INSTYTUT TECHNIKI BUDOWLANEJ

ul. Filtrowa 1

00-611 WARSZAWA

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

na:

„Dostawę systemu Firewall".

TO-250-30 IT/19

Zatwierdził:

ZASTĘPCA DYREKTORA

ds. Organizacyjno-Administracyjnych

mgr Joanna Krzemińska

Warszawa, dnia 18.09.2019 r.

Specyfikacja Istotnych Warunków Zamówienia zawiera:

ROZDZIAŁ I: INSTRUKCJA DLA WYKONAWCÓW.

ROZDZIAŁ II: FORMULARZ OFERTY ORAZ INNE FORMULARZE.

II.1 – FORMULARZ „OFERTA”

II.2– FORMULARZ „OŚWIADCZENIE O BRAKU PODSTAW DO WYKLUCZENIA”

II.3 – FORMULARZ „OŚWIADCZENIE O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU”

II.4 – FORMULARZ „DOŚWIADCZENIE”

II.4A – FORMULARZ „WYKAZ OSÓB”

II.5 – FORMULARZ „INFORMACJA DOTYCZĄCA PRZYNALEŻNOŚCI DO GRUPY KAPITAŁOWEJ”

ROZDZIAŁ III: SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA.

ROZDZIAŁ IV: ISTOTNE POSTANOWIENIA UMOWY.

ROZDZIAŁ V: KLAUZULA INFORMACYJNA O PRZETWARZANIU DANYCH OSOBOWYCH NA PODSTAWIE PRZEPISÓW PRAWA

Niniejsza Specyfikacja Istotnych Warunków Zamówienia zwana jest w dalszej treści „Specyfikacją Istotnych Warunków Zamówienia”, „SIWZ” lub „Specyfikacją”.

ROZDZIAŁ I INSTRUKCJA DLA WYKONAWCÓW .

1. Zamawiający.

Nazwa: Instytut Techniki Budowlanej

Adres: 00-611 Warszawa, ul. Filtrowa 1;

Telefon: /+48/ 22 825 04 71, adres e-mail: ci@itb.pl

Adres strony internetowej: www.itb.pl

2. Oznaczenie postępowania.

Postępowanie, którego dotyczy niniejsza SIWZ oznaczone jest znakiem: **TO-250-30 IT/19**. Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie.

3. Tryb postępowania.

3.1. Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego na podstawie art. 39 ustawy z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (tj. Dz. U. z 2018 poz. 1986 z późn. zm.) z zastosowaniem procedury opisanej w art. 24aa Pzp (zwanej dalej „procedurą odwróconą").

3.2. Ilekroć w niniejszej SIWZ zastosowane jest pojęcie „ustawa" lub „Pzp", należy przez to rozumieć ustawę Prawo zamówień publicznych, o której mowa w pkt 3.1.

4. Przedmiot zamówienia.

4.1. Dostawa systemu Firewall.

4.2. Właściwe dla przedmiotu zamówienia nazwy i kody określone we Wspólnym Słowniku Zamówień (CPV): 48821000-9 (serwery sieciowe), 32420000-3 (urządzenia sieciowe).

4.3. Szczegółowe określenie zakresu przedmiotu zamówienia zawarte jest w Rozdziale III niniejszej SIWZ.

4.4. Miejsce dostaw: ITB, Warszawa ul. Filtrowa 1 kod: 00-611; Warszawa ul. Ksawerów 21 kod: 02-656, Katowice al. Korfantego 191 kod: 40-153, Poznań ul. Taczaka 12 kod: 61-818, Pionki ul. Przemysłowa 2, kod: 26-670.

4.5. Zamawiający nie dopuszcza możliwości składania ofert częściowych.

4.6. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

5. Termin realizacji zamówienia.

Zamawiający wymaga, aby zamówienie zostało zrealizowane **w ciągu 5 tygodni** od dnia zawarcia umowy z podziałem na dwa etapy, z zastrzeżeniem lit. b) niniejszego punktu:

a) 4 tygodnie od zawarcia umowy, obejmuje:

- dostawę wszystkich elementów systemu Firewall,
- uruchomienie, konfigurację, instalację oprogramowania (licencji), wdrożenie wszystkich elementów wymienionych w Szczegółowym Opisie Przedmiotu Zamówienia.

b) 5-ty tydzień obejmuje przeprowadzenie szkolenia zgodnie z wymaganiami opisanymi w Szczegółowym Opisie Przedmiotu Zamówienia. Zasadę liczenia 5 tygodnia realizacji Przedmiotu Zamówienia ustala się od pierwszego poniedziałku po realizacji dostawy (dni szkolenia: poniedziałek – piątek).

6. Podstawy do wykluczenia oraz warunki udziału w postępowaniu, które muszą spełniać Wykonawcy.

6.1. O udzielenie zamówienia mogą ubiegać się Wykonawcy niepodlegający wykluczeniu na podstawie art. 24 ust.1 ustawy Pzp i spełniający warunki udziału w postępowaniu określone poniżej w pkt 6.2.

a) Dodatkowo Zamawiający wykluczy Wykonawcę na podstawie art. 24 ust. 5 pkt 1, 8, ustawy Pzp, tj.:

- 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 z późn. zm.),
- 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 z późn. zm.),
- 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, 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.

b) Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16–20 ustawy Pzp lub ust. 5, może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu Wykonawcy. Regulacji, o której mowa w zdaniu pierwszym nie stosuje się, jeżeli wobec Wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.

6.2. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki dotyczące:

a) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów

Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny.

b) zdolności technicznej lub zawodowej – w zakresie doświadczenia wykonawcy oraz w zakresie dysponowania osobami zdolnymi do wykonania zamówienia.

1) Zamawiający uzna, że Wykonawca spełnia warunek udziału w postępowaniu jeżeli wykaże, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, zrealizował co najmniej 2 podobne zamówienia, tj. zamówienia polegające na dostawie - urządzeń typu Firewall wraz z konfiguracją, o wartości minimum 100.000 PLN netto każde.

2) Zamawiający uzna, że Wykonawca spełnia warunek udziału w postępowaniu jeżeli wykaże, że dysponuje lub będzie dysponować w trakcie realizacji Przedmiotu Zamówienia minimum 2 osobami posiadającymi ważny certyfikat producenta urządzeń na poziomie co najmniej zaawansowanym z zakresu technologii wykorzystywanych na oferowanych urządzeniach. Zamawiający wymaga aby zamówienie było realizowane przez osoby wskazane w wykazie składanym na wezwanie Zamawiającego w trybie art. 26 ust. 2 PZP.

c) sytuacji ekonomicznej lub finansowej

Zamawiający nie precyzuje w tym zakresie żadnych wymagań, których spełnianie Wykonawca zobowiązany jest wykazać w sposób szczególny.

6.3. Zgodnie z art. 22a ustawy Pzp, Wykonawca może polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków prawnych. Wykonawca w takiej sytuacji zobowiązany jest do udowodnienia Zamawiającemu, iż 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. Zobowiązanie podmiotu powinno być złożone wraz z ofertą i dołączonym dokumentem potwierdzającym umocowanie osoby/ osób podpisującej/ych przedmiotowe zobowiązanie.

W celu oceny, czy Wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia oraz oceny, czy stosunek łączący Wykonawcę z podmiotami trzecimi gwarantuje rzeczywisty dostęp do ich zasobów, Zamawiający żąda przedłożenia wraz z ofertą dokumentów, które określają:

- zakres dostępnych Wykonawcy zasobów innego podmiotu,
- sposób wykorzystania zasobów innego podmiotu przez Wykonawcę, przy wykonywaniu zamówienia,
- zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia

Jeżeli ww. okoliczności będą wynikać z załączonego zobowiązania, Wykonawca może nie składać innych dokumentów. 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 oraz ust. 5 pkt 1, 4 i 8 ustawy.

6.4. Żaden z Wykonawców wspólnie ubiegających się o udzielenie zamówienia (spółki cywilne/konsorcja) nie może podlegać wykluczeniu na podstawie art. 24 ust. 1, ust. 5 pkt 1, 4, 8 ustawy Pzp, natomiast warunki udziału określone w pkt 6.2 w postępowaniu Wykonawcy muszą spełniać łącznie.

6.5. Ocena spełniania warunków udziału w postępowaniu oraz braku podstaw do wykluczenia będzie dokonana na zasadzie spełnia/nie spełnia na podstawie dokumentów i oświadczeń wymaganych w pkt 7 niniejszej Instrukcji dla Wykonawców.

7. Dokumenty i oświadczenia wymagane na potwierdzenie braku podstaw do wykluczenia Wykonawcy z postępowania, spełniania warunków udziału w postępowaniu i potwierdzające spełnienie przez oferowane dostawy wymagań Zamawiającego.

7.1. Do oferty każdy Wykonawca musi dołączyć aktualne na dzień składania ofert oświadczenie w zakresie braku podstaw do wykluczenia zgodne z treścią formularza zamieszczonego w Rozdziale II.2 SIWZ (Formularz „Oświadczenie o braku podstaw do wykluczenia") oraz oświadczenie w zakresie spełniania warunków udziału w postępowaniu zgodne z treścią formularza zamieszczonego w Rozdziale II.3 SIWZ (Formularz „Oświadczenia o spełnianiu warunków udziału w postępowaniu").

7.2. 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 odpowiednio informacje o tych podmiotach w oświadczeniach, o których mowa w pkt 7.1.

7.3. Zamawiający przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów:

A.: Potwierdzających spełnienie warunków udziału w postępowaniu:

7.3.1. Wykaz wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, dostaw w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, o których mowa w punkcie 6.2. lit. b) ppkt 1), według formularza zamieszczonego w Rozdziale II.4 SIWZ (Formularz "Doświadczenie") wraz z załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane (a w przypadku świadczeń okresowych lub ciągłych są wykonywane), a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy. Pod pojęciem dostaw Zamawiający rozumie zamówienia potwierdzające spełnianie opisanych w punkcie 6.2. lit. b) ppkt 1) warunków. W przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

7.3.2. Na potwierdzenie warunku określonego w pkt 6.2 lit. b) ppkt 2) SIWZ Wykonawca składa:
- wykaz osób według formularza zamieszczonego w Rozdziale II.4 A SIWZ wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, tj. informacjami o posiadanych certyfikatach wymaganych w pkt 6.2.lit ppkt 2 według formularza zamieszczonego w Rozdziale II.4 A SIWZ (Formularz "Wykaz Osób")

B. Potwierdzających brak podstaw do wykluczenia:

a) Odpis 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.

Dokumenty wymienione w pkt 7.3.2. B należy przedłożyć także w odniesieniu do innych podmiotów, o których mowa w pkt 6.3.

W przypadku, gdyby w ww. dokumentach podano wartości w walucie innej niż złoty polski, Zamawiający dokona przeliczenia na złoty polski wg średniego kursu NBP z dnia zamieszczenia ogłoszenia o zamówieniu w Biuletynie Zamówień Publicznych. Jeśli w dniu publikacji ogłoszenia Narodowy Bank Polski nie ogłosił kursu średniego, Zamawiający dokona przeliczenia stosując średni kurs z ostatniego dnia roboczego przed publikacją ogłoszenia.

7.4. Zgodnie z art. 24 ust. 11 ustawy, Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o których mowa w art. 86 ust. 5 Pzp (oraz w pkt. 12.4. SIWZ), przekaże Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 Pzp, sporządzone zgodnie z treścią formularza zamieszczonego w Rozdziale II.5 (Formularz "Informacja dotycząca przynależności do grupy kapitałowej"). Oświadczenie powinno być złożone w siedzibie Zamawiającego w oryginale. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

7.5. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia oświadczenia wymienione w punkcie 7.1., 7.4. składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia z pkt 7.1. mają potwierdzać spełnianie warunków udziału w postępowaniu i brak podstaw wykluczenia. Dokumenty wymienione w punkcie 7.3. powinien przedłożyć ten spośród Wykonawców składających wspólną ofertę, który potwierdza spełnienie danego warunku udziału w postępowaniu. W przypadku wspólnego ubiegania się Wykonawców o zamówienie z przedkładanych dokumentów, powinno wynikać, że żaden z tych Wykonawców nie podlega wykluczeniu i łącznie spełniają warunki udziału w postępowaniu.

7.6. Oświadczenia i dokumenty, o których mowa w pkt. 6.3., 7.1., 7.4., 7.8., 10.3. ppkt 1-4), powinny zostać złożone w oryginale. Pozostałe dokumenty należy złożyć w oryginale lub kopii poświadczonej przez Wykonawcę za zgodność z oryginałem (wymagane poświadczenie każdej zapisanej strony dokumentu).

7.7. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, w zakresie dokumentów, które każdego z nich dotyczą.

7.8. Zamawiający wymaga dołączenia do oferty oświadczenia Wykonawcy lub Producenta oferowanych urządzeń typu Firewall, że ich serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta i wskazania tego podmiotu. Zamawiający dopuszcza oświadczenie Wykonawcy zamiast oświadczenia producenta.

7.9. W celu potwierdzenia, że oferowane urządzenia typu Firewall spełniają wymagania Zamawiającego, do oferty należy załączyć, w formie wydruku, aktualne na dzień składania ofert dokumenty producenta w postaci **kart katalogowych poszczególnych oferowanych urządzeń Firewall Typu A i Typu B.**

7.10. W celu potwierdzenia, że oferowane urządzenia typu Firewall spełniają wymagania Zamawiającego, Zamawiający zweryfikuje parametry urządzeń na podstawie testów **którego oferta zostanie najwyżej oceniona wg kryteriów**. Wszelkie testy będą przeprowadzone przez Wykonawcę na jego koszt i ryzyko. Zamawiający wymaga gotowości oferenta do przeprowadzenia testów w terminie nie dłuższym niż 12 dni kalendarzowych liczonym od dnia otwarcia ofert, które będą przeprowadzone w przywołanym terminie.

7.11. W przypadku braku potwierdzenia przez Wykonawcę do którego Zamawiający skieruje wezwanie, o którym mowa w pkt. 7.3. SIWZ, spełniania warunków udziału w postępowaniu lub niepotwierdzenia braku podstaw do wykluczania, Zamawiający powtórzy procedurę opisaną w pkt 14.1. SIWZ, badając ofertę oraz kierując wezwanie do Wykonawcy, który uzyskał kolejny wynik w rankingu ofert.

7.12. Zamawiający odrzuci ofertę w przypadkach określonych w art. 89 ust. 1 ustawy Pzp.

8. Sposób porozumiewania się Zamawiającego z Wykonawcami.

8.1. .Wszelkie oświadczenia, pytania, wnioski, zawiadomienia oraz inne informacje Zamawiający oraz Wykonawcy będą przekazywać sobie pisemnie z dopuszczeniem możliwości przekazywania oświadczeń, wniosków, zawiadomień i informacji przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. oświadczeniu usług drogą elektroniczną (Dz.U. z 2017 r poz. 1219). Zamawiający wymaga niezwłocznego potwierdzenia faktu otrzymania oświadczenia, pytania, wniosku, zawiadomienia czy informacji przesłanej drogą elektroniczną na adres podany w pkt 8.5. SIWZ. Zamawiający na żądanie Wykonawcy będzie dokonywał analogicznych potwierdzeń. Zamawiający w przypadku przekazywania oświadczeń, wniosków, zawiadomień i informacji drogą elektroniczną posługuje się tylko adresem e-mail podanym przez Wykonawcę jako właściwy do kontaktu.

8.2 Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści specyfikacji istotnych warunków zamówienia. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści specyfikacji istotnych warunków zamówienia wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu, o którym mowa w zdaniu poprzednim, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.

8.3. Zamawiający nie zamierza zwoływać zebrania wszystkich Wykonawców.

8.4. Informacje będą udzielane w dni robocze w godzinach od 10^{00} do 14^{00}.

8.5. Osoby upoważnione do kontaktów z Wykonawcami: Aneta Płonka tel. 22 57 96 319, email: to@itb.pl

9. Termin, do którego Wykonawca będzie związany złożoną ofertą.

9.1. Termin związania ofertą wynosi 30 dni. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

9.2. Wykonawca, samodzielnie lub na wniosek Zamawiającego, może przedłużyć termin związania ofertą, z tym że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie terminu, o którym mowa w pkt 9.1. o oznaczony okres, nie dłuższy jednak niż 60 dni.

10. Opis sposobu przygotowania ofert.

10.1. Wykonawca może złożyć jedną ofertę na całość zamówienia, a oferta musi obejmować wszystkie koszty realizacji przedmiotu zamówienia określone w niniejszej SIWZ, w tym również wszelkie koszty towarzyszące wykonaniu, o których mowa w Rozdziale IV – „Istotne Postanowienia Umowy"

10.2. Oferta powinna być podpisana własnoręcznie zgodnie z zasadami reprezentacji obowiązującymi Wykonawcę. Ponadto, oferta powinna być sporządzona zgodnie z treścią formularza „OFERTA" zamieszczonego w Rozdziale II.1 wraz z Formularzem Cenowym.

10.3. Do oferty należy załączyć wymagane dokumenty, oświadczenia i pełnomocnictwa wymienione w SIWZ:

1) Pełnomocnictwo do reprezentowania Wykonawców wspólnie ubiegających się o udzielenie zamówienia (w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia).

2) Pełnomocnictwo do podpisania oferty (o ile prawo do podpisania oferty nie wynika z innych dokumentów złożonych wraz z ofertą).

3) Dokumenty, o których mowa w pkt 6.3. i 7.1.

4) Oświadczenia Wykonawcy lub Producenta oferowanych urządzeń typu Firewall, że ich serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta. Zamawiający dopuszcza oświadczenie Wykonawcy zamiast oświadczenia producenta.

5) W celu potwierdzenia, że oferowane urządzenia typu Firewall spełniają wymagania Zamawiającego, do oferty należy załączyć w formie wydruku, aktualne na dzień złożenia oferty dokumenty producenta urządzeń typu Firewall w postaci kart katalogowych dla poszczególnych oferowanych urządzeń Firewall Typu A i Typu B.

Dokumenty z ppkt 1-4) należy złożyć w oryginale.

10.4. Oferta, oświadczenia i dokumenty, dla których Zamawiający określił wzory w formie załączników do niniejszej SIWZ, powinny być sporządzone zgodnie z tymi wzorami, co do treści oraz opisu kolumn i wierszy.

10.5. Oferta, oświadczenia i dokumenty powinny być sporządzone w formie pisemnej (ręcznie lub w postaci wydruku komputerowego), w języku polskim, w formie zapewniającej pełną czytelność treści.

10.6. Wszelkie zmiany w treści oferty, a w szczególności każde przerobienie, przekreślenie, uzupełnienie, nadpisanie, przesłonięcie korektorem, etc. musi być parafowane lub podpisane przez Wykonawcę – w przeciwnym wypadku nie będzie ono uwzględnione.

10.7. Wszystkie strony oferty wraz z załącznikami zawierające jakąkolwiek treść powinny być kolejno ponumerowane oraz ze sobą połączone, z zastrzeżeniem sytuacji opisanej w pkt 10.9. W treści oferty powinna być umieszczona informacja o ilości stron oferty wraz z załącznikami do oferty.

10.8. Oferta powinna zawierać spis załączników.

10.9. W przypadku, gdyby oferta zawierała informacje stanowiące tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, Wykonawca powinien w sposób niebudzący wątpliwości zastrzec, które spośród zawartych w ofercie informacji stanowią tajemnicę przedsiębiorstwa. Informacje te winny być umieszczone w osobnym wewnętrznym opakowaniu, kartki winny być ze sobą połączone, a strony ponumerowane z zachowaniem ciągłości numeracji, o której mowa w pkt 10.7.

10.10. Ofertę wraz z pozostałymi dokumentami należy umieścić w opakowaniu uniemożliwiającym odczytanie jego zawartości bez uszkodzenia tego opakowania. Opakowanie winno być oznaczone nazwą (firmą) i adresem Wykonawcy, zaadresowane do Zamawiającego na adres:

Instytut Techniki Budowlanej, ul. Filtrowa 1, 00-611 Warszawa

oraz opisane:

Oferta:

„Dostawa systemu Firewall."

„**Nie otwierać przed 27.09. 2019 r. godz. 12.00 "**

10.11. Wymagania określone w pkt 10.7. – 10.10. nie stanowią treści oferty i ich niespełnienie nie będzie skutkować odrzuceniem oferty, lecz wszelkie negatywne konsekwencje mogące wyniknąć z niezachowania tych wymagań będą obciążały Wykonawcę.

10.12. Przed upływem terminu składania ofert, Wykonawca może wprowadzić zmiany do złożonej oferty lub wycofać ofertę. Oświadczenia o wprowadzonych zmianach lub wycofaniu oferty winny być doręczone Zamawiającemu na piśmie pod rygorem nieważności przed upływem terminu składania ofert. Oświadczenia winny być opakowane tak, jak oferta, a opakowanie winno zawierać odpowiednio dodatkowe oznaczenie wyrazem: „ZMIANA" lub „WYCOFANIE".

11. Miejsce i termin składania ofert.

11.1. Oferty powinny być złożone w siedzibie Zamawiającego w Warszawie przy ul. Filtrowej 1 w pokoju nr 27, w terminie do dnia **27.09.2019 r. godz. 11.00.**

11.2. Ofertę złożoną po terminie składania ofert Zamawiający niezwłocznie zwraca Wykonawcy bez otwierania.

12. Miejsce, termin i tryb otwarcia ofert.

12.1. Oferty zostaną otwarte w siedzibie Instytutu Techniki Budowlanej w Warszawie, przy ul. Filtrowej 1, w dniu **27.09. 2019 r. godz. 11.30**

12.2. Otwarcie ofert jest jawne.

12.3. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia. W trakcie otwarcia ofert Zamawiający odczyta nazwę (firmę) oraz adres Wykonawcy, którego oferta jest otwierana oraz informacje dotyczące ceny oferty, terminu wykonania zamówienia i warunków płatności zawartych w ofercie.

12.4 Niezwłocznie po otwarciu ofert Zamawiający zamieści na stronie internetowej informacje dotyczące:

1) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia;

2) firm oraz adresów Wykonawców, którzy złożyli oferty w terminie;

3) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

13. Opis sposobu obliczenia ceny oferty.

13.1. Cena oferowana za wykonanie przedmiotu zamówienia określonego w Rozdziale III SIWZ, winna być umieszczona na Formularzu ofertowym stanowiącym Załącznik nr 1 do Rozdziału II.1. Dodatkowo w pkt 15 Formularza ofertowego należy podać ceny jednostkowe.

13.2. Cena oferty oraz ceny jednostkowe powinny być wyrażone w PLN z dokładnością do jednego grosza (do dwóch miejsc po przecinku).

13.3. Cena oferty powinna uwzględniać wszelkie należne opłaty, w szczególności podatki – w tym podatek VAT oraz wszelkie inne ewentualne obciążenia. Zamawiający wymaga, aby w ofercie uwzględnione były takie stawki podatku VAT, jakie obowiązują w dniu złożenia oferty.

Prawidłowe ustalenie podatku VAT należy do obowiązków Wykonawcy – zgodnie z przepisami Ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz.U. z 2018 r. poz. 2174 z późn. zm.).

13.4. Jeżeli Wykonawca złoży ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku. Zamawiający informuje, iż jest płatnikiem podatku od towarów VAT i posiada numer identyfikacji podatkowej NIP 525-000-93-58.14.

14. Informacje o trybie kwalifikacji Wykonawców i oceny ofert.

14.1. Z uwagi na skorzystanie przez Zamawiającego z procedury odwróconej, Zamawiający najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. Oznacza to, że Zamawiający w toku czynności oceny ofert nie dokona podmiotowej oceny wszystkich Wykonawców (ocena spełniania warunków udziału w postępowaniu, braku podstaw do wykluczenia). W pierwszej kolejności zostanie dokonana ocena ofert pod kątem przesłanek odrzucenia oferty (art. 89 ust. 1 Pzp) oraz kryteriów oceny ofert opisanych w SIWZ, po czym dopiero wyłącznie w odniesieniu do Wykonawcy, którego oferta zostanie oceniona jako najkorzystniejsza (uplasuje się na najwyższej pozycji rankingowej), Zamawiający dokona oceny podmiotowej Wykonawcy, tj. zbada oświadczenia i dokumenty które były wymagane do złożenia wraz z ofertą, a następnie wezwie do przedłożenia oświadczeń lub dokumentów zgodnie z postanowieniami pkt. 7.3, w trybie art. 26 ust. 2 Pzp.

14.2. W toku dokonywania badania i oceny ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert. Niedopuszczalne jest prowadzenie między Zamawiającym a Wykonawcą negocjacji dotyczących złożonej oferty oraz, z zastrzeżeniem art. 87 ust. 2 ustawy, dokonywanie jakiejkolwiek zmiany w jej treści.

15. Kryteria wyboru oferty najkorzystniejszej.

15.1. Przy dokonywaniu wyboru oferty najkorzystniejszej Zamawiający stosować będą następujące kryteria:

1) Cena – 90 %

2) Zestaw dodatkowych funkcjonalności – 10 %

15.2. Zamawiający dokona oceny ofert na podstawie kryteriów określonych powyżej w oparciu o zasady określone poniżej:

1) kryterium CENA – 90%

Punkty za kryterium Cena zostaną obliczone wg następującego wzoru:

$$Q_{Pi} = \frac{C_{Pmin}}{C_{Pi}} \cdot 90$$

gdzie:

Q_{Pi}– liczba punktów przyznana ocenianej ofercie

C_{Pmin} – najniższa cena oferowana w postępowaniu

C_{Pi}– cena zawarta w ocenianej ofercie

Maksymalna ilość punktów jaką można uzyskać w tym kryterium wynosi 90 pkt.
Przyznawane punkty będą wyliczane do dwóch miejsc po przecinku.

2) Kryterium ZESTAW DOATKOWYCH FUNKCJONALNOŚCI – 10%
Dla elementów wymienionych w pkt 2 Rozdziału III Szczegółowy Opis Przedmiotu Zamówienia.
Zamawiający przyzna następującą liczbę punktów:

- **5 punktów – jeśli rozwiązanie zaproponowane przez Wykonawcę spełnia wszystkie wymienione poniżej dodatkowe funkcjonalności:**

Parametry punktowane (wymienione parametry dotyczą każdego z urządzeń firewall – wszystkie oferowane urządzenia firewall muszą posiadać wszystkie wymienione funkcjonalności aby zostały przyznane punkty):

- Urządzanie musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia Active Directory. W przypadku próby wysłania poświadczeń Active Directory do niezaufanej strony lub serwisu administrator może zdefiniować odpowiednią politykę blokującą dla takiego zdarzenia. Jeżeli funkcjonalność wymaga zakupu licencji wtedy Zamawiający wymaga jej dostarczenia dla urządzeń typu A na przynajmniej 12 miesięcy, a na urządzeniach typu B wystarczy możliwość rozbudowy o tę funkcjonalność.
- Urządzenie musi posiadać funkcjonalność definiowania i przydzielania dla ruchu webowego odmiennych profili kontrolujących transfer różnych rodzajów plików lub profili ochrony typu AV, IPS, AS ze względu na kategorię URL. Moduł filtrowania stron WWW musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
- System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujących rodzaj i ilość mechanizmów uwierzytelniających (MFA-multifactor authentication) przy ruchu generowanym do wybranych zasobów (niezależnie od tego czy firewall zna tożsamość danego użytkownika)

- **3 punkty – jeśli rozwiązanie zaproponowane przez Wykonawcę spełnia wszystkie wymienione poniżej dodatkowe funkcjonalności:**

Parametry punktowane (wymienione parametry dotyczą każdego z urządzeń firewall – wszystkie oferowane urządzenia firewall muszą posiadać wszystkie wymienione funkcjonalności aby zostały przyznane punkty):

- Administrator urządzenia musi mieć możliwość zdefiniowania, dla każdej reguły bezpieczeństwa, innego serwera Syslog.
- Urządzenie musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
- Urządzenie musi posiadać interfejs API który musi być jego integralną częścią i umożliwiać konfigurowanie i sprawdzanie stanu urządzenia bez użycia konsoli do zarządzania lub linii poleceń (CLI).

- **2 punkty – jeśli rozwiązanie zaproponowane przez Wykonawcę spełnia wszystkie wymienione poniżej dodatkowe funkcjonalności:**

Parametry punktowane (wymienione parametry dotyczą każdego z urządzeń firewall – wszystkie oferowane urządzenia firewall muszą posiadać wszystkie wymienione funkcjonalności aby zostały przyznane punkty):

- Zezwolenie dostępu dla aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
- Urządzenie musi mieć możliwość tworzenia dynamicznych obiektów adresowych do których, na podstawie zdefiniowanych etykiet, można w automatyczny sposób przypisywać adresy IP. Powinna istnieć możliwość ręcznego tworzenia etykiet bezpośrednio na urządzeniu lub automatycznego pobierania ich z zewnętrznych systemów np. VMware vCenter lub ESX(i) oraz skojarzonych z tymi etykietami adresów IP. Powinna istnieć możliwość wykorzystania tak zbudowanych obiektów adresowych w politykach bezpieczeństwa.

Maksymalna ilość punktów, jaką można uzyskać w tym kryterium wynosi 10 pkt.

15.3 Zamówienie zostanie udzielone Wykonawcy, który otrzyma najwyższą sumaryczną liczbę punktów w kryteriach.

15.4. Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że dwie lub więcej ofert uzyska taką samą liczbę punktów Zamawiający spośród tych ofert wybierze ofertę z niższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie lub koszcie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w złożonych ofertach.

15.5. Z wybranym Wykonawcą zawarta zostanie umowa na warunkach określonych w Rozdziale IV SIWZ.

15.6. Nie przewiduje się aukcji elektronicznej.

16. Zabezpieczenie należytego wykonania umowy.

16.1. Wybrany Wykonawca zobowiązany jest do wniesienia zabezpieczenia należytego wykonania umowy na kwotę stanowiącą 5% całkowitego wynagrodzenia brutto Wykonawcy określonego w §7 ust. 1 Istotnych Postanowień Umowy w następujących formach (do wyboru):

a. pieniądzu, przelewem na wskazany przez Zamawiającego rachunek bankowy: **Bank PEKAO SA 16124059181111000049069512;**

b. poręczeniach bankowych;

c. poręczeniach pieniężnych spółdzielczych kas oszczędnościowo-kredytowych, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;

d. gwarancjach bankowych;

e. gwarancjach ubezpieczeniowych;

f. poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

16.2 Warunki i termin zwrotu lub zwolnienia zabezpieczenia należytego wykonania umowy określone zostały w Rozdziale IV niniejszej SIWZ.

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

17.1 Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.

17.2. Zamawiający zawiadomi o wyniku postępowania wszystkich Wykonawców, którzy złożyli oferty.

17.3. Wykonawcy, którego oferta zostanie wybrana Zamawiający wskaże miejsce i termin podpisania umowy. Umowa podpisana zostanie w terminie nie krótszym niż 5 dni od dnia przekazania

zawiadomienia o wyborze oferty. Zamawiający może zawrzeć umowę przed upływem terminów, o których mowa w zdaniu poprzednim, jeżeli w niniejszym postępowaniu zostanie złożona tylko jedna oferta lub zachodzą przesłanki określone w art. 94 ust.2 pkt 3 ustawy Pzp.

17.4. Jeżeli Wykonawca, którego oferta została wybrana, uchyli się od zawarcia umowy lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający będzie mógł wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ponownego ich badania i oceny, chyba, że zachodzą przesłanki do unieważnienia postępowania.

17.5. Wykonawca, którego oferta zostanie wybrana, zobowiązany będzie, po uprawomocnieniu się decyzji o wyborze jego oferty a przed podpisaniem umowy, przedłożyć Zamawiającemu:

a. informację o osobach, które będą podpisywały umowę ze strony Wykonawcy, przekazania innych danych odnoszących się do Wykonawcy, jakie zostaną zawarte w umowie (w szczególności numeru konta bankowego, na jakie następować będą płatności oraz dokumentu gwarancji lub poręczenia jeśli zabezpieczenie należytego wykonania umowy będzie wnoszone w formie gwarancji lub poręczenia. Treść dokumentu będzie podlegała akceptacji przez Zamawiającego).
b. Umowę regulującą zasady współpracy Wykonawców składających wspólną ofertę, stwierdzającą solidarną odpowiedzialność wszystkich Wykonawców za realizację zamówienia oraz zawierająca upoważnienie dla jednego z Wykonawców do składania i przyjmowania oświadczeń wobec Zamawiającego w imieniu wszystkich Wykonawców, a także do otrzymywania należnych płatności (dotyczy Wykonawców wspólnie ubiegających się o udzielenie zamówienia).
c. Dowodu wniesienia zabezpieczenia należytego wykonania umowy.
d. Pełnomocnictwo do podpisania umowy, o ile upoważnienie to nie wynika z dokumentów złożonych wraz z ofertą.

17.6. O terminie na przedłożenie dokumentów, o których mowa w pkt 17.5., Wykonawca zostanie powiadomiony przez Zamawiającego odrębnym pismem.

17.7. Warunkiem podpisania umowy jest wcześniejsze wniesienie zabezpieczenia należytego wykonania umowy.

18. Pouczenie o środkach ochrony prawnej (Dział VI ustawy Pzp).

18.1. Wykonawcy lub innemu podmiotowi przysługują środki ochrony prawnej jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Pzp.

18.2. Środki ochrony prawnej przysługują również organizacjom zrzeszającym Wykonawców, wpisanym na listę organizacji uprawnionych do wnoszenia środków ochrony prawnej, prowadzoną przez Prezesa Urzędu Zamówień Publicznych pod warunkiem że dotyczą ogłoszenia o zamówieniu lub specyfikacji istotnych warunków zamówienia.

18.3. Odwołanie przysługuje wyłącznie wobec czynności;

1) określenia warunków udziału w postępowaniu;
2) wykluczenia odwołującego z postępowania o udzielenie zamówienia;
3) odrzucenia oferty odwołującego;
4) opisu przedmiotu zamówienia;
5) wyboru najkorzystniejszej oferty.

18.4. Odwołanie wnosi się:

a) w terminie 5 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia - jeżeli zostały przesłane przy użyciu środków komunikacji elektronicznej albo w terminie 10 dni - jeżeli zostały przesłane w inny sposób;

b) w terminie 5 dni od dnia zamieszczenia ogłoszenia w Biuletynie Zamówień Publicznych lub zamieszczenia SIWZ na stronie internetowej jeżeli odwołanie dotyczy treści ogłoszenia lub specyfikacji istotnych warunków zamówienia;

c) w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia jeżeli odwołanie dotyczy czynności innych niż określone powyżej w lit. a i b.

18.5. Wykonawca może w terminie przewidzianym do wniesienia odwołania poinformować Zamawiającego o niezgodnej z przepisami ustawy czynności podjętej przez niego lub zaniechania czynności, do której on zobowiązany na podstawie ustawy, na które nie przysługuje odwołanie na podstawie art. 180 ust. 2 PZP.

18.6. Odwołanie wnosi się do Prezesa Izby w formie pisemnej w postaci papierowej lub w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym.

18.7. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, określać żądanie, zawierać zwięzłe przytoczenie zarzutów oraz okoliczności faktycznych i prawnych uzasadniających wniesienie odwołania.

18.8. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia drogą elektroniczną.

18.9. Zamawiający przesyła niezwłocznie, nie później niż w terminie 2 dni od dnia otrzymania, kopię odwołania innym Wykonawcom uczestniczącym w postępowaniu o udzielenie zamówienia, a jeżeli odwołanie dotyczy treści ogłoszenia o zamówieniu lub postanowień specyfikacji istotnych warunków zamówienia, zamieszcza ją również na stronie internetowej, na której jest zamieszczone ogłoszenie o zamówieniu lub jest udostępniana specyfikacja, wzywając Wykonawców do przystąpienia do postępowania odwoławczego. Zgłoszenie przystąpienia doręcza się Prezesowi Izby w postaci papierowej albo elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, a kopię przesyła się Zamawiającemu oraz Wykonawcy wnoszącemu odwołanie.

18.10. Szczegółowe zasady korzystania ze środków ochrony prawnej reguluje Dział VI ustawy Pzp.

19. Klauzula informacyjna z art. 13 RODO do zastosowania przez zamawiających w celu związanym z postępowaniem o udzielenie zamówienia publicznego

19.1 Zgodnie z art. 13 ust. 1 i 2 ogólnego rozporządzenia PE i RE 679/ 2016 o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (RODO) informuję, iż:

1. Administratorem Pani/Pana danych osobowych udostępnionych przez Wykonawcę jest Instytut Techniki Budowlanej z siedzibą w 00-611 Warszawa, ul. Filtrowa 1.

2. Dane kontaktowe inspektora ochrony danych osobowych: Instytut Techniki Budowlanej; 00-611 Warszawa, ul. Filtrowa 1; telefon 22 5796 466; adres email: iod@itb.pl

3. Dane osobowe Pani/Pana udostępnione przez Wykonawcę przetwarzane będą w celu związanym z postępowaniem o udzielenie zamówienia publicznego p.n. „Dostawa systemu Firewall”. Podstawa prawna przetwarzania rozporządzenie PE i RE 679/ 2016 RODO art. 6 ust. 1 lit. c.

4. Odbiorcami Pani/Pana danych osobowych udostępnionych przez Wykonawcę będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96

ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 ze zm.), dalej „ustawa Pzp".

5. Dane osobowe Pani/Pana udostępnione przez Wykonawcę będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy.

6. Obowiązek podania przez Wykonawcę danych osobowych bezpośrednio dotyczących Pani/Pana jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp.

7. Podane przez Wykonawcę Pani/Pana dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji, w tym do profilowania stosowanie do art. 22 RODO.

8. Klauzula niniejsza dotyczy danych osobowych podanych przez Wykonawcę, które Instytut Techniki Budowlanej pozyska podczas niniejszego postępowania i realizacji umowy.

9. Pracownicy Wykonawcy Pani/Pan posiadają:

   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   - na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
   - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

10. Pracownikom wykonawcy Pani/Panu nie przysługuje:

    - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
    - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
    - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

11. W przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1–3 RODO wymagałoby niewspółmiernie dużego wysiłku, które Instytut Techniki Budowlanej może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu.

12. Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego lub konkursu.

** ***Wyjaśnienie:*** *skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.*

*** ***Wyjaśnienie:*** *prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.*

20. Podwykonawstwo.

20.1. Zamawiający żąda wskazania przez Wykonawcę w ofercie części zamówienia, której wykonanie zamierza powierzyć podwykonawcom oraz podania przez Wykonawcę - o ile są znane - firm podwykonawców. Ww. wskazanie ma nastąpić w Formularzu Oferty.

20.2. W przypadku zmiany albo rezygnacji z podwykonawcy, na którego zasoby Wykonawca powoływał się na zasadach określonych w art. 22a ustawy Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, iż proponowany inny podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż wymagany w trakcie postępowania o udzielenie zamówienia.

20.3. Jeżeli powierzenie podwykonawcy, o którym mowa w pkt 20.2., wykonania części zamówienia następuje w trakcie jego realizacji, Wykonawca na żądanie Zamawiającego przedstawia oświadczenie lub dokumenty potwierdzające brak podstaw wykluczenia wobec tego podwykonawcy.

20.4. Jeżeli Zamawiający stwierdzi, że wobec danego podwykonawcy zachodzą przesłanki wykluczenia, Wykonawca obowiązany jest zastąpić tego podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia podwykonawcy.

20.5. Pozostałe postanowienia dotyczące podwykonawców zostaną określone we wzorze umowy załączonym do SIWZ.

ROZDZIAŁ II FORMULARZ OFERTY ORAZ INNE FORMULARZE.

ROZDZIAŁ II.1 FORMULARZ „OFERTA”

(pieczęć Wykonawcy/ów)	**OFERTA**

Do:

Instytutu Techniki Budowlanej

ul. Filtrowa 1

00-611 Warszawa

Nawiązując do ogłoszenia o postępowaniu o zamówienie publiczne prowadzonym w trybie przetargu nieograniczonego na ***„Dostawę systemu Firewall”***

MY NIŻEJ PODPISANI

.....

.....

działając w imieniu i na rzecz

.....

.....

{nazwa (firma) i dokładny adres Wykonawcy/ów}

1. **SKŁADAMY OFERTĘ** na wykonanie przedmiotu zamówienia zgodnie ze Specyfikacją Istotnych Warunków Zamówienia w postępowaniu znak (dalej „SIWZ”) **TO-250-30 IT/19**.
2. **OŚWIADCZAMY,** że zapoznaliśmy się z SIWZ i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
3. **OŚWIADCZAMY,** że sposób reprezentacji Wykonawcy/Wykonawców dla potrzeb niniejszego zamówienia jest następujący: .....

   .....

{wypełniają jedynie przedsiębiorcy składający wspólnie ofertę – spółki cywilne lub konsorcja}

4. **ZOBOWIĄZUJEMY SIĘ** do realizacji zamówienia na warunkach określonych w Rozdziale III SIWZ – Szczegółowy Opis Przedmiotu Zamówienia i IV – Istotne Postanowienia Umowy
5. **Oferujemy** wykonanie całego przedmiotu zamówienia za:

- netto: …… zł netto (słownie złotych:……/100),
- plus podatek VAT …..%: tj. ……zł (słownie złotych:……/100
  co stanowi łącznie kwotę brutto: ……..zł (słownie złotych:…… ……/100),
  wg cen jednostkowych podanych w pkt. 15 niniejszej oferty.

OŚWIADCZAMY, iż oferowany system firewall posiada dodatkowe funkcjonalności określone w punkcie 15.2 SIWZ:

Parametry punktowane	Ilość punktów dla dodatkowych funkcjonalności oferowane of systemu Firewall	Oferowany system Firewall spełnia/nie spełnia dodatkowe funkcjonalności
• Urządzanie musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia Active Directory. W przypadku próby wysłania poświadczeń Active Directory do niezaufanej strony lub serwisu administrator może zdefiniować odpowiednią politykę blokującą dla takiego zdarzenia. Jeżeli funkcjonalność wymaga zakupu licencji wtedy Zamawiający wymaga jej dostarczenia dla urządzeń typu A na przynajmniej 12 miesięcy, a na urządzeniach typu B wystarczy możliwość rozbudowy o tę funkcjonalność. • Urządzenie musi posiadać funkcjonalność definiowania i przydzielania dla ruchu webowego odmiennych profili kontrolujących transfer różnych rodzajów plików lub profili ochrony typu AV, IPS, AS ze względu na kategorię URL. Moduł filtrowania stron WWW musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. • System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujących rodzaj i ilość mechanizmów uwierzytelniających (MFA-multifactor authentication) przy ruchu generowanym do wybranych zasobów (niezależnie od tego czy firewall zna tożsamość danego użytkownika)	5	Spełnia / Nie spełnia
• Administrator urządzenia musi mieć możliwość zdefiniowania, dla każdej reguły bezpieczeństwa, innego serwera Syslog. • Urządzenie musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. • Urządzenie musi posiadać interfejs API który musi być jego integralną częścią i umożliwiać konfigurowanie i sprawdzanie stanu urządzenia bez użycia konsoli do zarządzania lub linii poleceń (CLI).	3	Spełnia / Nie spełnia
• Zezwolenie dostępu dla aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM). • Urządzenie musi mieć możliwość tworzenia dynamicznych obiektów adresowych do których, na podstawie zdefiniowanych etykiet, można w automatyczny sposób przypisywać adresy IP. Powinna istnieć możliwość ręcznego tworzenia etykiet bezpośrednio na urządzeniu lub automatycznego pobierania ich z zewnętrznych systemów np. VMware vCenter lub ESX(i) oraz skojarzonych z tymi etykietami adresów IP. Powinna istnieć możliwość wykorzystania tak zbudowanych obiektów adresowych w politykach bezpieczeństwa.	2	Spełnia / Nie spełnia

6. **OŚWIADCZAMY**, iż wybór naszej oferty będzie* / nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego.

   Wskazujemy następujące nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, oraz wskazujemy ich wartość bez kwoty podatku:…….....

7. **ZAMÓWIENIE ZREALIZUJEMY** sami* / z udziałem następujących podwykonawców (proszę podać firmy):

   ……,

   (wskazać części zamówienia powierzonego do wykonania podwykonawcom i o ile jest to wiadome, podać firmy podwykonawców).

8. **OŚWIADCZAMY**, że serwis urządzeń typu Firewall będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta tj. …….. (wskazać podmiot realizujący serwis).

9. **OŚWIADCZAMY, że zapoznali**śmy się z istotnymi postanowieniami umowy określonymi w SIWZ i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach określonych w SIWZ, w miejscu i terminie wyznaczonym przez Zamawiającego.

10. **AKCEPTUJEMY** warunki płatności oraz okres gwarancji określony przez Zamawiającego w istotnych postanowieniach umowy.

11. **OŚWIADCZAMY**, iż – za wyjątkiem informacji i dokumentów zawartych w ofercie, oraz w dokumentach złożonych wraz z ofertą, na stronach nr od ____ do ____ - niniejsza oferta oraz wszelkie załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

12. **UWAŻAMY SIĘ** za związanych niniejszą ofertą przez czas wskazany w SIWZ, tj. przez okres 30 dni.

13. **OFERTĘ** niniejszą wraz z załącznikami składamy na _____ kolejno ponumerowanych stronach.

14. **ZAŁĄCZNIKAMI** do niniejszej oferty są:
    1) Oświadczenie o spełnianiu warunków udziału w postępowaniu (Rozdział II.3, formularz „Oświadczenie o spełnieniu warunków udziału w postępowaniu").
    2) Oświadczenie o braku podstaw do wykluczenia (Rozdział II.2, formularz „Oświadczenie o braku podstaw do wykluczenia").
    3) Oświadczenia Wykonawcy lub Producenta oferowanych urządzeń typu Firewall, że ich serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta. Zamawiający dopuszcza oświadczenie Wykonawcy zamiast oświadczenia producenta.
    4) W celu potwierdzenia, że oferowane urządzenia typu Firewall spełniają wymagania Zamawiającego, do oferty, należy załączyć w formie wydruku, aktualne na dzień złożenia oferty dokumenty producenta oferowanych urządzeń typu Firewall w postaci kart katalogowych dla poszczególnych urządzeń Firewall Typu A i Typu B.

15. **OFERUJEMY**

Składając ofertę w postępowaniu o zamówienie publiczne prowadzone w trybie przetargu nieograniczonego oferujemy dostawę urządzeń typu firewall w następujących cenach jednostkowych[1]:

Lp.	Przedmiot zamówienia	Liczba	Cena jednostkowa netto	Producent i model oferowanego urządzenia.
1	2	3	4	5
1.	Urządzenia Firewall TYP A (w tym oprogramowanie, szkolenie i inne koszty wynikające zgodnie z OPZ)	2		
2.	Urządzenia Firewall TYP B (w tym oprogramowanie, szkolenie i inne koszty wynikające zgodnie z OPZ)	3		

16. **OŚWIADCZAM,** że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**

17. **ZOBOWIĄZUJEMY** się, w przypadku wyboru naszej oferty, przed zawarciem umowy do wniesienia zabezpieczenia należytego wykonania umowy w kwocie 5% wartości zamówienia z podatkiem VAT.

_____ dnia …….. 2019 roku _____

(podpis upoważnionego przedstawiciela Wykonawcy)

** niewłaściwe skreślić*

*** W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*

[1] **Uwaga:**Dla wierszy 1-2 należy załączyć w formie wydruku, aktualne na dzień złożenia oferty dokumenty producenta w postaci kart katalogowych dla poszczególnych oferowanych urządzeń Firewall Typu A i Typu B.

(pieczęć Wykonawcy/ów)	**OŚWIADCZENIE o braku podstaw do wykluczenia**

TO-250-30 IT/19
Nr postępowania

MY NIŻEJ PODPISANI[2]

.....

.....

działając w imieniu i na rzecz

.....

.....

{nazwa (firma) i dokładny adres Wykonawcy }

składając ofertę w postępowaniu o zamówienie publiczne prowadzonym w trybie przetargu nieograniczonego na **„Dostawę systemu Firewall”**, **oświadczamy**, że nie podlegamy wykluczeniu z przedmiotowego postępowania na podstawie art. 24 ust. 1 ani ust. 5 pkt 1, 8 ustawy Pzp.

....., dnia ..... 2019 roku .....

(podpis upoważnionego przedstawiciela Wykonawcy)

Ponadto oświadczamy jak poniżej:

Oświadczamy*, że zachodzą w stosunku do nas 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, ust. 5 pkt 1, 4, 8).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 24 ust. 8 ustawy Pzp podjąłem następujące środki naprawcze:

……

……. *(miejscowość),* dnia …… r. ……

(podpis upoważnionego przedstawiciela Wykonawcy)

Oświadczenie dotyczące podmiotu, na którego zasoby powołuje się Wykonawca:

Oświadczamy*, że w stosunku do następującego/ych podmiotu/tów, 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 zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

……. *(miejscowość),* dnia ……. r. ……

(podpis upoważnionego przedstawiciela Wykonawcy)

[2] Uwaga: w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenie składa odrębnie każdy z Wykonawców wspólnie ubiegających się o zamówienie.

Oświadczenie dotyczące podawanych informacji:

Oświadczamy, 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 upoważnionego przedstawiciela Wykonawcy)

***** - *Zastosować jeśli dotyczy.*

ROZDZIAŁ II.3 FORMULARZ „OŚWIADCZENIE O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU”

(pieczęć Wykonawcy/ów)	**OŚWIADCZENIE o spełnianiu warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy Prawo zamówień publicznych**

TO-250-30 IT/19
nr postępowania

MY NIŻEJ PODPISANI

.....

.....

działając w imieniu i na rzecz

.....

.....

{nazwa (firma) i dokładny adres Wykonawcy/ów oraz NIP/PESEL, KRS/CEiDG w zależności od podmiotu }

składając ofertę w postępowaniu o zamówienie publiczne prowadzonym w trybie przetargu nieograniczonego na **„Dostawę systemu Firewall”**, **OŚWIADCZAMY**, iż spełniamy warunki udziału określone w przedmiotowym postępowaniu.

....., dnia ..... 2019 roku .....

(podpis upoważnionego przedstawiciela Wykonawcy)

Ponadto oświadczamy jak poniżej:

Oświadczamy*, że w celu wykazania spełniania warunków udziału w postępowaniu, określonych przez Zamawiającego w pkt……., polegamy na zasobach następującego/ych podmiotu/ów:

……

……

(wskazać części zamówienia powierzonego do wykonania podwykonawcom i o ile jest to wiadome, podać firmy podwykonawców).

....., dnia ..... 2019 roku .....

(podpis upoważnionego przedstawiciela Wykonawcy)

Oświadczenie dotyczące podawanych informacji:

Oświadczamy, 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 upoważnionego przedstawiciela Wykonawcy)

***** - *Zastosować jeśli dotyczy.*

ROZDZIAŁ II.4 FORMULARZ „DOŚWIADCZENIE”

(pieczęć Wykonawcy/ów)	**„DOŚWIADCZENIE”**

TO-250-30 IT/19
Nr postępowania

Składając ofertę w postępowaniu o zamówienie publiczne prowadzonym w trybie przetargu nieograniczonego na **„Dostawę systemu Firewall”**, oświadczamy, że zrealizowaliśmy w ciągu ostatnich 3 lat następujące podobne zamówienia:

Lp.	Opis zamówienia	Data realizacji	Wartość netto	Nazwa i adres Zamawiającego (odbiorcy)
1		od …… do ……		
2		od …… do ……		

Załączam dokumenty potwierdzające należyte wykonanie usług wyżej wymienionych.

....., dnia ..... 2019 roku .....

(podpis upoważnionego przedstawiciela Wykonawcy)

ROZDZIAŁ II.4 A **FORMULARZ „WYKAZ OSÓB”**

(PIECZĘĆ WYKONAWCY/ÓW)	**„WYKAZ OSÓB”**

TO-250-30 IT/19

Nr Postępowania

składając ofertę w postępowaniu o zamówienie publiczne prowadzonym w trybie przetargu nieograniczonego na „dostawę systemu firewall”, oświadczamy, że dysponujemy, bądź będziemy dysponować n.w. osobami, które będą uczestniczyć w wykonywaniu zamówienia:

Imię i nazwisko	Certyfikat, zgodnie z pkt 6.2 lit. b) ppkt 2) SIWZ	Informacja o podstawie dysponowania wymienioną osobą

……..... dn. **.....**

.....

(podpis upoważnionego przedstawiciela Wykonawcy)

ROZDZIAŁ II.5 FORMULARZ „INFORMACJA DOTYCZĄCA PRZYNALEŻNOŚCI DO GRUPY KAPITAŁOWEJ”

Wzór oświadczenia

(pieczęć Wykonawcy/ów)	**INFORMACJA DOTYCZĄCA PRZYNALEŻNOŚCI DO GRUPY KAPITAŁOWEJ**

TO-250-30 IT/19
Nr postępowania

MY NIŻEJ PODPISANI[3]

.....

.....

działając w imieniu i na rzecz

.....

.....

{nazwa (firma) i dokładny adres Wykonawcy }

W związku ze złożeniem oferty w postępowaniu o zamówienie publiczne prowadzonym w trybie przetargu nieograniczonego na **„Dostawę systemu Firewall”**

oświadczamy, że:

1) *nie należymy do grupy kapitałowej o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp**

2) należymy do grupy kapitałowej następujących Wykonawców ubiegających się o przedmiotowe zamówienie *:

LP.	Nazwa podmiotu	Adres głównej siedziby

Jednocześnie w załączeniu do niniejszego oświadczenia przedstawiamy dowody, że powiązania ze wskazanymi powyżej Wykonawcami nie prowadzą do zakłócenia konkurencji w przedmiotowym postępowaniu o udzielenie zamówienia.

....., dnia ..... 2019 roku .....

(podpis upoważnionego przedstawiciela Wykonawcy)

[3] Uwaga: w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenie składa w oryginale odrębnie każdy z Wykonawców wspólnie ubiegających się o zamówienie.
*niepotrzebne skreślić

Oświadczenie dotyczące podawanych informacji:

Oświadczamy, że wszystkie informacje podane w niniejszym oświadczeniu są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

…… *(miejscowość),* dnia ……. r.

……

(podpis upoważnionego przedstawiciela Wykonawcy)

ROZDZIAŁ III SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA (SOPZ)

1. Nazwa zamówienia nadana przez Zamawiającego:

„Dostawa systemu Firewall".

2. Przedmiot zamówienia.

Przedmiotem zamówienia jest wymiana posiadanego przez Zamawiającego systemu Firewall, wdrożenie i konfiguracja oprogramowania do zarządzania oferowanymi urządzeniami, a także szkolenie z zaoferowanego systemu Firewall.

Zamówienie obejmuje w szczególności:

- Dostawę dwóch głównych urządzeń typu firewall pracujących samodzielnie - TYP A, które posiada deklarację zgodności CE .
- Dostawę trzech dodatkowych urządzeń typu firewall pracujących samodzielnie - TYP B, które posiada deklarację zgodności CE .
- Urządzenia muszą pochodzić od jednego producenta. W kolejnych punktach termin „urządzenie" określa funkcje lub parametry indywidualnie dla pojedynczego urządzenia.
- Dostawę systemu centralnego zarządzania urządzeniami.
- Montaż, konfigurację dostarczonego sprzętu wraz z przeniesieniem obecnie wykorzystywanej konfiguracji na działających urządzeniach Zamawiającego we wszystkich lokalizacjach ITB – Warszawa(Filtrowa, Ksawerów), Poznań, Pionki, Katowice.
- Wdrożenie i konfigurację wszystkich niezbędnych komponentów systemu Firewall umożliwiających pełne wykorzystanie urządzeń zgodnie z wymaganiami SOPZ.
- Przeprowadzenie szkoleń z zakresu obsługi i wykorzystania funkcjonalności dostarczonego systemu Firewall i oprogramowania.

Każde z urządzeń firewall Typ A i Typ B musi spełniać następujące funkcjonalności:

- Urządzenie musi być dostarczone jako samodzielne, dedykowane fizyczne urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej rozwiązania musi występować moduł zarządzania i moduł przetwarzania danych.
- Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
- Urządzenie nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
- Urządzenie musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
- Urządzenie musi być wyposażone w dedykowany port zarządzania out-of-band.
- Urządzenie musi zapewniać obsługę dla IPv6.
- Urządzenie musi zapewnić możliwość statycznej i dynamicznej translacji adresów NAT między IPv4 i IPv6.
- Reguły zabezpieczeń firewall muszą być tworzone zgodnie z ustaloną polityką opartą o profile oraz obiekty.
- Polityka zabezpieczeń firewall musi uwzględniać adresy IP źródłowe i docelowe, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie.
- Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach.
- Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.
- Urządzenie musi działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (w warstwie 2 modelu OSI), w trybie transparentnym oraz trybie pasywnego nasłuchu. Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych biorących udział w transmisji.
- Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w

pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/wirtualna domena, itp.).

- Zarządzanie systemem zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz z graficznej konsoli GUI. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Dopuszcza się, aby polityki mogły być tworzone tylko z graficznej konsoli GUI.
- Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive i Active-Active w przypadku pracy z drugim takim samym urządzeniem posiadającym taki sam zestaw licencji.
- Urządzenie musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP, mapowanie 1 adres publiczny na 1 adres prywatny oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
- Urządzenie musi umożliwiać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. Urządzenia muszą umożliwiać stworzenie co najmniej 6 klas dla różnego rodzaju ruchu sieciowego.
- Urządzenie musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
- Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3.
- Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż RIP, OSPF oraz BGP.
- Urządzenie musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu w tym:
    - Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami.
    - Możliwość blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
- Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
- Urządzenie musi posiadać osobny zestaw polityk definiujący ruch zaszyfrowany SSL oraz SSH, który należy poddać lub wykluczyć z operacji deszyfrowania rozdzielny od polityk bezpieczeństwa.
- Urządzenie musi posiadać możliwość automatycznego pobierania listy stron WWW lub adresów IP z zewnętrznego systemu oraz używania ich w politykach bezpieczeństwa.
- Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony informującej użytkownika o próbie pobrania pliku i możliwości kontunuowania lub zaniechania pobrania.
- Urządzenie zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów, dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning"). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
- Urządzenie musi identyfikować co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Tor, BitTorrent, eMule.
- Urządzenie musi zapewnić możliwość definiowania własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.
- System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie wyłącznie na podstawie rozszerzenia.
- Urządzenie musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Urządzenie musi umożliwiać konfigurację tuneli VPN w trybie route-based VPN.
- Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN oraz IPSec.
- Urządzenie musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy

połączeniu do Internetu poza siecią korporacyjną).

- Producent urządzenia musi udostępniać dedykowanego klienta binarnego VPN dla platform Windows, Mac oraz Android.
- Urządzenie musi transparentnie ustalać tożsamość użytkowników sieci w oparciu o Active Directory oraz Ms Exchange. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym Citrix oraz Windows Terminal Services, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
- Urządzenie musi mieć możliwość czytania oryginalnych adresów IP stacji końcowych z nagłówka X-Forwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
- Urządzenie musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
- Urządzenie musi pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i kategorii stron WWW.
- Urządzenie musi pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
- Urządzenie musi być rozwiązaniem o uznanej na rynku pozycji i musi znajdować się w kwadracie „Leaders" lub „Challengers" raportu Gartnera pt. „Magic Quadrant of Network Enterprise Firewalls" w raportach opublikowanych w przeciągu 2 ostatnich lat.
- Urządzenie musi być fabrycznie nowe, aktualnie obecne w linii produktowej producenta.
- Urządzenie musi pochodzić z autoryzowanego kanału sprzedażowego producenta na terenie Unii Europejskiej.
- Urządzenie nie może znajdować się na liście „end-of-sale" oraz „end-of-support" producenta.
- Dostęp do najnowszej wersji oprogramowania, serwis sprzętowy i ewentualne licencje/subskrypcje na aktualizacje bazy aplikacji muszą być ważne przynajmniej przez okres **12** miesięcy.
- Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.
- Rozwiązanie musi posiadać możliwość podłączenia urządzeń firewall pod scentralizowany system zarządzania pochodzący od tego samego producenta. W ramach postępowania należy dostarczyć platformę zarządzającą spełniającą następujące wymagania:
    - Zamawiający wymaga dostarczenia fizycznej lub wirtualnej platformy zarządzającej pozwalającej na centralne zarządzanie urządzeniami, logowanie i raportowanie zdarzeń z podłączonych do niej firewalli. Platforma musi pochodzić od tego samego producenta co urządzenia podstawowe.
    - Konsola zarządzająca w wersji wirtualnej musi zostać dostarczona w postaci maszyny wirtualnej instalowanej w środowisku VMWare
    - Konsola zarządzająca musi umożliwiać zarządzanie przynajmniej 20 urządzeniami pochodzącymi od tego samego producenta oraz być objęta wsparciem serwisowym na okres 12 miesięcy.
    - System zarządzania, logowania i raportowania musi pozwalać skonfigurować lub zapewniać przestrzeń dyskową o pojemności nie mniejszej niż 24 TB.
    - Konsola zarządzająca musi udostępniać dedykowane narzędzia dla łatwego przeszukiwania skorelowanych logów zebranych z zarządzanych firewalli.
    - Konsola zarządzająca, logująca i raportująca musi mieć możliwość korelowania zbieranych zdarzeń i informacji oraz budowania na ich podstawie wielu, dostosowanych do potrzeb Zamawiającego raportów statycznych i dynamicznych. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowaniu stron WWW. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
    - Konsola zarządzająca, logująca i raportująca musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa, aktualizację oprogramowania i sygnatur oraz funkcje audytu i backupu konfiguracji. Konsola zarządzania musi posiadać możliwość weryfikacji spójności i niesprzeczności wprowadzonej konfiguracji.

- Konsola zarządzająca musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.
- Konsola zarządzająca musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur.
- Konsola zarządzająca musi umożliwiać tworzenie obiektów o różnym zasięgu (lokalne, globalne).
- Konsola zarządzająca musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.
- Konsola zarządzając musi mieć możliwość pracy w klastrze niezawodnościowym z drugą taką samą instancją.

Parametry, które muszą być spełnione przez każde z urządzeń głównych - TYP A:

- Urządzenie musi być dostarczone w konfiguracji z minimum 12 portami Ethernet 1Gb/s w tym minimum 4 portami Ethernet Rj45 10/100/1000 oraz 8 portami typu SFP 1G.
- Urządzenie musi posiadać przepustowość w ruchu nie mniej niż 1 Gbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 750 Mbps.
- Urządzenie musi obsłużyć minimum 120000 jednoczesnych sesji oraz 8000 nowych połączeń na sekundę.
- Urządzenie musi zapewniać wydajność przynajmniej 400 Mbps dla ruchu IPSec VPN.
- Urządzenie musi umożliwiać zestawienie przynajmniej 1500 równoczesnych tuneli site-to-site.
- Urządzenie musi być w obudowie typu rack 1RU.
- Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention) i innego złośliwego kodu (wirusy, spyware, malware), filtracja plików, danych i URL.
- Urządzenie musi umożliwiać wykluczenie z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.
- Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
- Urządzenie musi zapewniać zestawienie przynajmniej 1000 sesji SSL VPN.
- Urządzenie musi posiadać funkcjonalność weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający wymaga dostarczenia subskrypcji dla tej usługi na okres **12** miesięcy.
- Urządzenie musi posiadać funkcjonalność sterowania zachowaniem binarnego klienta VPN z poziomu systemu - połączenie automatyczne bądź ręczne przez użytkownika a także umożliwiać sprawdzenie czy klient posiada zainstalowane oprogramowanie antywirusowe. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający wymaga dostarczenia subskrypcji dla tej usługi na okres **12** miesięcy.
- Urządzenie musi posiadać funkcjonalność zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający wymaga dostarczenia subskrypcji dla tej usługi na okres **12** miesięcy.
- Urządzenie musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum **12** miesięcy.
- Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum **12** miesięcy.
- Urządzenie musi umożliwiać filtrowanie stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza przypisania URL do kategorii musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.W ramach zamówienia Zamawiający wymaga subskrypcji tej usługi na okres minimum **12** miesięcy.

- Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
- Urządzenie musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. Jeśli ta funkcjonalność wymaga dodatkowej subskrypcji to Zamawiający wymaga tej usługi na okres minimum **12** miesięcy.
- Urządzenie musi zapewniać moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików w czasie nie przekraczającym 30 minut. Jeżeli funkcjonalność ta wymaga dodatkowej licencji wtedy Zamawiający wymaga subskrypcji tej usługi na okres minimum **12** miesięcy.
- Administrator urządzenia musi mieć możliwość przeglądania z poziomu urządzenia informacji o plikach które zostały wysłane do analizy w systemie "Sand-Box", informacji jak przesłane pliki zachowywały się w środowisku testowym, które z nich i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki przesyłali. Jeżeli funkcjonalność ta wymaga dodatkowej licencji wtedy Zamawiający wymaga subskrypcji tej usługi na okres minimum **12** miesięcy.

Parametry, które muszą być spełnione przez każde z urządzeń dodatkowych - TYP B:

- Urządzenie musi być dostarczone w konfiguracji z minimum 8 portami Ethernet RJ45 10/100/1000.
- Urządzenie musi posiadać przepustowość w ruchu nie mniej niż 500 Mbps dla kontroli firewall z włączoną funkcją kontroli aplikacji. Przepustowość dla ruchu rzeczywistego z włączoną pełną funkcjonalnością (ochrona IPS, antywirus, antyspyware, identyfikacja aplikacji) nie może być mniejsza niż 250 Mbps.
- Urządzenie musi obsłużyć minimum 60000 jednoczesnych sesji oraz 4000 nowych połączeń na sekundę.
- Urządzenie musi zapewniać wydajność przynajmniej 100 Mbps dla ruchu IPSec VPN.
- Urządzenie musi umożliwiać zestawienie przynajmniej 1000 równoczesnych tuneli site-to-site.
- Urządzenie musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi umożliwiać deszyfracje niezaufanego ruchu HTTPS i poddania go właściwej inspekcji.
- Urządzenie musi mieć możliwość rozbudowy o funkcjonalność wykluczenia z inspekcji komunikacji szyfrowanej ruchu wrażliwego na bazie co najmniej: kategoryzacji stron URL oraz dodania własnych wyjątków.
- Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (IPS, AV, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AM, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
- Urządzenie musi zapewniać zestawienie przynajmniej 250 sesji SSL VPN.
- Urządzenie musi umożliwiać weryfikację poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci lub wybranych jej zasobów. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia dla urządzeń dodatkowych.
- Urządzenie ma umożliwiać sterowanie zachowaniem binarnego klienta VPN z poziomu systemu - połączenie automatyczne bądź ręczne przez użytkownika a także umożliwiać sprawdzenie czy klient posiada zainstalowane oprogramowanie antywirusowe. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia dla urządzeń dodatkowych.
- Urządzenie musi zapewniać możliwość zestawienia tuneli VPN SSL bez konieczności instalowania klienta na stacji końcowej – clientless VPN. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia dla urządzeń dodatkowych.
- Urządzenie musi posiadać możliwość uruchomienia funkcji wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS). Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia dla urządzeń dodatkowych.
- Urządzenie musi posiadać możliwość uruchomienia funkcji inspekcji antywirusowej, kontrolującej przynajmniej protokoły: SMTP, HTTP, POP3, IMAP oraz podstawowe rodzaje plików. Baza AV musi być przechowywana na urządzeniu i regularnie aktualizowana w sposób automatyczny. Jeśli wymaga to zakupu dodatkowej subskrypcji,

Zamawiający nie wymaga jej dostarczenia dla urządzeń dodatkowych.

- Urządzenie musi umożliwiać filtrowanie stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza przypisania URL do kategorii musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia dla urządzeń dodatkowych.
- Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
- Urządzenie musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. Jeśli wymaga to zakupu dodatkowej subskrypcji, Zamawiający nie wymaga jej dostarczenia dla urządzeń dodatkowych.

Parametry punktowane:

- 5 punktów – jeśli rozwiązanie zaproponowane przez Wykonawcę spełnia wszystkie wymienione poniżej dodatkowe funkcjonalności:

Parametry punktowane (wymienione parametry dotyczą każdego z urządzeń firewall – wszystkie oferowane urządzenia firewall muszą posiadać wszystkie wymienione funkcjonalności aby zostały przyznane punkty):

- Urządzanie musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysyłać swoje poświadczenia Active Directory. W przypadku próby wysłania poświadczeń Active Directory do niezaufanej strony lub serwisu administrator może zdefiniować odpowiednią politykę blokującą dla takiego zdarzenia. Jeżeli funkcjonalność wymaga zakupu licencji wtedy Zamawiający wymaga jej dostarczenia dla urządzeń typu A na przynajmniej 12 miesięcy, a na urządzeniach typu B wystarczy możliwość rozbudowy o tę funkcjonalność.
- Urządzenie musi posiadać funkcjonalność definiowania i przydzielania dla ruchu webowego odmiennych profili kontrolujących transfer różnych rodzajów plików lub profili ochrony typu AV, IPS, AS ze względu na kategorię URL. Moduł filtrowania stron WWW musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
- System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujących rodzaj i ilość mechanizmów uwierzytelniających (MFA-multifactor authentication) przy ruchu generowanym do wybranych zasobów (niezależnie od tego czy firewall zna tożsamość danego użytkownika)

- 3 punkty – jeśli rozwiązanie zaproponowane przez Wykonawcę spełnia wszystkie wymienione poniżej dodatkowe funkcjonalności:

Parametry punktowane (wymienione parametry dotyczą każdego z urządzeń firewall – wszystkie oferowane urządzenia firewall muszą posiadać wszystkie wymienione funkcjonalności aby zostały przyznane punkty):

- Administrator urządzenia musi mieć możliwość zdefiniowania, dla każdej reguły bezpieczeństwa, innego serwera Syslog.
- Urządzenie musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
- Urządzenie musi posiadać interfejs API który musi być jego integralną częścią i umożliwiać konfigurowanie i sprawdzanie stanu urządzenia bez użycia konsoli do zarządzania lub linii poleceń (CLI).

- 2 punkty – jeśli rozwiązanie zaproponowane przez Wykonawcę spełnia wszystkie wymienione poniżej dodatkowe funkcjonalności:

Parametry punktowane (wymienione parametry dotyczą każdego z urządzeń firewall – wszystkie oferowane urządzenia firewall muszą posiadać wszystkie wymienione funkcjonalności aby zostały przyznane punkty):

- Zezwolenie dostępu dla aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
- Urządzenie musi mieć możliwość tworzenia dynamicznych obiektów adresowych do których, na podstawie zdefiniowanych etykiet, można w automatyczny sposób przypisywać adresy IP. Powinna istnieć możliwość ręcznego tworzenia etykiet bezpośrednio na urządzeniu lub automatycznego pobierania ich z zewnętrznych systemów np. VMware vCenter lub ESX(i) oraz skojarzonych z tymi etykietami adresów IP. Powinna istnieć możliwość wykorzystania tak zbudowanych obiektów adresowych w politykach bezpieczeństwa.

UWAGA:
Zamawiający będzie weryfikował parametry urządzeń na podstawie dokumentacji producenta. Wykonawca musi dostarczyć do każdego z oferowanych urządzeń **kartę katalogową potwierdzającą spełnienie wymagań SOPZ**. Zamawiający zastrzega sobie także prawo do weryfikacji parametrów urządzeń na podstawie testów (Wezwanie do przeprowadzenia testów zostanie wysłane do Wykonawcy, którego oferta została najwyżej oceniona wg kryteriów). Wszelkie testy będą przeprowadzone przez Wykonawcę na jego koszt i ryzyko.
Zamawiający wymaga gotowości oferenta do przeprowadzenia testów w terminie nie dłuższym niż 12 dni kalendarzowych liczonym od dnia otwarcia ofert, które będą przeprowadzone w przywołanym terminie. Wykonawca zadeklaruje gotowość przeprowadzenia testów urządzenia (Typ-A i Typ – B) we własnym środowisku testowym. Potwierdzenie wszystkich wymagań zdefiniowanych w SOPZ będzie pozytywnym wynikiem testów.

Opis testów:
Testy będą się składały z dwóch części: funkcjonalnej oraz wydajnościowej z wykorzystaniem dedykowanego urządzenia typu appliance (generator ruchu) umożliwiającego wytworzenie ruchu o wymaganej charakterystyce i wolumenie Dodatkowo, Zamawiający zastrzega sobie prawo do zweryfikowania, że zaproponowane rozwiązanie spełnia minimalne wymagania funkcjonalne oraz opcjonalne właściwości zadeklarowane przez Wykonawcę.
Wykonawca w terminie wykonania testów musi przygotować kompletne środowisko testowe, w szczególności urządzenia i oprogramowanie składające się na oferowany system oraz wszelkie inne elementy konieczne do przeprowadzenia testów.

Warunki serwisu technicznego i procedura zgłoszeń

- Wsparcie techniczne (w szczególności: gwarantowana pomoc w eksploatacji oprogramowania i urządzeń udzielana użytkownikowi) musi być świadczone w języku polskim poprzez autoryzowanego Partnera producenta urządzeń typu Firewall w zakresie świadczenia pomocy serwisowej. Do ofert należy dołączyć oświadczenie Wykonawcy lub Producenta oferowanych urządzeń typu Firewall, że ich serwis będzie realizowany przez Autoryzowanego Partnera Serwisowego Producenta lub bezpośrednio przez Producenta i wskazanie tego podmiotu. Zamawiający dopuszcza oświadczenie Wykonawcy zamiast oświadczenia producenta.
- Wsparcie techniczne musi być świadczone przez okres **12** miesięcy dla każdego z urządzeń/systemów. W wypadku wystąpienia awarii zamawiający otrzyma urządzenie objęte gwarancją w trybie następnego dnia roboczego, przy czym wszelkie zgłoszenia przyjmowane muszą być w trybie 24/7. Wraz z dostarczonym urządzeniem będzie świadczony dostęp do strony pomocy technicznej producenta oraz możliwość pobierania aktualizacji oprogramowania związanego z oferowanym urządzeniem.

Certyfikaty techniczne w zakresie wsparcia:

Wykonawca musi posiadać minimum 2 osoby legitymujące się ważnym certyfikatem technicznym producenta urządzeń na poziomie co najmniej zawansowanym z zakresu technologii wykorzystywanych na zamawianych urządzeniach.

Zakres Szkolenia

1. Wykonawca w ramach zamówienia przeprowadzi szkolenie w języku polskim w formie praktycznych warsztatów oraz wykładów teoretycznych dla 4 osób (administratorów Zamawiającego) w wymiarze minimum 5 dni (8 godzin dziennie) w 5-tym tygodniu od daty zawarcia umowy.

2. Szkolenie będzie prowadzone przez inżyniera z wiedzą praktyczną potwierdzoną certyfikatem technicznym producenta.

3. Wykonawca pokryje wszelkie koszty związane z przygotowaniem środowiska szkoleniowego oraz przeprowadzaniem szkolenia. Jeżeli miejsce szkolenia będzie oddalone od siedziby Zamawiającego o ponad 30 km. Wykonawca pokryje również koszty zakwaterowania oraz dojazdu.

4. Szkolenia będą oceniane przez ich uczestników pod kątem wiedzy merytorycznej, sposobu jej przekazania przez prowadzącego a także wpływu przekazanych informacji na poprawę/uzyskanie wiedzy i umiejętności koniecznych do prawidłowego korzystania z dostarczonego rozwiązania. Po przeprowadzeniu szkolenia, każdy z uczestników wypełni anonimową ankietę oceniając zbiorczo powyższe aspekty w skali od 1-5 przy czym poszczególnym ocenom zostaną przypisane następujące znaczenia:

    1- Niedostateczny
    2- Dopuszczający

3- Dostateczny
4- Dobry
5- Bardzo dobry

Uzasadnienie oceny z przeprowadzonego szkolenia będzie oceną opisową zgodnie z powyższą skalą. Administratorzy przekażą swoją ocenę bezpośrednio Zamawiającemu. Zamawiający niezwłocznie przekazuje wyniki ankiet Wykonawcy.

5. Przeprowadzenie szkoleń będzie udokumentowane Protokołami Odbioru Szkolenia. Protokół Odbioru Szkolenia zostanie podpisany w ciągu 2 dni roboczych od daty przeprowadzenia danego szkolenia, z zastrzeżeniem, że w przypadku szkoleń podstawą podpisania tego dokumentu będzie uzyskanie średniej z ocen uczestników każdego szkolenia na poziomie minimum 3,75. W przypadku nieuzyskania średniej, o której mowa w zdaniu poprzednim Zamawiający w terminie 2 dni roboczych na podstawie informacji uzyskanych od uczestników przekaże swoje zastrzeżenia i uwagi. Na podstawie tych informacji Wykonawca zaproponuje stosowne rozwiązania mające na celu uzyskanie wymaganej średniej ocen np. powtórne przeprowadzenie całego szkolenia, w tym przez innego wykładowcę, rozszerzenie zakresu szkolenia o elementy nieujęte lub niedostatecznie omówione, przekazanie dodatkowych materiałów szkoleniowych, dodatkowe konsultacje, w tym mailowe lub telefoniczne. Zaproponowane rozwiązania będą podlegały uzgodnieniom z Zamawiającym. Po zakończeniu powyższych działań naprawczych, o ile będą one polegały na przeprowadzeniu szkolenia w całości lub części, uczestnicy szkolenia ponownie dokonają ocen wedle skali i sposobu, o którym powyżej. W przypadku ponownego nieuzyskania wymaganej średniej, powyżej procedura wskazana w niniejszym ustępie podlega ponowieniu. W przypadku dwukrotnego ponowienia procedury naprawczej i nieuzyskania wymaganej średniej, Zamawiającemu przysługuje prawo do zlecenia przeprowadzenia szkolenia innej firmie na koszt Wykonawcy.

   (dni szkolenia: poniedziałek – piątek)

Szkolenie musi obejmować następującą tematykę :

1. Architektura rozwiązania firewall
2. Konfiguracja wstępna urządzenia
3. Konfiguracja sieciowa: interfejsy, strefy (o ile zaoferowane urządzenia firewall obsługują tę funkcjonalność), translacje adresów IP
4. Konfiguracja polityk i reguł bezpieczeństwa
5. Konfiguracja silników ochrony np. IPS,
6. Konfiguracja silnika rozpoznania aplikacji
7. Identyfikacja użytkowników
8. Konfiguracja sieci VPN – site-to-site i zdalny dostęp
9. Konfiguracja firewalli wirtualnych
10. Konfiguracja HA (wysoka dostępność)
11. Analiza ruchu SSL – deszyfracja
12. Konfiguracja dostępu administracyjnego i zarządzanie uprawnieniami administratorów
13. Monitorowanie urządzenia
14. Diagnostyka urządzenia
15. Tworzenie raportów i wykorzystywania silnika raportującego
16. Analiza logów diagnostycznych dla ruchu
17. Narzędzia diagnostyczne wbudowane w urządzenia
18. Sposoby i algorytmy izolowania problemów na urządzeniach
19. Architektura systemu zarządzania
20. Konfiguracja systemu zarządzania
21. Definiowanie obiektów
22. Współdzielenie obiektów
23. Dodawanie urządzeń do systemu zarządzania i ich grupowanie
24. Szablony wykorzystywane w systemie zarządzania
25. Zarządzanie dostępem administracyjnym i uprawnieniami administratorów
26. Centralne narzędzia zarządzania – analiza incydentów, analiza logów, narzędzia diagnostyczne
27. Centralne narzędzia monitorowania większej liczby firewalli
28. Sposoby i algorytmy izolowania problemów w systemie zarządzania
29. Konfiguracja HA (wysoka dostępność) dla systemu zarządzania

Zakres wdrożenia

Wykonawca w ramach zamówienia dostarczy urządzenia w uzgodnionym terminie na wskazany przez Zamawiającego

adres, przeprowadzi fizyczną instalację oraz konfigurację urządzeń obejmującą :

1. Migrację konfiguracji z zastępowanych urządzeń Cisco ASA
2. Podstawowa konfiguracja zapór ogniowych
3. Podstawowa konfiguracja centralnej konsoli zarządzającej oraz integracja z urządzeniami firewall
4. Konfiguracja sieciowa urządzeń, w tym adresacja interfejsów, routingi.
5. Wgranie i instalacja najnowszego stabilnego oprogramowania dla urządzenia.
6. Przeniesienie obiektów oraz polityk bezpieczeństwa, NAT.
7. Konfiguracja deszyfracji wybranego ruchu (SSL, SSH) wraz z wykrywaniem niebezpieczeństw w wewnątrz szyfrowanych połączeń.
8. Migracja polityk wykorzystujących protokół i port na polityki oparte na rzeczywistych aplikacjach
9. Konfiguracja profili bezpieczeństwa (Antywirus, IPS, typy plików)
10. Przeniesienie i konfiguracja istniejących tuneli VPN
11. Konfiguracja klienckiego VPN wraz z weryfikacją stacji końcowych użytkowników.
12. Konfiguracja identyfikacji użytkowników w oparciu o AD.
13. Konfiguracja logowania zdarzeń do zewnętrznych systemów.
14. Konfiguracja reguł DoS
15. Konfiguracja reguł QoS dla wybranego ruchu.
16. Konfiguracja generowania raportów oraz automatów wysyłających wygenerowane raporty.
17. Konfiguracja musi zostać przeprowadzona z centralnej konsoli zarządzania w sposób spójny (z wykorzystaniem współdzielonych obiektów, profili, polityk oraz innych ustawień)
18. Wykonanie dokumentacji technicznej zawierającej kluczowe elementy konfiguracyjne, schemat połączeń oraz ruchu sieciowego, napotkane problemy. Dokumentacja zostanie wykonana po etapie testów na środowisku preprodukcyjnym, po finalnym przeprowadzeniu konfiguracji i wykonaniu testów na środowisku produkcyjnym. Dokumentacja powinna zawierać:
    a. Analizę infrastruktury sieciowej Zamawiającego
    b. Projekt techniczny i schemat instalacji w infrastrukturze Zamawiającego
    c. Podręcznik administratora opisujący poszczególne funkcje urządzeń oraz ich obsługę.

Plan wdrożenia:
Wykonawca przeprowadzi wstępną konfigurację urządzeń, która następnie zostanie udokumentowana oraz zostaną wykonane testy prawidłowego funkcjonowania w środowisku preprodukcyjnym obejmującym wydzielone obszary sieci oraz wybrane funkcjonalności. Wszelkie odstępstwa i błędy wychwycone na tym etapie zostaną udokumentowane oraz usunięte. Wstępna konfiguracja obejmuje następujące elementy:

- Utworzenie konfiguracji sieciowej i routingu
- Przeniesienie reguł firewall z pełnym wykorzystaniem identyfikacji aplikacji oraz reguł NAT
- Konfiguracja ochrony przed zagrożeniami na wybranych przepływach.
- Identyfikacja użytkowników
- Konfiguracja wybranych tuneli VPN
- Konfiguracja usługi Client VPN dla Windows, Mac, Android, IOS wraz z wykorzystaniem weryfikacji stanu stacji końcowych.
- Konfiguracja różnych metod podłączenia użytkowników zdalnych w zależności od posiadanego systemu, tożsamości.

Następnie wykonawca przeprowadzi finalną konfigurację z uwzględnieniem wykrytych i usuniętych problemów na wcześniejszym etapie oraz dokona przeniesienia i konfiguracji pozostałych wymaganych funkcji dla całej infrastruktury Zamawiającego. Wykonawca przeprowadzi testy, dokona weryfikacji poprawności funkcjonowania poszczególnych elementów, udokumentuje napotkane błędy i problemy oraz dokona ich naprawy oraz optymalizacji systemu.

3. Termin realizacji zamówienia

Zamówienie zostanie zrealizowane **w ciągu 5 tygodni** od dnia zawarcia umowy z podziałem na dwa etapy, z zastrzeżeniem lit. b) niniejszego punktu:

a) 4 tygodnie od zawarcia umowy, obejmuje:
    - dostawę wszystkich elementów systemu Firewall,
    - uruchomienie, konfigurację, instalację oprogramowania (licencji), wdrożenie wszystkich elementów wymienionych w Szczegółowym Opisie Przedmiotu Zamówienia.
b) 5-ty tydzień obejmuje przeprowadzenie szkolenia zgodnie z wymaganiami opisanymi w Szczegółowym Opisie Przedmiotu Zamówienia. Zasadę liczenia 5 tygodnia realizacji Przedmiotu Zamówienia ustala się od pierwszego poniedziałku po realizacji dostawy (dni szkolenia: poniedziałek – piątek).

4 Wymagania ogólne

4.1 Wraz z urządzeniami dostarczone zostanie okablowanie logiczne niezbędne do prawidłowego podłączenia i uruchomienia systemu Firewall.

4.2 Wszystkie urządzenia powinny zawierać osprzęt wymagany do prawidłowego podłączenia i instalacji oferowanych urządzeń.

4.3 Dostawa powinna obejmować wszystkie komponenty (na przykład: kable logiczne, złącza, przejściówki, szyny, elementy montażowe) niezbędne do prawidłowego połączenia, instalacji i uruchomienia wszystkich zamawianych komponentów

4.4 Całość dostarczonego systemu Firewall musi zapewniać pełną kompatybilność, oraz jak najlepsze dopasowanie rozwiązań technicznych, konfiguracyjnych, programowych gwarantujących bezkolizyjną integrację zamawianych komponentów na poziomie funkcjonalnym całego systemu Firewall.

5 Warunki gwarancji

5.1 Gwarancja liczona będzie od daty podpisania bezusterkowego protokołu odbioru urządzeń systemu Firewall.

5.2 Gwarancja dotyczy wszystkich podzespołów znajdujących się w urządzeniach typu Firewall.

5.3 Zgłoszenie wady dokonane będzie telefonicznie, na adres e-mail Wykonawcy lub za pomocą formularza zamieszczonego na stronie internetowej wskazanej przez Wykonawcę. Sposób komunikacji zostanie ustalony w dniu podpisania umowy.

5.4 Działania gwarancyjne i serwisowe w okresie gwarancji wykonywane są środkami i na koszt Wykonawcy, łącznie z kosztami transportu, dojazdu, delegacji, części i usług itp.

5.5 W okresie gwarancyjnym awarie muszą być usuwane w trybie – naprawa następnego dnia roboczego w każdej z lokalizacji ITB – Warszawa, Katowice, Pionki, Poznań.

5.6 Jeżeli po naprawie, wymianie urządzeń typu Firewall, wymagana będzie re-instalacja oprogramowania lub ponowna konfiguracja, Wykonawca zobowiązany jest do jej wykonania na własny koszt zgodnie z licencjami przypisanymi do danego urządzenia. Urządzenie dostarczone po naprawie lub wymianie do Zamawiającego musi posiadać identyczna konfigurację jak urządzenie przekazane do wymiany lub naprawy.

5.7 Nie wywiązanie się w terminie ze zobowiązań przez Wykonawcę upoważnia Zamawiającego do zlecenia wykonania usługi innej firmie na koszt Wykonawcy.

5.8 W razie braku możliwości naprawy sprzętu u Zamawiającego, przewiezienie go do punktu serwisowego Wykonawcy nastąpi po uzgodnieniu z Działem IT Zamawiającego.

5.9 Każde urządzenie będące w naprawie musi być zwrócone z protokółem opisującym szczegółowo naprawę oraz nazwą lub nazwy wymienionych podzespołów.

5.10 W przypadku wystąpienia trzykrotnej awarii danego urządzenia, dostawca wymieni całe urządzenie na nowe.

5.11 Wykonawca zapewni realizację serwisu gwarancyjnego Producenta lub Autoryzowanego Partnera Serwisowego Producenta.

ROZDZIAŁ IV ISTOTNE POSTANOWIENIA UMOWY

UMOWA nr …….

zawarta w Warszawie, w dniu ……2019 r. pomiędzy:
Instytutem Techniki Budowlanej z siedzibą przy ul. Filtrowej 1, 00-611 Warszawa, posiadającym nr NIP 525-000-93-58, REGON: 000063650, KRS 0000158785 prowadzonym przez Sąd Rejonowy dla Miasta Stołecznego Warszawy XVI Wydział Gospodarczy Krajowego Rejestru Sądowego, zwanym dalej Zamawiającym, reprezentowanym przez:
……..
a ……. z siedzibą w ……, zwanym dalej Wykonawcą, reprezentowanym przez:

§ 1

Przedmiotem umowy jest wymiana podsiadanego przez Zamawiającego systemu Firewall, wdrożenie i konfiguracja oprogramowania do zarządzania , a także szkolenie z zaoferowanego systemu Firewall, zgodnie z ofertą Wykonawcy z dnia …….. i Szczegółowym Opisem Przedmiotu Zamówienia zawartym w Rozdziale III SIWZ (dalej „SOPZ") stanowiącymi integralną część niniejszej umowy.

§ 2

Przedmiot umowy zostanie zrealizowane **w ciągu 5 tygodni** od dnia zawarcia umowy z podziałem na dwa etapy, z zastrzeżeniem lit. b) niniejszego paragrafu:

a) 4 tygodnie od zawarcia umowy, obejmuje:
- dostawę wszystkich elementów systemu Firewall,
- uruchomienie, konfigurację, instalację oprogramowania (licencji), wdrożenie wszystkich elementów wymienionych w Szczegółowym Opisie Przedmiotu Zamówienia.

b) 5-ty tydzień obejmuje przeprowadzenie szkolenia zgodnie z wymaganiami opisanymi w Szczegółowym Opisie Przedmiotu Zamówienia. Zasadę liczenia 5 tygodnia realizacji Przedmiotu Zamówienia ustala się od pierwszego poniedziałku po realizacji dostawy (dni szkolenia: poniedziałek – piątek).

§ 3

1. Przedmiot umowy zostanie dostarczony na koszt i ryzyko Wykonawcy.
2. Miejsce dostawy przedmiotu umowy: ITB, Warszawa ul. Filtrowa 1, Warszawa ul. Ksawerów 21, Katowice al. Korfantego 191, Poznań ul. Taczaka 12, Pionki ul. Przemysłowa 2
3. Wykonawca oświadcza, że dostarczone przez niego urządzenia:
   a. są fabrycznie nowe,
   b. charakteryzują się parametrami nie gorszymi niż opisane w Rozdziale III SIWZ i ofercie,
   c. posiadają deklarację zgodności CE.
4. Odbiór przedmiotu umowy przez Zamawiającego zostanie dokonany w dwóch etapach, w ciągu 3 dni roboczych od dnia zgłoszenia przez Wykonawcę:
   a) Zakończenia uruchomienia, konfiguracji, instalacji oprogramowania, wdrożenia wszystkich elementów wymienionych w SOPZ systemu Firewall, co zostanie potwierdzone podpisaniem protokołu odbioru częściowego bez uwag,
   b) po zakończeniu szkolenia, co zostanie potwierdzone podpisaniem protokołu odbioru końcowego bez uwag,

c) W toku odbioru Zamawiający sprawdzi zgodność dostarczonych urządzeń i oprogramowania z Ofertą i SOPZ oraz prawidłowość instalacji.

d) W przypadku stwierdzenia nieprawidłowości, niezgodności, niekompletności lub wad zostanie to opisane w protokole i Zamawiający wyznaczy termin na usunięcie nieprawidłowości, niezgodności, niekompletności lub wad.

e) Po upływie wyznaczonego terminu Zamawiający przystąpi ponownie do odbioru.

f) Odbiór zakończy się podpisaniem bezusterkowego protokołu końcowego odbioru przez obie strony.

g) W przypadku, gdyby stwierdzone nieprawidłowości, niezgodności, niekompletności lub wady nie zostały usunięte w terminie, Zamawiający będzie mógł odstąpić od Umowy w całości lub części. W przypadku odstąpienia od części Umowy, w pozostałym zakresie zostanie podpisany bezusterkowy protokół odbioru końcowego.

h) Wykonawca zobowiązany jest do przygotowania protokołu odbioru częściowego z dokładnym opisem przedmiotu dostawy, w szczególności z wykazem numerów seryjnych przedmiotu umowy oraz czasu trwania gwarancji.

i) Wykonawca dostarczy do Zamawiającego instrukcję obsługi i kartę gwarancyjną każdego urządzenia w języku polskim nie później niż w dniu odbioru częściowego.

§ 4

1. Do kontaktów Zamawiającego z Wykonawcą zostają wyznaczone następujące osoby:

……..

2. Do kontaktów z Zamawiającym Wykonawca wyznacza następujące osoby:

……

3. Zmiana osób, o których mowa w ust 1 i 2, nie stanowi zmiany Umowy wymagającej sporządzenia aneksu.
4. Do realizacji umowy należy skierować osoby wskazane w wykazie osób złożonym na wezwanie Zamawiającego w trybie art. 26 ust. 2 ustawy Prawo zamówień publicznych.

§ 5

1. Wykonawca udziela Zamawiającemu gwarancji na okres 12 miesięcy zgodnie z postanowieniami i na warunkach określonych w Rozdziale III SIWZ *Szczegółowy opis przedmiotu zamówienia*.
2. Okres gwarancji liczony jest od dnia dokonania bez zastrzeżeń odbioru częściowego przedmiotu umowy.
3. Wykonawca zapewni realizację serwisu gwarancyjnego Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
4. W dokumencie gwarancji Wykonawca wskaże dane kontaktowe, pod którymi Zamawiający będzie mógł zgłaszać wady.
5. Niezależnie od uprawnień wynikających z udzielonej gwarancji Zamawiający może korzystać z uprawnień wynikających z rękojmi.

§ 6

1. Tytułem zabezpieczenia należytego wykonania Umowy ustala się zabezpieczenie w wysokości 5% całkowitego wynagrodzenia Wykonawcy brutto, o którym mowa w §7 ust. 1 niniejszej Umowy, tj. kwotę ..... PLN (słownie złotych: ……).
2. W dniu zawarcia Umowy Wykonawca wniósł ustaloną w ust. 1 kwotę zabezpieczenia w formie .....
3. Zamawiający wyraża zgodę na zmianę formy wniesionego zabezpieczenia należytego wykonania umowy w trakcie trwania umowy, na jedną lub kilka form określonych w art. 148 ust. 1 ustawy Pzp.
4. Zamawiający zwróci Wykonawcy zabezpieczenie należytego wykonania Umowy w terminie 30 dni od daty podpisania bez zastrzeżeń przez upoważnionych przedstawicieli Stron bezusterkowego protokołu końcowego odbioru o którym mowa w § 3 ust. 4 Umowy, z zastrzeżeniem ust. 5.
5. Zamawiający pozostawi na zabezpieczenie roszczeń z tytułu gwarancji za wady, kwotę odpowiadającą 30% zabezpieczenia tj. ……PLN.

§ 7

1. Z tytułu realizacji przedmiotu umowy opisanego w § 1 w zakresie zamówienia Zamawiający zapłaci Wykonawcy wynagrodzenie w kwocie netto ..... PLN (słownie złotych: .....), do której zostanie doliczony ……% podatek VAT, co w sumie daje kwotę brutto ..... PLN, (słownie złotych: .....)
2. Zapłata wynagrodzenia, o którym mowa w ust. 1 płatna będzie przelewem na rachunek wskazany przez Wykonawcę na fakturze, przy czym należność zostanie zapłacona przez Zamawiającego nie później niż 21 dni od doręczenia prawidłowo wystawionej faktury do siedziby Zamawiającego.

3. Podstawą do wystawienia faktury przez Wykonawcę jest protokół bezusterkowego odbioru końcowego przedmiotu niniejszej umowy podpisany przez Zamawiającego. Protokół końcowy umowy zostanie podpisany po całkowitym wdrożeniu systemu Firewall wraz z przeprowadzonym szkoleniem potwierdzonym podpisanym protokołem szkolenia wraz z dostarczeniem dokumentu gwarancji.
4. Za dzień zapłaty strony przyjmują dzień wydania dyspozycji dokonania przelewu bankowi prowadzącemu rachunek Zamawiającego.
5. Strony przewidują możliwość zmiany wynagrodzenia Wykonawcy, o którym mowa w ust.1 w przypadku ustawowej zmiany stawki podatku VAT.
6. Wykonawca nie może dokonać cesji żadnych praw i roszczeń, przenieść obowiązków wynikających z umowy na rzecz osoby trzeciej bez uprzedniej pisemnej zgody Zamawiającego.

§ 8

1. Zamawiający ma prawo do naliczenia kar umownych Wykonawcy za:
   1) opóźnienie w dostawie lub instalacji któregokolwiek z elementów przedmiotu umowy w wysokości 1 % wynagrodzenia brutto za dany element za każdy dzień opóźnienia,
   2) opóźnienie w usunięciu stwierdzonych przy odbiorze nieprawidłowości, niezgodności, niekompletności lub wad w wysokości 0,8 % wynagrodzenia brutto określonego za dany element dostawy za każdy dzień opóźnienia, liczony od dnia wyznaczonego na usunięcie nieprawidłowości, niezgodności, niekompletności lub wad,
   3) opóźnienia w usunięciu wad stwierdzonych w okresie gwarancji w wysokości 0,4 % wynagrodzenia brutto określonego za dany element dostawy za każdy dzień opóźnienia, liczony od dnia wyznaczonego na usunięcie wady,
   4) odstąpienie od całości umowy przez którąkolwiek ze stron z przyczyn leżących po stronie Wykonawcy - w wysokości 10% wynagrodzenia brutto określonego w § 7 ust. 1,
   5) odstąpienie od części Umowy przez którąkolwiek ze stron z przyczyn leżących po stronie Wykonawcy - w wysokości 10% wynagrodzenia brutto za część Umowy, co do której następuje odstąpienie,
   6) za realizację serwisu gwarancyjnego przez podmiot inny niż Producent lub Autoryzowany Partner Serwisowy Producenta – 5.000,- zł za każdy stwierdzony przypadek.
2. Kary umowne płatne będą w ciągu 14 dni od dostarczenia Wykonawcy noty księgowej wystawionej przez Zamawiającego. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującego mu wynagrodzenia należnego z tytułu Umowy, jak również z zabezpieczenia umowy.
3. W przypadku nieterminowej zapłaty wynagrodzenia, Wykonawcy przysługuje prawo do żądania odsetek ustawowych za opóźnienie.
4. Strony zastrzegają sobie prawo dochodzenia odszkodowania przewyższającego wysokość kar umownych na zasadach ogólnych.

§ 9

1. Zmiana postanowień zawartej umowy może nastąpić w przypadkach określonych w art. 144 ustawy Pzp oraz przypadku wystąpienia jednej z następujących okoliczności:
   a) brak możliwości dostarczenia, w terminie umownym, urządzeń wskazanych w Ofercie, wynikający z przyczyn obiektywnych i niezależnych od stron – w takim przypadku zmiana polegać będzie na zastąpieniu oferowanego sprzętu sprzętem o nie gorszych lub lepszych parametrach,
   b) pojawienia się na rynku urządzeń Producenta sprzętu nowszej generacji, o lepszych parametrach i pozwalających na zaoszczędzenie kosztów eksploatacji – w takim przypadku zmiana polegać będzie na zastąpieniu oferowanego sprzętu sprzętem o lepszych parametrach i pozwalających na zaoszczędzenie kosztów eksploatacji,
   c) zaprzestania produkcji urządzeń wskazanych w Ofercie przez Producenta – w takim przypadku zmiana polegać będzie na zastąpieniu oferowanego sprzętu sprzętem o nie gorszych lub lepszych parametrach.
2. W każdym z powyższych przypadków Wykonawca jest zobowiązany do pisemnego udowodnienia powyższych okoliczności oraz wskazania nowych urządzeń o parametrach nie gorszych lub lepszych niż

wskazane w treści Szczegółowego Opisu Przedmiotu Zamówienia oraz ofercie Wykonawcy i wykazania, że parametry te są odpowiednio nie gorsze lub lepsze.

3. Zamawiający zastrzega sobie prawo do sprawdzenia zasadności zmiany, w tym porównania parametrów nowo wskazanych urządzeń . Zmiana musi zostać zatwierdzona przez Zamawiającego
4. Zmiany dokonane w oparciu o zapisy ustępu 1 nie mogą stanowić podstawy do zmiany oferowanych cen. Zmiany dokonane w oparciu o zapisy ustępu 1 nie mogą stanowić podstawy do zmiany terminów realizacji zamówienia, chyba że zajdą szczególne okoliczności niezależne od Wykonawcy, które Wykonawca jest zobowiązany udowodnić załączając stosowne wyjaśnienia i dokumenty a dokonanie zmiany będzie zgodne z podstawowymi zasadami ustawy Prawo zamówień publicznych, w szczególności z zasadą uczciwej konkurencji.

§ 10

1. Zamawiający ma prawo do odstąpienia od umowy w przypadku:
   1) opóźnienia przez Wykonawcę w realizacji umowy w terminie wskazanym w § 2 litera a) lub b) umowy przekraczającego 7 dni – w takim wypadku Zamawiający ma prawo do odstąpienia według swojego wyboru od całości umowy lub do odstąpienia od części Umowy, w szczególności tej części, co do której Wykonawca pozostaje w opóźnieniu;
   2) niezgodności dostarczanego sprzętu ze szczegółowym opisem przedmiotu zamówienia – w takim wypadku Zamawiający ma prawo do odstąpienia według swojego wyboru od całości lub części Umowy, w szczególności w stosunku do elementu dostawy , który jest niezgodny z opisem przedmiotu zamówienia,
   3) gdyby stwierdzone przy odbiorze nieprawidłowości, niezgodności, niekompletności lub wady nie zostały usunięte w terminie – w takim wypadku Zamawiający ma prawo do odstąpienia według swojego wyboru od całości umowy lub w stosunku do elementu dostawy.
2. Oświadczenie o odstąpieniu należy złożyć na piśmie w terminie 30 dni od powzięcia wiadomości o zaistnieniu podstaw do odstąpienia.
   W przypadkach określonych w ust. 1 Wykonawca zobowiązany jest do zapłaty Zamawiającemu kar umownych, zgodnie z § 8.

§ 11.[4]

1. Wykonawca wykona Przedmiot Umowy samodzielnie / z udziałem podwykonawców.
2. Zgodnie z przedłożoną przez siebie ofertą, Wykonawca może powierzyć wykonanie części Przedmiotu Umowy podwykonawcom w zakresie ……..
3. W przypadku powierzenia przez Wykonawcę realizacji części Przedmiotu Umowy Podwykonawcy, Wykonawca jest zobowiązany do dokonania we własnym zakresie zapłaty wynagrodzenia należnego Podwykonawcy z zachowaniem terminów płatności określonych w umowie z Podwykonawcą.
4. Wykonawca będzie odpowiadał w stosunku do Zamawiającego za działania, zaniechania, uchybienia i zaniedbania Podwykonawców jak za swoje własne
5. Wszystkie warunki i wymagania określone w umowie w stosunku do czynności i prac Wykonawcy odnoszą się również do czynności i prac wykonywanych przez Podwykonawców.
6. Zamawiającemu przysługuje prawo żądania od Wykonawcy zmiany podwykonawcy, jeżeli realizuje on powierzone czynności w sposób niezgodny z postanowieniami umowy.
7. Wykonawca zobowiązany jest do koordynacji prac realizowanych przez podwykonawców.
8. W przypadku zmiany lub rezygnacji z podwykonawcy, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 22a ust. 1 ustawy Pzp, w celu wykazania spełniania warunków udziału w postępowaniu, Wykonawca jest obowiązany wykazać Zamawiającemu, iż proponowany inny

[4] § 11 ust. 1 umowy zostanie uzupełniony na etapie zawierania Umowy. W przypadku, gdy Wykonawca będzie realizował Przedmiot Umowy z podwykonawcą lub podwykonawcami, Wykonawca wskaże w § 11 ust. 1 umowy – w zakresie ściśle określonym w złożonej ofercie - części zamówienia, której wykonanie powierzy podwykonawcy/podwykonawcom, natomiast jeżeli Wykonawca będzie realizował Przedmiot Umowy samodzielnie ust. 2-8 zostaną usunięte.

podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia publicznego.

9. Jeżeli powierzenie podwykonawcy, o którym mowa w ust. 8 wykonania części zamówienia następuje w trakcie jego realizacji, Wykonawca na żądanie Zamawiającego przedstawia oświadczenie lub dokumenty potwierdzające brak podstaw wykluczenia wobec tego podwykonawcy.
10. Jeżeli Zamawiający stwierdzi, że wobec danego podwykonawcy zachodzą przesłanki wykluczenia, Wykonawca obowiązany jest zastąpić tego podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia podwykonawcy

§ 12

1. W związku z realizacją przedmiotowej Umowy (wyłącznie tym celu) zamawiający i wykonawca przetwarzają dane osobowe. Zakres i cel przetwarzania danych osobowych przez Strony są różne. Nie zachodzi proces powierzenia danych a każdej ze Stron przysługuje status **odrębnego** Administratora Danych Osobowych.
2. Strony zobowiązują się stosować wymogi Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane dalej RODO, oraz ustawę o ochronie danych osobowych z dnia 10 maja 2018 r., a także wszelkie przepisy i regulacje w przedmiocie przetwarzania danych osobowych. Odniesienia do ustawodawstwa obejmują również jakiekolwiek jego późniejsze zmiany.
3. Strony oświadczają, że zapewnią wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi prawa i chroniło prywatność osób, których dane dotyczą.
4. Strony zobowiązują się:
    a. przetwarzać dane osobowe w sposób zapewniający adekwatny stopień bezpieczeństwa, odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych. Strony zabezpieczą dane osobowe przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, uszkodzeniem, zniszczeniem, utratą lub nieuzasadnioną modyfikacją;
    b. dołożyć należytej staranności przy przetwarzaniu danych osobowych;
    c. przetwarzać dane osobowe wyłącznie w celu realizacji niniejszej Umowy.
5. Dane osobowe, będą traktowane jako informacje chronione, a osoby działające w imieniu Stron zostały upoważnione do przetwarzania danych osobowych, przeszkolone i zobowiązane do zachowania danych osobowych w tajemnicy.
6. W czasie przetwarzania danych osobowych, Strony zobowiązują się do współdziałania w procesie przetwarzania danych osobowych, w tym niezwłocznego informowania się wzajemnie o wszystkich okolicznościach mających, lub mogących mieć wpływ na bezpieczeństwo przetwarzania danych osobowych.
7. W związku z faktem, że pomiędzy Stronami Umowy będącymi dwoma administratorami danych osobowych dochodzi do udostępniania danych osobowych Strony powinny zrealizować obowiązek informacyjny. Klauzulę obowiązek informacyjny do zastosowania przez zamawiającego określają zapisy w SIWZ pkt. 19. Oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO określa załącznik nr 1, pkt 16 Oferty.

§ 13

Informacje poufne

1. Wykonawca zobowiązuje się w okresie obowiązywania Umowy oraz po jej wygaśnięciu lub rozwiązaniu, do zachowania w ścisłej tajemnicy wszelkich informacji dotyczących Zamawiającego, obejmujących:

1) dane osobowe – chronione na podstawie Rozporządzenia (RODO);

2) informacje stanowiące tajemnicę przedsiębiorstwa - chronione na podstawie ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r., poz. 1010 z późn. zm.);

3) informacje, które mogą mieć wpływ na funkcjonowanie lub stan bezpieczeństwa Zamawiającego.

2. Informacje, o których mowa w ust. 1 oraz ust. 2, zwane są dalej „Informacjami Poufnymi".

3. Informacje Poufne mogą być udostępnione wyłącznie osobom dającym rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym dla należytego wykonania przedmiotu Umowy.

4. Każdy z Pracowników Wykonawcy**, przed przystąpieniem do świadczenia Usług objętych Przedmiotem zamówienia,** musi złożyć pisemne zobowiązanie o zachowaniu poufności i nieudostępnianiu nikomu informacji, które mógłby pozyskać w toku wykonywania prac związanych z realizacją przedmiotu zamówienia. Wzór zobowiązania stanowi Załącznik nr 3 do Umowy.

5. Ujawnianie Informacji Poufnych, niezależnie od sposobu ich ujawnienia, w wypadku gdy ma zostać dokonane w celu innym niż należyte wykonanie Umowy, jest dopuszczalne tylko za uprzednim zezwoleniem drugiej Strony, wyrażonym w formie pisemnej pod rygorem nieważności, przy czym w razie wątpliwości należy skonsultować zamiar ujawnienia Informacji Poufnej z przedstawicielem drugiej Strony.

6. W przypadku, gdy Strona została zobowiązana do ujawnienia Informacji Poufnych w całości lub w części uprawnionemu organowi, w granicach obowiązującego prawa, Strona ta zobowiązana jest jedynie uprzedzić drugą Stronę o nałożonym na nią obowiązku.

7. W razie powzięcia przez Stronę wiedzy o nieuprawnionym ujawnieniu Informacji Poufnych zobowiązana jest niezwłocznie powiadomić o tym fakcie drugą Stronę w celu umożliwienia jej podjęcia stosowanych środków zapobiegawczych.

8. Strona ma obowiązek zapewnić ochronę Informacji Poufnych według najwyższych przewidzianych prawem standardów, w tym zapewnić ochronę systemów i sieci teleinformatycznych, w których są przetwarzane, przechowywane lub przekazywane Informacje Poufne drugiej Strony, a także kontrolować ochronę Informacji Poufnych oraz przestrzegać przepisów o ochronie poufności informacji.

§ 14

1. Strony zobowiązują się rozstrzygać spory w drodze polubownej. W razie braku polubownego załatwiania sporów, spory powstałe przy realizacji niniejszej umowy będą rozstrzygane przez sąd właściwy miejscowo dla siedziby Zamawiającego.
2. W sprawach nieuregulowanych w niniejszej umowie stosuje się przepisy ustawy Prawo zamówień publicznych i ustawy Kodeks cywilny.
3. Integralną część niniejszej umowy stanowią załączniki:
   1) Specyfikacja Istotnych Warunków Zamówienia wraz z załącznikami,
   2) Oferta Wykonawcy z dnia …….. wraz z załącznikami.
   3) Wzór zobowiązania pracownika Wykonawcy o zachowaniu poufności.
4. Umowę niniejszą sporządzono w 2 jednobrzmiących egzemplarzach, po 1 egzemplarzu dla każdej ze Stron.

Zamawiający **Wykonawca**

Załącznik nr 3 do umowy

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Zgodnie z realizacją umowy nr ……

z dnia ……

Ja, niżej podpisany

……

działając jako

……

w imieniu firmy

……

na rzecz Instytutu Techniki Budowlanej
zobowiązuje się:

1. Zachować w ścisłej tajemnicy wszystkie informacje Zamawiającego związane z wykonaniem umowy a w szczególności: dane osobowe, informacje stanowiące tajemnicę przedsiębiorstwa Zamawiającego, informacje, które mogą mieć wpływ na funkcjonowanie lub stan bezpieczeństwa Zamawiającego, a w szczególności informacje techniczne i konfiguracyjne infrastruktury informatycznej, stosowanych zabezpieczeń, procedur ciągłości działania, zasad monitoringu infrastruktury teleinformatycznej i ich nadzorowania, wykorzystywanego oprogramowania i rozwiązań systemowych w zakresie bezpieczeństwa informacji.
2. Wykorzystać uzyskane informacje jedynie w celu realizacji umowy.
3. Nie kopiować ani w jakikolwiek sposób nie rozpowszechniać uzyskanych informacji w całości lub częściach osobom trzecim bez uzyskania uprzednio pisemnego upoważnienia Zamawiającego.
4. Zachowania w tajemnicy uzyskanych haseł dostępu do systemów informatycznych, serwerów, infrastruktury informatycznej ITB, zapewnienia ich bezpieczeństwa przed udostępnieniem osobom trzecim i nieupoważnionym. Przekazane hasła upoważnionym osobom wymienionym w zleceniu wykorzystać wyłącznie w celu realizacji przedmiotu zlecenia.

Powyższe oświadczenie jest obowiązujące od dnia rozpoczęcia prac.

.....
podpis osoby składającej oświadczenie

Potwierdzam, że ww. osoba reprezentuje firmę…….. i wykonuje prace zgodnie z umową.

……
podpis osoby upoważnionej