ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).	**Spełnia/Nie spełnia***
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.	**Spełnia/Nie spełnia***
3.	Ilość/rodzaj portów	Nie mniej niż 2 porty WAN Ethernet Interfaces 10/100 Base-TX. Nie mniej niż 1 port DMZ Ethernet 10/100 Base-TX Nie mniej niż 5 portów Ethernet 10/100/1000 Base-TX. Nie mniej niż 256 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard IEEE802.1q Urządzenie musi posiadać SD slot 1 szt.	*Liczba portów WAN* Ethernet Interfaces 10/100 BASE-TX..... *Liczba portów* DMZ Ethernet 10/100 BASE-TX..... *Liczba portów* Ethernet 10/100/1000 BASE-X..... *Liczba interfejsów wirtualnych*..... *Liczba slotów SD*..... **Spełnia/Nie spełnia***

4.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: - kontrolę dostępu - zaporę ogniową klasy Stateful Inspection - ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP). Kontrola AV powinna bazować na analizie plików z wykorzystaniem technologii proxy. - poufność danych - IPSec VPN oraz SSL VPN - ochronę przed atakami - Intrusion Prevention System [IPS/IDS] - oraz funkcjonalności uzupełniających: - kontrolę treści – Web Filter [WF] - kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP; POP3, IMAP) - kontrolę pasma oraz ruchu [QoS i Traffic shaping] - kontrolę aplikacji (minimum IM oraz P2P)	**Spełnia/Nie spełnia***
5.	Zasada działania (tryby)	Urządzenie musi dawać możliwość ustawienia jednego z dwóch trybów pracy: - jako router/NAT (3.warstwa ISO-OSI) - lub jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.	**Spełnia/Nie spełnia***
6.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników sieci, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem (m.in. pasmo gwarantowane i maksymalne, priorytety).	**Spełnia/Nie spełnia***
7.	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. - Nie mniej niż 4000 sygnatur ataków. - Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie Możliwość wykrywania anomalii protokołów i ruchu	**Spełnia/Nie spełnia***
8.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT.	**Spełnia/Nie spełnia***
9.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne ustawienia wszystkich funkcji bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.	**Spełnia/Nie spełnia***

10.	Połączenia VPN	Wymagane nie mniej niż: - Tworzenie połączeń w topologii Site-to-site oraz Client-to-site - Dostawca musi udostępniać klienta VPN własnej produkcji - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności - Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	**Spełnia/Nie spełnia***
11.	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: - haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia - haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP - haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie musi umożliwiać budowę logowania Single Sign On w środowisku Active Directory oraz eDirectory bez dodatkowych opłat licencyjnych.	**Spełnia/Nie spełnia***
12.	Wydajność	Obsługa nie mniej niż **80 tys** jednoczesnych połączeń i **3 tys** nowych połączeń na sekundę Przepływność nie mniejsza niż **1 Gbps** dla ruchu nieszyfrowanego i **70 Mbps** dla VPN (3DES). Obsługa nie mniej niż **500** jednoczesnych tuneli VPN	*Liczba jednoczesnych połączeń.....* *Liczba nowych połączeń.....* *Przepływność Gbps dla ruchu nie szyfrowanego.....* *Przepływność Mbps dla VPN (3DES).....* *Liczba jednoczesnych tuneli VPN.....* **Spełnia/Nie spełnia***
13.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive.	**Spełnia/Nie spełnia***
14.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz wbudowaną konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: - haseł statycznych - haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB. Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.	**Spełnia/Nie spełnia***

15.	Zarządzanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym: - Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej - Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości - Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia - Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia - Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) Zapis i zdalne wykonywanie skryptów na urządzeniach.	**Spełnia/Nie spełnia***
16.	Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: - Zbieranie logów z urządzeń bezpieczeństwa - Generowanie raportów - Skanowanie podatności stacji w sieci - Zdalną kwarantannę dla modułu antywirusowego System musi posiadać również funkcję lokalnego logowania i przechowywania logów o sumarycznym rozmiarze min. 16GB.	*sumaryczna wielkość logów* .... **Spełnia/Nie spełnia***
17.	Integracja systemu zarządzania	Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych.. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów.	**Spełnia/Nie spełnia***
18.	Oprogramowanie	oprogramowanie typu antywirus, antyspam, IPS, Web Filter licencja minimum na 12 miesięcy Możliwość aktualizacji firmwareprzez minimum na 12 miesięcy	..... **Spełnia/Nie spełnia***

F. FortiAnalyzer 100C 1szt

Wymagane parametry równoważności:

Lp.		Wymagane minimalne parametry techniczne	Dane techniczne oferowanego sprzętu *(należy zbędne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent:** ..... **Model:** ..... **Rok produkcji:** ..... (**należy uzupełnić wszystkie wykropkowane pola)*			
1.	Architektura systemu ochrony	System logowania i raportowania musi stanowić centralne repozytorium danych gromadzonych przez wiele urządzeń oraz aplikacji klienckich z możliwością definiowania własnych raportów na podstawie predefiniowanych wzorców. Jednocześnie, dla zapewnienia bezpieczeństwa i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta.	**Spełnia/Nie spełnia***
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.	**Spełnia/Nie spełnia***
3.	Parametry fizyczne systemu	Nie mniej niż 1 port Ethernet 10/100 Nie mniej niż 2 porty Ethernet 10/100/1000 Powierzchnia dyskowa - minimum 1 TB	*Podać liczbę portów* *Liczba portów* Ethernet 10/100..... 10/100/1000..... *Wielkość dysku*..... **Spełnia/Nie spełnia***
4.	Funkcjonalności podstawowe i uzupełniające	System musi zapewniać: - Składowanie oraz archiwizację logów z możliwością ich grupowania w oparciu o urządzenia, użytkowników - Możliwość gromadzenia zawartości przesyłanych za pośrednictwem protokołów Web, FTP; email, IM oraz na ich podstawie analizowania aktywności użytkowników w sieci - Kwarantannę dla współpracujących z nim urządzeń. Kwarantanna obejmuje zainfekowane lub wskazane przez analizę heurystyczną pliki. - Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących - Wyświetlanie nowych logów w czasie rzeczywistym - Analizowanie ruchu w sieci poprzez nasłuch całej komunikacji w segmencie sieci z możliwością jej zapisu i późniejszej analizy - Analizę podatności stacji w sieci wraz z możliwością raportowania wykrytych luk - Export zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych) Urządzenie musi realizować funkcje skanowania podatności stacji w sieci.	**Spełnia/Nie spełnia***

5.	Parametry wydajnościowe	Urządzenie musi obsługiwać: - nie mniej niż 100 urządzeń sieciowych i 100 urządzeń klienckich /VPN-client/	*Liczba urządzeń sieciowych*..... *Liczba urządzeń klienckich*..... **Spełnia/Nie spełnia***
6.	Zarządzanie	System udostępnia: Lokalny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH i konsolę szeregową	**Spełnia/Nie spełnia***
7.	Zasilanie	Zasilanie z sieci 230V/50Hz.	**Spełnia/Nie spełnia***
8.	Oprogramowanie	Możliwość aktualizacji firmware przez minimum na 12 miesięcy	**Spełnia/Nie spełnia***

G. FortiManager VM 1szt.

Wymagane parametry równoważności:

Lp.	Wymagane minimalne parametry techniczne		Dane techniczne oferowanego sprzętu *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent:** ..... **Model:** ..... **Rok produkcji:** ..... *(*należy uzupełnić wszystkie wykropkowane pola)*			
1,	Tryb pracy	Możliwość obsługi minimum 10 instancji wirtualnych VDOM oraz minimum 50 klientami VPN. Minimum jeden interfejs sieciowy.	*Ilość instancji wirtualnych* ..... *Ilość interfejsów sieciowych* ..... **Spełnia/Nie spełnia***

H. FortiAP 223B 48szt

Wymagane parametry równoważności:

Lp.	Wymagane minimalne parametry techniczne		Dane techniczne oferowanego sprzętu *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent:** ..... **Model:** ..... **Rok produkcji:** ..... *(*należy uzupełnić wszystkie wykropkowane pola)*			
1.	Tryb pracy	Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. Ze względu na instniejącą infrastrukturę i uzyskania wymaganego poziomu bezpieczeństwa kontroler sieci wireless ma być uruchomiony w obrębie urządzenia bezpieczeństwa gwarantującego ochronę dla obsługiwanych sieci wireless i przewodowych. W posiadaniu Zamawiającego jest urządzenie klasy UTM – Fortigate 800C.	**Spełnia/Nie spełnia***

2.	Obudowa	Kompaktowa obudowa z tworzywa sztucznego (o max średnicy lub przekątnej 18cm i grubości max 4 cm) umożliwiającą montaż na suficie lub ścianie wewnątrz budynku. Wymaga się aby interfejs sieciowy i inne gniazda - jeśli występują-zlokalizowane były na ściance od strony montażowej urządzenia.	*Wymiary obudowy:* ..... **Spełnia/Nie spełnia***
3.	Moduł radiowy	Musi być wyposażone w dwa niezależne moduły radiowe, jeden z nich ma pracować w paśmie 5 GHz a/n lub 2,4 GHz b/g/n (do wyboru), drugi natomiast ma zapewniać obsługę zakresu 2,4 GHz b/g/n. Musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID. Wymagana moc nadawania min 17dBm.	*Ilość niezależnych modułów radiowych:* ..... *Ilość jednocześnie rozgłaszanych SSID:* ..... *Moc nadawania:* ..... **Spełnia/Nie spełnia***
4.	Anteny	Minimum 4 anteny wbudowane	*Ilość wbudowanych anten:* ..... **Spełnia/Nie spełnia***
5.	Interfejsy	Minimum 1 interfejs w standardzie 10/100/1000 Base-TX	*Ilość interfejsów w standardzie 10/100/1000 Base-TX:* ..... **Spełnia/Nie spełnia***
6.	Zasilanie	Możliwość zasilania w standardzie PoE 802.3af	**Spełnia/Nie spełnia***
7.	Oprogram owanie	Możliwosć aktualizacji firmware przez minimum na 12 miesięcy	**Spełnia/Nie spełnia***

I. FortiWeb 400C 1szt

Wymagane parametry równoważności:

Lp.	**Wymagane minimalne parametry techniczne**	**Dane techniczne oferowanego sprzętu** *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent: .....** **Model: .....** **Rok produkcji: .....** *(*należy uzupełnić wszystkie wykropkowane pola)*		
1. Architektura systemu	System ochrony aplikacji webowych oraz Firewall XML - którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. System powinien umożliwiać lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów. Powinna istnieć możliwość implementacji systemu inline w trybach Reverse Proxy lub Transparentnym, jak również implementacji w trybie nasłuchu.	**Spełnia/Nie spełnia***

2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa.	**Spełnia/Nie spełnia***
3.	Parametry fizyczne systemu	Nie mniej niż 4 porty Ethernet 10/100/1000 Base-T Powierzchnia dyskowa - minimum 1 TB W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability)z trybem Active-Passive Obudowa urządzenia o wysokości do 1U przystosowana do montażu w standardowej szafie teletechnicznej 19 cali (urządzenie musi zostać dostarczone z kompletem akcesoriów umożliwiających montaż w szafie *19")*	*Ilość portów 10/100/Base T :* …… *Powierzchnia dyskowa:* …… *Wysokość obudowy* …… **Spełnia/Nie spełnia***
4.	Funkcjonalności podstawowe i uzupełniające	System powinien realizować co najmniej poniższe funkcjonalności: Tryb auto-uczenia - przyspieszający i ułatwiający implementację Podział obciążenia na kilkanaście serwerów (loadballancing) Akcelerację SSL dla wybranych serwisów w centrum danych Możliwość analizy poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje) Firewall XML realizujący z możliwością routingu w oparciu o kontent, walidacją schematów XML oraz weryfikacją WDSL. Firewall aplikacji webowych chroniący przed takimi zagrożeniami jak: • SQL and OS Command Injection • Cross Site Scripting (XSS) • Cross Site Request Forgery • Outbound Data Leakage • HTTP Request Smuggling • Buffer Overflow • Encoding Attacks • Cookie Tampering / Poisoning • Session Hijacking • Broken Access Control j • Forceful Browsing /Directory Traversal Oraz innymi podatnościami specyfi kowanym i przez listę OWASP Top 10.	**Spełnia/Nie spełnia***
5.	Parametry wydajnościowe	Urządzenie musi prawidłowo obsługiwać przepustowość dla ruchu http - min 100 Mbps	**Spełnia/Nie spełnia***
6.	Sygnatury, subskrypcje	Aktualizacja baz sygnatur powinna być systematycznie aktualizowana zgodnie ze zdefiniowanych harmonogramem (Scheduler)	**Spełnia/Nie spełnia***
7.	Zarządzanie	Lokalny graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS, SSH	**Spełnia/Nie spełnia***
8.	Zasilanie	Zasilanie z sieci 230V/50Hz.	**Spełnia/Nie spełnia***
9.	Oprogramowanie	oprogramowanie typu antywirus, web security service, IP reputation service, licencje minimum na 12 miesięcy Możliwosć aktualizacji firmware przez minimum na 12 miesięcy	**Spełnia/Nie spełnia***

J. FortiGate 800C – 2szt.

Wymagane parametry równoważności:

Lp.	Wymagane minimalne parametry techniczne		Dane techniczne oferowanego sprzętu *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
Oferowane urządzenia: **Producent: .....** **Model: .....** **Rok produkcji: .....** *(*należy uzupełnić wszystkie wykropkowane pola)*			
1.	Architektura systemu ochrony	System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania. Dlatego, główne urządzenie ochronne [gateway] nie może posiadać twardego dysku, w zamian używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizoanego układu ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie).	**Spełnia/Nie spełnia***
8.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia.	*Nazwa systemu operacyjnego:* .... **Spełnia/Nie spełnia***
9.	Ilość/rodzaj portów	Nie mniej niż 2 porty 10-GbE SFP+, 12 portów Ethernet 10/100/1000 Base-TX, 8 portów współdzielonych 10/100/1000 RJ45 lub SFP, 2 pary portów z funkcją Bypass Protection.	*Ilość portów 10-GbE SFP+:* ..... *Ilość portów Ethernet 10/100/1000 Base-TX:* ..... *Ilość portów współdzielonych 10/100/1000 RJ45 lub SFP:* ..... *Ilość par portów z funkcją Bypass Protection:* ..... **Spełnia/Nie spełnia***

10.	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: a) kontrolę dostępu - zaporę ogniową klasy Stateful Inspection b) ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM, SMTPS, POP3S, IMAPS, HTTPS) c) poufność danych - IPSec VPN oraz SSL VPN d) ochronę przed atakami - Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających: e) kontrolę treści – Web Filter [WF] f) kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP, SMTPS, POP3S, IMAPS) g) kontrolę pasma oraz ruchu [QoS i Traffic shaping] h) kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P) i) zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Preention) j) SSL proxy z możliwością pełniej analizy szyfrowanej komunikacji dla wybranych protokołów	**Spełnia/Nie spełnia***
11.	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: jako router/NAT (3.warstwa ISO-OSI) lub jako most /transparent bridge/ . Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.	**Spełnia/Nie spełnia***
12.	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).	**Spełnia/Nie spełnia***
13.	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. • Nie mniej niż 3900 sygnatur ataków. • Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie • Możliwość wykrywania anomalii protokołów i ruchu	*Ilość sygnatur ataków:……..* **Spełnia/Nie spełnia***
14.	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT.	**Spełnia/Nie spełnia***

15.	Wirtualizacja i routing dynamiczny	Możliwość definiowania w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego. Protokoły routingu dynamicznego, nie mniej niż RIPv2, OSPF, BGP-4 i PIM.	*Ilość możliwych do zdefiniowania w urządzeniu wirtualnych firewalli bez dodatkowych licencji:……* *Obsługiwane protokoły routingu dynamicznego:* …… …… **Spełnia/Nie spełnia***
16.	Połączenia VPN	Wymagane nie mniej niż: 1. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site 2. Dostawca musi udostępniać klienta VPN własnej produkcji realizującego następujące mechanizmy ochrony końcówki: 1) firewall 2) antywirus 3) web filtering 4) antyspam 3. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności 4. Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN) 5. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth	**Spełnia/Nie spełnia***
17.	Uwierzytelnianie użytkowników	System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: 6. haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie urządzenia 7. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP 8. haseł dynamicznych (RADIUS, RSA SecureID) w oparciu o zewnętrzne bazy danych Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory bez dodatkowych opłat licencyjnych.	**Spełnia/Nie spełnia***

18.	Wydajność	Obsługa nie mniej niż 7 milionów jednoczesnych połączeń i 190 000 nowych połączeń na sekundę. Przepływność nie mniejsza niż 20 Gbps dla ruchu nieszyfrowanego i 8 Gbps dla VPN (3DES). Obsługa nie mniej niż 10 000 jednoczesnych tuneli VPN.	*Ilość jednoczesnych połączeń:* …… *Ilość nowych połączeń na sekundę:* …… *Przepływność dla ruchu nieszyfrowanego:* …… *Przepływność dla ruchu VPN:* …… *Ilość obsługiwanych jednoczesnych tuneli VPN:* …… **Spełnia/Nie spełnia***
19.	Funkcjonalność zapewniająca niezawodność	Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Możliwość połączenia dwóch identycznych urządzeń w klaster typu Active-Active lub Active-Passive	**Spełnia/Nie spełnia***
20.	Zasilanie	Zasilanie z sieci 230V/50Hz.	**Spełnia/Nie spełnia***
21.	Konfiguracja i zarządzanie	Możliwość konfiguracji poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. Administratorzy muszą być uwierzytelniani za pomocą: 1. haseł statycznych 2. haseł dynamicznych (RADIUS, RSA SecureID) System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.	**Spełnia/Nie spełnia***

22.	Zarządzanie	Ze względu na instniejącą infrastrukturę Zamawiajacego, urządzenie musi być w pełni kompatybilne (tj. istnieje możliwość pełnego konfigurowania jego funkcji i zarządzania nim i monitorowania obciążenia) z urządzeniem FortiManager w wersji oprogramowania min. **v4 MR3 Patch 7**	*Urządzenie jest pełni kompatybilne (tj. istnieje możliwość pełnego konfigurowania jego funkcji i zarządzania nim i monitorowania obciążenia) z urządzeniem FortiManager w wersji oprogramowania:* …… **Spełnia/Nie spełnia***
23.	Raportowanie	Ze względu na instniejącą infrastrukturę Zamawiajacego, urządzenie musi być w pełni kompatybilne (tj. istnieje możliwość zbierania logów z urządzeń, generowania raportów, skanowania podatności stacji w sieci, zdalną kwarantannę dla modułu antywirusowego) z urządzeniem FortiAnalyzer w wersji oprogramowania min. **v4 MR3 Patch 7**	*Urządzenie jest w pełni kompatybilne (tj. istnieje możliwość zbierania logów z urządzeń, generowania raportów, skanowania podatności stacji w sieci, zdalną kwarantannę dla modułu antywirusowego) z urządzeniem FortiAnalyzer w wersji oprogramowania:* …… **Spełnia/Nie spełnia***

Lp.	Wymagania dotyczące spełniania przez oferowane urządzenia równoważne odpowiednich norm jakości, warunków gwarancji oraz serwisu		Dokumenty oraz wymogi odnośnie gwarancji i serwisu *(*niepotrzebne skreślić, a wymagane pola uzupełnić)*
1.	Certyfikaty	Oferowane urządzenia muszą posiadać: **Certyfikat ISO 9001:2008 lub równoważny dla producenta sprzętu** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)* **Deklaracja zgodności CE** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)* **Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)* **Certyfikat ICSA Labs dla producenta sprzętu dla funkcji: Firewall, IPSec, Network IPS, Antywirus** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)* **Certyfikat UTM NSS Approved dla oferowanych urządzeń** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)* **Certyfikat EAL4+ dla oferowanych urządzeń** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę)*	*Certyfikat ISO dla producenta:* **Tak/Nie*** *Deklaracja zgodności CE:* **Tak/Nie*** *Potwierdzenie spełnienia ROHS:* **Tak/Nie*** **Spełnia/Nie spełnia*** *Certyfikat ICSA Labs dla producenta:* **Tak/Nie*** *Certyfikat UTM NSS Approved dla urządzeń:* **Tak/Nie*** *Certyfikat EAL4+ dla urządzeń:* **Tak/Nie***

2	Gwarancja, serwis	Urządzenia powinny być objęte serwisem gwarancyjnym producenta przez okres min. 12 miesięcy. Urządzenia powinny mieć ważne subskrypcje dla wszystkich funkcji ochronnych przez okres min. 12 miesięcy. Wykonawca zapewni wizytę certyfikowanego inżyniera w siedzibie Zamawiającego celem zweryfikowania poprawności konfiguracji i działania oferowanych rozwiązań, nie rzadziej niż jedna na kwartał w trakcie trwania serwisu gwarancyjnego. **Firma serwisująca musi posiadać certyfikat ISO 9001:2008 lub równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń** *(załączyć do oferty dokument potwierdzający spełnianie wymogu wraz z tłumaczeniem na język polski poświadczonym przez Wykonawcę).* **Serwis urządzeń musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta- wymagane oświadczenie Wykonawcy potwierdzające, że serwis będzie realizowany przez producenta lub autoryzowanego partnera serwisowego producenta** *(załączyć do oferty oświadczenie).* Możliwość przedłużenia gwarancji, serwisu oraz subskrypcji o kolejne lata.	*Okres gwarancji producenta:.....miesięcy* *Okres ważności subskrypcji:.....miesięcy* *Ilośc wizyt certyfikowanego inżyniera: ..... na kwartał* *Certyfikat ISO na świadczenie usług serwisowych:* **Tak/Nie*** *Oświadczenie dot. serwisu:* **Tak/Nie*** **Spełnia/Nie spełnia***
3	Lokalizacja serwisu producenta	**Zamawiający wymaga, aby serwis sprzętu świadczony był przez organizację serwisową producenta, mającą swoją placówkę serwisową na terenie Polski** *(załączyć do oferty oświadczenie Wykonawcy lub inny dokument potwierdzający spełnienie wymogu).*	**Spełnia/Nie spełnia***

.....
(data, imię i nazwisko oraz podpis
upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 6 do SIWZ
wzór

Umowa nr.....

zawarta w dniu ..... w Warszawie pomiędzy:
Polską Akademią Nauk z siedzibą w Warszawie (00-901) w Pałacu Kultury i Nauki przy Placu Defilad 1, posiadającą REGON: 000325713, NIP: 525-15-75-083, reprezentowaną przez: Pana Tadeusza Latałę - Kanclerza Polskiej Akademii Nauk, zwaną dalej w Umowie „Zamawiającym" a
..... zwanym dalej w Umowie „Wykonawcą", reprezentowanym przez: .....
Zamawiający i Wykonawca zwani są dalej w Umowie także łącznie „Stronami", a indywidualnie — „Stroną".
Umowa została zawarta w wyniku przeprowadzenia przez Zamawiającego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego (znak 24/ZP/2016), zgodnie z ustawą z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 ze zm) - dalej „ustawa Pzp"

§ 1
PRZEDMIOT UMOWY

1. Przedmiotem Umowy, zwanym dalej „Zamówieniem" jest przedłużenie pakietu licencji obejmującego: gwarancję, wsparcie techniczne, możliwość aktualizacji oprogramowania dla urządzeń typu UTM, AP, analizujących ruch sieciowy, monitorujących ruch www i zabezpieczających serwery poczty elektronicznej używanych przez Zamawiającego oraz subskrypcję bezpieczeństwa w zakresie antywirus ,antyspam, IPS, Web filter dla urządzeń typu UTM, w zakresie antywirus , antyspam dla rządzeń zabezpieczających serwery poczty elektronicznej, w zakresie antywirus, web security service, IP Reputation Service dla urządzeń monitorujących ruch www, szczegółowo opisanych w Załączniku nr 1 do Umowy oraz Ofercie Wykonawcy z dnia....., stanowiącej załącznik nr 2 do Umowy.
2. Ilekroć w Umowie jest mowa o Pakiecie licencji należy przez to rozumieć wszystkie usługi, o których mowa w ust. 1 na zasadach określonych w Umowie.
3. Ilekroć w niniejszej Umowie mowa jest o dniach roboczych należy przez nie rozumieć kolejne dni od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy.

UWAGA: W przypadku zaoferowania rozwiązania równoważnego treść niniejszej umowy zostanie skorygowana w taki sposób, aby uwzględniała dostawę sprzętu i oprogramowania, wdrożenie i instalację, przeprowadzenie testów i przeszkolenie personelu Zamawiającego, zgodnie z warunkami określonymi w Załącznikach nr 1 i 1a do SIWZ.

§ 2
ZOBOWIĄZANIA WYKONAWCY

1. Wykonawca oświadcza, że posiada prawo do zawarcia niniejszej umowy na warunkach w niej ustalonych i do sprzedaży Pakietu licencji producenta wraz z nośnikami oprogramowania (egzemplarze oprogramowania).

2. Wykonawca oświadcza, że korzystanie przez Zamawiającego z pakietu licencji, o których mowa w §1 ust. 1 Umowy, na zasadach określonych w licencji nie będzie naruszać prawa własności intelektualnej osób trzecich, w tym majątkowych praw autorskich, patentów ani praw do baz danych.
3. Pakiet licencji, o którym mowa powyżej, będzie miał charakter niewyłączny, nieograniczony terytorialnie na okres wskazany w Załączniku nr 1 do Umowy.
4. Wykonawca zobowiązuje się wykonać Umowę przy zachowaniu najwyższej staranności, uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z zasadami współczesnej wiedzy technicznej i stosowanymi normami technicznymi.
5. Wykonawca nie może powierzyć wykonania Przedmiotu Umowy osobom trzecim bez uprzedniej pisemnej zgody Zamawiającego. W przypadku powierzenia wykonania Przedmiotu Umowy osobom trzecim, Wykonawca ponosi odpowiedzialność za ich działania i zaniechania jak za własne działania i zaniechania.
6. Wykonawca zobowiązuje się, że jeżeli to Wykonawca udziela licencji na korzystanie z oprogramowania objętego pakietem licencji, o którym mowa w §1 ust. 1 Umowy, nie będzie korzystał z ustawowego uprawnienia do wypowiedzenia umowy licencyjnej, ani prawa do odstąpienia od umowy przysługującego mu na podstawie art. 56 ust. 1 Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2016 r., poz. 666 ze zm.) - dalej jako „Prawo autorskie" - w okresie wskazanym w Załączniku nr 1 do Umowy.
7. Wykonawca gwarantuje - w przypadku kiedy Wykonawca zapewnia udzielenie Pakietu licencji o którym mowa w §1 ust. 1 Umowy, którego faktycznie udziela producent niebędący Wykonawcą - że w przypadku skorzystania przez producenta z ustawowego uprawnienia do wypowiedzenia umowy lub prawa do odstąpienia od umowy przysługującego mu na podstawie art. 56 ust. 1 Prawa autorskiego, Wykonawca zapewni nowy pakiet licencji w okresie wskazanym w Załączniku nr 1 do Umowy.
8. Wykonawca zobowiązany będzie do ustosunkowania się bez zbędnej zwłoki do pytań i wniosków Zamawiającego związanych z realizacją przedmiotu Umowy, nie później jednak niż w terminie 3 (trzech) dni roboczych od momentu otrzymania zapytania.

§ 3
ZOBOWIĄZANIA ZAMAWIAJĄCEGO

Zamawiający zobowiązuje się do zrealizowania płatności za przedmiot niniejszej Umowy na warunkach określonych w niniejszej Umowie.

§ 4
REALIZACJA 1 ODBIÓR PRZEDMIOTU UMOWY

1. Dostawa przedmiotu zamówienia nastąpi w terminie ..... dni kalendarzowych od dnia zawarcia Umowy, zgodnie z zasadami określonymi poniżej.
2. Wykonawca przekaże Zamawiającemu za pomocą faksu na numer .....lub poczty elektronicznej na adres **admin@pan.pl** certyfikaty serwisowe dla urządzeń potwierdzające nabycie przez Zamawiającego subskrypcji pakietu licencji na okres, o którym mowa w § 2 ust. 3 Umowy.
3. Przejście na Zamawiającego praw wynikających z Licencji następuje z chwilą odbioru przez Zamawiającego oprogramowania. Za prawidłowe dostarczenie oprogramowania uznaje się przekazanie Zamawiającemu nośników danych z oprogramowaniem lub udostepnienie oprogramowania na stronie producenta celem samodzielnego pobrania przez Zamawiającego.

4. Zamawiający potwierdzi otrzymanie informacji, o których mowa w ust. 2 w ciągu maksymalnie 2 dni roboczych od jej odebrania.
5. Wykonawca wystawi fakturę za realizację przedmiotu zamówienia najpóźniej w ciągu 14 dni od daty uzyskania potwierdzenia od Zamawiającego, o którym mowa w ust. 4 Umowy.
6. W przypadku opóźnienia Wykonawcy w realizacji przedmiotu Umowy przekraczającego 10 dni roboczych, Zamawiający ma prawo do odstąpienia od Umowy z przyczyn leżących po stronie Wykonawcy i żądania zapłaty kary umownej w wysokości określonej w § 6 ust. 1 Umowy. Oświadczenie o odstąpieniu, o którym mowa w zdaniu poprzedzającym winno być złożone w terminie 14 dni roboczych od dnia, w którym upłynął 10 dzień roboczy opóźnienia Wykonawcy.

§ 5
WYNAGRODZENIE 1 WARUNKI PŁATNOŚCI

1. Z tytułu należytego wykonania Umowy Zamawiający zapłaci Wykonawcy wynagrodzenie w wysokości ..... zł (słownie złotych: .....) w tym podatek VAT w wysokości:..... zł (słownie złotych:.....).
2. Wynagrodzenie, o którym mowa w ust. 1 powyżej ma charakter ryczałtowy i obejmuje wszystkie koszty niezbędne do wykonania przedmiotu zamówienia.
3. Płatność dokonana będzie przelewem na rachunek bankowy wskazany na fakturze wystawionej przez Wykonawcę, w terminie ..... dni od daty doręczenia Zamawiającemu przez Wykonawcę prawidłowo wystawionej faktury VAT.
4. Za datę zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.

§ 6
SKUTKI NIEWYKONANIA
LUB NIEWŁAŚCIWEGO WYKONANIA UMOWY

1. W przypadku odstąpienia od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, Wykonawca będzie zobowiązany do zapłacenia Zamawiającemu kary umownej w wysokości 15 % wynagrodzenia całkowitego brutto, określonego w § 5 ust. 1 Umowy.
2. W przypadku opóźnienia Wykonawcy w realizacji przedmiotu Umowy w stosunku do terminu określonego w § 4 ust. 1 Umowy Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,5 % wynagrodzenia, określonego w § 5 ust. 1 Umowy, za każdy rozpoczęty dzień opóźnienia.
3. Zamawiający może także odstąpić od Umowy w przypadku przewidzianym w art. 145 ustawy Pzp.
4. Zamawiający jest uprawniony do potrącenia należnych Zamawiającemu kar umownych z wynagrodzenia przysługującego Wykonawcy na co Ten wyraża zgodę.
5. Zamawiający zastrzega możliwość dochodzenia na zasadach ogólnych odszkodowania przewyższającego wysokość kar umownych.
6. Odstąpienie od umowy nie zwalnia Wykonawcy z obowiązku zapłaty kar umownych.
7. Kary umowne są niezależne od siebie i należą się w pełnej wysokości, nawet w przypadku, gdy w wyniku jednego zdarzenia, naliczana jest więcej niż jedna kara.

§ 7
ZMIANA UMOWY

1. Zamawiający dopuszcza możliwość zmiany Umowy w zakresie dotyczącym Opisu przedmiotu zamówienia, co do sposobu realizacji zamówienia przez Wykonawcę, w następujących przypadkach:
   a) wystąpienia konieczności wprowadzenia zmian doprecyzowujących treści Umowy, jeżeli potrzeba ich wprowadzenia wynika z rozbieżności lub niejasności w Umowie, których nie można usunąć w inny sposób, a zmiana będzie umożliwiać usunięcie rozbieżności i doprecyzowanie Umowy w celu jednoznacznej interpretacji jej zapisów;
   b) konieczności zrealizowania przedmiotu Umowy przy zastosowaniu innych rozwiązań technicznych/technologicznych niż wskazane w Ofercie Wykonawcy w sytuacji, gdyby zastosowanie przewidzianych rozwiązań groziłoby niewykonaniem lub wadliwym wykonaniem przedmiotu Umowy;
2. Zmiana umowy opisana w ust. 1 powyżej nie spowoduje zmiany ceny zaproponowanej przez Wykonawcę w ofercie.
3. Nie stanowią zmiany Umowy w rozumieniu art. 144 ustawy PZP następujące przypadki (wymagają jedynie poinformowania drugiej Strony w formie pisemnej z 3 (trzy) dniowym wyprzedzeniem):
   a) zmiana danych teleadresowych Stron;
   b) zmiana danych rejestrowych Stron;
   c) zmiana sposobu prowadzenia korespondencji pomiędzy Stronami
   d) zmiana osób do kontaktu lub ich danych kontaktowych .

§ 8
KLAUZULA WALORYZACYJNA

1. Strony zobowiązują się dokonać zmiany wysokości wynagrodzenia należnego Wykonawcy, o którym mowa w 5 ust. 1 umowy, w formie pisemnego aneksu, każdorazowo w przypadku wystąpienia jednej z następujących okoliczności:
   a) zmiany stawki podatku od towarów i usług,
   b) zmiany wysokości minimalnego wynagrodzenia ustalonego na podstawie przepisów o minimalnym wynagrodzeniu za pracę,
   c) zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne - na zasadach i w sposób określony w ust. 2 - 12, jeżeli zmiany te będą miały wpływ na koszty wykonania Umowy przez Wykonawcę.
2. Zmiana wysokości wynagrodzenia należnego Wykonawcy w przypadku zaistnienia przesłanki, o której mowa w ust. 1 li. a) , będzie odnosić się wyłącznie do części przedmiotu umowy zrealizowanej, zgodnie z terminami ustalonymi umową, po dniu wejścia w życie przepisów zmieniających stawkę podatku od towarów i usług oraz wyłącznie do części przedmiotu Umowy, do której zastosowanie znajdzie zmiana stawki podatku od towarów i usług.
3. W przypadku zmiany, o której mowa w ust. 1 lit. a) , wartość wynagrodzenia netto nie zmieni się, a wartość wynagrodzenia brutto zostanie wyliczona na podstawie nowych przepisów.
4. Zmiana wysokości wynagrodzenia w przypadku zaistnienia przesłanki, o której mowa w ust. 1 lit. b) lub c) lub 3, będzie obejmować wyłącznie część wynagrodzenia należnego

Wykonawcy, w odniesieniu do której nastąpiła zmiana wysokości kosztów wykonania umowy przez Wykonawcę w związku z wejściem w życie przepisów odpowiednio zmieniających wysokość minimalnego wynagrodzenia za pracę lub dokonujących zmian w zakresie zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub w zakresie wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne.

5. W przypadku zmiany, o której mowa w ust. 1 lit. b), wynagrodzenie Wykonawcy ulegnie zmianie o kwotę odpowiadającą wzrostowi kosztu Wykonawcy w związku ze zwiększeniem wysokości wynagrodzeń pracowników realizujących zamówienie do wysokości aktualnie obowiązującego minimalnego wynagrodzenia za pracę, z uwzględnieniem wszystkich obciążeń publicznoprawnych od kwoty wzrostu minimalnego wynagrodzenia. Kwota odpowiadająca wzrostowi kosztu Wykonawcy będzie odnosić się wyłącznie do części wynagrodzenia pracowników realizujących zamówienie, o których mowa w zdaniu poprzedzającym, odpowiadającej zakresowi, w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu umowy.
6. W przypadku zmiany, o której mowa w ust. 1 lit. c), wynagrodzenie Wykonawcy ulegnie zmianie o kwotę odpowiadającą zmianie kosztu Wykonawcy ponoszonego w związku z wypłatą wynagrodzenia pracownikom realizującym zamówienie. Kwota odpowiadająca zmianie kosztu Wykonawcy będzie odnosić się wyłącznie do części wynagrodzenia pracowników realizujących zamówienie, o których mowa w zdaniu poprzedzającym, odpowiadającej zakresowi, w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy.
7. W celu zawarcia aneksu, o którym mowa w ust. 1, każda ze Stron może wystąpić do drugiej Strony z wnioskiem o dokonanie zmiany wysokości wynagrodzenia należnego Wykonawcy, wraz z uzasadnieniem zawierającym w szczególności szczegółowe wyliczenie całkowitej kwoty, o jaką wynagrodzenie Wykonawcy powinno ulec zmianie, oraz wskazaniem daty, od której nastąpiła bądź nastąpi zmiana wysokości kosztów wykonania Umowy uzasadniająca zmianę wysokości wynagrodzenia należnego Wykonawcy.
8. W przypadku zmian, o których mowa w ust. 1 lit. b) lub c), jeżeli z wnioskiem występuje Wykonawca, jest on zobowiązany dołączyć do wniosku dokumenty, z których będzie wynikać, w jakim zakresie zmiany te mają wpływ na koszty wykonania Umowy, w szczególności:
   a) pisemne zestawienie wynagrodzeń (zarówno przed jak i po zmianie) pracowników realizujących zamówienie, wraz z określeniem zakresu (części etatu), w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu Umowy oraz części wynagrodzenia odpowiadającej temu zakresowi - w przypadku zmiany, o której mowa w ust. 1 lit. b), lub
   b) pisemne zestawienie wynagrodzeń (zarówno przed jak i po zmianie) pracowników realizujących zamówienie, wraz z kwotami składek uiszczanych do Zakładu Ubezpieczeń Społecznych/Kasy Rolniczego Ubezpieczenia Społecznego w części finansowanej przez Wykonawcę, z określeniem zakresu (części etatu), w jakim wykonują oni prace bezpośrednio związane z realizacją przedmiotu umowy oraz części wynagrodzenia odpowiadającej temu zakresowi - w przypadku zmiany, o której mowa w ust. 1 lit. c)
9. W przypadku zmiany, o której mowa w ust. 1 lit. c), jeżeli z wnioskiem występuje Zamawiający, jest on uprawniony do zobowiązania Wykonawcy do przedstawienia w wyznaczonym terminie, nie krótszym niż 7 dni, dokumentów, z których będzie wynikać w jakim zakresie zmiana ta ma wpływ na koszty wykonania umowy, w tym pisemnego zestawienia wynagrodzeń, o którym mowa w ust. 8 lit. b.

10. W terminie 14 dni od dnia przekazania wniosku, o którym mowa w ust. 7, Strona, która otrzymała wniosek, przekaże drugiej Stronie informację o zakresie, w jakim akceptuje wniosek oraz wskaże kwotę, o którą wynagrodzenie należne Wykonawcy powinno ulec zmianie, albo informację o niezatwierdzeniu wniosku wraz z uzasadnieniem.
11. W przypadku otrzymania przez Stronę informacji o braku akceptacji wniosku lub częściowej akceptacji wniosku, Strona ta może ponownie wystąpić z wnioskiem, o którym mowa w ust. 7. W takim przypadku przepisy ust. 8 - 10 oraz 12 stosuje się odpowiednio.
12. Zawarcie aneksu nastąpi nie później niż w terminie 14 dni od dnia akceptacji wniosku o dokonanie zmiany wysokości wynagrodzenia należnego Wykonawcy.

§ 9
POSTANOWIENIA KOŃCOWE

1. Wszelka korespondencja, dokumenty i oświadczenia Stron w związku z realizacją niniejszej Umowy prowadzona będzie pisemnie i przesyłana listem poleconym albo pocztą kurierską, albo składana osobiście w siedzibie:
   a) dla Zamawiającego: Polska Akademia Nauk, Plac Defilad 1, 00-901 Warszawa do rąk: .....
   b) dla Wykonawcy: .....
2. Upoważnionymi Przedstawicielami są:
   a) ze strony Zamawiającego:.....
   b) ze strony Wykonawcy:.....
3. Wszelkie wierzytelności Wykonawcy powstałe w związku z Umową lub w wyniku jej realizacji nie mogą być bez uprzedniej pisemnej zgody Zamawiającego przeniesione przez Wykonawcę na osoby trzecie (art. 509 §1 Kodeksu cywilnego).
4. Załączniki stanowią integralną część Umowy.
5. W zakresie nieuregulowanym w Umowie stosuje się przepisy ustawy Pzp oraz Kodeksu cywilnego.
6. Wszelkie spory wynikłe z Umowy bądź z nią związane rozstrzygać będzie sąd powszechny właściwy dla siedziby Zamawiającego.
7. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, jednym dla Zamawiającego
   i jednym dla Wykonawcy.

Załączniki:
1. Załącznik nr 1 — Szczegółowy opis przedmiotu zamówienia
2. Załącznik nr 1a (w przypadku, gdy umowa jest zawierana z Wykonawcą oferującym rozwiązanie równoważne)
3. Załącznik nr 2 — Oferta Wykonawcy

Zamawiający

Wykonawca