

**SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA**  
**UDZIELANEGO PRZEZ NARODOWY FUNDUSZ ZDROWIA CENTRALA**  
**ul. Grójecka 186, 02-390 Warszawa; fax 22 572 63 05**

Postępowanie jest prowadzone w trybie przetargu nieograniczonego, zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2007 r. Nr 223, poz. 1655), zwanej dalej „ustawą”.

**INFORMACJE OGÓLNE**

Zamawiającym jest: **Narodowy Fundusz Zdrowia (w skrócie „NFZ”), w Warszawie przy ul. Grójeckiej 186.**

Przedmiotem zamówienia jest: **dostawa zespołu urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej NFZ.**

Specyfikacja istotnych warunków niniejszego zamówienia, zwana dalej „Specyfikacją”, określa:

- 1) opis przedmiotu zamówienia (rozdział 1),
- 2) opis procedury postępowania o udzielenie zamówienia (rozdział 2),
- 3) sposób przygotowania oferty, warunki wymagane w stosunku do oferty, warunki udziału w postępowaniu, wymagane dokumenty lub oświadczenia (rozdział 3),
- 4) zasady rozpatrywania, oceny ofert oraz wyboru oferty najkorzystniejszej (rozdział 4).

Do specyfikacji załączono:

- 1) opis przedmiotu zamówienia (załącznik nr 1),
- 2) wzór umowy o wykonanie zamówienia (załącznik nr 2),
- 3) formularz oferty (załącznik nr 3),
- 4) formularz oświadczenia o spełnianiu warunków udziału w postępowaniu (załącznik nr 4),
- 5) formularz oświadczenia w sprawie oferowanego przedmiotu zamówienia (załącznik nr 5),
- 6) formularz wykazu wykonanych dostaw (załącznik nr 6),
- 7) formularz oświadczenia w sprawie cen jednostkowych (załącznik nr 7).

**1. OPIS PRZEDMIOTU ZAMÓWIENIA**

**1.1. Określenie przedmiotu zamówienia**

Przedmiotem zamówienia jest **dostawa zespołu urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej NFZ**. Przez dostawę Zamawiający rozumie także instalację, skonfigurowanie, wdrożenie i uruchomienie zgodnie z załącznikiem nr 1 do Specyfikacji.

Miejsce realizacji zamówienia: miejsce wskazane przez Zamawiającego na terenie województwa mazowieckiego.

Szczegółową charakterystykę przedmiotu zamówienia określa opis przedmiotu zamówienia zawarty w załączniku nr 1 do Specyfikacji.

Szczegółowy zakres praw i obowiązków związanych z realizacją zamówienia określa wzór umowy stanowiący załącznik nr 2 do Specyfikacji.

**1.2. Termin realizacji zamówienia**

Zamawiający wymaga, by zamówienie zostało zrealizowane w **terminie nie przekraczającym 5 miesięcy od daty podpisania umowy**.

**1.3. Termin płatności**

Należne Wykonawcy wynagrodzenie z tytułu realizacji zamówienia będzie regulowane w terminie 14 dni od daty otrzymania prawidłowo wystawionej faktury, wraz z podpisanym przez przedstawicieli Stron protokołem odbioru przedmiotu umowy.

Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone wyłącznie w złotych polskich (PLN).

#### **1.4. Gwarancja i serwis**

Zamawiający wymaga, by Wykonawca udzielił na dostarczone, zamontowane i uruchomione **urządzenia 12 miesięcznej gwarancji**, przy czym serwis będzie realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu.

Zamawiający wymaga, by czas usunięcia awarii w okresie gwarancji nie przekraczał 24 godzin od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym).

Zamawiający wymaga, by serwis obejmował dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;

#### **1.5. Podmioty uprawnione do składania ofert**

Wykonawcą może być osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która ubiega się o udzielenie zamówienia publicznego i złożyła ofertę.

**Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takim przypadku Wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.**

Jeżeli oferta Wykonawców, którzy wspólnie ubiegają się o udzielenie zamówienia została wybrana, Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego, umowy regulującej współpracę tych Wykonawców.

Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ponoszą solidarną odpowiedzialność za wykonanie umowy i wniesienie zabezpieczenia należytego wykonania umowy.

#### **1.6. Udział podwykonawców w wykonaniu zamówienia**

Zamawiający żąda wskazania przez Wykonawcę w ofercie części zamówienia, której wykonanie powierzy podwykonawcom. Zamawiający nie określa w specyfikacji, która część zamówienia nie może być powierzona podwykonawcom.

## **2. PROCEDURA POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA**

### **2.1. Informacje ogólne**

Postępowanie jest prowadzone w trybie przetargu nieograniczonego zgodnie z przepisami ustawy. Postępowanie o udzielenie zamówienia prowadzi się w języku polskim.

### **2.2. Sposób uzyskania specyfikacji, porozumiewania się z Wykonawcami oraz przekazywania oświadczeń lub dokumentów oraz osoby uprawnione do porozumiewania się z Wykonawcami.**

#### **2.2.1. Sposób uzyskania specyfikacji**

Specyfikację można pobrać ze strony internetowej [www.nfz.gov.pl](http://www.nfz.gov.pl)

Specyfikację można również odebrać osobiście w siedzibie Zamawiającego przy ul. Grójeckiej 186 w Warszawie, piętro II, pok. 2.48A lub złożyć wniosek do Zamawiającego na adres: Narodowy Fundusz Zdrowia, ul. Grójecka 186, 02-390 Warszawa, fax 0 22 572-63-05.

Zamawiający przekazuje nieodpłatnie specyfikację do rąk przedstawiciela wnioskodawcy lub niezwłocznie przysyła na wskazany adres, nie później niż w ciągu 5 dni od dnia otrzymania wniosku o jej przekazanie.

#### **2.2.2. Sposób porozumiewania się z Wykonawcami oraz przekazywania oświadczeń lub dokumentów**

Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują pisemnie.

Oświadczenia, wnioski, zawiadomienia oraz informacje przekazane za pomocą teleksu, telefaxu lub drogą elektroniczną uważa się za złożone w terminie, jeżeli ich treść dotarła do adresata przed upływem terminu i została niezwłocznie potwierdzona pisemnie.

#### **2.2.3. Osoby uprawnione do porozumiewania się z Wykonawcami**

Uprawnionymi do porozumiewania się z Wykonawcami pracownikami Zamawiającego są:

- 1) w sprawach dotyczących strony formalnej niniejszego postępowania:
  - **Zbigniew Johne** w budynku przy ul. Grójeckiej 186, w godz. 09:00-15:00, tel. 0-22 572-62-65,
- 2) w sprawach dotyczących przedmiotu zamówienia:
  - **Krzysztof Szymański** w budynku przy ul. Grójeckiej 186, w godz. 09:00-15:00, tel. 0-22 572-61-62.

### **2.3. Udzielanie wyjaśnień oraz zmiany w treści specyfikacji**

Zgodnie z art. 38 ustawy, Zamawiający jest obowiązany niezwłocznie udzielić wyjaśnień treści specyfikacji istotnych warunków zamówienia, chyba że prośba o wyjaśnienie treści specyfikacji wpłynęła do Zamawiającego na mniej niż 6 dni przed terminem składania ofert. Treść zapytań wraz z wyjaśnieniami (bez ujawniania źródła zapytania) Zamawiający przekazuje Wykonawcom, którym przekazał specyfikację, a jeżeli specyfikacja jest udostępniana na stronie internetowej zamieszcza na tej stronie.

Zamawiający nie przewiduje zwołania zebrania Wykonawców w celu wyjaśnienia wątpliwości dotyczących treści specyfikacji.

Zamawiający zastrzega, że zgodnie z art. 38 ust. 4 ustawy, w szczególnie uzasadnionych przypadkach może w każdym czasie przed upływem terminu składania ofert zmodyfikować treść specyfikacji. Dokonaną modyfikację Zamawiający przekazuje niezwłocznie wszystkim Wykonawcom, którym przekazano specyfikację, a jeżeli specyfikacja jest udostępniana na stronie internetowej, zamieszcza także na tej stronie.

### **2.4. Wadium**

Zgodnie z art. 45 ustawy Wykonawca jest obowiązany wnieść na rzecz Zamawiającego wadium.

Wadium wynosi **100.000,00 zł (słownie: sto tysięcy złotych)**.

Wadium musi obejmować cały okres związania ofertą.

Termin wniesienia wadium upływa **w dniu 20.05.2008 r. o godz. 10:00**.

Zamawiający przyjmuje wadium wnoszone w jednej lub kilku następujących formach: w pieniądzu, poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym, gwarancjach bankowych, gwarancjach ubezpieczeniowych, 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 (t.j. Dz.U. z 2007 r. Nr 42, poz. 275). Wadium wnoszone w pieniądzu wpłaca się przelewem na rachunek bankowy wskazany przez Zamawiającego.

Dowodem wniesienia wadium będzie:

- 1) pokwitowanie przelewu kwoty pieniężnej na dobro rachunku Zamawiającego na rachunek bankowy **77 1130 1017 0020 0734 8625 7421**, potwierdzone faktycznym wpływem środków na rachunek przed upływem terminu wnoszenia wadium,
- 2) dokument potwierdzający zobowiązanie do pokrycia wadium (wadium w formie niepieniężnej).

Wadium wnoszone w innej formie niż w pieniądzu, powinno zawierać bezwzględne i nieodwołalne zobowiązanie podmiotu udzielającego do wypłaty kwoty wadium w przypadkach wymienionych w art. 46 ust. 5 ustawy.

### **2.5. Zwrot oraz przepadek wadium przetargowego**

Zamawiający niezwłocznie zwróci oferentom wadium, jeżeli zajdzie jedna z poniższych przesłanek:

- 1) upływie terminu związania ofertą,
- 2) zawarto umowę w sprawie zamówienia publicznego i wniesiono zabezpieczenie należytego wykonania umowy,
- 3) Zamawiający unieważnił postępowanie o udzielenie zamówienia, a protesty zostały ostatecznie rozstrzygnięte lub upłynął termin do ich wnoszenia.

Zamawiający zwróci niezwłocznie wadium na wniosek Wykonawcy:

- 1) który wycofał ofertę przed upływem terminu składania ofert,
- 2) który został wykluczony z postępowania,
- 3) którego oferta została odrzucona.

Zwrot wadium wniesionego w pieniądzu nastąpi wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszonymi o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wskazany przez Wykonawcę.

Wadium wniesione w formie innej niż pieniężnej, zwracane jest bez odsetek.

Zgodnie z art. 46 ust. 5 ustawy, Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca, którego oferta została wybrana:

- 1) odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie,
- 2) nie wniósł zabezpieczenia należytego wykonania umowy,
- 3) zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.

## **2.6. Sposób składania ofert**

Oferty należy składać w zamkniętych kopertach w Narodowym Funduszu Zdrowia Centrali w Warszawie, przy ul. Grójeckiej 186, II piętro, pok.2.48A, **do dnia 20.05.2008 r. do godz. 10:00.**

**Sporządzoną ofertę należy opakować w kopertę oznaczoną dokładną nazwą i adresem Wykonawcy oraz napisem „DOSTAWA ZESPOŁU URZĄDZEŃ DO CENTRUM PRZETWARZANIA DANYCH. OTWORZYĆ W DNIU 20.05.2008 R.”.**

Złożona oferta zostanie zarejestrowana w ten sposób, że osoba przyjmująca oznaczy kopertę kolejnym numerem oraz odnotuje datę i dokładny czas wpływu. Na żądanie Wykonawcy zostanie wydany dowód wpływu oferty, zawierający odcisk pieczęci organizatora przetargu, nazwisko i imię osoby przyjmującej, oznaczenie przetargu oraz datę i dokładny czas wpływu.

**Jeżeli oferta jest wysyłana za pomocą przesyłki kurierskiej/listowej, Wykonawca powinien zaznaczyć, że przesyłka zawiera ofertę. Zamawiający nie ponosi odpowiedzialności za następstwa spowodowane brakiem zabezpieczenia oferty lub brakiem ww. informacji.**

Zamawiający zastrzega, że wyłączne ryzyko nieterminowego dostarczenia oferty oraz pomyłkowego otwarcia wskutek nienależytego oznaczenia koperty ponosi Wykonawca.

Oferty złożone po terminie Zamawiający zwraca bez otwierania po upływie terminu przewidzianego na wniesienie protestu.

Zgłoszenia i pisma przesyłane faxem nie będą traktowane jako oferty.

Przed upływem terminu składania ofert, Wykonawca może wycofać ofertę lub wprowadzić zmiany do złożonej oferty. Informacja o wycofaniu oferty lub zmiany do oferty Wykonawca winien doręczyć Zamawiającemu na piśmie przed upływem terminu składania ofert. Oświadczenie o wycofaniu oferty lub wprowadzeniu zmian winno być opakowane tak jak oferta, a opakowanie winno być dodatkowo oznaczone odpowiednio wyrazem „WYCOFANIE” lub „ZMIANA”. Opakowania te będą otwierane w terminie otwarcia ofert, określonym w niniejszej Specyfikacji.

Jeżeli oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji powinny one być umieszczone w osobnej wewnętrznej kopercie zatytułowanej „DOSTAWA ZESPOŁU URZĄDZEŃ DO CENTRUM PRZETWARZANIA DANYCH. Tajemnica przedsiębiorstwa”.

Zamawiający zastrzega, że zgodnie z art. 8 ust. 3 ustawy, nie może ujawnić: informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert, zastrzegł, że nie mogą one być udostępniane. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4 ustawy.

Przez tajemnicę przedsiębiorstwa rozumie się nie ujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. Wykonawca nie może zastrzec swojej nazwy (firmy) oraz adresu, a także informacji dotyczących ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

## **2.7. Termin związania ofertą**

Wykonawca jest związany treścią oferty przez okres 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

W uzasadnionych przypadkach co najmniej na 7 dni przed upływem terminu związania ofertą Zamawiający może tylko raz zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

## **2.8. Otwarcie ofert**

Z zawartością ofert nie można zapoznać się przed upływem terminu otwarcia ofert.

Otwarcie ofert odbędzie się **w dniu 20.05.2008 r. o godz. 10:30** w Narodowym Funduszu Zdrowia w Warszawie przy ul. Grójeckiej 186, pok. 2.48A.

Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

Otwarcie ofert jest jawne.

Polegać będzie ono na otwarciu złożonych ofert, podaniu nazwy (firmy) i adresu Wykonawców, informacji dotyczących ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

Informacje te zostaną odnotowane w protokole postępowania. Czynności tych dokonają członkowie komisji przetargowej.

W przypadku, gdy Wykonawca nie był obecny przy otwarciu ofert, na jego wniosek, Zamawiający prześle mu informacje podawane podczas otwarcia ofert.

## **2.9. Informacja o trybie rozpatrywania ofert**

Zamawiający wykluczy z postępowania Wykonawców, o których mowa w art. 24 ustawy.

Zgodnie z art. 87 ust. 1 ustawy, w toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert. Nie jest dopuszczalne prowadzenie negocjacji między Zamawiającym a Wykonawcą dotyczących złożonej oferty oraz z zastrzeżeniem art. 87 ust. 2 ustawy dokonywanie jakiegokolwiek zmiany w jej treści.

Zgodnie z art. 87 ust. 2 ustawy, oczywiste omyłki pisarskie oraz omyłki rachunkowe w obliczeniu ceny zostaną poprawione przez Zamawiającego, o czym niezwłocznie zawiadomieni zostaną wszyscy Wykonawcy, którzy złożyli oferty.

Zamawiający w celu ustalenia, czy oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia zwraca się w formie pisemnej do Wykonawcy o udzielenie w określonym terminie wyjaśnień dotyczących elementów oferty mających wpływ na wysokość ceny.

Zamawiający, oceniając wyjaśnienia, bierze pod uwagę obiektywne czynniki, w szczególności oszczędność metody wykonania zamówienia, wybrane rozwiązania techniczne, wyjątkowo sprzyjające warunki wykonywania zamówienia dostępne dla Wykonawcy, oryginalność projektu Wykonawcy oraz wpływ pomocy publicznej udzielonej na podstawie odrębnych przepisów.

Zamawiający odrzuca ofertę Wykonawcy, który nie złożył wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz z dostarczonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

Zamawiający wzywa Wykonawców, którzy w określonym terminie nie złożyli oświadczeń lub dokumentów, o których mowa w art. 25 ust. 1 ustawy, lub którzy złożyli dokumenty, o których mowa w art. 25 ust. 1 ustawy, zawierające błędy, do ich uzupełnienia w wyznaczonym terminie, chyba że mimo ich uzupełnienia oferta Wykonawcy podlega odrzuceniu lub konieczne byłoby unieważnienie postępowania; oświadczenia lub dokumenty powinny potwierdzać spełnianie przez Wykonawcę warunków udziału w postępowaniu, nie później niż w dniu wyznaczonym przez Zamawiającego jako termin uzupełnienia oświadczeń lub dokumentów. Zamawiający wzywa także, w wyznaczonym przez siebie terminie, do złożenia wyjaśnień dotyczących oświadczeń lub dokumentów, o których mowa w art. 25 ust. 1 ustawy.

Zamawiający odrzuca oferty, w przypadku zaistnienia przesłanek, o których mowa w art. 89 ust. 1 ustawy.

Oferty ważne, podlegają ocenie według kryterium określonego w Specyfikacji.

Ponadto Zamawiający badać będzie, czy nie zachodzą przesłanki do unieważnienia postępowania z przyczyn określonych w art. 93 ust. 1 ustawy.

## **2.10. Środki ochrony prawnej przysługujące Wykonawcy w toku postępowania o udzielenie zamówienia**

Wykonawcom a także innym osobom, których interes prawny, w uzyskaniu zamówienia, doznał lub może doznać uszczerbku, w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki ochrony prawnej określone w Dziale VI ustawy (art. 179 – art. 198).

## **2.11. Zawiadomienie o wyborze oferty i powiadomienie o nim uczestników postępowania**

1. Niezwłocznie po wyborze najkorzystniejszej oferty zamawiający zawiadamia Wykonawców, którzy złożyli oferty, o:
  - 1) wyborze najkorzystniejszej oferty, podając nazwę (firmę), siedzibę i adres Wykonawcy, którego ofertę wybrano oraz uzasadnienie jej wyboru, a także nazwy (firmy), siedziby i adresy Wykonawców, którzy złożyli oferty wraz ze streszczeniem oceny i porównania złożonych ofert zawierającym punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,
  - 2) Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne,
  - 3) Wykonawcach, którzy zostali wykluczeni z postępowania o udzielenie zamówienia, podając uzasadnienie faktyczne i prawne.
2. Niezwłocznie po wyborze najkorzystniejszej oferty zamawiający zamieszcza informacje o wyborze najkorzystniejszej oferty, podając nazwę (firmę), siedzibę i adres Wykonawcy, którego ofertę wybrano oraz uzasadnienie jej wyboru, a także nazwy (firmy), siedziby i adresy Wykonawców, którzy złożyli oferty wraz ze streszczeniem oceny i porównania złożonych ofert zawierającym punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację na stronie internetowej oraz w miejscu ogólnie dostępnym w swojej siedzibie.

## **2.12. Zabezpieczenie należytego wykonania umowy**

Wykonawca jest zobowiązany do wniesienia zabezpieczenia należytego wykonania umowy na sumę stanowiącą 5 % ceny całkowitej /brutto/ podanej w ofercie.

Dopuszczalne są następujące formy zabezpieczenia:

- 1) w pieniądzu - wpłacane przelewem na konto bankowe Zamawiającego:  
**77 1130 1017 0020 0734 8625 7421,**
- 2) w poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym, gwarancjach bankowych, gwarancjach ubezpieczeniowych, 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.

**Zabezpieczenie może być wnoszone według wyboru Wykonawcy w jednej lub kilku formach.**

Kwoty pieniężne wpłacone tytułem zabezpieczenia Zamawiający przechowuje na oprocentowanym rachunku bankowym.

Zamawiający zwraca zabezpieczenie wniesione w pieniądzu z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszonymi o koszty prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.

Wykonawca jest obowiązany wnieść całość zabezpieczenia **najpóźniej w dniu podpisania umowy**. Zwrot zabezpieczenia nastąpi na warunkach określonych w umowie. Wadium wniesione w pieniądzu przez Wykonawcę, którego oferta została wybrana, za zgodą tego Wykonawcy zaliczane jest przez Zamawiającego na poczet zabezpieczenia należytego wykonania umowy. W trakcie realizacji umowy Wykonawca może dokonać zmiany formy zabezpieczenia, na jedną lub kilka form, o których mowa w pkt 1 i 2. Zmiana formy zabezpieczenia jest dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości

## **2.13. Tryb zawarcia umowy**

Treść umowy o realizację zamówienia zostanie ustalona zgodnie z treścią wybranej oferty i załączonego do specyfikacji wzoru umowy.

Zamawiający zawrze umowę w terminie nie krótszym niż 7 dni od dnia przekazania zawiadomienia o wyborze oferty, nie później jednak niż przed upływem terminu związania ofertą, z zastrzeżeniem art. 94 ust. 1a ustawy. (art. 94 ust. 1a. „Umowa w sprawie zamówienia publicznego może zostać zawarta po upływie terminu związania ofertą, jeżeli zamawiający przekazał Wykonawcom informację o wyborze oferty przed upływem terminu związania ofertą, a Wykonawca wyraził zgodę na zawarcie umowy na warunkach określonych w złożonej ofercie”).

## **3. SPOSÓB PRZYGOTOWANIA OFERTY, WARUNKI UDZIAŁU W POSTĘPOWANIU, WARUNKI WYMAGANE W STOSUNKU DO OFERTY, WYMAGANE DOKUMENTY LUB OŚWIADCZENIA**

### **3.1. Ogólne warunki wymagane w stosunku do oferty**

1. Każdy Wykonawca może złożyć jedną ofertę. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
2. Ofertę składa się pod rygorem nieważności w formie pisemnej. Zamawiający nie wyraża zgody na złożenie oferty w postaci elektronicznej.
3. Treść oferty musi odpowiadać treści specyfikacji.
4. Ofertę sporządza się w języku polskim.
5. Zaleca się aby oferta wraz z załączonymi do oferty oświadczeniami i dokumentami była zszyta lub spięta (np. zbindowana) i posiadała ponumerowane strony.
6. Oferta winna być sporządzona zgodnie z treścią formularza oferty załączonego do specyfikacji. Oferent może złożyć ofertę na własnych formularzach, których treść musi być zgodna z formularzami załączonymi do specyfikacji.
7. Nie jest dopuszczalne składanie ofert wariantowych. Zamawiający nie dopuszcza składania ofert częściowych.
8. Ofertę (wypełniony formularz oferty wraz z wymaganymi przez SIWZ oświadczeniami) muszą podpisać osoby uprawnione, które zgodnie z obowiązującymi przepisami prawa oraz treścią załączonego odpisu z właściwego rejestru lub ewidencji mogą skutecznie składać oświadczenia woli w imieniu Wykonawcy. Ofertę podpisać może pełnomocnik Wykonawcy, jeżeli do oferty zostanie załączone pełnomocnictwo do podejmowania określonych czynności, wynikających z ustawy, w postępowaniach o udzielenie zamówień publicznych, w których bierze udział Wykonawca, albo szczególne dotyczące niniejszego postępowania.

**DOKUMENT PEŁNOMOCNICTWA MUSI BYĆ ZŁOŻONY W ORYGINALE LUB POŚWIADCZONEJ NOTARIALNIE ZA ZGODNOŚĆ Z ORYGINAŁEM KOPII.**

**Podpisy złożone przez Wykonawcę powinny być opatrzone czytelnym imieniem i nazwiskiem lub pieczęcią imienną.**

9. **Wykonawcy występujący wspólnie** muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu albo pełnomocnika do reprezentowania ich w postępowaniu i do zawarcia umowy w sprawie przedmiotowego zamówienia publicznego. Fakt ustanowienia pełnomocnika musi wynikać z załączonych do oferty dokumentów (np. pełnomocnictwa).

**Wypełniając formularz oferty, jak również inne dokumenty powołując się na Wykonawcę**, w miejscu np. nazwa i adres Wykonawcy, należy wpisać dane dotyczące wszystkich Wykonawców składających ofertę wspólną.

10. Dla zapewnienia czytelności oferta powinna zostać wypełniona drukiem maszynowym, lub czytelnym pismem ręcznym (długopisem lub nieścieralnym atramentem), oferta może mieć także postać wydruku komputerowego.
11. Poprawki muszą być parafowane przez osobę, która podpisała ofertę.
12. **Załączone do oferty dokumenty** muszą być przedłożone w formie oryginałów, bądź kserokopii poświadczonych „za zgodność z oryginałem” przez Wykonawcę na każdej zapisanej stronie kserowanego dokumentu. Poświadczenie ”za zgodność z oryginałem” musi zostać sporządzone przez osoby uprawnione, które zgodnie z obowiązującymi przepisami prawa oraz treścią załączonego odpisu z właściwego rejestru, ewidencji lub pełnomocnictwa mogą skutecznie składać oświadczenia woli w imieniu Wykonawcy. **Podpisy złożone przez Wykonawcę powinny być opatrzone czytelnym imieniem i nazwiskiem lub pieczęcią imienną.** Uznaje się, że pełnomocnictwo do podpisania oferty obejmuje pełnomocnictwo do poświadczenia za zgodność z oryginałem kopii dokumentów załączanych do oferty. Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii wyłącznie wtedy, gdy złożona przez Wykonawcę kopia dokumentu jest nieczytelna lub budzi wątpliwości co do jej prawdziwości.
13. Dokumenty sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski, poświadczonym przez Wykonawcę.

**3.2. Opis warunków udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków**

O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:

- spełniają warunki udziału w postępowaniu określone w art. 22 ust. 1 ustawy, tj.:
  - 1) posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień;
  - 2) posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia;
  - 3) znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia;
  - 4) nie podlegają wykluczeniu z postępowania o udzielenie zamówienia.
- nie podlegają wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 24 ustawy,
- złożą oświadczenie o spełnianiu warunków udziału w postępowaniu zgodnie z załącznikiem do Specyfikacji,
- wykonali co najmniej 2 dostawy, w okresie ostatnich trzech lat przed dniem wszczęcia postępowania o udzielenie zamówienia, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, odpowiadające swoim rodzajem dostawie stanowiącej przedmiot zamówienia, tj. dostawy sprzętu sieciowego, o wartości przekraczającej 2.000.000,00 zł brutto każda, z podaniem ich wartości, przedmiotu, daty wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane należycie,
- wykażą się posiadaniem środków finansowych lub zdolności kredytowej w wysokości nie mniejszej niż 2.000.000,00 zł.

W celu potwierdzenia, że Wykonawca posiada uprawnienia do wykonywania określonej działalności lub czynności oraz nie podlega wykluczeniu na podstawie art. 24 ustawy, musi przedstawić dokumenty wymienione w pkt 3.5.1 - 3.5.5. Specyfikacji.

W celu potwierdzenia, że Wykonawca posiada niezbędną wiedzę i doświadczenie oraz dysponuje potencjałem technicznym i osobami zdolnymi do wykonania zamówienia musi przedstawić dokumenty wymienione w pkt 3.5.6. Specyfikacji.

W celu potwierdzenia, że Wykonawca znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia musi przedstawić dokumenty wymienione w pkt 3.5.7. Specyfikacji.

Ocena spełniania warunków udziału w postępowaniu nastąpi na podstawie złożonych wraz z ofertą dokumentów i oświadczeń, o których mowa w pkt 3.5. Specyfikacji. Ocena spełniania warunków zostanie dokonana według formuły spełnia / nie spełnia warunków udziału w postępowaniu. Nie spełnienie warunków udziału w postępowaniu skutkować będzie wykluczeniem z postępowania.

### **3.3. Warunki wymagane w stosunku do treści formularza oferty**

Oferent winien sporządzić ofertę zgodnie z treścią formularza załączonego do specyfikacji (załącznik nr 3).

#### **3.3.1. Oświadczenie o oferowanej cenie za realizację przedmiotu zamówienia**

Zamawiający wymaga, by oferowane cena za realizację zamówienia zostały przedstawione w PLN w rozbiciu na: cenę netto, podatek od towarów i usług – VAT oraz cenę brutto.

Jako podstawę do oceny ofert Zamawiający przyjmuje cenę brutto za realizację zamówienia, która w toku postępowania nie może ulec zmianie.

Wszystkie ceny powinny zawierać w sobie ewentualne upusty proponowane przez Wykonawcę (niedopuszczalne są żadne negocjacje cenowe). Ceny należy podać w złotych i groszach (PLN).

#### **3.3.2. Oświadczenie o akceptacji terminu realizacji zamówienia**

Wykonawca jest obowiązany zaakceptować termin realizacji zamówienia określony w pkt 1.2. Specyfikacji.

#### **3.3.3. Oświadczenie o akceptacji wymagań określających przedmiot zamówienia**

Wykonawca jest obowiązany zaakceptować przedstawione przez Zamawiającego wymagania i zakres świadczonych usług określających przedmiot zamówienia. Wymagania dotyczące przedmiotu zamówienia określono w opisie przedmiotu zamówienia.

#### **3.3.4. Oświadczenie o akceptacji warunków płatności**

Zamawiający wymaga, by Wykonawca zaakceptował przedstawione przez Zamawiającego warunki płatności z tytułu realizacji umowy.

#### **3.3.5. Oświadczenie o akceptacji warunków gwarancji i serwisu**

Zamawiający wymaga, by Wykonawca zaakceptował przedstawione przez Zamawiającego warunki gwarancji i serwisu.

Zamawiający wymaga, by Wykonawca udzielił na dostarczone, zamontowane i uruchomione **urządzenia 12 miesięcznej gwarancji**, przy czym serwis będzie realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu;

Zamawiający wymaga, by czas usunięcia awarii w okresie gwarancji nie przekraczał 24 godzin od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym).

Zamawiający wymaga, by serwis obejmował dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania.

#### **3.3.6. Oświadczenie o akceptacji przedstawionych przez Zamawiającego warunków umownych realizacji zamówienia**

Wykonawca jest obowiązany zaakceptować przedstawione przez Zamawiającego warunki umowne realizacji zamówienia i zobowiązać się w przypadku wyboru jego oferty do zawarcia umowy na wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego. Treść warunków umownych określa wzór umowy załączony do specyfikacji.

#### **3.3.7. Oświadczenie o wniesieniu przez Wykonawcę wadium przetargowego**

Wykonawca zobowiązany jest do złożenia oświadczenia o wniesieniu na rzecz Zamawiającego wadium przetargowego. Zwrot wadium nastąpi automatycznie jeżeli Wykonawca określi numer zwrotny konta lub inny sposób zwrotu wadium w razie zaistnienia ku temu przesłanek.



### **3.3.8. Oświadczenie Wykonawcy, czy wykona sam zamówienie, czy powierzy wykonanie części zamówienia podwykonawcom**

Wykonawca zobowiązany jest do złożenia oświadczenia, czy wykona sam zamówienie, czy powierzy wykonanie części zamówienia podwykonawcom.

### **3.3.9. Oświadczenie o dokumentach załączonych do oferty**

Dla zachowania porządku dokumentów załączanych do oferty Wykonawca obowiązany jest o ich wskazanie w formularzu oferty. Będą to dokumenty przewidziane w pkt 3.4. i 3.5. specyfikacji.

## **3.4. Warunki wymagane w stosunku do treści oświadczeń oraz dokumentów załączanych do formularza oferty**

### **3.4.1 Dowód wpłaty wymaganego wadium przetargowego**

Wykonawca zobowiązany jest załączyć do oferty dowód wniesienia wymaganego wadium przetargowego (dowód wpłaty wadium na dobro wskazanego w specyfikacji rachunku Zamawiającego) lub załączyć do oferty dokument (**oryginał**) potwierdzający zobowiązanie do pokrycia wadium (wadium w formie niepieniężnej).

### **3.4.2. Oświadczenia w sprawie oferowanego przedmiotu zamówienia**

Wykonawca jest zobowiązany złożyć oświadczenie w sprawie oferowanego przedmiotu zamówienia zgodnie z załącznikiem nr 5 do Specyfikacji.

### **3.4.3. Oświadczenie o poszczególnych cenach jednostkowych oferowanego przedmiotu zamówienia**

Wykonawca jest obowiązany złożyć oświadczenie o poszczególnych cenach jednostkowych oferowanego przedmiotu zamówienia zgodnie z załączonym formularzem stanowiącym załącznik nr 7 do Specyfikacji.

### **3.4.4. Kalkulacja pobieranej mocy przez Urządzenie sieciowe Typ I**

Wykonawca jest zobowiązany złożyć kalkulację pobieranej mocy dla oferowanej konfiguracji. Zamawiający dopuszcza wydruk ze strony internetowej producenta sprzętu potwierdzony przez przedstawiciela producenta w kraju.

### **3.4.5. Oświadczenia o kompatybilności urządzeń**

W przypadku oferowania urządzeń różnych producentów, należy dostarczyć oświadczenia ich producentów o pełnej wzajemnej kompatybilności oraz oświadczenia producentów o współpracy ich autoryzowanych placówek serwisowych w zakresie usuwania problemów powstających na styku urządzeń. Złożenie oświadczenia nie dotyczy Wykonawców oferujących cały sprzęt sieciowy pochodzący od jednego producenta.

## **3.5. Wykaz dokumentów, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu**

W celu potwierdzenia spełniania warunków udziału w postępowaniu Wykonawca zobowiązany jest załączyć do oferty następujące oświadczenia i dokumenty:

### **3.5.1. Oświadczenie o spełnianiu warunków udziału w postępowaniu**

Wykonawca jest obowiązany złożyć oświadczenie o spełnianiu warunków udziału w postępowaniu (zgodnie z załącznikiem nr 4 do Specyfikacji).

### **3.5.2. Dokument stwierdzający prowadzenie działalności gospodarczej**

Dokumentem takim będzie aktualny odpis z właściwego rejestru albo aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej, **wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.**

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokument musi być złożony przez każdego Wykonawcę.

### **3.5.3. Dokumenty potwierdzające wywiązywanie się z obowiązków płatności podatków, opłat oraz składek na ubezpieczenie zdrowotne i społeczne**

Dokumentami takimi będą aktualne zaświadczenia właściwego naczelnika urzędu skarbowego oraz właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające odpowiednio, że Wykonawca nie zalega z opłacaniem podatków, opłat oraz składek na ubezpieczenie zdrowotne i społeczne, lub zaświadczeń, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu.

Za aktualne zaświadczenia uznaje się jedynie zaświadczenia **wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.**

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokumenty /zaświadczenia/ muszą być złożony przez każdego Wykonawcę.

#### **3.5.4. Informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 4-8 ustawy**

Dokumentem takim będzie aktualna (**wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert**) informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 4-8 ustawy.

Art. 24 ust. 1 pkt 4-8 ustawy Prawo zamówień publicznych:

„Art. 24. 1. Z postępowania o udzielenie zamówienia wyklucza się:

- 4) osoby fizyczne, które prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,
- 5) spółki jawne, których wspólnika prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,
- 6) spółki partnerskie, których partnera lub członka zarządu prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,
- 7) spółki komandytowe oraz spółki komandytowo-akcyjne, których komplementariusza prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,
- 8) osoby prawne, których urzędującego członka organu zarządzającego prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego”.

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokument musi być złożony przez każdego Wykonawcę.

### 3.5.5. Informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9 ustawy

Dokumentem takim będzie aktualna (wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert) informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9 ustawy.

„Art. 24. 1. Z postępowania o udzielenie zamówienia wyklucza się:

9) podmioty zbiorowe, wobec których sąd orzekł zakaz ubiegania się o zamówienia, na podstawie przepisów o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary”

Przepisy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary zawiera ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary /Dz.U. Nr 197, poz. 1661 z późn. zm./

**Jeżeli Wykonawca jest** podmiotem zbiorowym w rozumieniu przepisów w. wym. ustawy zobowiązany jest do złożenia informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9 – „Informację o podmiocie zbiorowym z Krajowego Rejestru Karnego”

**Jeżeli Wykonawca nie jest** podmiotem zbiorowym w rozumieniu przepisów ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary nie składa informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9 ustawy.”

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, dokument musi być złożony przez każdego Wykonawcę.

### 3.5.6. Wykaz wykonanych w okresie ostatnich 3 lat dostaw wraz z dokumentami, że dostawy te zostały wykonane należycie

Wykonawcy zobowiązani są przedstawić pisemny wykaz (zgodnie z załącznikiem nr 6 do Specyfikacji) - co najmniej 2 dostaw wykonanych w okresie ostatnich trzech lat przed dniem wszczęcia postępowania o udzielenie zamówienia, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, odpowiadających swoim rodzajem dostawie stanowiącej przedmiot zamówienia, tj. dostawie sprzętu sieciowego, o wartości przekraczającej 2.000.000,00 zł brutto każda, z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane należycie.

Przez wykonanie dostaw należy rozumieć ich ostateczny odbiór. W wykazie należy wpisać dostawy, których odbiór ostateczny miał miejsce w ww. latach.

Datę wykonania należy określić jako dzień, miesiąc i rok.

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek musi spełniać co najmniej 1 podmiot lub warunek podmioty te mogą spełniać łącznie.

### 3.5.7. Dokument potwierdzający wysokość posiadanych środków finansowych lub zdolność kredytową

Dokumentem takim będzie informacja banku lub spółdzielczej kasy oszczędnościowo-kredytowej, w którym Wykonawca posiada rachunek, potwierdzającej wysokość posiadanych środków finansowych lub zdolność kredytową Wykonawcy w wysokości nie mniejszej niż 2.000.000,00 zł., wystawionej nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, wyżej wymieniony warunek musi spełniać co najmniej 1 podmiot lub warunek podmioty te mogą spełniać łącznie.

### 3.5.8. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej zamiast dokumentu:

- 1) o którym mowa w pkt 3.5.2, 3.5.3, 3.5.5. - składa dokument lub dokumenty wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania potwierdzające odpowiednio, że:
  - a) nie otwarto jego likwidacji ani nie ogłoszono upadłości,
  - b) nie zalega z uiszczeniem podatków, opłat, składek na ubezpieczenie społeczne i zdrowotne albo, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
  - c) nie orzeczono wobec niego zakazu ubiegania się o zamówienie,
- 1) o którym mowa w pkt 3.5.4 – składa zaświadczenie właściwego organu sądowego lub administracyjnego kraju pochodzenia albo zamieszkania osoby, której dokumenty dotyczą, w zakresie określonym w art. 24 ust. 1 pkt 4-8 ustawy.

Dokumenty, o których mowa w pkt 1 lit a i c oraz w pkt 2 powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert. Dokument, o którym mowa w pkt 1 lit. b powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.

Jeżeli w kraju pochodzenia osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt 1 i pkt 2 zastępuje je się dokumentem zawierającym oświadczenie złożone przed notariuszem, właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio kraju pochodzenia osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania.

#### **4.ZASADY ROZPATRYWANIA, OCENY OFERT ORAZ WYBORU OFERTY NAJKORZYSTNIEJSZEJ**

##### **4.1. Podstawy wykluczenia Wykonawcy z postępowania**

1. Z postępowania o udzielenie zamówienia wyklucza się:
  - 1) Wykonawców, którzy w ciągu ostatnich 3 lat przed wszczęciem postępowania wyrządzili szkodę nie wykonując zamówienia lub wykonując je nienależycie, a szkoda ta nie została dobrowolnie naprawiona do dnia wszczęcia postępowania, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które Wykonawca nie ponosi odpowiedzialności;
  - 2) Wykonawców, w stosunku do których otwarto likwidację lub których upadłość ogłoszono, z wyjątkiem Wykonawców, którzy po ogłoszeniu upadłości zawarli układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli poprzez likwidację majątku upadłego;
  - 3) Wykonawców, którzy zalegają z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadków gdy uzyskali oni przewidziane prawem zwolnienie, odroczenie, rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
  - 4) osoby fizyczne, które prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
  - 5) spółki jawne, których wspólnika prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
  - 6) spółki partnerskie, których partnera lub członka zarządu prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
  - 7) spółki komandytowe oraz spółki komandytowo-akcyjne, których komplementariusza prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
  - 8) osoby prawne, których urzędującego członka organu zarządzającego prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego;
  - 9) podmioty zbiorowe, wobec których sąd orzekł zakaz ubiegania się o zamówienia, na podstawie przepisów o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary;
  - 10) Wykonawców, którzy nie spełniają warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 pkt 1-3 ustawy.

2. Z postępowania o udzielenie zamówienia wyklucza się również Wykonawców, którzy:
  - 1) wykonywali bezpośrednio czynności związane z przygotowaniem prowadzonego postępowania lub posługiwali się w celu sporządzenia oferty osobami uczestniczącymi w dokonywaniu tych czynności, chyba że udział tych Wykonawców w postępowaniu nie utrudni uczciwej konkurencji; przepisu nie stosuje się do Wykonawców, którym udziela się zamówienia na podstawie art. 62 ust. 1 pkt 2 ustawy lub art. 67 ust. 1 pkt 1 i 2 ustawy;
  - 2) złożyli nieprawdziwe informacje mające wpływ na wynik prowadzonego postępowania;
  - 3) nie złożyli oświadczenia o spełnianiu warunków udziału w postępowaniu lub dokumentów potwierdzających spełnianie tych warunków lub złożone dokumenty zawierają błędy, z zastrzeżeniem art. 26 ust. 3 ustawy;
  - 4) nie wnieśli wadium, w tym również na przedłużony okres związania ofertą, lub nie zgodzili się na przedłużenie okresu związania ofertą.
3. Zamawiający zawiadamia równocześnie Wykonawców, którzy zostali wykluczeni z postępowania o udzielenie zamówienia, podając uzasadnienie faktyczne i prawne, z zastrzeżeniem art. 92 ust. 1 pkt 3.
4. Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.

#### **4.2. Podstawy do odrzucenia oferty**

Zamawiający odrzuca ofertę, jeżeli:

- 1) jest niezgodna z ustawą;
- 2) jej treść nie odpowiada treści specyfikacji istotnych warunków zamówienia;
- 3) jej złożenie stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji;
- 4) zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia;
- 5) została złożona przez Wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia lub nie zaproszonego do składania ofert;
- 6) zawiera omyłki rachunkowe w obliczeniu ceny, których nie można poprawić na podstawie art. 88 ustawy, lub błędy w obliczeniu ceny;
- 7) Wykonawca w terminie 7 dni od dnia otrzymania zawiadomienia nie zgodził się na poprawienie omyłki rachunkowej w obliczeniu ceny;
- 8) jest nieważna na podstawie odrębnych przepisów.

#### **4.3.1. Ocena ofert**

Do oceny ofert zakwalifikowanych jako ważne Zamawiający przyjął kryterium określone w ogłoszeniu o zamówieniu wraz ze wskazaniem jego znaczenia (wagą wyrażoną w % udziale w ocenie oferty).

Zaokrąglenia w obliczeniach końcowych punktacji – do dwóch miejsc po przecinku.

Szczegółowe zasady oceny z tytułu kryterium zostały przedstawione poniżej.

##### **4.3.1. Kryterium: CENA (KOSZT) (100% wagi oceny)**

Z tytułu niniejszego kryterium maksymalna ilość punktów wynosi 100.

Oferta o najkorzystniejszej (najniższej) cenie brutto uzyska 100 pkt. Pozostałe ceny obliczone dla badanych ofert zostaną porównane z ofertą o najkorzystniejszej (najniższej) cenie brutto, stosując poniższy wzór:

$$K_m = \frac{C_n}{C_m} \times 100 \text{ pkt}$$

- Gdzie:
- m** – oznacza kolejną badaną ofertę,
  - K<sub>m</sub>** – oznacza **wynik oceny kolejnej badanej oferty w zakresie kryterium ceny (kosztu)**,
  - C<sub>n</sub>** – oznacza **najkorzystniejszą (najniższą) cenę brutto badanej oferty**,
  - C<sub>m</sub>** – oznacza **cenę brutto kolejnej badanej oferty**.

#### 4.3.2. Ocena łączna

Dla każdej oferty wyniki oceny z tytułu kryterium zostaną obliczone według poniższego wzoru.

$$O = K_m \times X \times W_c$$

Gdzie:  $O$  – oznacza ocenę łączną oferty  
 $K_m$  – oznacza wynik oceny kolejnej badanej oferty w zakresie kryterium ceny,  
 $X$  – oznacza niezmienną liczbę członków Komisji przetargowej biorących udział w ocenie,  
 $W_c$  – oznacza wagę oceny kryterium.

#### 4.4. Wybór oferty najkorzystniejszej

Zamawiający wybierze ofertę, która uzyska najwyższą ilość punktów zgodnie z wzorem określonym w pkt 4.3.2.

#### 4.5. Ponowny wybór oferty w razie nieuzasadnionej odmowy podpisania umowy

Jeżeli Wykonawca, którego oferta została wybrana, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może wybierać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzania ich ponownej oceny, chyba że zachodzą przesłanki, o których mowa w art. 93 ust. 1 ustawy.

#### 4.6. Unieważnienie postępowania

1. Zamawiający unieważnia postępowanie o udzielenie zamówienia, jeżeli:
  - 1) nie złożono żadnej oferty nie podlegającej odrzuceniu albo nie wpłynął żaden wniosek o dopuszczenie do udziału w postępowaniu od Wykonawcy nie podlegającego wykluczeniu;
  - 2) cena najkorzystniejszej oferty przewyższa kwotę, którą zamawiający może przeznaczyć na sfinansowanie zamówienia;
  - 3) w przypadkach, o których mowa w art. 91 ust. 5 ustawy, zostały złożone oferty dodatkowe o takiej samej cenie;
  - 4) wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie publicznym, czego nie można było wcześniej przewidzieć;
  - 5) postępowanie obarczone jest wadą uniemożliwiającą zawarcie ważnej umowy w sprawie zamówienia publicznego.
2. O unieważnieniu postępowania o udzielenie zamówienia zamawiający zawiadamia równocześnie wszystkich Wykonawców, którzy:
  - 1) ubiegali się o udzielenie zamówienia – w przypadku unieważnienia postępowania przed upływem terminu składania ofert,
  - 2) złożyli oferty – w przypadku unieważnienia postępowania po upływie terminu składania ofert – podając uzasadnienie faktyczne i prawne.

## OPIS PRZEDMIOTU ZAMÓWIENIA

### dostawa zespołu urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej

#### I. Opis techniczny elementów wchodzących w skład zespołu urządzeń

1. Całość dostarczanego sprzętu musi być fabrycznie nowa, nie używana we wcześniejszych projektach.
2. Ze względu na pożądaną pełną kompatybilność, cały sprzęt sieciowy dostarczany w ramach postępowania powinien pochodzić od jednego producenta; w przypadku oferowania urządzeń różnych producentów, należy dostarczyć oświadczenia ich producentów o pełnej wzajemnej kompatybilności oraz oświadczenia producentów o współpracy ich autoryzowanych placówek serwisowych w zakresie usuwania problemów powstających na styku urządzeń.
3. Zamawiający wymaga dołączenia do urządzeń dokumentacji - instrukcje obsługi w języku polskim lub angielskim (w wersji elektronicznej lub drukowanej).
4. Zamawiający wymaga zapewnienia serwisu bezpłatnej aktualizacji dostarczonego oprogramowania (update'ów, sygnatur i innych) do najnowszej dostępnej wersji przez okres 12 miesięcy.

W skład zespołu urządzeń wchodzi następujące elementy:

#### URZĄDZENIA SIECIOWE TYP I

**Tabela 1 – specjalizowane przełączniki sieciowe agregujące usługi – 2 komplety fabrycznie nowe**

Lp.	Nazwa parametru	Wymagany, minimalny parametr
1	Charakter urządzenia	modularny przełącznik sieciowy, dostosowany do montażu w szafie 19", wyposażonym w przynajmniej 9 gniazd przeznaczonych do instalacji modułów;
2	Architektura urządzenia	- łączne pasmo przełącznika na poziomie min. 640 Gb/s z dostępnym pasmem min. 40 Gb/s (full duplex) na każdy z modułów; - obsługa przetwarzania rozproszonego (karty liniowe muszą mieć możliwość obsługi ruchu bez udziału karty zarządzającej) – wymagana obsługa przetwarzania rozproszonego dla wszystkich kart interfejsów; - możliwość zdublowania karty zarządzającej – w przypadku rozbudowy o drugą kartę przełączenie przy awarii nie może przekroczyć 2s (awaria jednej karty zarządzającej nie może powodować degradacji wydajności urządzenia); - 512 MB pamięci RAM (możliwość rozbudowy do 1GB) oraz 128 MB pamięci nieulotnej typu Flash;
3	Wydajność przełączania urządzenia	48 Mpps per slot;
4	Zarządzanie urządzeniem	- CLI (SSHv2, Telnet), console (port szeregowy konsoli), SNMPv3;
5	Wyposażenie w moduły (karty liniowe) z następującymi portami	- urządzenie ma być wyposażone w 4 porty 10 GigabitEthernet o zmiennej konfiguracji interfejsów (definiowane przez Xenpak, X2, XFP) – w oferowanej wersji obsadzone konwerterami typu LR przeznaczone do pracy na światłowodzie jednomodowym o zasięgu 10 km; porty bez nadsubskrypcji pasma; - urządzenie ma być wyposażone w 48 portów GigabitEthernet typu 10/100/1000BaseT z obsługą ramek typu Jumbo (do 9216B); porty te mają być obsadzone na 1 module; dopuszczalna nadsubskrypcja pasma na poziomie do 1,2:1 z możliwością wykorzystania 40 portów bez nadsubskrypcji; - urządzenie ma być wyposażone w 24 porty GigabitEthernet typu SX przeznaczone do pracy na światłowodzie wielomodowym i o zasięgu przynajmniej 200 metrów z obsługą ramek typu Jumbo (do 9216B); porty te mają być zrealizowane poprzez wkładki typu SFP/GBIC na dedykowanej karcie liniowej; dopuszczalna nadsubskrypcja pasma na poziomie do 1,2:1 z możliwością wykorzystania 20 portów bez nadsubskrypcji; - urządzenie ma być wyposażone w 2 porty GigabitEthernet (bez nadsubskrypcji pasma) ze stykiem definiowanym poprzez wkładki typu SFP/GBIC – jeden z interfejsów musi umożliwiać pracę z medium miedzianym - 10/100/1000BaseT - moduły wymienne z urządzeniem używanym w Centrum Przetwarzania Danych Zamawiającego typ Cisco Catalyst 6509;
6	Wyposażenie w moduł (kartę liniową) z funkcjonalnością zapory	- wydajność co najmniej 4,5Gbps oraz 3Mpps; - obsługa co najmniej 900.000 jednoczesnych sesji; - obsługa konfiguracji co najmniej 100 interfejsów wewnętrznych VLAN;

	ogniowej (ang. firewalla stateful)	<ul style="list-style-type: none"> <li>- obsługa konfiguracji w trybie failover z drugim równoważnym urządzeniem;</li> <li>- obsługa pracy w trybie transparentnym (warstwa L2);</li> <li>- obsługa routingu dynamicznego – co najmniej RIP i OSPF;</li> <li>- konfiguracja przez interfejs CLI, interfejs graficzny dostępny przez przeglądarkę internetową oraz przez dedykowane narzędzie zarządzania centralnego dla produktów bezpieczeństwa sieciowego (dostarczanego przez producenta);</li> <li>- możliwość wirtualizacji modułu (stworzenia min. 2 wirtualnych kontekstów z możliwością rozbudowy do min. 100);</li> <li>- konfiguracja i monitorowanie przez posiadane przez Zamawiającego oprogramowanie Cisco Security Manager PRO;</li> </ul>
7	Wyposażenie w moduł (kartę liniową) z funkcjonalnością równoważenia obciążenia (ang. loadbalancingu) oraz akceleracji sesji SSL	<ul style="list-style-type: none"> <li>- sprzętowy rozdział ruchu w oparciu o informację z warstwy L4-L7 modelu ISO/OSI;</li> <li>- przepustowość 8 Gbps z możliwością rozbudowy do min. 16Gbps bez konieczności rozbudowy sprzętu;</li> <li>- obsługa min. 4.000.000 równoczesnych połączeń TCP;</li> <li>- obsługa min. 300.000 połączeń na sekundę w warstwie L4</li> <li>- obsługa wirtualizacji (dostarczone urządzenie musi obsługiwać min. 5 wirtualnych instancji z możliwością rozbudowy do min. 100);</li> <li>- wsparcie dla trybu routera oraz mostu (w tym dla różnych wirtualnych instancji możliwość konfiguracji trybów routera lub mostu niezależnie);</li> <li>- obsługa konfiguracji w trybie failover z drugim urządzeniem;</li> <li>- zintegrowana funkcjonalność akceleracji sesji SSL z wydajnością 5.000 tuneli na sekundę z możliwością zwiększenia ilości obsługiwanych tuneli SSL do 15.000 bez rozbudowy sprzętu;</li> <li>- mechanizmy inspekcji protokołów warstwy L7, w szczególności inspekcji ruchu HTTP, FTP, DNS, RTSP, ICMP;</li> <li>- obsługa monitorowania stanu serwerów i na tej podstawie dokonywania decyzji o przełączeniu połączenia do konkretnego serwera w oparciu o: ICMP, generyczne próbkowanie TCP/UDP, Echo, Finger, DNS, Telnet, FTP, HTTP, HTTPS, SMTP, POP3, IMAP, Radius lub skrypty;</li> <li>- obsługa zarządzania (konfiguracja, monitoring) przez CLI (linia komend) oraz przez graficzny interfejs użytkownika, z wykorzystaniem zewnętrznej aplikacji zarządzającej (na platformy MS Windows lub Linux) – oprogramowanie musi być dostarczone w ramach urządzenia;</li> </ul>
8	Funkcjonalności urządzenia	<ul style="list-style-type: none"> <li>- możliwość zmiany konfiguracji „w locie”, bez konieczności restartu urządzenia (dotyczy dowolnych zmian konfiguracji);</li> <li>- możliwość zapisu konfiguracji w pliku tekstowym i jej importu/eksportu za pomocą protokołu FTP lub TFTP;</li> <li>- możliwość jednoczesnej instalacji kilku obrazów systemu operacyjnego i programowego wyboru kolejności ich uruchamiania;</li> <li>- możliwość definiowania skryptów określających polityki przekazywania zdarzeń do systemów zarządzających (korelacja, zależności parametrów, diagnostyka);</li> <li>- obsługa min. 4000 aktywnych sieci wirtualnych VLAN; możliwość współpracy z urządzeniami Zamawiającego typ Cisco Catalyst 6509 w zakresie centralnej konfiguracji VLAN z automatyczną dystrybucją informacji na pozostałe urządzenia ;</li> <li>- obsługa sprzętowej weryfikacji źródła pakietu względem tablicy routingu (uRPF);</li> <li>- sprzętowe wsparcie technologii MPLS;</li> <li>- obsługa agregacji portów zgodnie z LACP;</li> <li>- sprzętowe wsparcie technologii tunelowania GRE (Generic Routing Encapsulation);</li> <li>- sprzętowe wsparcie dla IPv6;</li> <li>- wykrywanie łączy jednokierunkowych;</li> <li>- obsługa WCCPv2;</li> <li>- przełączanie w warstwie trzeciej, obsługa routingu statycznego oraz protokołów dynamicznego routingu RIP, OSPF, BGP;</li> </ul>



	<p>- obsługa następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:</p> <ul style="list-style-type: none"> <li>a) protokół IEEE 802.1w Rapid Spanning Tree umożliwiający szybką konwergencję sieci w warstwie 2 modelu OSI;</li> <li>b) protokół IEEE 802.1s Multiple Spanning Tree;</li> <li>c) możliwość grupowania portów w grupy transmisyjne z wykorzystaniem portów pochodzących z różnych kart liniowych;</li> <li>d) możliwość instalacji i wymiany zasilaczy, wentylatorów, kart liniowych, modułów zarządzania/przełączania w trakcie pracy (hot swap);</li> <li>e) wsparcie dla protokołu VRRP/HSRP;</li> </ul> <p>- obsługa zarządzania ruchem (QoS – klasyfikacja ruchu na podstawie rozpoznawania aplikacji, adresów, portów, oznaczeń TOS, IP Precedence, DSCP itp., kolejkovanie z obsługa kolejki priorytetowej, statyczne i dynamiczne ograniczanie pasma, RSVP);</p> <p>- obsługa wysyłania statystyk ruchu zgodnie z netFlow, J-Flow, S-Flow – w przypadku utraty połączenia z serwerem zbierającym statystyki wymagane jest lokalne chache’owanie min. 100 000 wpisów;</p> <p>- obsługa kontroli wydajności sieci (opóźnienia, jitter, dostępność) w oparciu o konfigurowalne próbki ruchu pomiędzy urządzeniami (DHCP, DNS, HTTP, FTP, SNMP, TCP, UDP);</p> <p>- wsparcie dla logicznego podziału ruchu na poziomie warstw drugiej (VLAN) i trzeciej (wirtualne instancje routingowe, wirtualne routery – w ramach poszczególnych instancji wymagany routing dynamiczny OSPF, BGP);</p> <p>- obsługa następujących mechanizmów związanych z zapewnieniem bezpieczeństwa w sieci:</p> <ul style="list-style-type: none"> <li>a) możliwość szyfrowanego zdalnego zarządzania z linii komend z wykorzystaniem protokołu SSH;</li> <li>b) autoryzacja użytkowników dołączających się do portów przez mechanizm IEEE 802.1x i zdalny serwer RADIUS;</li> <li>c) przydział sieci VLAN poprzez mechanizm IEEE 802.1x;</li> <li>d) możliwość blokowania ruchu pomiędzy poszczególnymi portami dostępowymi w obrębie tego samego VLAN’u z pozostawieniem możliwości komunikacji z portem nadrzędnym (prywatny VLAN);</li> <li>e) możliwość autoryzacji dostępu administracyjnego do urządzenia poprzez zdalny serwer AAA Zamawiającego – Cisco CS-ACS (min. 10 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend);</li> <li>f) możliwość dokonywania sprzętowego filtrowania ruchu na podstawie następujących parametrów: źródłowy/docelowy adres IP, źródłowy/docelowy port TCP; usługa ta ma być realizowana sprzętowo, bez wpływu na wydajność przełączania;</li> <li>g) możliwość ograniczenia dostępu do danego portu do pojedynczej lub kilku stacji o statycznie określonych adresach MAC lub do określonej ilości stacji o dynamicznie przyswajanych adresach MAC; w wypadku naruszenia ograniczenia powinna istnieć możliwość wyłączenia portu i poinformowania stacji zarządzającej poprzez SNMP Trap Notification;</li> <li>h) DHCP Snooping;</li> <li>i) dynamiczna inspekcja ARP;</li> <li>j) kontrola ruchu broadcast;</li> </ul> <p>- obsługa ruchu IP Multicast z wykorzystaniem protokołów IGMP v1, v2, v3, PIM oraz IGMP Snooping, mBGP;</p> <p>- możliwość lokalnej obserwacji ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu;</p> <p>- możliwość zdalnej obserwacji ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN;</p> <p>- dla pracy w sieci z włączonym protokołem IEEE 802.1d Spanning Tree :</p> <ul style="list-style-type: none"> <li>a) obsługa natychmiastowego przejścia danego portu ze stanu <i>Blocking</i> do stanu <i>Forwarding</i> po dołączeniu stacji końcowej do tego portu;</li> <li>b) umożliwienie ignorowania przez dany port ramek protokołu Spanning Tree (STP BPDU), w szczególności istotna jest funkcja pozwalająca na zablokowanie próby wymuszenia zmiany topologii STP (np. zmiana Root Bridge) przez nieuprawnionych użytkowników na stacjach końcowych;</li> </ul>
--	--

		<ul style="list-style-type: none"> <li>- urządzenie ma mieć możliwość instalacji następujących dodatkowych interfejsów: <ul style="list-style-type: none"> <li>a) ATM (interfejsy E3, OC-3);</li> <li>b) PoS (Packet over SONET/SDH);</li> <li>c) Ethernet (10/100/1000, GE, 10GE);</li> </ul> </li> <li>- urządzenie ma mieć możliwość instalacji następujących dodatkowych dedykowanych sprzętowych modułów usługowych: <ul style="list-style-type: none"> <li>a) moduł IDS – dla inspekcji ruchu kierowanego do krytycznych zasobów w sieci i wykrywania włamań sieciowych; wymagana wydajność na poziomie min. 500Mbps;</li> <li>b) moduł szyfrowania IPSec dla szyfrowania ruchu skoncentrowanego w Data Center z wykorzystaniem algorytmu AES i przy wydajności nie mniejszej niż 2 Gbps; wymagana obsługa 8,000 tunelowań IPSec;</li> <li>c) moduł detekcji anomalii sieciowych służący do analizowania ruchu pod kątem wystąpienia ataków DDoS; moduł powinien analizować ruch w sieci, a następnie na podstawie analizy statystycznej oceniać czy w danej chwili występuje atak DDoS;</li> <li>d) moduł ograniczający skutki ataku sieciowego DDoS, działający w powiązaniu z modułem detekcji anomalii sieciowych i służący do przekierowania i odrzucania ruchu który został zidentyfikowany jako zagrożenie w sieci;</li> <li>e) moduł służący do monitoringu i zbierania statystyki w sieci, implementujący pełną funkcjonalność RMON (Remote Monitoring, wszystkie 9 grup) oraz SMON (RMON Extensions for Switched Networks) oraz umożliwiający obserwację bieżącego ruchu i rejestrację pakietów;</li> <li>f) modułu bramy głosowej do przyłączenia lokalnej sieci telefonicznej do sieci operatorskiej poprzez porty E1;</li> </ul> </li> </ul>
9	Zasilanie	<ul style="list-style-type: none"> <li>- napięcie: 230V, prąd przemienny: 50Hz, przewody zasilające;</li> <li>- 2 redundantne zasilacze o mocy wystarczającej (każdy) do obsługi w pełni obsadzonego modułami urządzenia (<b>wymagane załączenie do oferty kalkulacji pobieranej mocy dla oferowanej konfiguracji, potwierdzonej przez producenta rozwiązania</b>);</li> </ul>
10	Instalacja i konfiguracja	<ul style="list-style-type: none"> <li>- instalacja w szafie 19" (zapewnienie pełnego wyposażenia montażowego) oraz konfiguracja i uruchomienie zespołu urządzeń przy współpracy z administratorami sieci Zamawiającego;</li> <li>- wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację przełączników w infrastrukturze sieci;</li> </ul>
11	Gwarancja i serwis	<ul style="list-style-type: none"> <li>- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu;</li> <li>- usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym);</li> <li>- serwis musi obejmować dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;</li> </ul>
12	Wymagania dodatkowe	<ul style="list-style-type: none"> <li>- zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego: <ul style="list-style-type: none"> <li>a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy;</li> <li>b) dostęp do narzędzi konfiguracyjnych;</li> <li>c) dostęp do dokumentacji sprzętu i oprogramowania;</li> </ul> </li> </ul>

		<p>- Wykonawca zapewni w uzgodnionym z Zamawiającym terminie, co najmniej 4 dniowe szkolenie (4 x 8 godzin) autoryzowane dla grupy do 3 osób, przeprowadzone w autoryzowanym ośrodku szkoleniowym producenta, poza siedzibą Zamawiającego, kończące się wydaniem imiennych certyfikatów. Szkolenie, co do zakresu pokrywające się ze szkoleniem producenta <b>Urządzeń Typ I</b> - odnoszącym się do zagadnień:</p> <p>a) ogólna charakterystyka rozwiązania - moduł równoważenia obciążenia z akceleracją sesji SSL;</p> <p>b) zagadnienia projektowe:</p> <ol style="list-style-type: none"> <li>1) topologie;</li> <li>2) wirtualizacja;</li> <li>3) zarządzanie zasobami;</li> <li>4) autoryzacja użytkowników;</li> </ol> <p>c) konfiguracja linii poleceń;</p> <p>d) zarządzanie modułem;</p> <p>e) mechanizmy bezpieczeństwa;</p> <p>f) mechanizmy przełączania zawartości;</p> <p>g) mechanizmy monitorowania;</p> <p>h) przetwarzanie protokołów L7;</p> <p>i) mechanizmy akceleracji SSL;</p> <p>j) integracja funkcjonalności.</p> <p>W ramach szkolenia, każdy uczestnik otrzyma materiały szkoleniowe. Dopuszczalne jest przeprowadzenie szkolenia w języku polskim lub angielskim. Nie jest dopuszczalne prowadzenie szkolenia w innych językach lub z wykorzystaniem tłumacza. Szkolenie musi obejmować wykłady teoretyczne i laboratoria praktyczne. W przypadku organizacji szkolenia poza Warszawą, Wykonawca pokryje wszystkie koszty związane z organizacją dojazdu i zapewnieniem wyżywienia oraz zakwaterowania uczestników.</p> <p>- współpraca z systemem Cisco Security MARS (Monitoring, Analysis and Response System) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji oraz aktywne wsparcie dla wszelkich mechanizmów bezpieczeństwa;</p>
--	--	---

## URZĄDZENIA SIECIOWE TYP II

**Tabela 1 – specjalizowane moduły z funkcjonalnością zapory sieciowej (ang. stateful firewall) do przełączników sieciowych Zamawiającego firmy Cisco – model Catalyst 6509 – 2 komplety fabrycznie nowe**

<i>Lp.</i>	<i>Nazwa parametru</i>	<i>Wymagany, minimalny parametr</i>
1	Charakter urządzenia	- specjalizowany moduł do posiadanych przez Zamawiającego switchy Cisco Catalyst 6509 z Supervisor 720-3B;
2	Charakterystyka modułu (karty liniowej) z funkcjonalnością zapory sieciowa (ang. firewalla stateful)	<ul style="list-style-type: none"> <li>- wydajność co najmniej 4,5Gbps oraz 3Mpps;</li> <li>- obsługa co najmniej 900.000 jednoczesnych sesji;</li> <li>- obsługa konfiguracji co najmniej 100 interfejsów wewnętrznych VLAN;</li> <li>- obsługa konfiguracji w trybie failover z drugim równoważnym urządzeniem;</li> <li>- obsługa pracy w trybie transparentnym (warstwa L2);</li> <li>- obsługa routingu dynamicznego – co najmniej RIP i OSPF;</li> <li>- konfiguracja przez interfejs CLI, interfejs graficzny dostępny przez przeglądarkę internetową oraz przez dedykowane narzędzie zarządzania centralnego dla produktów bezpieczeństwa sieciowego (dostarczanego przez producenta);</li> <li>- możliwość wirtualizacji modułu (stworzenia min. 2 wirtualnych kontekstów z możliwością rozbudowy do min. 100);</li> <li>- konfiguracja i monitorowanie przez posiadane przez Zamawiającego oprogramowanie Cisco Security Manager PRO;</li> </ul>
3	Instalacja i konfiguracja	<ul style="list-style-type: none"> <li>- instalacja oraz konfiguracja i uruchomienie przy współpracy z administratorami sieci Zamawiającego;</li> <li>- wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację w infrastrukturze sieci;</li> </ul>
4	Gwarancja i serwis	<ul style="list-style-type: none"> <li>- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu;</li> <li>- usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym);</li> <li>- serwis musi obejmować dostarczanie aktualizacji oprogramowania i wsparcie</li> </ul>

		producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;
5	Wymagania dodatkowe	- zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego: a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy; b) dostęp do narzędzi konfiguracyjnych; c) dostęp do dokumentacji sprzętu i oprogramowania; - współpraca z systemem Cisco Security MARS (Monitoring, Analysis and Response System) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji oraz aktywne wsparcie dla wszelkich mechanizmów bezpieczeństwa;

**Tabela 2 – specjalizowane moduły z funkcjonalnością równoważenia obciążenia (ang. loadbalancingu) oraz akceleracji sesji SSL do przełączników sieciowych Zamawiającego firmy Cisco – model Catalyst 6509 – 2 komplety fabrycznie nowe**

<i>Lp.</i>	<i>Nazwa parametru</i>	<i>Wymagany, minimalny parametr</i>
1	Charakter urządzenia	- specjalizowany moduł do posiadanych przez Zamawiającego switchy Cisco Catalyst 6509 z Supervisor 720-3B;
2	Charakterystyka modułu (karty liniowej) z funkcjonalnością równoważenia obciążenia (ang. loadbalancingu) oraz akceleracji sesji SSL	- sprzętowy rozdziału ruchu w oparciu o informację z warstwy L4-L7 modelu ISO/OSI; - przepustowość 4 Gbps z możliwością rozbudowy do min. 16Gbps bez konieczności rozbudowy sprzętu; - obsługa min. 4.000.000 równoczesnych połączeń TCP; - obsługa min. 300.000 połączeń na sekundę w warstwie L4 - obsługa wirtualizacji (dostarczone urządzenie musi obsługiwać min. 5 wirtualnych instancji z możliwością rozbudowy do min. 100); - wsparcie dla trybu routera oraz mostu (w tym dla różnych wirtualnych instancji możliwość konfiguracji trybów routera lub mostu niezależnie); - obsługa konfiguracji w trybie failover z drugim urządzeniem; - zintegrowana funkcjonalność akceleracji sesji SSL z wydajnością 1.000 tuneli na sekundę z możliwością zwiększenia ilości obsługiwanych tuneli SSL do 15.000 bez rozbudowy sprzętu; - mechanizmy inspekcji protokołów warstwy L7, w szczególności inspekcji ruchu HTTP, FTP, DNS, RTSP, ICMP; - obsługa monitorowania stanu serwerów i na tej podstawie dokonywania decyzji o przełączeniu połączenia do konkretnego serwera w oparciu o: ICMP, generyczne próbkowanie TCP/UDP, Echo, Finger, DNS, Telnet, FTP, HTTP, HTTPS, SMTP, POP3, IMAP, Radius lub skrypty; - obsługa zarządzania (konfiguracja, monitoring) przez CLI (linia komend) oraz przez graficzny interfejs użytkownika, z wykorzystaniem zewnętrznej aplikacji zarządzającej (na platformy MS Windows lub Linux) – oprogramowanie musi być dostarczone w ramach urządzenia;
3	Instalacja i konfiguracja	- instalacja oraz konfiguracja i uruchomienie przy współpracy z administratorami sieci Zamawiającego; - wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację w infrastrukturze sieci;
4	Gwarancja i serwis	- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu; - usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym); - serwis musi obejmować dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;
5	Wymagania dodatkowe	- zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego: a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy; b) dostęp do narzędzi konfiguracyjnych; c) dostęp do dokumentacji sprzętu i oprogramowania;

**Tabela 3 – specjalizowane moduły z interfejsami GigabitEthernet do przełączników sieciowych Zamawiającego firmy Cisco – model Catalyst 6509 – 2 komplety fabrycznie nowe**

<i>Lp.</i>	<i>Nazwa parametru</i>	<i>Wymagany, minimalny parametr</i>
1	Charakter urządzenia	- specjalizowany moduł do posiadanych przez Zamawiającego switchy Cisco Catalyst 6509 z Supervisor 32;
2	Charakterystyka modułu (karty liniowej) z interfejsami GigabitEthernet	- 8 interfejsów GigabitEthernet realizowanych poprzez wkładki typu SFP/GBIC na dedykowanej karcie liniowej; - 4 interfejsy GigabitEthernet mają być typu SX przeznaczone do pracy na światłowodzie wielomodowym i o zasięgu przynajmniej 200 metrów; - 4 interfejsy GigabitEthernet mają być typu 1000BaseT przeznaczone do pracy na medium miedzianym;
3	Instalacja i konfiguracja	- instalacja oraz konfiguracja i uruchomienie przy współpracy z administratorami sieci Zamawiającego; - wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację w infrastrukturze sieci;
4	Gwarancja i serwis	- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu; - usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym); - serwis musi obejmować dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;
5	Wymagania dodatkowe	- zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego: a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy; b) dostęp do narzędzi konfiguracyjnych; c) dostęp do dokumentacji sprzętu i oprogramowania;

### URZĄDZENIA SIECIOWE TYP III

**Tabela 1 – specjalizowane przełączniki sieciowe do obsługi węzłów Internetowych– 4 komplety fabrycznie nowe**

<i>Lp.</i>	<i>Nazwa parametru</i>	<i>Wymagany, minimalny parametr</i>
1	Charakter urządzenia	- przełącznik sieciowy, dostosowany do montażu w szafie 19", 1U; - min. 64MB flash, 256MB RAM;
2	Interfejsy sieciowe	- 44 porty GigabitEthernet typu 10/100/1000 BaseT (RJ-45); - 4 porty GigabitEthernet typu combo (realizowane poprzez wkładki typu SFP/GBIC 1000BaseSX przeznaczone do pracy na światłowodzie wielomodowym i o zasięgu przynajmniej 200 metrów);
3	Wydajność urządzenia	- matryca przełączająca o szybkości min. 96 Gbps (wszystkie porty muszą mieć możliwość pracy z pełną szybkością - wirespeed); - wydajnością przełączania na poziomie min. 70 Mpps (L 2/3/4, realizowane sprzętowo); - wprowadzanie opóźnienia pakietów nie większego niż 6 μs (dla pakietów 64B);
4	Zarządzanie urządzeniem	- zarządzanie przez konsolę szeregową, SSHv2, SNMPv3, RMON, HTTPS; - aktualizacja oprogramowania przez SCP;
5	Funkcjonalności urządzenia	- wbudowane reflektometry (TDR) na wszystkich portach 10/100/1000; - obsługa min. 2000 aktywnych sieci VLAN; - obsługa przełączania w warstwie 2: a) obsługa min. 32.000 adresów MAC; b) obsługa VLAN 802.1q; c) dynamiczne zestawianie trunków; d) możliwość uruchomienia centralnej definicji sieci VLAN i propagacji bazy na inne przełączniki w domenie administracyjnej; e) obsługa STP, RSTP, MSTP; f) agregacja portów w grupy zgodnie z LACP; g) IGMP snooping (v1, v2, v3); h) wykrywanie łączy jednokierunkowych; i) możliwość konfiguracji portu jako 10/100;

		<ul style="list-style-type: none"> <li>j) sprzętowa kontrola wolumenu ruchu rozgłoszeniowego(broadcast);</li> <li>k) sprzętowa obsługa QinQ;</li> <li>l) obsługa ramek jumbo (9216B) na wszystkich portach;</li> </ul>
		<ul style="list-style-type: none"> <li>- obsługa przełączania w warstwie 3:</li> <li>a) routing IPv4 i IPv6 statyczny oraz RIPv2, RIPng, OSPF, BGP, routing multicast MBGP, PIM, IGMP (v1, v2, v3);</li> <li>b) obsługa mechanizmów redundancji bramy (VRRP/HSRP);</li> <li>c) obsługa WCCPv2;</li> </ul>
		<ul style="list-style-type: none"> <li>- obsługa mechanizmów QoS:</li> <li>a) konfiguracja per port i per VLAN;</li> <li>b) cztery sprzętowe kolejki na port;</li> <li>c) obsługa kolejek priorytetowych (strict priority);</li> <li>d) obsługa IP Precedence i DSCP;</li> <li>e) klasyfikacja i oznaczanie pakietów w oparciu o DSCP, ToS, nagłówki L3 i L4;</li> <li>f) obsługa policing-u i shaping-u;</li> </ul>
		<ul style="list-style-type: none"> <li>- obsługa mechanizmów bezpieczeństwa:</li> <li>a) autoryzacja dostępu w oparciu o RADIUS, TACACS+;</li> <li>b) 802.1x;</li> <li>c) listy kontroli dostępu (ACL) na poziomie portów i VLAN-ów;</li> <li>d) filtrowanie adresów MAC;</li> <li>e) możliwość kopiowania ruchu na określony port (SPAN) z przesyłaniem ruchu przez przełączniki (RSPAN) i możliwością filtracji ruchu kopiowanego;</li> <li>f) DHCP snooping;</li> <li>g) dynamiczna inspekcja ARP;</li> <li>h) private VLAN;</li> </ul>
		<ul style="list-style-type: none"> <li>- możliwość definiowania skryptów określających polityki przekazywania zdarzeń do systemów zarządzających (korelacja, zależności parametrów, diagnostyka);</li> </ul>
		<ul style="list-style-type: none"> <li>- możliwość definicji makr konfiguracyjnych dla portów (określenie listy poleceń konfiguracyjnych aplikowanych za pomocą pojedynczej komendy);</li> </ul>
		<ul style="list-style-type: none"> <li>- możliwość przechowywania wielu wersji systemu operacyjnego i konfiguracji kolejności prób ich uruchamiania; w przypadku braku prawidłowego obrazu w pamięci wewnętrznej przełącznika, możliwość uruchomienia obrazu z zewnętrznego serwera (typu TFTP, FTP, SCP lub podobny);</li> </ul>
		<ul style="list-style-type: none"> <li>- zmiany konfiguracji muszą być widoczne natychmiastowo – nie dopuszcza się konieczności częściowych lub całkowitych restartów urządzenia w celu uruchomienia zmian;</li> </ul>
		<ul style="list-style-type: none"> <li>- obsługa synchronizacji czasu ze źródłem zewnętrznym zgodnie z NTP lub SNTP;</li> </ul>
		<ul style="list-style-type: none"> <li>- redundantne wentylatory z możliwością wymiany w miejscu instalacji (moduł);</li> </ul>
6	Zasilanie	<ul style="list-style-type: none"> <li>- napięcie: 230V, prąd przemienny: 50Hz, przewody zasilające;</li> <li>- 2 redundantne zasilacze;</li> </ul>
7	Instalacja i konfiguracja	<ul style="list-style-type: none"> <li>- instalacja w szafie 19" (zapewnienie pełnego wyposażenia montażowego) oraz konfiguracja i uruchomienie przy współpracy z administratorami sieci Zamawiającego;</li> <li>- wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację przełączników w infrastrukturze sieci;</li> </ul>
8	Gwarancja i serwis	<ul style="list-style-type: none"> <li>- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu;</li> <li>- usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym);</li> <li>- serwis musi obejmować dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;</li> </ul>
9	Wymagania dodatkowe	<ul style="list-style-type: none"> <li>- zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego:</li> <li>a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy;</li> <li>b) dostęp do narzędzi konfiguracyjnych;</li> <li>c) dostęp do dokumentacji sprzętu i oprogramowania;</li> <li>- współpraca z systemem Cisco Security MARS (Monitoring, Analysis and Response System) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji oraz aktywne wsparcie dla wszelkich mechanizmów bezpieczeństwa;</li> </ul>

## URZĄDZENIA SIECIOWE TYP IV

Tabela 1 – specjalizowany router Internetowy – 1 komplet fabrycznie nowy

Lp.	Nazwa parametru	Wymagany, minimalny parametr
1	Charakter urządzenia	- urządzenie modułarne, posiadające min. 4 sloty do obsadzenia silnikami liniowymi i kartami zarządzającymi; - urządzenie musi mieć możliwość montażu w szafie 19” ;
2	Architektura urządzenia	- architektura rozproszona – każdy z silników liniowych musi mieć możliwość autonomicznego przełączania pakietów, bez udziału karty zarządzającej; każdy z silników liniowych musi posiadać możliwość instalacji min. dwóch kart interfejsów liniowych; - wymagane 2 redundantne karty zarządzające z synchronizacją stanu – przełączenie w przypadku awarii nie może powodować przerwy w przełączaniu pakietów; - każda z kart zarządzających oraz silników liniowych musi być wyposażona w pamięć DRAM o pojemności min. 2GB; dla kart zarządzających możliwość rozbudowy do min. 4GB; - min. 2GB pamięci nie ulotnej (flash); - zwielokrotnione wentylatory;
3	Wydajność urządzenia	- matryca przełączająca systemu min. 80 Gbps, min. 10Gbps (full duplex) dostępne dla każdego ze slotów; wydajność przełączania min. 16 Mpps per slot;
4	Zarządzanie urządzeniem	- dedykowany interfejs GE 10/100/1000 do zarządzania out-of-band z możliwością wykorzystania do przekazywania ruchu; - dostęp do urządzenia za pomocą konsoli szeregowej, dodatkowego interfejsu szeregowego (umożliwiającego podłączenie modemu), telnet, SSHv2, SNMPv3; - urządzenie musi posiadać możliwość raportowania do systemów zarządzających z wykorzystaniem jFlow, NetFlow, sFlow (konieczna jest sprzętowa obsługa funkcjonalności); wymagana możliwość eksportu statystyk dla ruchu MPLS, IPv4, IPv6; - współpraca z serwerami uwierzytelniającymi RADIUS/TACACS+ (autoryzacja i logowanie dostępu); - możliwość tworzenia grup administratorów z określonymi uprawnieniami i przydziału użytkowników do grup (1:N – pojedynczy użytkownik może być członkiem wielu grup); - możliwość partycjonowania urządzenia (z przydziałem do poszczególnych partycji dedykowanych zasobów sprzętowych, separacją zarządzania); - możliwość monitorowania działania sieci end-to-end (opóźnienia, jitter, straty pakietów; UDP, ICMP, MPLS) w oparciu o ruch próbkowy generowany przez urządzenie; - dostępne API XML do integracji z aplikacjami zewnętrznymi; - możliwość zabezpieczenia przed jednoczesnym konfigurowaniem urządzenia przez wielu użytkowników
5	Wymagane interfejsy sieciowe	- zainstalowane min. 5 interfejsów 1 GigabitEthernet obsadzonych: a) konwerterami 1000BaseSX - 2 sztuki; b) konwerterami 1000BaseT - 3 sztuki.
6	Funkcjonalności urządzenia	- nie blokująca matryca przełączająca z centralną kontrolą dostępu i kolejkowaniem dostępu do matrycy (eliminacja możliwości wystąpienia zjawiska head-of-line-blocking i zmian kolejności pakietów na poziomie matrycy przełączającej); - urządzenie musi umożliwiać instalację kart liniowych z następującymi interfejsami: a) ATM OC3, OC12; b) POS OC3, OC12, OC48, OC192; c) RPR OC12, OC48, OC192; d) FastEthernet, GigabitEthernet, 10GigabitEthernet; e) szeregowo E3; - urządzenie musi posiadać możliwość obsadzenia urządzenia co najmniej 4-ma portami 10-Gigabit Ethernet lub 40-ma portami Gigabit Ethernet z nadsubskrypcją pasma nie większą niż 2:1 (przy redundantnych kartach zarządzających); - urządzenie musi mieć możliwość płynnego konfigurowania interfejsów optycznych- wszystkie interfejsy 10 Gigabit Ethernet i Gigabit Ethernet muszą być definiowane przez moduły typu GBIC, mini-GBIC, SFP, Xenpak, X2, XFP – nie dopuszcza się stosowania kart o stałej konfiguracji portów; - routing w oparciu o RIP, RIPv2, OSPF, BGPv4, ISIS oraz routing statyczny; - możliwość ingerencji w decyzje routingowe w oparciu o polityki skryptowe; - obsługa min. 1.000.000 prefiksów w tablicach routingu i przełączania

		<ul style="list-style-type: none"> <li>- wsparcie dla mechanizmów w ramach obsługi IPv6: <ul style="list-style-type: none"> <li>b) statystyki jFlow/NetFlow/sFlow;</li> <li>c) Tunelowanie v6 do v4;</li> <li>d) ICMP, DNS, SSH, Telnet, traceroute dla IPv6;</li> <li>e) RIPng;</li> <li>f) ISIS dla IPv6;</li> <li>g) OSPFv3;</li> <li>h) BGP dla IPv6;</li> <li>i) IPv6 MPLS VPN (6VPE);</li> <li>j) IPv6 multicast (PIM, BGP, MLD).</li> </ul> </li> <li>- wsparcie obsługi ruchu multicast z wykorzystaniem: <ul style="list-style-type: none"> <li>a) IGMP v1, v2, v3;</li> <li>b) PIM (SM, SSM);</li> <li>c) MSDP;</li> <li>d) replikacja multicast na poziomie matrycy przełączającej.</li> </ul> </li> <li>- wsparcie w ramach funkcjonalności MPLS: <ul style="list-style-type: none"> <li>a) statystyki NetFlow/jFlow/sFlow;</li> <li>b) MPLS LDP;</li> <li>c) MPLS LSP;</li> <li>d) MPLS LSP Ping/Traceroute;</li> <li>e) MPLS CoS;</li> <li>f) MPLS Traffic Engineering (TE): <ul style="list-style-type: none"> <li>1) Diff-Serv Aware Traffic Engineering;</li> <li>2) Wsparcie dla OSPF;</li> <li>3) Wsparcie dla notyfikacji SNMP dla MPLS TE;</li> <li>4) RSVP TE.</li> </ul> </li> <li>g) MPLS Virtual Private Networks (VPN): <ul style="list-style-type: none"> <li>1) MPLS VPN ID;</li> <li>2) Wsparcie dla OSPF PE-CE;</li> <li>3) Wsparcie dla MPLS VPN inter-AS – IPv4 BGP Label Distribution;</li> <li>4) Multicast VPN (mVPN).</li> </ul> </li> </ul> </li> <li>- wsparcie dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci: <ul style="list-style-type: none"> <li>a) możliwość instalacji “na gorąco” zasilaczy, kart liniowych, redundantnych modułów zarządzania/routingu;</li> <li>b) protokół HSRP/VRRP;</li> <li>c) obsługa bezprzerwowego przekazywania pakietów (w przypadku przełączenia na zapasową kartę zarządzającą) dla BGP, OSPF, IS-IS, MPLS;</li> <li>d) możliwość agregacji łączy Ethernet: <ul style="list-style-type: none"> <li>1) obsługa 802.1q VLAN,</li> <li>2) obsługa LACP,</li> <li>3) obsługa MPLS,</li> <li>4) obsługa multicast,</li> <li>5) NetFlow/jFlow/sFlow;</li> </ul> </li> <li>e) modułarny system operacyjny: <ul style="list-style-type: none"> <li>1) oddzielne procesy dla poszczególnych funkcjonalności (np. przekazywanie pakietów, poszczególne protokoły routingu itp.) z chronionymi obszarami pamięci;</li> <li>2) możliwość restartowania poszczególnych procesów;</li> <li>3) możliwość aktualizacji poszczególnych modułów funkcjonalnych bez ingerencji w pozostałe;</li> <li>4) min. dwustopniowy proces zatwierdzania zmian w konfiguracji z możliwością powrotu do wcześniejszych jej wersji;</li> </ul> </li> </ul> </li> </ul>
--	--	--



		<p>- wsparcie dla następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:</p> <ul style="list-style-type: none"> <li>a) klasyfikacja pakietów: <ul style="list-style-type: none"> <li>1) identyfikacja ruchu w oparciu o IP Precedence, DSCP, ToS, VLAN ID, CoS, adresy MAC/IP, protokół;</li> <li>2) oznaczanie ruchu z wykorzystaniem IP Precedence, DSCP, ToS, EXP;</li> <li>3) oznaczanie bezwarunkowe (klasa) oraz warunkowe (w oparciu o policing);</li> </ul> </li> <li>b) zarządzanie zatorami: <ul style="list-style-type: none"> <li>1) kolejkovanie z obsługą kolejek priorytetowych – możliwość określania gwarancji pasma dla poszczególnych klas ruchu;</li> <li>2) kształtowanie ruchu (shaping);</li> <li>3) ograniczanie ruchu (policing);</li> </ul> </li> <li>c) unikanie zatorów: <ul style="list-style-type: none"> <li>1) mechanizmy wczesnego wykrywania zatorów (typu RED, WRED);</li> <li>2) mechanizmy selektywnego odrzucania pakietów.</li> </ul> </li> <li>d) możliwość filtrowania (listy kontroli dostępu) i priorytetyzacji (rate-limit, selektywne odrzucanie) ruchu kierowanego do modułu zarządzającego w celu ochrony przed atakami DoS/DDoS – min. 4 wejściowe kolejki sprzętowe dla karty zarządzającej; wymagana konfigurowalność mechanizmu;</li> <li>e) możliwość propagacji polityk QoS z wykorzystaniem BGP;</li> <li>f) mechanizmy priorytetyzacji dostępu do matrycy przełączającej w zależności od klasy ruchu;</li> <li>g) możliwość hierarchicznej konfiguracji mechanizmów QoS;</li> <li>h) min. 16 kolejek sprzętowych per port;</li> <li>i) obsługa QoS bez degradacji wydajności;</li> </ul> <p>- wsparcie dla następujących mechanizmów związanych z zapewnieniem bezpieczeństwa sieci:</p> <ul style="list-style-type: none"> <li>a) możliwość definiowania list dostępowych dla interfejsów urządzenia (ACL) i interfejsów administracyjnych: <ul style="list-style-type: none"> <li>1) filtrowanie w oparciu o adresy i protokoły IP, porty TCP/UDP,</li> <li>2) możliwość logowania ruchu zgodnego z poszczególnymi wpisami w ACL (z określeniem progu wywołania),</li> <li>3) liczniki sprzętowe wykorzystania ACL,</li> <li>4) mechanizmy optymalizacji długich ACL,</li> <li>5) obsługa ACL bez degradacji wydajności.</li> </ul> </li> <li>b) obsługa tuneli IPsec,</li> <li>c) weryfikacja źródła ruchu unicats względem tablicy routingu (uRPF),</li> <li>d) zarządzanie przez SSH,</li> <li>e) możliwość uwierzytelniania sesji protokołów routingowych (BGP, OSPF, IS-IS) oraz RSVP,</li> <li>f) mechanizmy wykrywania awarii łączy (Bidirectional Forwarding Detection – BFD).</li> </ul> <p>- urządzenie musi umożliwiać rozszerzenie funkcjonalności o sprzętową realizację:</p> <ul style="list-style-type: none"> <li>a) funkcjonalności firewall z kontrolą stanu sesji: <ul style="list-style-type: none"> <li>1) wydajność na poziomie min. 7 Gbps, 2Mpps,</li> <li>2) obsługa min. 100.000 jednoczesnych połączeń z szybkością min. 10.000 połączeń na sekundę,</li> <li>3) możliwość wirtualizacji funkcjonalności – obsługa min. 200 wirtualnych instancji z określeniem dostępnej wydajności, pamięci, parametrów zarządzania (adres, serwery autoryzacji),</li> <li>4) obsługa ramek jumbo (9000B),</li> <li>5) obsługa NAT/PAT,</li> <li>6) walidacja zgodności protokołów (FTP, HTTP, ICMP, DNS),</li> <li>7) filtracja ActiveX/Java,</li> <li>8) współpraca z serwerami autoryzacyjnymi (RADIUS/TACACS+).</li> </ul> </li> <li>b) funkcjonalności szyfrowania połączeń IPsec: <ul style="list-style-type: none"> <li>1) wydajność min. 2 Gbps (AES),</li> <li>2) obsługa min. 15.000 tuneli VPN (100 tuneli / sekundę),</li> <li>3) obsługa mechanizmów QoS dla tuneli VPN,</li> <li>4) wsparcie dla ruchu multicast dla tuneli VPN.</li> </ul> </li> </ul>
7	Wymagania dotyczące modułów urządzenia	<p>- moduły muszą być wzajemnie wymienne z <b>specjalizowanymi routerami rdzeniowymi</b> – <b>Urządzenie sieciowe TYP V</b> (nie dopuszcza się sytuacji, gdzie dla obsługi któregoś z modułów użytego w innym urządzeniu konieczna jest wymiana chassis, modułu zarządzania, panelu wentylacji, etc.);</p>

8	Zasilanie	- napięcie: 230V, prąd przemienny: 50Hz, przewody zasilające; - co najmniej 2 redundantne zasilacze o mocy pozwalającej na obsługę urządzenia (każdy);
9	Instalacja i konfiguracja	- instalacja w szafie 19" (zapewnienie pełnego wyposażenia montażowego) oraz konfiguracja i uruchomienie zespołu urządzeń przy współpracy z administratorami sieci Zamawiającego; - wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację w infrastrukturze sieci;
10	Gwarancja i serwis	- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu; - usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym); - serwis musi obejmować dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;
11	Wymagania dodatkowe	- zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego: a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy; b) dostęp do narzędzi konfiguracyjnych; c) dostęp do dokumentacji sprzętu i oprogramowania;  - Wykonawca zapewni w uzgodnionym z Zamawiającym terminie, co najmniej 5 dniowe szkolenie (5 x 8 godzin) autoryzowane dla grupy do 3 osób, przeprowadzone w autoryzowanym ośrodku szkoleniowym producenta, poza siedzibą Zamawiającego, kończące się wydaniem imiennych certyfikatów. Szkolenie, co do zakresu pokrywające się ze szkoleniem producenta <b>Urządzeń Typ IV i V</b> - odnoszącym się do zagadnień: a) charakterystyka urządzeń; b) modułarny system operacyjny; c) aktualizacje systemu operacyjnego; d) mechanizmy bezpieczeństwa (w tym wirtualizacja); e) konfiguracja protokołów routingu w środowiskach złożonych (wiele AS); f) konfiguracja obsługi multicast; g) konfiguracja MPLS (L3 VPN, MPLS TE); h) diagnozowanie i rozwiązywanie problemów. W ramach szkolenia, każdy uczestnik otrzyma materiały szkoleniowe. Dopuszczalne jest przeprowadzenie szkolenia w języku polskim lub angielskim. Nie jest dopuszczalne prowadzenie szkolenia w innych językach lub z wykorzystaniem tłumacza. Szkolenie musi obejmować wykłady teoretyczne i laboratoria praktyczne. W przypadku organizacji szkolenia poza Warszawą, Wykonawca pokryje wszystkie koszty związane z organizacją dojazdu i zapewnieniem wyżywienia oraz zakwaterowania uczestników.

## URZĄDZENIA SIECIOWE TYP V

Tabela 1 – specjalizowane routery rdzeniowe – 4 komplety fabrycznie nowe

Lp.	Nazwa parametru	Wymagany, minimalny parametr
1	Charakter urządzenia	- urządzenie modułarne, posiadające min. 4 sloty do obsadzenia silnikami liniowymi i kartami zarządzającymi; - urządzenie musi mieć możliwość montażu w szafie 19" ;
2	Architektura urządzenia	- architektura rozproszona – każdy z silników liniowych musi mieć możliwość autonomicznego przełączania pakietów, bez udziału karty zarządzającej; każdy z silników liniowych musi posiadać możliwość instalacji min. dwóch kart interfejsów liniowych; - możliwość instalacji redundantnej karty zarządzającej z synchronizacją stanu – przełączenie w przypadku awarii nie może powodować przerwy w przełączaniu pakietów; - każda z kart zarządzających oraz silników liniowych musi być wyposażona w pamięć DRAM o pojemności min. 2GB; dla kart zarządzających możliwość rozbudowy do min. 4GB; - min. 2GB pamięci nie ulotnej (flash); - wielokrotnione wentylatory;
3	Wydajność urządzenia	- matryca przełączająca systemu min. 80 Gbps, min. 10Gbps (full duplex) dostępne dla każdego ze slotów; wydajność przełączania min. 16 Mpps per slot;

4	Zarządzanie urządzeniem	<ul style="list-style-type: none"> <li>- dedykowany interfejs GE 10/100/1000 do zarządzania out-of-band z możliwością wykorzystania do przekazywania ruchu;</li> <li>- dostęp do urządzenia za pomocą konsoli szeregowej, dodatkowego interfejsu szeregowego (umożliwiającego podłączenie modemu), telnet, SSHv2, SNMPv3;</li> <li>- urządzenie musi posiadać możliwość raportowania do systemów zarządzających z wykorzystaniem jFlow, NetFlow, sFlow (konieczna jest sprzętowa obsługa funkcjonalności); wymagana możliwość eksportu statystyk dla ruchu MPLS, IPv4, IPv6;</li> <li>- współpraca z serwerami uwierzytelniającymi RADIUS/TACACS+ (autoryzacja i logowanie dostępu);</li> <li>- możliwość tworzenia grup administratorów z określonymi uprawnieniami i przydziału użytkowników do grup (1:N – pojedynczy użytkownik może być członkiem wielu grup);</li> <li>- możliwość partycjonowania urządzenia (z przydziałem do poszczególnych partycji dedykowanych zasobów sprzętowych, separacją zarządzania);</li> <li>- możliwość monitorowania działania sieci end-to-end (opóźnienia, jitter, straty pakietów; UDP, ICMP, MPLS) w oparciu o ruch próbkowy generowany przez urządzenie;</li> <li>- dostępne API XML do integracji z aplikacjami zewnętrznymi;</li> <li>- możliwość zabezpieczenia przed jednoczesnym konfigurowaniem urządzenia przez wielu użytkowników;</li> </ul>
5	Wymagane interfejsy sieciowe	<ul style="list-style-type: none"> <li>- zainstalowane min. 3 interfejsy 10 GigabitEthernet obsadzone: <ul style="list-style-type: none"> <li>a) konwerterami ER (10 Gigabit Ethernet extended-reach (ER) - światłowodowe połączenie jednomodowe do 40 km) - 1 sztuka;</li> <li>b) konwerterami LR (10 Gigabit Ethernet long-reach (LR) – światłowodowe połączenie jednomodowe do 10 km - SMF) - 2 sztuki.</li> </ul> </li> <li>- zainstalowane min. 10 interfejsów 1 GigabitEthernet obsadzonych konwerterami 1000BaseSX – (światłowodowe połączenie wielomodowe - MMF);</li> </ul>
6	Funkcjonalności urządzenia	<ul style="list-style-type: none"> <li>- nie blokująca matryca przełączająca z centralną kontrolą dostępu i kolejkowaniem dostępu do matrycy (eliminacja możliwości wystąpienia zjawiska head-of-line-blocking i zmian kolejności pakietów na poziomie matrycy przełączającej);</li> <li>- urządzenie musi umożliwiać instalację kart liniowych z następującymi interfejsami: <ul style="list-style-type: none"> <li>a) ATM OC3, OC12;</li> <li>b) POS OC3, OC12, OC48, OC192;</li> <li>c) RPR OC12, OC48, OC192;</li> <li>d) FastEthernet, GigabitEthernet, 10GigabitEthernet;</li> <li>e) szeregowo E3;</li> </ul> </li> <li>- urządzenie musi posiadać możliwość obsadzenia urządzenia co najmniej 4-ma portami 10-Gigabit Ethernet lub 40-ma portami Gigabit Ethernet z nadsubskrypcją pasma nie większą niż 2:1 (przy redundantnych kartach zarządzających);</li> <li>- urządzenie musi mieć możliwość płynnego konfigurowania interfejsów optycznych- wszystkie interfejsy 10 Gigabit Ethernet i Gigabit Ethernet muszą być definiowane przez moduły typu GBIC, mini-GBIC, SFP, Xenpak, X2, XFP – nie dopuszcza się stosowania kart o stałej konfiguracji portów;</li> <li>- routing w oparciu o RIP, RIPv2, OSPF, BGPv4, ISIS oraz routing statyczny;</li> <li>- możliwość ingerencji w decyzje routingu w oparciu o polityki skryptowe;</li> <li>- obsługa min. 1.000.000 prefiksów w tablicach routingu i przełączania;</li> <li>- wsparcie dla mechanizmów w ramach obsługi IPv6: <ul style="list-style-type: none"> <li>a) statystyki jFlow/NetFlow/sFlow;</li> <li>b) Tunelowanie v6 do v4;</li> <li>c) ICMP, DNS, SSH, Telnet, traceroute dla IPv6;</li> <li>d) RIPng;</li> <li>e) ISIS dla IPv6;</li> <li>f) OSPFv3;</li> <li>g) BGP dla IPv6;</li> <li>h) IPv6 MPLS VPN (6VPE);</li> <li>i) IPv6 multicast (PIM, BGP, MLD).</li> </ul> </li> <li>- wsparcie obsługi ruchu multicast z wykorzystaniem: <ul style="list-style-type: none"> <li>a) IGMP v1, v2, v3;</li> <li>b) PIM (SM, SSM, bidirectional);</li> <li>c) MSDP;</li> <li>d) replikacja multicast na poziomie matrycy przełączającej.</li> </ul> </li> </ul>

		<p>- wsparcie w ramach funkcjonalności MPLS:</p> <ul style="list-style-type: none"> <li>a) statystyki NetFlow/jFlow/sFlow;</li> <li>b) MPLS LDP;</li> <li>c) MPLS LSP;</li> <li>d) MPLS LSP Ping/Traceroute;</li> <li>e) MPLS CoS;</li> <li>f) MPLS Traffic Engineering (TE): <ul style="list-style-type: none"> <li>1) Diff-Serv Aware Traffic Engineering;</li> <li>2) Wsparcie dla OSPF;</li> <li>3) Wsparcie dla notyfikacji SNMP dla MPLS TE;</li> <li>4) RSVP TE.</li> </ul> </li> <li>g) MPLS Virtual Private Networks (VPN): <ul style="list-style-type: none"> <li>1) MPLS VPN ID;</li> <li>2) Wsparcie dla OSPF PE-CE;</li> <li>3) Wsparcie dla MPLS VPN inter-AS – IPv4 BGP Label Distribution;</li> <li>4) Multicast VPN (mVPN).</li> </ul> </li> </ul>
		<p>- wsparcie dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:</p> <ul style="list-style-type: none"> <li>a) możliwość instalacji “na gorąco” zasilaczy, kart liniowych, redundantnych modułów zarządzania/routingu;</li> <li>b) protokół HSRP/VRRP;</li> <li>c) obsługa bezprzerwowego przekazywania pakietów (w przypadku przełączenia na zapasową kartę zarządzającą) dla BGP, OSPF, IS-IS, MPLS;</li> <li>d) możliwość agregacji łączy Ethernet: <ul style="list-style-type: none"> <li>1) obsługa 802.1q VLAN,</li> <li>2) obsługa LACP,</li> <li>3) obsługa MPLS,</li> <li>4) obsługa multicast,</li> <li>5) NetFlow/jFlow/sFlow.</li> </ul> </li> <li>e) modułarny system operacyjny: <ul style="list-style-type: none"> <li>1) oddzielne procesy dla poszczególnych funkcjonalności (np. przekazywanie pakietów, poszczególne protokoły routingu itp.) z chronionymi obszarami pamięci;</li> <li>2) możliwość restartowania poszczególnych procesów;</li> <li>3) możliwość aktualizacji poszczególnych modułów funkcjonalnych bez ingerencji w pozostałe;</li> <li>4) min. dwustopniowy proces zatwierdzania zmian w konfiguracji z możliwością powrotu do wcześniejszych jej wersji;</li> </ul> </li> </ul>
		<p>- wsparcie dla następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:</p> <ul style="list-style-type: none"> <li>a) klasyfikacja pakietów: <ul style="list-style-type: none"> <li>1) identyfikacja ruchu w oparciu o IP Precedence, DSCP, ToS, VLAN ID, CoS, adresy MAC/IP, protokół;</li> <li>2) oznaczanie ruchu z wykorzystaniem IP Precedence, DSCP, ToS, EXP;</li> <li>3) oznaczanie bezwarunkowe (klasa) oraz warunkowe (w oparciu o policing);</li> </ul> </li> <li>b) zarządzanie zatorami: <ul style="list-style-type: none"> <li>1) kolejkowanie z obsługą kolejek priorytetowych – możliwość określania gwarancji pasma dla poszczególnych klas ruchu;</li> <li>2) kształtowanie ruchu (shaping);</li> <li>3) ograniczanie ruchu (policing);</li> </ul> </li> <li>c) unikanie zatorów: <ul style="list-style-type: none"> <li>1) mechanizmy wczesnego wykrywania zatorów (typu RED, WRED);</li> <li>2) mechanizmy selektywnego odrzucania pakietów.</li> </ul> </li> <li>d) możliwość filtrowania (listy kontroli dostępu) i priorytetyzacji (rate-limit, selektywne odrzucanie) ruchu kierowanego do modułu zarządzającego w celu ochrony przed atakami DoS/DDoS – min. 4 wejściowe kolejki sprzętowe dla karty zarządzającej; wymagana konfigurowalność mechanizmu;</li> <li>e) możliwość propagacji polityk QoS z wykorzystaniem BGP;</li> <li>f) mechanizmy priorytetyzacji dostępu do matrycy przełączającej w zależności od klasy ruchu;</li> <li>g) możliwość hierarchicznej konfiguracji mechanizmów QoS;</li> <li>h) min. 16 kolejek sprzętowych per port;</li> <li>i) obsługa QoS bez degradacji wydajności;</li> </ul>

		<p>- wsparcie dla następujących mechanizmów związanych z zapewnieniem bezpieczeństwa sieci:</p> <ol style="list-style-type: none"> <li>a) możliwość definiowania list dostępowych dla interfejsów urządzenia (ACL) i interfejsów administracyjnych: <ol style="list-style-type: none"> <li>1) filtrowanie w oparciu o adresy i protokoły IP, porty TCP/UDP,</li> <li>2) możliwość logowania ruchu zgodnego z poszczególnymi wpisami w ACL (z określeniem progu wywołania),</li> <li>3) liczniki sprzętowe wykorzystania ACL,</li> <li>4) mechanizmy optymalizacji długich ACL,</li> <li>5) obsługa ACL bez degradacji wydajności.</li> </ol> </li> <li>b) obsługa tuneli IPsec,</li> <li>c) weryfikacja źródła ruchu unicast względem tablicy routingu (uRPF),</li> <li>d) zarządzanie przez SSH,</li> <li>e) możliwość uwierzytelniania sesji protokołów routingowych (BGP, OSPF, IS-IS) oraz RSVP,</li> <li>f) mechanizmy wykrywania awarii łączy (Bidirectional Forwarding Detection – BFD).</li> </ol> <p>- urządzenie musi umożliwiać rozszerzenie funkcjonalności o sprzętową realizację:</p> <ol style="list-style-type: none"> <li>c) funkcjonalności firewall z kontrolą stanu sesji: <ol style="list-style-type: none"> <li>1) wydajność na poziomie min. 7 Gbps, 2Mpps,</li> <li>2) obsługa min. 100.000 jednoczesnych połączeń z szybkością min. 10.000 połączeń na sekundę,</li> <li>3) możliwość wirtualizacji funkcjonalności – obsługa min. 200 wirtualnych instancji z określeniem dostępnej wydajności, pamięci, parametrów zarządzania (adres, serwery autoryzacji),</li> <li>4) obsługa ramek jumbo (9000B),</li> <li>5) obsługa NAT/PAT,</li> <li>6) walidacja zgodności protokołów (FTP, HTTP, ICMP, DNS),</li> <li>7) filtracja ActiveX/Java,</li> <li>8) współpraca z serwerami autoryzacyjnymi (RADIUS/TACACS+).</li> </ol> </li> <li>d) funkcjonalności szyfrowania połączeń IPsec: <ol style="list-style-type: none"> <li>1) wydajność min. 2 Gbps (AES),</li> <li>2) obsługa min. 15.000 tuneli VPN (100 tuneli / sekundę),</li> <li>3) obsługa mechanizmów QoS dla tuneli VPN,</li> <li>4) wsparcie dla ruchu multicast dla tuneli VPN.</li> </ol> </li> </ol>
7	Wymagania dotyczące modułów urządzenia	- moduły muszą być wzajemnie wymienne z <b>specjalizowanym routerem Internetowym – Urządzenie sieciowe TYP IV</b> (nie dopuszcza się sytuacji, gdzie dla obsługi któregoś z modułów użytego w innym urządzeniu konieczna jest wymiana chassis, modułu zarządzania, panelu wentylacji, etc.);
8	Zasilanie	- napięcie: 230V, prąd przemienny: 50Hz, przewody zasilające; - co najmniej 2 redundantne zasilacze o mocy pozwalającej na obsługę urządzenia (każdy);
9	Instalacja i konfiguracja	- instalacja w szafie 19” (zapewnienie pełnego wyposażenia montażowego) oraz konfiguracja i uruchomienie zespołu urządzeń przy współpracy z administratorami sieci Zamawiającego; - wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację w infrastrukturze sieci;
10	Gwarancja i serwis	- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu; - usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym); - serwis musi obejmować dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;
11	Wymagania dodatkowe	- zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego: a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy; b) dostęp do narzędzi konfiguracyjnych; c) dostęp do dokumentacji sprzętu i oprogramowania;

## URZĄDZENIA SIECIOWE TYP VI

**Tabela 1 – specjalizowane urządzenia typu firewall (zapora sieciowa) – 2 komplety fabrycznie**

<i>Lp.</i>	<i>Nazwa parametru</i>	<i>Wymagany, minimalny parametr</i>	
1	Charakter urządzenia	urządzenie dedykowane (appliance);	
2	Typ obudowy	możliwość instalacji w szafie 19" (wyposażenie montażowe), wysokość 1RU;	
3	Ilość interfejsów sieciowych	4 x GigabitEthernet 10/100/1000 BaseT 1 Gbps oraz 1 x FastEthernet 10/100 BaseTX 100 Mbps;	
4	Ilość pamięci RAM urządzenia	1024 MB	
5	Ilość portów szeregowych	2 (port konsoli oraz port AUX) ;	
6	Ilość slotów na moduły rozszerzeń	1	
7	Charakter pracy urządzenia	kompletne rozwiązanie firewall/VPN/IPS;	
8	Zasilanie	napięcie: 230V, prąd przemienny: 50Hz, przewody zasilające	
9	Zarządzanie urządzeniem	poprzez przeglądarkę WWW (HTTPS); CLI (SSH)	
10	Praca w wysokiej dostępności – HA (ang. High Availability)	tak (tryby pracy: Aktywny/Aktywny (Active/Active) oraz Aktywny/Rezerwowy (Active/Standby); wymagana jest możliwość pracy równoległej urządzenia z drugim takim samym urządzeniem jako urządzenie zapasowe (failover) i jednocześnie możliwość jednoczesnej obsługi ruchu przez oba urządzenia w trybie Active/Active (Aktywny/Aktywny); w momencie awarii urządzenia aktywnego urządzenie zapasowe musi przejąć obsługę istniejących sesji w sposób nie zakłócający ich przebiegu (tryb stateful failover firewall – podtrzymywanie sesji firewalla);	
11	Wydajność dla ruchu nieszyfrowanego	650 Mbps	
12	Wydajność dla ruchu VPN szyfrowanego 3DES/AES	320 Mbps	
13	Ilość obsługiwanych sesji	400.000, min. 25.000 nowych połączeń na sekundę	
15	Obsługiwana ilość jednoczesnych zestawionych tuneli VPN (IPsec)	5000	
16	Obsługiwana ilość jednoczesnych zestawionych tuneli WebVPN (SSL)	100 z możliwością rozbudowy do 2500	
17	Ilość obsługiwanych interfejsów VLAN	200	
18	Wymagany zainstalowany moduł w slotach rozszerzeń obsługujący funkcjonalność IPS	Architektura urządzenia	- praca w trybach in-line oraz promiscuous;
		Wydajność	- co najmniej 450 Mbps dla ruchu poddanego inspekcji IPS;
		Zarządzanie urządzeniem	- zarządzana przez linię komend (CLI) z wykorzystaniem protokołu SSH; - możliwość konfiguracji i monitorowania przez posiadane przez Zamawiającego oprogramowanie Cisco Security Manager PRO;
		Funkcjonalność i urządzenia	- identyfikacja, klasyfikacja i powstrzymywanie ruchu zagrażającego bezpieczeństwu organizacji w tym: a) robaki sieciowe; b) adware; c) spyware; d) wirusy sieciowe; e) nadużycia aplikacyjne.

		<ul style="list-style-type: none"> <li>- wykrywanie i powstrzymanie działań wskazujących na przekroczenie polityk bezpieczeństwa w tym: <ul style="list-style-type: none"> <li>a) działania z wykorzystaniem komunikatorów internetowych;</li> <li>b) działania z wykorzystaniem aplikacji peer-to-peer;</li> <li>c) filtracja w oparciu o typy MIME.</li> </ul> </li> <li>- wykrywanie robaków internetowych oraz wirusów sieciowych w szczególności z wykorzystaniem analizy anomalii ruchu w monitorowanych segmentach sieci;</li> <li>- wykrywanie nadużyć w pakietach IP-in-IP;</li> <li>- analiza kontekstowa – wykrywanie ataków ukryte w wielu następujących po sobie pakietach;</li> <li>- inspekcja aplikacyjna co najmniej dla protokołów: <ul style="list-style-type: none"> <li>a) FTP,</li> <li>b) Simple Mail Transfer Protocol (SMTP),</li> <li>c) HTTP,</li> <li>d) SMB,</li> <li>e) Domain Name System (DNS),</li> <li>f) remote procedure call (RPC),</li> <li>g) NetBIOS,</li> <li>h) Network News Transfer Protocol (NNTP),</li> <li>i) generic routing encapsulation (GRE),</li> <li>j) Telnet.</li> </ul> </li> <li>- wykrywanie anomalii związanych z ruchem w monitorowanym segmencie sieci;</li> <li>- wykrywanie anomalii związanych z protokołami (w szczególności odstępstw od normalnych zachowań zdefiniowanych przez odpowiednie dokumenty RFC);</li> <li>- wykrywanie ataków związanych z działaniami w warstwie 2 modelu OSI w szczególności ataków na ARP oraz ataków Man-in-the-middle w środowisku przełączanym;</li> <li>- mechanizmy zapobiegające „omijaniu” systemów IPS w szczególności: <ul style="list-style-type: none"> <li>a) normalizacji ruchu;</li> <li>b) scalania strumieni TCP;</li> <li>c) deobfuscation;</li> <li>d) scalające (defragmentujące) dla pakietów IP.</li> </ul> </li> <li>- mechanizmy dla OS Fingerprinting – identyfikacji systemu operacyjnego hosta dla celów przyszłej oceny znaczenia ataku;</li> <li>- definiowanie kryteriów oceny znaczenia ataku w oparciu o co najmniej następujące parametry: <ul style="list-style-type: none"> <li>a) ważność zdarzenia (potencjalne zagrożenie jeżeli ruch zostanie dopuszczony – nie będzie filtrowany);</li> <li>b) wartość zasobu (określenie krytyczności atakowanego urządzenia dla organizacji);</li> <li>c) potencjalna skuteczność ataku (wstępne określenie czy atak mógł być skuteczny);</li> </ul> </li> <li>- wskazanie limitów na pasmo dla określonych aplikacji celem zapobiegania wykorzystaniu całego pasma przez atakującego;</li> </ul>
		<p>Dodatkowe funkcjonalności urządzenia</p> <ul style="list-style-type: none"> <li>- monitoring ruchu IPv6;</li> </ul>
18	Funkcjonalności urządzenia	<ul style="list-style-type: none"> <li>- wsparcie dla obsługi bezpieczeństwa warstwy aplikacyjnej;</li> <li>- obsługa transparentnego zabezpieczenia typu firewall w warstwie 2;</li> <li>- obsługa technologii 2 wirtualnych urządzeń (ang. virtual devices) (opcjonalnie 10), z ograniczeniami dot. dynamicznego routingu, VPN oraz obsługi multicastów.</li> <li>- funkcjonalność „stateful failover” dla ruchu VPN;</li> <li>- wsparcie dla obsługi protokołów OSPF, RIP;</li> <li>- obsługa mechanizmów związane z obsługą ruchu Multicast;</li> <li>- współpraca z serwerami CA;</li> <li>- obsługa inspekcji ruchu głosowego w zakresie protokołów H.323, SIP;</li> </ul>

		- obsługa mechanizmów kolejkowania ruchu z obsługą kolejki absolutnego priorytetu;
		- możliwość zainstalowania modułu sprzętowego obsługującego funkcje bezpieczeństwa dotyczące: ochrony antywirusowej, systemu anti-spamowego, systemu anti-spyware, systemu anti-phishing lub możliwość zainstalowania modułu sprzętowego obsługującego funkcje ips (możliwość przeprowadzania dualnych operacji w trybie „promiscous” oraz w trybie „inline”);
19	Instalacja i konfiguracja	- instalacja w szafie 19” (zapewnienie pełnego wyposażenia montażowego) oraz konfiguracja i uruchomienie przy współpracy z administratorami sieci Zamawiającego; - wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację w infrastrukturze sieci;
20	Gwarancja i serwis	- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu; - usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym); - serwis musi obejmować dostarczanie aktualizacji oprogramowania (w tym sygnatur IPS) i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;
21	Wymagania dodatkowe	- dostarczenie wraz z urządzeniem dedykowanego oprogramowania klienta VPN. Oprogramowanie musi mieć możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych MS Windows, Solaris i Linux, a także komputerach Mac. Oprogramowanie musi umożliwiać zestawienie do urządzenia połączeń VPN z komputerów osobistych PC. Oprogramowanie to powinno pochodzić od tego samego producenta, co oferowane urządzenie i powinno być objęte jego jednolitym wsparciem technicznym. - zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego: a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy; b) dostęp do narzędzi konfiguracyjnych; c) dostęp do dokumentacji sprzętu i oprogramowania; - współpraca z systemem Cisco Security MARS (Monitoring, Analysis and Response System) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji oraz aktywne wsparcie dla wszelkich mechanizmów bezpieczeństwa;

## URZĄDZENIA SIECIOWE TYP VII

**Tabela 1 – specjalizowane moduły typu ips (system zapobiegania włamaniom) do urządzeń typu firewall Zamawiającego firmy Cisco – model ASA 5520 – 2 komplety fabrycznie nowe**

<i>Lp.</i>	<i>Nazwa parametru</i>	<i>Wymagany, minimalny parametr</i>
1	Charakter urządzenia	- specjalizowany moduł typu IPS do posiadanych przez Zamawiającego urządzeń typu firewall Cisco ASA 5520;
2	Architektura urządzenia	- praca w trybach in-line oraz promiscous;
3	Wydajność	- co najmniej 450 Mbps dla ruchu poddawanego inspekcji IPS;
4	Zarządzanie urządzeniem	- zarządzana przez linię komend (CLI) z wykorzystaniem protokołu SSH; - możliwość konfiguracji i monitorowania przez posiadane przez Zamawiającego oprogramowanie Cisco Security Manager PRO;
5	Funkcjonalności urządzenia	- identyfikacja, klasyfikacja i powstrzymanie ruchu zagrażającego bezpieczeństwu organizacji w tym: f) robaki sieciowe; g) adware; h) spyware; i) wirusy sieciowe; j) nadużycia aplikacyjne. - wykrywanie i powstrzymanie działań wskazujących na przekroczenie polityk bezpieczeństwa w tym: d) działania z wykorzystaniem komunikatorów internetowych; e) działania z wykorzystaniem aplikacji peer-to-peer; f) filtracja w oparciu o typy MIME.



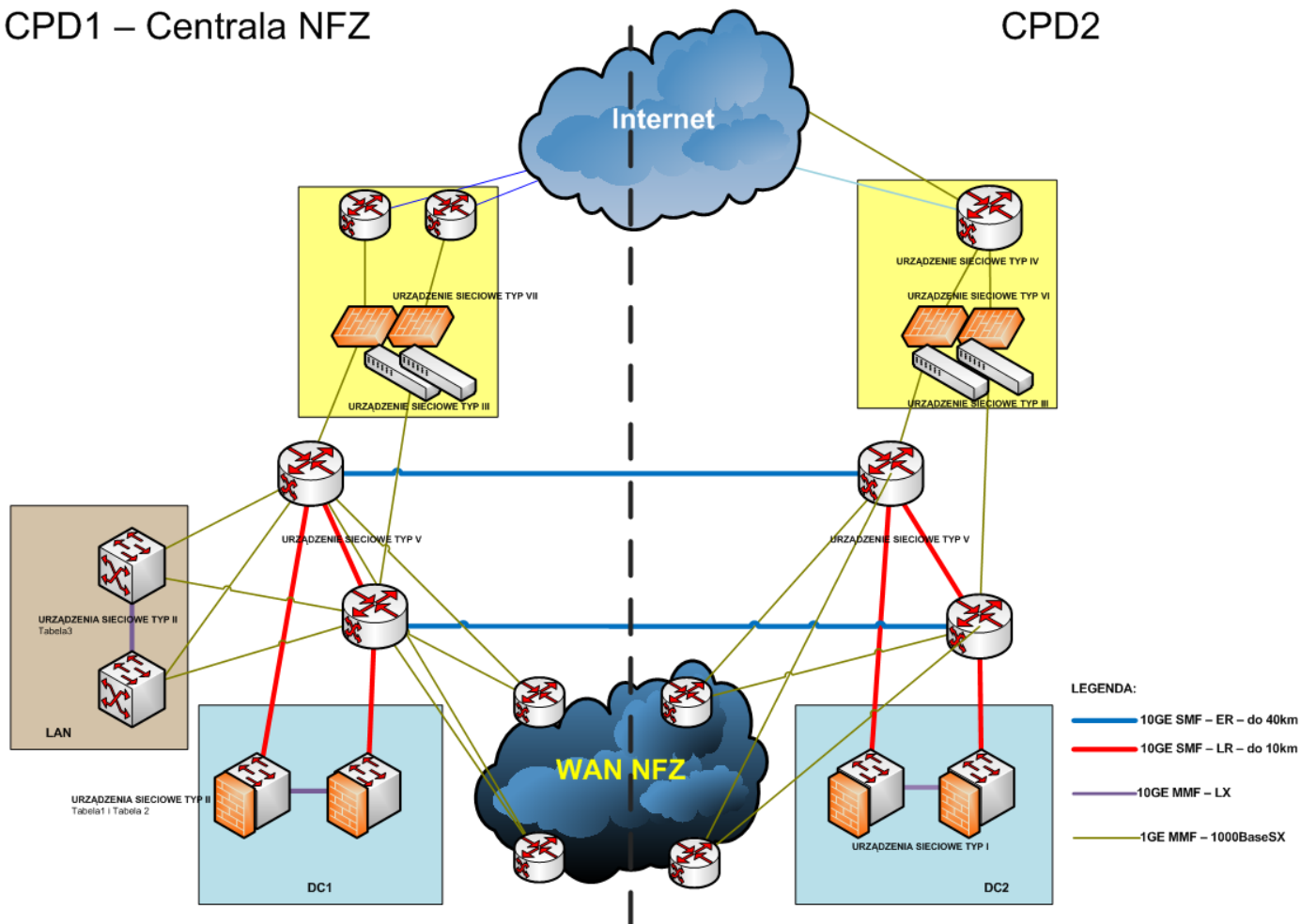
		<p>- wykrywanie robaków internetowych oraz wirusów sieciowych w szczególności z wykorzystaniem analizy anomalii ruchu w monitorowanych segmentach sieci;</p> <p>- wykrywanie nadużyć w pakietach IP-in-IP;</p> <p>- analiza kontekstowa – wykrywanie ataków ukryte w wielu następujących po sobie pakietach;</p> <p>- inspekcja aplikacyjna co najmniej dla protokołów:</p> <p>k) FTP,</p> <p>l) Simple Mail Transfer Protocol (SMTP),</p> <p>m) HTTP,</p> <p>n) SMB,</p> <p>o) Domain Name System (DNS),</p> <p>p) remote procedure call (RPC),</p> <p>q) NetBIOS,</p> <p>r) Network News Transfer Protocol (NNTP),</p> <p>s) generic routing encapsulation (GRE),</p> <p>t) Telnet.</p> <p>- wykrywanie anomalii związanych z ruchem w monitorowanym segmencie sieci;</p> <p>- wykrywanie anomalii związanych z protokołami (w szczególności odstępstw od normalnych zachowań zdefiniowanych przez odpowiednie dokumenty RFC);</p> <p>- wykrywanie ataków związanych z działaniami w warstwie 2 modelu OSI w szczególności ataków na ARP oraz ataków Man-in-the-middle w środowisku przełączanym;</p> <p>- mechanizmy zapobiegające „omijaniu” systemów IPS w szczególności:</p> <p>e) normalizacji ruchu;</p> <p>f) scalania strumieni TCP;</p> <p>g) deobfuscation;</p> <p>h) scalające (defragmentujące) dla pakietów IP.</p> <p>- mechanizmy dla OS Fingerprinting – identyfikacji systemu operacyjnego hosta dla celów przyszłej oceny znaczenia ataku;</p> <p>- definiowanie kryteriów oceny znaczenia ataku w oparciu o co najmniej następujące parametry:</p> <p>d) ważność zdarzenia (potencjalne zagrożenie jeżeli ruch zostanie dopuszczony – nie będzie filtrowany);</p> <p>e) wartość zasobu (określenie krytyczności atakowanego urządzenia dla organizacji);</p> <p>f) potencjalna skuteczność ataku (wstępne określenie czy atak mógł być skuteczny);</p> <p>- wskazanie limitów na pasmo dla określonych aplikacji celem zapobiegania wykorzystaniu całego pasma przez atakującego;</p>
6	Dodatkowe funkcjonalności urządzenia	- monitoring ruchu IPv6;
7	Instalacja i konfiguracja	<p>- instalacja w szafie 19” (zapewnienie pełnego wyposażenia montażowego) oraz konfiguracja i uruchomienie przy współpracy z administratorami sieci Zamawiającego;</p> <p>- wymagane jest zapewnienie wszelkich kabli połączeniowych oraz elementów zapewniających instalację w infrastrukturze sieci;</p>
8	Gwarancja i serwis	<p>- gwarancja przez min. 12 m-cy, serwis realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu;</p> <p>- usunięcie awarii – 24 godz. od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym);</p> <p>- serwis musi obejmować dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania;</p>
9	Wymagania dodatkowe	<p>- zapewnienie samodzielnego dostępu do serwisu webowego producenta umożliwiającego:</p> <p>a) pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres 12 m-cy;</p> <p>b) dostęp do narzędzi konfiguracyjnych;</p> <p>c) dostęp do dokumentacji sprzętu i oprogramowania;</p> <p>- współpraca z systemem Cisco Security MARS (Monitoring, Analysis and Response System) wykorzystywanym w sieci Zamawiającego do monitorowania zdarzeń i ich korelacji oraz aktywne wsparcie dla wszelkich mechanizmów bezpieczeństwa;</p>

## II. Warunki wdrożenia i uruchomienia systemu

1. Całość systemu (rozwiązania) ma zostać zainstalowana, skonfigurowana, wdrożona i uruchomiona wg. uzgodnień z Zamawiającym zgodnie z jego wymaganiami i przy jego współudziale. Prace powinny obejmować następujące etapy:
  - 1.1. Przeprowadzenie analizy aktualnej struktury oraz konfiguracji urządzeń sieciowych w węzłach centralnych Zamawiającego,
  - 1.2. Przedstawienie harmonogramu prac, zaakceptowanego przez Zamawiającego,
  - 1.3. Opracowanie projektu technicznego obejmującego szczegóły implementacyjne rozwiązań, w porozumieniu z Zamawiającym.
  - 1.4. Przeprowadzenia szkoleń pracowników Zamawiającego.
  - 1.5. Dostawy instalacji komponentów systemu.
  - 1.6. Konfiguracja i uruchomienie urządzeń w środowisku testowym, ew. w ograniczonej grupie urządzeń.
  - 1.7. Właściwa konfiguracja i uruchomienie całego systemu - przełączenia ruchu produkcyjnego na nową infrastrukturę.
  - 1.8. Przeprowadzenie testów akceptacyjnych - walidacja rozwiązania (audyt konfiguracji względem opracowanego projektu implementacji) i opracowania dokumentacji powykonawczej.
  - 1.9. Opracowanie dokumentacji powykonawczej i zaleceń powdrożeniowych, obejmującej:
    - a) procedury operacyjne dla administratorów;
    - b) instrukcje z zadaniami administracyjnymi;
    - c) procedury backupów i awaryjne (ratunkowe).
2. Zamawiający wyznaczy po swojej stronie Kierownika Projektu, który będzie koordynował wszystkie prace oraz działania wynikające z powyższego zamówienia po stronie Zamawiającego. Zamawiający wymaga by Wykonawca po swojej stronie wyznaczył osobę, która będzie pełniła nadzór nad wszystkimi pracami wdrożeniowymi.
3. W zespole wdrożeniowym będą uczestniczyć ze strony Zamawiającego administratorzy sieci i systemów.
4. W ramach wdrożenia Zamawiający wymaga zintegrowanie całego środowiska z następującymi systemami urządzeniami zamawiającego i uruchomienia ustalonych funkcjonalności :
  - 4.1. Cisco CS-MARS;
  - 4.2. Cisco ASA model 5520;
  - 4.3. Cisco CS-ACS;
  - 4.4. Cisco Catalyst – switche serii 6500, 3550;
  - 4.5. Cisco routery serii 7xxx;
5. Zamawiający wymaga, aby w projekcie powykonawczym (części technicznej) całego systemu, znalazły się wszelkie składniki systemu, w tym także elementy, które były rekonfigurowane w celu poprawnej pracy całości rozwiązania.
6. Zamawiający wymaga, aby wszystkie prace, które mogą spowodować przestoje w pracy sieci produkcyjnej, były przeprowadzane w godzinach 16.30 – 7.30. Zamawiający dopuszcza prowadzenie prac wdrożeniowych w dni wolne od pracy po wcześniejszym uzgodnieniu terminu.
7. Ogólny opis i schemat systemu
  - 7.1. Wdrożenie i uruchomienie zespołu specjalizowanych urządzeń typ I, II, III, IV, V, VI i VII zg. z wymaganiami ustalonymi z Zamawiającym oraz integracja z urządzeniami Zamawiającego;
  - 7.2. Uruchomienie funkcjonalności redundancji i HA w strefach bezpieczeństwa sieci – w tym w rdzeniu oraz routingu dynamicznego oraz zaawansowanych mechanizmów bezpieczeństwa oraz integracja z systemami sieciowymi Zamawiającego.

CPD1 – Centrala NFZ

CPD2



Schemat połączeń zespołu urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej.

**UMOWA ...../2008**

zawarta w dniu ..... 2008 r. w Warszawie pomiędzy Narodowym Funduszem Zdrowia Centralą z siedzibą w Warszawie przy ul. Grójeckiej 186, NIP 107-00-010-57, zwaną dalej ZAMAWIAJĄCYM, reprezentowanym przez:

a  
.....zwaną dalej WYKONAWCĄ, reprezentowaną przez:

W wyniku przeprowadzonego postępowania o udzielenie zamówienia w trybie przetargu nieograniczonego zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2007 r. Nr 223, poz. 1655), zawarto umowę następującej treści:

## § 1

1. Przedmiotem umowy jest **dostawa zespołu urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej**. Przez dostawę Zamawiający rozumie także instalację, skonfigurowanie, wdrożenie i uruchomienie zgodnie z załącznikiem nr 1 do umowy.
2. Wykonawca oświadcza, że przed złożeniem oferty zapoznał się ze wszystkimi warunkami, które są niezbędne do wykonania przez niego przedmiotu zamówienia bez konieczności ponoszenia przez Zamawiającego jakichkolwiek dodatkowych kosztów.

## § 2

1. Strony ustalają, że **dostawa, instalacja, skonfigurowanie, wdrożenie i uruchomienie zespołu urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej** nastąpi w terminie nie przekraczającym 5 miesięcy od daty podpisania umowy, tj. do dnia .....
2. Wykonawca dostarcza przedmiot umowy w miejsce wskazane przez Zamawiającego na terenie województwa mazowieckiego na własny koszt i ryzyko.
3. Odbiór przedmiotu umowy potwierdzony zostanie protokołem odbioru.
4. Protokół odbioru, o którym mowa w ust. 3, ze strony Zamawiającego podpisuje osoba pełniąca funkcję Naczelnika Wydziału Eksploatacji.
5. Ewentualne usterki stwierdzone przy odbiorze przedmiotu umowy, w tym ujawnione w wyniku przeprowadzonych przez Zamawiającego testów eksploatacyjnych, zostaną usunięte przez Wykonawcę w terminie 3 dni od daty ich zgłoszenia Wykonawcy.
6. Wykonawca zapewni szkolenie zgodnie z opisem technicznym, który stanowi załącznik nr 1 do umowy.

## § 3

1. Ustala się cenę za realizację przedmiotu umowy w wysokości:
  - 1) netto ..... złotych (słownie złotych .....
  - 2) podatek VAT ..... złotych (słownie złotych .....
  - 3) brutto ..... złotych (słownie złotych .....
2. Wykaz cen jednostkowych urządzeń stanowi załącznik nr 2 do umowy.
3. Podstawą do wystawienia faktury za realizację przedmiotu umowy jest protokół odbioru, o którym mowa w § 2 ust. 3, sporządzony pisemnie z udziałem Stron.
4. Zapłata wynagrodzenia nastąpi przelewem na rachunek bankowy Wykonawcy w terminie 14 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury wraz z podpisanym przez przedstawicieli Stron zbiorczym protokołem odbioru przedmiotu umowy.
5. Za datę zapłaty Strony ustalają dzień, w którym Zamawiający wydał swojemu bankowi polecenie przelewu wynagrodzenia na rachunek bankowy Wykonawcy, wskazany na fakturze.
6. Zamawiający zapłaci Wykonawcy za opóźnienie w zapłacie, o której mowa w ust. 4 odsetki ustawowe za okres od dnia wymagalności do dnia zapłaty.

#### § 4

1. Wykonawca na dostarczone urządzenia udziela 12 miesięcznej gwarancji. Okres gwarancji liczony jest od daty podpisania protokołu odbioru, o którym mowa w § 2 ust. 3.
2. Strony ustalają, że serwis gwarancyjny prowadzony będzie w miejscu instalacji urządzeń, przez .....
3. Wykonawca oświadcza, że serwis obejmuje dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania.
4. Wszystkie koszty związane ze świadczeniem gwarancji ponosi Wykonawca.
5. Wykonawca oświadcza, że czas naprawy awarii w okresie gwarancji nie przekroczy 24 godzin od chwili zgłoszenia.
6. Strony ustalają, że zgłoszenia wysłane po godz. 15:00 traktowane będą jako zgłoszone w następnym dniu roboczym.

#### § 5

Zamawiający może odstąpić od umowy o ile Wykonawca wykonuje dostawę (instalacja, skonfigurowanie, wdrożenie i uruchomienie) wadliwie lub w sposób sprzeczny z umową, a w szczególności dostarcza przedmiot umowy niezgodnie ze złożoną ofertą.

#### § 6

1. Wykonawca zapłaci Zamawiającemu karę umowną:
  - 1) za odstąpienie od umowy przez Zamawiającego z przyczyn, o których mowa w § 5 w wysokości 10% ceny brutto określonej w § 3 ust. 1 pkt 3,
  - 2) za opóźnienie w oddaniu przedmiotu umowy w wysokości 0,2% ceny brutto określonej w § 3 ust. 1 pkt 3 za każdy dzień opóźnienia,
  - 3) za opóźnienie w usunięciu usterek stwierdzonych przy odbiorze lub ujawnionych w okresie gwarancji w wysokości 0,2% ceny brutto określonej w § 3 ust. 1 pkt 3 za każdy dzień opóźnienia liczonej od dnia wyznaczonego na ich usunięcie.
2. Zamawiającemu przysługuje prawo dochodzenia odszkodowania przewyższającego karę umowną.
3. Zamawiający zastrzega sobie prawo potrącenia naliczonej kary umownej i odszkodowania z przysługującego Wykonawcy wynagrodzenia wynikającego z wystawionej faktury na co Wykonawca wyraża zgodę.

#### § 7

1. Wykonawca wnosi zabezpieczenie należytego wykonania umowy w wysokości 5% ceny brutto, o której mowa w § 3 ust. 1 pkt 3 tj. .... (słownie: .....złoty).
2. Jeżeli Wykonawca wykona usługę zgodnie z umową:
  - 1) **70 %** zabezpieczenia zostanie zwolnione Wykonawcy w ciągu 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane,
  - 2) **30 %** zabezpieczenia zostanie zwolnione Wykonawcy nie później niż w 15 dniu po upływie gwarancji.

#### § 8

Strony ustalają, że w razie powstania okoliczności, o których mowa w §6, Zamawiającemu przysługuje prawo naliczenia odpowiednich kar umownych i potrącenia ich z wystawionej faktury. W przypadku opóźnienia w usunięciu usterek w okresie gwarancji, Zamawiającemu przysługuje prawo potrącenia ich z zabezpieczenia należytego wykonania umowy, o którym mowa w § 7 ust. 1.

#### § 9

W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym czego nie można było przewidzieć w chwili zawarcia umowy, Zamawiający może odstąpić od umowy w terminie 30 dni od daty powzięcia wiadomości o tych okolicznościach.

#### § 10

Zakazuje się zmian postanowień zawartej umowy w stosunku do treści oferty, chyba, że konieczność wprowadzania takich zmian wynika z okoliczności, których nie można było przewidzieć w chwili zawarcia umowy lub zmiany te są korzystne dla Zamawiającego.

#### § 11

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

#### § 12

Spory powstałe na tle realizacji niniejszej umowy będą rozstrzygane przez sąd właściwy miejscowo dla siedziby Zamawiającego.

§ 13

W sprawach nie uregulowanych w umowie zastosowanie mają przepisy ustawy Prawo zamówień publicznych oraz przepisy Kodeksu cywilnego.

§ 14

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego, jeden dla Wykonawcy.

ZAMAWIAJĄCY

WYKONAWCA

pieczęć Wykonawcy

....., dnia .....

**Oferta**

Nazwa Wykonawcy .....

Adres Wykonawcy .....

tel. .... fax.....

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

**składa ofertę na dostawę zespołu urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej NFZ**

**1. Oświadczenie o oferowanej cenie:**

- 1) cena netto ..... zł  
(słownie:.....)
- 2) podatek od towarów i usług VAT – ..... zł  
(słownie: .....) )
- 3) cena brutto ..... zł  
(słownie:.....)

**2. Oświadczenie o akceptacji terminu realizacji zamówienia:**

Oświadczam, że bez zastrzeżeń przyjmuję przedstawiony przez Zamawiającego termin realizacji zamówienia nie przekraczający 5 miesięcy od daty podpisania umowy.

**3. Oświadczenie o akceptacji wymagań określających przedmiot zamówienia:**

Oświadczam, że akceptuję wszystkie wymagania określone w załączniku do Specyfikacji „Opis przedmiotu zamówienia” i stwierdzam, że oferowany zespół urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej NFZ spełnia określone w nim wymogi w pełnym zakresie.

**4. Oświadczenie o akceptacji warunków gwarancji i serwisu**

Oświadczam, że na dostarczone, zamontowane i uruchomione urządzenia udzielam **12 miesięcznej gwarancji**, przy czym serwis będzie realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu) w miejscu instalacji sprzętu.

Oświadczam, że czas usunięcia awarii w okresie gwarancji nie przekroczy 24 godzin od momentu zgłoszenia (zgłoszenia wysłane po godz. 15 traktowane są jako przyjęte w następnym dniu roboczym).

Oświadczam, że serwis obejmuje dostarczanie aktualizacji oprogramowania i wsparcie producenta przy rozwiązywaniu problemów z bieżącą eksploatacją sprzętu i oprogramowania.

**5. Oświadczenie o akceptacji warunków płatności:**

Oświadczam, że bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki płatności za realizację zamówienia.

.....  
**Podpis i pieczęć Wykonawcy**

**6. Oświadczenie o akceptacji przedstawionych przez Zamawiającego warunków umownych realizacji zamówienia:**

Oświadczam, że bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki umowne realizacji zamówienia określone we wzorze umowy załączonym do specyfikacji. Zobowiązuję się w przypadku wyboru naszej oferty do zawarcia umowy na wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego.

**7. Wniesienie przez Wykonawcę na rzecz Zamawiającego wadium przetargowego**

Wadium przetargowe zostało wniesione na rzecz Zamawiającego w dniu .....

- w pieniądzu przelewem na rachunek bankowy
- w formie .....

W razie zaistnienia przesłanek zwrotu wadium, proszę o jego zwrot na:

- nr konta .....
- na adres .....

**8. Oświadczenie Wykonawcy, czy wykona sam zamówienie, czy powierzy wykonanie części zamówienia podwykonawcom**

Oświadczamy, że realizację przedmiotu zamówienia:

- wykonamy sami \*
- powierzmy wykonanie części zamówienia podwykonawcom zgodnie z poniższym zestawieniem \*

\* właściwe zaznaczyć

Lp.	Części zamówienia, której wykonanie Wykonawca powierzy podwykonawcom

**9. Oświadczenie o dokumentach załączonych do oferty:**

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

.....  
**Podpis i pieczęć Wykonawcy**



pieczęć Wykonawcy

ZAŁĄCZNIK NR 4 DO SPECYFIKACJI

....., dnia .....

## OŚWIADCZENIE WYKONAWCY O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU

/nazwa (firma) i adres Wykonawcy/  
.....  
.....

( w przypadku Wykonawców występujących wspólnie należy wymienić wszystkich Wykonawców )

Niniejszym oświadczamy, że spełniamy warunki udziału w postępowaniu o zamówienie publiczne na **Dostawę zespołu urządzeń do Centrum Przetwarzania Danych (CPD) NFZ w ramach infrastruktury sieciowej NFZ**

tj.:

- 1) posiadamy uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień;
- 2) posiadamy niezbędną wiedzę i doświadczenie oraz dysponujemy potencjałem technicznym i osobami zdolnymi do wykonania zamówienia;
- 3) znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia;
- 4) nie podlegamy wykluczeniu z postępowania o udzielenie zamówienia.

.....  
**podpis i pieczęć Wykonawcy \***

\* w przypadku Wykonawców występujących wspólnie podpisuje Pełnomocnik lub wszyscy Wykonawcy

**Oświadczenie w sprawie oferowanego przedmiotu zamówienia**

Nazwa Wykonawcy.....

Adres Wykonawcy: .....

l.p.	URZĄDZENIE	<b>NAZWA URZĄDZENIA</b> <b>NAZWA PRODUCENTA</b> <b>MODEL</b> <b>(dodatkowe informacje umożliwiające identyfikację urządzeń)</b>
1	URZĄDZENIE SIECIOWE TYP I	
	Specjalizowane przełączniki sieciowe agregujące usługi	
2	URZĄDZENIE SIECIOWE TYP II	
	Specjalizowane moduły z funkcjonalnością zapory sieciowej	
	Specjalizowane moduły z funkcjonalnością równoważenia obciążenia	
	Specjalizowane moduły z interfejsami GigabitEthernet	
3	URZĄDZENIE SIECIOWE TYP III	
	Specjalizowane przełączniki sieciowe do obsługi węzłów Internetowych	
4	URZĄDZENIE SIECIOWE TYP IV	
	Specjalizowany router Internetowy	
5	URZĄDZENIE SIECIOWE TYP V	
	Specjalizowany router rdzeniowy	
6	URZĄDZENIE SIECIOWE TYP VI	
	Specjalizowany urządzenie typu firewall	
7	URZĄDZENIE SIECIOWE TYP VII	
	Specjalizowany moduł typu ips	

.....  
**podpis i pieczęć Wykonawcy**

pieczęć Wykonawcy

....., dnia .....

**WYKAZ WYKONANYCH DOSTAW**

Należy podać: co najmniej 2 dostawy wykonane w okresie ostatnich trzech lat przed dniem wszczęcia postępowania o udzielenie zamówienia, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, odpowiadających swoim rodzajem dostawie stanowiącej przedmiot zamówienia, tj. , dostawie sprzętu sieciowego, o wartości przekraczającej 2.000.000,00 zł brutto każda, z podaniem ich wartości, przedmiotu, dat wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane należycie.

Przez wykonanie dostaw należy rozumieć ich ostateczny odbiór. W wykazie należy wpisać dostawy, których odbiór ostateczny miał miejsce w wyżej wym. latach.

Datę wykonania zamówienia należy określić jako dzień, miesiąc i rok.

Przedmiot	Wartość zamówienia /brutto/ w PLN	Data wykonania /dzień, miesiąc i rok/	Nazwa i adres odbiorcy
1	2	3	4

Uwaga ! Wszystkie wartości należy podać w PLN.

**Wykonawcy zobowiązani są załączyć do oferty dokumenty potwierdzające, że wskazane w wykazie dostawy zostały wykonane należycie.**

.....  
Podpis i pieczęć Wykonawcy

Nazwa Wykonawcy: .....

Adres Wykonawca: .....

**OŚWIADCZENIE O POSZCZEGÓLNYCH CENACH JEDNOSTKOWYCH**

Lp.	Oznaczenie	Cena jednostkowa netto (zł)	Zapotrzebowanie Zamawiającego	Cena łączna netto (zł)	Podatek VAT (zł)	Cena łączna brutto (zł)
	URZĄDZENIE SIECIOWE TYP I					
	Specjalizowane przełączniki sieciowe agregujące usługi		2 komplety			
	URZĄDZENIE SIECIOWE TYP II					
	Specjalizowane moduły z funkcjonalnością zapory sieciowej		2 komplety			
	Specjalizowane moduły z funkcjonalnością równoważenia obciążenia		2 komplety			
	Specjalizowane moduły z interfejsami GigabitEthernet		2 komplety			
	URZĄDZENIE SIECIOWE TYP III					
	Specjalizowane przełączniki sieciowe do obsługi węzłów Internetowych		2 komplety			
	URZĄDZENIE SIECIOWE TYP IV					
	Specjalizowany router Internetowy		1 komplet			
	URZĄDZENIE SIECIOWE TYP V					
	Specjalizowany router rdzeniowy		4 komplety			
	URZĄDZENIE SIECIOWE TYP VI					
	Specjalizowany urządzenie typu firewall		2 komplety			
	URZĄDZENIE SIECIOWE TYP VII					
	Specjalizowany moduły typu ips		2 komplety			
			<b>RAZEM</b>			

.....  
podpis i pieczęć Wykonawcy