Znak sprawy AZP – 2611 - 29/08

pieczęć Zamawiającego

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 z późn. zm.), zwanej dalej „ustawą".

INFORMACJE OGÓLNE

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

Nazwa nadana zamówieniu przez Zamawiającego: **dostawa zespołu urządzeń dla systemu redundantnych węzłów sieci rozległej.**

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 wykazu wykonanych dostaw (załącznik nr 5),
6) formularz wykazu osób, które będą wykonywać zamówienie (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 dla systemu redundantnych węzłów sieci rozległej WAN w Centrali NFZ w Warszawie oraz w Oddziałach Wojewódzkich. W ramach zamówienia Wykonawca będzie zobowiązany do dostawy komponentów systemu, przygotowania projektu technicznego obejmującego szczegóły implementacyjne rozwiązań i świadczenia powykonawczej asysty technicznej zgodnie z załącznikiem nr 1 do Specyfikacji.
Miejsce realizacji zamówienia: siedziba Zamawiającego, inne miejsce na terenie m.st. Warszawy wskazane przez Zamawiającego oraz Oddziały Wojewódzkie zgodnie z załącznikiem nr 1 do Specyfikacji.
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 zakresie:
- dostawy komponentów systemu, przygotowania projektu technicznego obejmującego szczegóły implementacyjne rozwiązań **- w terminie 8 tygodni od daty zawarcia umowy,**
- świadczenia powykonawczej asysty technicznej **- w terminie 6 miesięcy od daty dostawy zespołu urządzeń systemu**, potwierdzonego protokołem odbioru.

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 urządzenia 36 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. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych telefonicznie w godzinach pracy Zamawiającego, oraz przez całą dobę - faxem, e-mailem lub WWW; Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań.
W przypadku urządzeń, dla których jest wymagany dłuższy czas na usunięcie awarii, Zamawiający dopuszcza podstawienie na ten czas sprzętu o nie gorszych parametrach funkcjonalnych. Usunięcie awarii w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki.
Przez cały okres trwania gwarancji:
1) Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w godzinach pracy Zamawiającego w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń.
2) Zamawiający uzyska dostęp do części chronionych stron internetowych producentów urządzeń (min. 18 kont dostępowych), umożliwiający:

- pobieranie nowych wersji oprogramowania,
- dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
- dostęp do pomocy technicznej producentów.

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 zastrzega w Specyfikacji części zamówienia, która 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
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, od poniedziałku do piątku w godz. 09:00-15:00,
2) w sprawach dotyczących przedmiotu zamówienia:
   - **Krzysztof Daniszewski** w budynku przy ul. Grójeckiej 186, od poniedziałku do piątku w godz. 09:00-15:00,

2.3. Udzielanie wyjaśnień oraz zmiany w treści Specyfikacji

Zgodnie z art. 38 ustawy, Zamawiający jest obowiązany niezwłocznie udzielić wyjaśnień treści Specyfikacji, 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 uzasadnionych przypadkach może przed upływem terminu składania ofert zmienić treść Specyfikacji. Dokonaną zmianę Specyfikacji Zamawiający przekazuje niezwłocznie wszystkim wykonawcom, którym przekazano Specyfikację, a jeżeli Specyfikacja jest udostępniana na stronie internetowej, zamieszcza ją 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 14.01.2009 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. 4a i 5 ustawy.

2.5. Zwrot oraz przepadek wadium przetargowego

Zamawiający niezwłocznie zwróci oferentom wadium, jeżeli zajdzie jedna z poniższych przesłanek:
1) upłynie termin 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. 4a ustawy, Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 ustawy, nie złożył dokumentów lub oświadczeń, o których mowa w art. 25 ust. 1 ustawy lub pełnomocnictw, chyba że udowodni, że wynika to z przyczyn nieleżących po jego stronie.
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 14.01.2009 r. do godz. 10:00.**
Sporządzoną ofertę należy opakować w kopertę oznaczoną dokładną nazwą i adresem Wykonawcy oraz napisem „DOSTAWA ZESPOŁU URZĄDZEŃ DLA SYSTEMU REDUNDANTNYCH WĘZŁÓW SIECI ROZLEGŁEJ. OTWORZYĆ W DNIU 14.01.2009 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 DLA SYSTEMU REDUNDANTNYCH WĘZŁÓW SIECI ROZLEGŁEJ. 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.
Wykonawca samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni. Przedłużenie okresu związania ofertą jest dopuszczalne tylko z jednoczesnym przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

2.8. Otwarcie ofert

Z zawartością ofert nie można zapoznać się przed upływem terminu otwarcia ofert.
Otwarcie ofert odbędzie się **w dniu 14.01.2009 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 jakichkolwiek zmiany w jej treści.
Zgodnie z art. 87 ust. 2 ustawy, Zamawiający poprawi:
1) oczywiste omyłki pisarskie,
2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
3) inne omyłki polegające na niezgodności oferty ze specyfikacją, niepowodujące istotnych zmian w treści oferty

o czym niezwłocznie zawiadomi Wykonawcę, którego oferta została poprawiona.
Zamawiający poprawi m.in. następujące omyłki:
- błędne obliczenie prawidłowo podanej w ofercie stawki podatku od towaru i usług;
- błędne zsumowanie w ofercie wartości netto i kwoty podatku od towaru i usług.

Zamawiający nie poprawi omyłki polegającej na zastosowaniu przy obliczaniu ceny błędnej stawki podatku od towarów i usług.
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 pełnomocnictw 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 oraz spełnianie przez oferowane dostawy wymagań określonych przez Zamawiającego, nie później niż w dniu wyznaczonym przez Zamawiającego jako termin uzupełnienia oświadczeń lub dokumentów**.** Zamawiający wzywa także, w wyznaczonym przez Zamawiającego jako termin uzupełnień pełnomocnictw, oświadczeń lub dokumentów.
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 których mowa w ust. 1 pkt 1, na stronie internetowej (www.nfz.gov.pl) oraz w miejscu publicznie 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

Zamawiający zawrze umowę w terminie nie krótszym niż 10 dni od dnia przekazania zawiadomienia o wyborze oferty. Zamawiający może zawrzeć umowę przed upływem wskazanego terminu, jeżeli w postępowaniu o udzielenie zamówienia została złożona tylko jedna oferta.

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 powinna 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 poświadczonej „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:

1) spełniają warunki udziału w postępowaniu określone w art. 22 ust. 1 ustawy, tj.:
   a) posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień;
   b) posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia lub przedstawią pisemne zobowiązanie innych podmiotów do udostępnienia potencjału technicznego i osób zdolnych do wykonania zamówienia;
   c) znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia;
   d) nie podlegają wykluczeniu z postępowania o udzielenie zamówienia.
2) nie podlegają wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 24 ustawy,
3) złożą oświadczenie o spełnianiu warunków udziału w postępowaniu zgodnie z załącznikiem do Specyfikacji,
4) 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. co najmniej 1 dostawę polegającą na dostawie routerów i/lub urządzeń zapory ogniowej (firewall) oraz co najmniej 1 dostawię polegającą na dostawie urządzeń służących ochronie stron www i/lub poczty elektronicznej o łącznej wartości (dla obu dostaw) co najmniej 5 mln. zł brutto (słownie: pięć milionów złotych, z podaniem ich wartości, przedmiotu, daty wykonania i odbiorców oraz załączenia dokumentów potwierdzających, że dostawy te zostały wykonane należycie,
5) dysponują lub będą dysponować co najmniej 4 osobami, które będą uczestniczyć w przygotowaniu projektu technicznego oraz będą świadczyć usługę asysty technicznej, które posiadają najwyższy stopień specjalizacji potwierdzony certyfikatami w zakresie technologii sieciowych WAN/LAN, potwierdzony/wydany przez producenta/ów urządzeń sieciowych, które Wykonawca zaoferuje Zamawiającemu oraz co najmniej dwie osoby z wymienionych wyżej, które posiadają poświadczenie bezpieczeństwa upoważniające je do dostępu do informacji niejawnych, stanowiących tajemnice służbową o klauzuli minimum "poufne" oraz zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych wydanych na podstawie ustawy o ochronie informacji niejawnych z dnia 22 stycznia 1999 roku (Dz.U. z 2005 r., Nr 196, poz. 1631) wraz z dokumentami potwierdzającymi uprawnienia tych osób,
6) wykażą się posiadaniem środków finansowych lub zdolności kredytowej w wysokości nie mniejszej niż 2.000.000,00 zł.

W celu potwierdzenia, że Wykonawca 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. – 3.5.7. Specyfikacji.

W celu potwierdzenia, że Wykonawca znajduje się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia musi przedstawić dokumenty wymienione w pkt 3.5.8. 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 oferowana cena za realizację zamówienia została przedstawiona 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.

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 spełnianiu przez oferowane urządzenia wymagań określających przedmiot zamówienia

Wykonawca jest obowiązany oświadczyć, że oferowane urządzenia wymagań określających przedmiot zamówienia przedstawione przez Zamawiającego wymagania określające 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 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.

3.3.6. Oświadczenie o akceptacji warunków gwarancji

Zamawiający wymaga, by Wykonawca udzielił na dostarczone urządzenia 36 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. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych telefonicznie w godzinach pracy Zamawiającego, oraz przez całą dobę - faxem, e-mailem lub WWW; Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań.
W przypadku urządzeń, dla których jest wymagany dłuższy czas na usunięcie awarii, Zamawiający dopuszcza podstawienie na ten czas sprzętu o nie gorszych parametrach funkcjonalnych. Usunięcie awarii w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki.
Przez cały okres trwania gwarancji:
1) Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w godzinach pracy Zamawiającego w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń.
2) Zamawiający uzyska dostęp do części chronionych stron internetowych producentów urządzeń (min. 18 kont dostępowych), umożliwiający:

- pobieranie nowych wersji oprogramowania,
- dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
- dostęp do pomocy technicznej producentów.

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. 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.

3.5. 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 potwierdzającymi, 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. co najmniej 1 dostawę polegającą na dostawie routerów i/lub urządzeń zapory ogniowej (firewall) oraz co najmniej 1 dostawę polegającą na dostawie urządzeń służących ochronie stron www i/lub poczty elektronicznej o łącznej wartości (dla obu dostaw) co najmniej 5 mln. zł brutto (słownie: pięć milionów złotych) 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. Wykaz osób, które będą wykonywać zamówienie wraz z udokumentowanymi aktualnymi upoważnieniami dostępu do informacji niejawnych oznaczonych klauzulą „Poufne”

Wykonawca powinien przedstawić pisemny wykaz osób, którymi dysponuje lub będzie dysponował i które będą uczestniczyć w wykonywaniu zamówienia /zgodnie z załącznikiem nr 5/, co najmniej 4 osób, które będą uczestniczyć w przygotowaniu projektu technicznego oraz będą świadczyć usługę asysty technicznej, które posiadają najwyższy stopień specjalizacji potwierdzony certyfikatami w zakresie technologii sieciowych WAN/LAN, potwierdzony/wydany przez producenta/ów urządzeń sieciowych, które Wykonawca zaoferuje Zamawiającemu oraz co najmniej dwie osoby z wymienionych wyżej, które posiadają poświadczenie bezpieczeństwa upoważniające je do dostępu do informacji niejawnych, stanowiących tajemnice służbową o klauzuli minimum "poufne" oraz zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych wydanych na podstawie ustawy o ochronie informacji niejawnych z dnia 22 stycznia 1999 roku (Dz.U. z 2005 r., Nr 196, poz. 1631). **UWAGA – należy załączyć dokumenty potwierdzające uprawnienia tych osób aktualne na dzień otwarcia ofert oraz przez cały okres trwania umowy.**
Wykonawca jest zobowiązany złożyć pisemne zobowiązanie innych podmiotów do udostępnienia osób zdolnych do wykonania zamówienia o ile sytuacja ta go dotyczy.
W przypadku składania oferty przez podmioty występujące wspólnie, wyżej wymieniony warunek może zostać spełniony łącznie.

3.5.8. 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.

3.5.9. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczpospolitej Polskiej zamiast dokumentu:

1) o którym mowa w pkt 3.5.2, 3.5.3. i 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,
2) 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 wyrządzili szkodę, nie wykonując zamówienia lub wykonując je nienależycie, jeżeli szkoda ta została stwierdzona prawomocnym orzeczeniem sądu wydanym w okresie 3 lat przed wszczęciem postępowania,
   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 ustawy.
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 z zastrzeżeniem art. 87 ust. 2 pkt 3 ustawy,
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 błędy w obliczaniu ceny,
7) wykonawca w terminie 3 dni od dnia doręczenia zawiadomienia nie zgodził się na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3 ustawy,
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 (100% wagi oceny)

Z tytułu niniejszego kryterium maksymalna liczba 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:

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

Gdzie: **m** – oznacza kolejną badaną ofertę,
K_m – oznacza **wynik oceny kolejnej badanej oferty w zakresie kryterium ceny (kosztu)**,
C_n – oznacza **najkorzystniejszą (najniższą) cenę brutto badanej oferty,**
C_m – oznacza **cenę brutto kolejnej badanej oferty.**

4.3.2. Ocena łączna

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

$$O_l = K_m \times X \times W_C$$

Gdzie: **O_l**– 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 liczbę 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, w przypadku wystąpienia przesłanek określonych w art. 93 ust. 1 ustawy.
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

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

I. Opis przedmiotu zamówienia.

1. Przedmiotem zamówienia jest dostawa zespołu urządzeń dla systemu Redundantnych węzłów sieci rozległej WAN w Centrali NFZ w Warszawie, w miejscu na terenie m.st. Warszawy wskazanym przez Zamawiającego oraz w Oddziałach Wojewódzkich.

   Lista lokalizacji, w których będzie uruchomiony system:
   1) Centrala NFZ Warszawa, ul. Grójecka 186,
   2) OW NFZ Warszawa, ul. Chałubińskiego 8,
   3) OW NFZ Poznań, ul. Grunwaldzka 158,
   4) OW NFZ Olsztyn, ul. Żołnierska 16,
   5) OW NFZ Kielce, ul. Jana Pawła II 9,
   6) OW NFZ Katowice, ul. Kossutha 13,
   7) OW NFZ Gdańsk, ul. Podwale Staromiejskie 69,
   8) OW NFZ Białystok, ul. Pałacowa 3,
   9) OW NFZ Rzeszów, ul. Zamkowa 8,
   10) OW NFZ Opole, ul. Głogowska 37,
   11) OW NFZ Szczecin, ul. Arkońska 45,
   12) OW NFZ Kraków, ul. Józefa 21,
   13) OW NFZ Łódź, ul. Kopcińskiego 58,
   14) OW NFZ Zielona Góra, ul. Podgórna 9B,
   15) OW NFZ Lublin, ul. Szkolna 16,
   16) OW NFZ Bydgoszcz, ul. Słowackiego 3,
   17) OW NFZ Wrocław, ul. Joannitów 6,

2. W ramach zamówienia Wykonawca będzie zobowiązany do:
   1) dostawy komponentów systemu
   2) przygotowania projektu technicznego obejmującego szczegóły implementacyjne rozwiązań
   3) świadczenia powykonawczej asysty technicznej

3. Całość dostarczanego sprzętu musi być fabrycznie nowa, nieużywana we wcześniejszych projektach.

4. 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.

II. Szczegółowe wymagania techniczne

1. W skład systemu Redundantnych węzłów sieci rozległej WAN wchodzą następujące elementy:
   1) Routery dostępowe dla Centrali NFZ (pkt. 1.1) – 3 sztuki.
   2) Routery dostępowe dla Oddziałów Wojewódzkich (pkt. 1.2) – 16 sztuk.
   3) Urządzenia ochrony styku z siecią WAN (pkt. 1.3) – 32 sztuki.
   4) Przełączniki do obsługi węzła styku z siecią WAN (pkt. 1.4) – 32 sztuki.
   5) Urządzenia systemu ochrony ruchu Web dla Centrali NFZ (pkt. 1.5) – 1 komplet.
   6) Urządzenia systemu ochrony ruchu Web dla Oddziałów Wojewódzkich (pkt. 1.6) – 16 kompletów.
   7) Urządzenia systemu ochrony ruchu pocztowego (pkt. 1.7) – 16 kompletów.
   8) System zarządzania ochroną aplikacyjną i raportowania (pkt. 1.8) – 1 komplet.
   9) Rozbudowa systemu zarządzania elementami bezpieczeństwa (pkt. 1.9) – 1 sztuki.

1.1. Routery dostępowe dla Centrali NFZ

1) urządzenie modularne posiadające możliwość instalacji co najmniej sześciu modułów interfejsowych,
2) wyposażone w trzy interfejsy GigabitEthernet Dual-physical z możliwością programowego wyboru styku miedzianego 10/100/1000 lub światłowodowego (GBIC, SFP lub równoważne),
3) wyposażone w redundantne zasilacze AC 230V
4) wydajność urządzenia nie mniejsza niż 2Mpps (pakiety 64B),
5) co najmniej 1GB DRAM oraz min. 64MB pamięci Flash – ilość pamięci nie ulotnej musi pozwalać na przechowywanie dwóch niezależnych obrazów oprogramowania systemowego
6) możliwość instalacji następujących portów
    a) ATM (OC-3, E3)
    b) PoS (OC-3)
    c) HSSI
    d) Fast/Gigabit Ethernet
    e) szeregowe E1, E3
7) obsługa ochrony kryptograficznej ruchu:
    a) sprzętowe wsparcie szyfrowania – wydajność nie mniejsza niż 900Mbps (pakiety 1400B, IPSec AES256)
    b) wsparcie dla standardów IPSec/IKE: RFC 2401-2411, 2451
    c) autoryzacja RSA i DH
    d) obsługa funkcji hash SHA i MD5
    e) obsługa min. 1000 tuneli IPSec
    f) obsługa mechanizmu dynamicznego zestawiania tuneli IPSec między oddziałami w topologii hub-and-spoke (permanentnie zestawione tunele z hub-em, dynamicznie zestawiane tunele spoke-spoke przy pojawieniu się transmisji)
    g) obsługa szyfrowania beztunelowego w oparciu o GDOI (RFC 3547)
8) obsługa tzw.routing między sieciami VLAN w oparciu o trunking 802.1Q
9) możliwość tzw. tunelowania przesyłanych danych – obsługa minimum protokołu GRE.
10) routing protokołu IPv4 i IPv6 (protokoły dynamicznego routingu OSPF, BGPv4, RIPv1v2) oraz VRRP/HSRP, Policy-Based Routing (PBR), GRE
11) obsługa MPLS (LDP, TE)
12) możliwość wirtualizacji tablic routingu i przełączania urządzenia (kreowania niezależnych przestrzeni adresowych)
13) wsparcie dla PPP, Frame-Relay, Frame-Relay switching, HDLC, ISDN
14) funkcjonalność stateful firewall
15) gwarancja jakości usług za pomocą mechanizmów Low-Latency Queuing (LLQ), Class-Based Weighted Fair Queuing (CBWFQ), Policing, Marking, Shaping, Committed Access Rate (CAR), Generic Traffic Shaping (GTS), Frame Relay Traffic Shaping (FRTS), Priority Queueing (PQ) , WRED
16) funkcja access-list, PAP/CHAP, NAT
17) współpraca z RADIUS, TACACS+
18) Web Cache Communication Protocol (WCCPv1, WCCPv2)
19) obsługa multicast routing PIMv1v2, IGMPv3 (IPv4 I IPv6)
20) obsługa SNMPv3, SSHv2, Netflow/J-Flow/S-Flow
21) możliwość rozbudowy o routing IPX
22) plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi być możliwy do edycji w trybie off-line. Konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieu lotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
23) możliwość montażu w szafie 19”

1.2. Routery dostępowe dla Oddziałów Wojewódzkich

1) urządzenie modularne posiadające możliwość instalacji różnorodnych interfejsów i modułów, co najmniej:
    a) interfejsy Ethernet (FE, GE)
    b) interfejsy szeregowe (V.35, EIA/TIA-449, X.21)
    c) interfejsy ADSL
    d) interfejsy SHDSL
    e) modemy V.90
    f) interfejsy ISDN BRI (styk S/T)
    g) interfejsy ATM
2) wyposażone w co najmniej 2 interfejsy GE 10/100/1000 (jeden z możliwością pracy jako optyczny ze stykiem definiowanym przez konwertery typu SFP, GBIC lub równoważne)

3) wyposażone w zintegrowany wewnętrzny moduł sprzętowego wsparcia szyfracji DES, 3DES, AES128, AES192, AES256 o wydajności min. 150 Mbps
4) wyposażony w pamięć co najmniej 64 MB pamięci Flash i 256 MB pamięci DRAM
5) wbudowane redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V,
6) funkcje bezpieczeństwa:
    a) szyfrowania połączeń 3DES oraz AES z obsługą QoS:
        - IPSEC
        - obsługa mechanizmu dynamicznego zestawiania tuneli IPSec między oddziałami w topologii hub-and-spoke (permanentnie zestawione tunele z hub-em, dynamicznie zestawiane tunele spoke-spoke przy pojawieniu się transmisji)
        - szyfrowanie beztunelowe w oparciu o GDOI (RFC 3547)
    b) firewall:
        - kontrola ruchu stateful inspection
        - monitorowanie warstw 4-7 modelu ISO/OSI (kontrola protokołów – min. HTTP(s). (E)SMTP, POP3, FTP, DNS, SSH, ICMP, TCP, UDP)
        - obsługa wielu stref DMZ
        - ochrona przed atakami DoS (TCP Intercept, TCP SYN, Flood)
        - praca w trybie routed (L3) oraz transparent (L2)
        - wydajność 300 Mbps
    c) możliwość uruchomienia oprogramowania współpracującego z dostępnymi systemami kontroli kondycji bezpieczeństwa hostów. Np. Network Access Protection, Network Admission Control etc,
    d) możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS albo TACACS+.
    e) weryfikacja źródła danych (uRPF)
    f) klasyfikacja ruchu w oparciu o sygnatury aplikacyjne (np. rozróżnianie ruchu HTTP i P2P na portcie 80/TCP)
    g) funkcje opisane w tym punkcie muszą działać jednocześnie (dopuszczalna degradacja wydajności).
7) funkcje QoS:
    a) klasyfikacja ruchu w oparciu o adresy IP, porty TCP/UDP, DSCP, IP Precedence i sygnatury aplikacyjne
    b) kolejkowanie z obsługą kolejki priorytetowej
    c) obsługa ograniczania (policing) i kształtowania (shaping) ruchu
8) zarządzalne przez SNMPv3, SSHv2, konsolę szeregową, HTTPS (oczekiwane są narzędzia dodatkowe w postaci kreatorów połączeń, etc.)
9) porty dedykowane dla zarządzania: port konsoli, port asynchroniczny dla przyłączenia modemu.
10) protokoły/mechanizmy:
    a) routing IPv4 RIPv2, OSPF, BGPv4,
    b) routing IPv6 RIPng, OSPFv3, MP-BGP,
    c) DHCP (klient, serwer),
    d) VPN (IPSec), szyfrowanie beztunelowe zgodne z GDOI (RFC 3547)
    e) Policy Based Routing (PBR),
    f) Frame Relay, PPP,
    g) GRE,
    h) HSRP lub VRRP,
    i) IGMPv3,
    j) 802.1Q na portach Ethernet – możliwość zdefiniowania oddzielnych stref bezpieczeństwa na poszczególnych VLANach
    k) NAT, NAT-PT,
    l) NetFlow, JFlow, sFlow lub równoważny,
    m) RSVP,
    n) WCCP (v2),
    o) PIM (PIM-DM, PIM-SM, SSM), IGMPv3
    p) funkcjonalność bramy głosowej H.323, SIP, zasoby DSP pozwalające na obsługę min. 64 strumieni G.711
11) urządzenie musi umożliwiać rozbudowę funkcjonalności o funkcjonalność wirtualnej centrali abonenckiej dla min. 100 telefonów IP
12) plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nie ulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
13) obudowa wykonana z metalu - ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej
14) możliwość montażu w szafie 19’’.

1.3. Urządzenia ochrony styku z siecią WAN

1) urządzenie modularne pozwalające na uzyskanie funkcji firewall, VPN (sprzętowe wsparcie szyfracji), sondy IPS, kontroli ruchu
2) wyposażone w co najmniej cztery interfejsy Gigabit Ethernet 10/100/1000
3) wyposażone w co najmniej jeden interfejs dla zarządzania pozapasmowego (OOB)
4) wyposażone w moduł sprzętowego wsparcia szyfracji DES i AES
5) minimum dwa porty dedykowane dla zarządzania: port konsoli, port asynchroniczny dla przyłączenia modemu
6) co najmniej jeden port USB (tokeny, certyfikaty etc.)
7) co najmniej 64MB pamięci Flash
8) co najmniej 512MB pamięci DRAM
9) dodatkowy slot pozwalający na wykorzystanie modułów funkcjonalnych zwiększających standardową funkcjonalność urządzenia, a w szczególności
    a) moduł umożliwiający osiągniecie pełnej funkcjonalności systemu IPS (Intrusion Prevention System)
    b) moduł umożliwiający osiągniecie funkcjonalności ochrony antywirusowej, antyspyware, antyspamowej, filtrowania i blokowania odwołań do niepożądanych adresów URL oraz filtrowania zawartości poczty elektronicznej e-mail
    c) moduł zwiększający ilość obsługiwanych interfejsów o co najmniej 4 porty Gigabit Ethernet
10) zasilacz umożliwiający zasilanie prądem przemiennym 230V
11) wydajność
    a) co najmniej 450 Mbps ruchu poddawanego inspekcji przez mechanizmy ściany ogniowej
    b) co najmniej 200 Mbps ruchu szyfrowanego
    c) terminowanie co najmniej 500 jednoczesnych sesji VPN
    d) możliwość terminowania jednocześnie 500 sesji WebVPN
    e) obsługa co najmniej 250.000 jednoczesnych sesji/połączeń z prędkością 10.000 połączeń na sekundę
    f) obsługa min. 2 wirtualnych instancji firewall z możliwością rozbudowy do 20-tu
12) oprogramowanie – funkcjonalność:
    a) ściana ogniowa śledząca stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
    b) bez ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
    c) dostarczone wraz z dedykowanym oprogramowaniem klienta VPN. Oprogramowanie musi mieć możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows, Solaris i Linux, a także komputerach Mac. Oprogramowanie musi umożliwiać zestawienie do urządzenia stanowiącego przedmiot postępowania 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.
    d) możliwość operowania jako transparentna ściana ogniowa warstwy drugiej ISO OSI
    e) możliwość routingu pakietów zgodnie z protokołami RIP, OSPF
    f) mechanizmy związane z obsługą ruchu multicast
    g) protokół NTP
    h) obsługa IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode
    i) współpraca z serwerami CA
    j) funkcjonalność Network Address Translation (NAT)
    k) mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w modelu active/standby oraz active/active
    l) funkcjonalność stateful Failover dla ruchu VPN
    m) mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
        - Hypertext Transfer Protocol (HTTP),
        - File Transfer Protocol (FTP),
        - Extended Simple Mail Transfer Protocol (ESMTP),
        - Domain Name System (DNS),
        - Simple Network Management Protocol (SNMP),
        - Internet Control Message Protocol (ICMP),
        - SQL*Net,
        - Network File System (NFS),
        - H.323 (wersje 1-4),
        - Session Initiation Protocol (SIP),
        - Real-Time Streaming Protocol (RTSP),
        - Lightweight Directory Access Protocol (LDAP), Internet Locator Service (ILS),
        - Sun Remote Procedure Call (RPC)
    n) inspekcja ruchu głosowego w zakresie protokołów H.323, SIP
    o) możliwość blokowania aplikacji tunelowanych z użyciem portu 80 w tym:

- blokowanie komunikatorów internetowych w tym AOL Instant Messenger, Microsoft Messenger, Yahoo Messenger
- blokowanie aplikacji typu peer-to-peer w tym KaZaA i Gnutella
- zapobieganie stosowaniu aplikacji typu GoToMyPC

p) obsługa protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP w tym: AUTH, DATA, EHLO, ETRN, HELO, HELP, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SEND, SOML, VRFY
q) możliwość inspekcji protokołów HTTP oraz FTP na nie standartowych portach
r) wsparcie stosu protokołów IPv6 w tym:
- dla list kontroli dostępu dla IPv6
- inspekcji aplikacyjnej co najmniej dla protokołów: HTTP, FTP, SMTP, ICMP

s) mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu
t) współpraca z serwerami autoryzacji (RADIUS, TACACS+ lub równoważny) w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik, o wielkości przekraczającej 4KB

13) zarządzanie i konfiguracja
a) możliwość eksportu informacji przez syslog
b) możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu RADIUS, TACACS+ lub równoważnego
c) konfigurowalne przez CLI oraz interfejs graficzny (oczekiwane są narzędzia dodatkowe w postaci kreatorów połączeń, etc.)
d) dostęp do urządzenia przez SSHv1 i SSHv2
e) obsługa funkcji SCP
f) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją
g) urządzenie musi umożliwiać jednoczesne przechowywanie w pamięci nie ulotnej co najmniej 3 niezależnych konfiguracji urządzenia
h) możliwość konfiguracji i monitorowania przez posiadane przez NFZ oprogramowanie Cisco Security Manager PRO

14) obudowa wykonana z metalu, nie dopuszcza się stosowania urządzeń w obudowie plastikowej
15) możliwość instalacji w rack 19”
16) certyfikacje branżowe
a) FIPS 140-2 Level 2
b) Common Criteria EAL4+

17) funkcjonalność IPS:
a) praca w trybach in-line oraz promiscous
b) identyfikacja, klasyfikacja i powstrzymywanie ruchu zagrażającego bezpieczeństwu organizacji w tym:
- robaki sieciowe
- adware
- spyware
- wirusy sieciowe
- nadużycia aplikacyjne

c) wykrywanie i powstrzymywanie działań wskazujących na przekroczenie polityk bezpieczeństwa w tym:
- działania z wykorzystaniem komunikatorów internetowych
- działania z wykorzystaniem aplikacji peer-to-peer
- filtracja w oparciu o typy MIME

d) wykrywanie robaków internetowych oraz wirusów sieciowych w szczególności z wykorzystaniem analizy anomalii ruchu w monitorowanych segmentach sieci
e) monitoring ruchu IPv6
f) wykrywanie nadużyć w pakietach IP-in-IP
g) analiza kontekstowa – wykrywanie ataków ukryte w wielu następujących po sobie pakietach
h) inspekcja aplikacyjna co najmniej dla protokołów: FTP, Simple Mail Transfer Protocol (SMTP), HTTP, SMB, Domain Name System (DNS), remote procedure call (RPC), NetBIOS, Network News Transfer Protocol (NNTP), generic routing encapsulation (GRE), Telnet.
i) wykrywanie anomalii związanych z ruchem w monitorowanym segmencie sieci
j) wykrywanie anomalii związanych z protokołami (w szczególności odstępstw od normalnych zachowań zdefiniowanych przez odpowiednie dokumenty RFC)
k) wykrywanie ataków związanych z działaniami w warstwie 2 modelu OSI w szczególności ataków na ARP oraz ataków Man-in-the-middle w środowisku przełączanym
l) mechanizmy zapobiegające „omijaniu” systemów IPS w szczególności:
m) normalizacji ruchu
n) scalania strumieni TCP
o) deobfuscation
p) scalające (defragmentujące) dla pakietów IP

- mechanizmy dla OS Fingerprinting – identyfikacji systemu operacyjnego hosta dla celów przyszłej oceny znaczenia ataku
- definiowanie kryteriów oceny znaczenia ataku w oparciu o co najmniej następujące parametry:

q) ważność zdarzenia (potencjalne zagrożenie jeżeli ruch zostanie dopuszczony – nie będzie filtrowany)
r) wartość zasobu (określenie krytyczności atakowanego urządzenia dla organizacji)
s) potencjalna skuteczność ataku (wstępne określenie czy atak mógł być skuteczny)

- wskazanie limitów na pasmo dla określonych aplikacji celem zapobiegania wykorzystaniu całego pasma przez atakującego
- wydajność co najmniej 350 Mbps dla ruchu poddawanego inspecji IPS
- zarządzana przez linię komend – CLI – z wykorzystaniem protokołu SSH
- protokół SDEE (lub równoważny) do komunikacji ze stacją zarządzającą

1.4. Przełączniki do obsługi węzła styku z siecią WAN

1) 24 interfejsy GE w standardzie 10/100/1000BaseT
2) 2 gniazda na interfejsy 10GE z możliwością pracy jako podwójne porty GE (dostarczone odpowiednie moduły lub adaptery) ze stykiem definiowanym przez X2, XenPak, SFP+, XFP, SFP, GBIC lub równoważne,
3) 2 interfejsy GE 1000BaseSX ze stykiem definiowanym przez interfejsy GBIC, SFP, mini-GBIC lub równoważne
4) możliwość łączenia urządzeń (min. 8 szt.) w jednorodnie zarządzane stosy (widziane z perspektywy interfejsów zarządzania CLI, GUI itp. jako pojedyncze urządzenie) – wydajność połączenia na poziomie min. 128 Gbps
5) automatyczne wykrywanie przeplotu (AutoMDIX) na portach 10/100/1000
6) matryca przełączająca o wydajności co najmniej 128 Gbps oraz przepustowość co najmniej 65 Mpps dla pakietów 64 bajtowych;
7) obsługa 4000 VLAN ID
8) mechanizmy zarządzania:
    a) dostęp do urządzenia przez konsolę szeregową, HTTPS, SSH i SNMPv3 (przez IPv4 i IPv6)
    b) obsługa Rapid STP (802.1r) i Multiple Instance STP (802.1w)
    c) obsługa trunku 802.1q na dowolnym porcie
    d) obsługa NTP
    e) diodowa sygnalizacja stanu urządzenia oraz poszczególnych portów
    f) mechanizm dystrybucji informacji o sieciach VLAN pomiędzy przełącznikami
    g) mechanizmy ochrony przełącznika przed atakami typu (D)DoS przez ograniczanie ruchu kierowanego do przełącznik
9) mechanizmy związane z zapewnieniem jakości usług w sieci:
    a) obsługa co najmniej czterech kolejek sprzętowych, wyjściowych dla różnego rodzaju ruchu
    b) mechanizm automatycznej konfiguracji portów do obsługi VoIP po wykryciu aparatu IP lub terminala wideo
    c) możliwość ograniczania pasma dostępnego na port (rate limiting) z granulacją co 8kbps
    d) klasyfikacja ruchu w oparciu o 802.1p, DSCP, adresy MAC, IP, porty UDP/TCP
10) mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a) możliwość autoryzacji użytkowników zgodna z 802.1x (z możliwością przypisania przez serwer autoryzacyjny sieci VLAN)
    b) możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
    c) możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports) z pozostawieniem możliwości komunikacji z portem nadrzędnym (designated port) lub funkcjonalność private VLAN
    d) monitorowanie zapytań i odpowiedzi DHCP (tzw. DHCP Snooping)
    e) możliwość tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika
    f) ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe
    g) obsługa list kontroli dostępu (ACL) z uwzględnieniem adresów MAC i IP, portów TCP/UDP bez spadku wydajności urządzenia
    h) min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend)
    i) współpraca z systemami kontroli dostępu do sieci typu NAC, NAP itp.
11) sprzętowa obsługa przełączania L3:
    a) IPv4: routing statyczny, RIPv2, OSPF, BGPv4
    b) obsługa VRRP, HSRP lub równoważnego protokołu
    c) możliwość definicji polityk routingowych (policy-based routing)
    d) możliwość wirtualizacji tablicy routingu – kreowania rozdzielnych przestrzeni adresowych
    e) możliwość rozbudowy funkcjonalności o IPv6: routing statyczny, RIPng, OSPFv3
12) obsługa ruchu multicast:
    a) PIM (PIM-DM, PIM-SM, SSM)

b) IGMPv3, IGMP snooping
13) obsługa grupowania portów w jeden kanał logiczny zgodnie z LACP (802.3ad)
14) plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line, tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nie ulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian
15) możliwość zastosowania zewnętrznego redundantnego zasilacza
16) możliwość montażu w szafie 19”
17) obudowa wykonana z metalu
18) poziom hałasu nie przekraczający 45dB (wg normy ISO 7779 w temp. 30oC)
19) min. 256MB pamięci DRAM oraz 64MB pamięci Flash
20) możliwość obsługi min. 8000 adresów MAC

1.5 Urządzenia systemu ochrony ruchu Web dla Centrali NFZ

1) Dostarczane rozwiązanie musi być dedykowaną, sprzętową platformą zawierającą:
   a) Mechanizmy filtrowania adresów WWW (ang.URL filtering).
   b) Mechanizmy filtrujące bazujące na ocenie reputacji adresów IP i nazw domen do których nawiązywane są połączenia HTTP z sieci wewnętrznej. Reputacja musi być ustalana za pomocą danych gromadzonych w globalnej bazie reputacji o parametrach opisanych w dalszej części Specyfikacji.
   c) Mechanizmy antywirusowe dla protokołu HTTP realizowane za pomocą dwóch niezależnych silników skanujących dostarczanych przez dwóch różnych producentów.
   d) Mechanizmy wykrywające podejrzane połączenia z sieci wewnętrznej, do adresów IP, bądź domen o złej reputacji, na wszystkich 65535 portach TCP/IP (wykrywanie tzw. Procesu „call-home”).
   e) Mechanizmy proxy, obejmujące deszyfrowanie i szyfrowanie sesji HTTPS w celu umożliwienia inspekcji ruchu nieszyfrowanego przez silniki antywirusowe.

2) Wszystkie wymienione powyżej funkcjonalności, muszą być wykonywane przez pojedyncze urządzenie z dedykowanym systemem operacyjnym, które można replikować w celu zapewnienia redundancji.
3) Rozwiązanie musi być dedykowanym serwerem proxy dla protokołu WWW działającym w trybie transparent proxy oraz forwarding proxy.
4) Rozwiązanie musi posiadać oddzielne fizyczne porty ethernetowe umożliwiające pasywne monitorowanie całego ruchu sieciowego, zarówno wchodzącego jak i wychodzącego z sieci chronionej.
5) Rozwiązanie powinno umożliwiać integrację z innymi serwerami proxy za pomocą obsługi nagłowka X-Forward-For w przypadku trybu pracy forward proxy oraz w trybie transparent proxy, za pomocą podszywania się (ang. IP spoofingu) pod oryginalne adresy IP użytkowników w celu ich przesyłania do innych serwerów proxy.
6) Rozwiązanie musi mieć możliwość integracji z infrastrukturą sieciową za pomocą protokołu WCCP.
7) Urządzenie musi być przystosowane do montażu w 19” szafie rackowej i mieć wysokość nie większa niż 2U.
8) Urządzenie musi posiadać redundantne zasilacze typu hot swap
9) Urządzenie musi posiadać dyski twarde o łącznej pojemności co najmniej 1.8TB typu hot swap pracujące w technologii RAID 1+0
10) Urządzenie musi posiadać co najmniej dwa, wielordzeniowe procesory.
11) Urządzenie musi posiadać co najmniej 8GB pamięci RAM
12) Urządzenie musi posiadać co najmniej 6 interfejsów typu GigabitEth
13) Urządzenie musi posiadać port szeregowy typu RS-232 (DB-9)
14) Konfiguracja urządzenia musi być przetrzymywana w pliku opartym o XML
15) Filtry URL powinny porównywać żądania wysyłane do internetu przez użytkowników z zasadami ustalonymi przez administratora w co najmniej 52 wstępnie zdefiniowanych kategoriach (bez ograniczeń ilościowych w przypadku własnych kategorii),
16) Baza stron WWW filtra URL musi zawierać co najmniej 20 milionów witryn (przyjmuje się, że odpowiada ponad 3 miliardom stron internetowych).
    Rozwiązanie musi posiadać dwustopniową ochronę przed złośliwym kodem przenoszonym w protokole HTTP (nie licząc Filtrowania URL).
    Pierwszą warstwą ochrony musi być sprawdzenie reputacji adresu IP bądź domeny, z którymi łączą się użytkownicy strefy chronionej, za pomocą danych zgromadzonych w globalnej bazie reputacji, która ustala reputacje w zakresie od -1 do 10, gdzie 10 jest wynikiem obarczonym najmniejszym zagrożeniem.
    Wynik ustalany powinien być na podstawie analizy co najmniej 50 różnych parametrów dotyczących adresów WWW między innymi, takich jak:

   a) • Czy strona znajduje się na tzw. internetowych „Czarnych listach” stron WWW
   b) • Czy strona znajduje się na tzw. Internetowych „Białych listach” stron WWW
   c) • W jakiej kategorii jest skatalogowana

d) • Jaką zawartość ma HTML
e) • Jak zachowuje się URL podczas połączenia
f) • Dane dotyczące globalnego ruchu sieciowego dotyczącego tej strony
g) • Dane podmiotu na który domena jest zarejestrowana
h) • Czy adres IP strony jest z puli adresów przydzielanych dynamicznie
i) • Czy adres nie znajduje się na liście serwerów na które się włamano
j) • Dane dotyczące właścicieli sieci, w których strona jest hostowana

17) Baza, która gromadzi dane do analizy musi zbierać informacje z co najmniej 120 000 źródeł na świecie i musi znajdować się w internecie nie krócej niż 5 lat.
18) Mechanizm filtrowania w zależności od reputacji powinien być wsparty drugą warstwą ochrony protokołu HTTP - dodatkowym mechanizmem skanowania zawartości tego protokołu za pomocą silników skanujących dostarczanych przez co najmniej dwóch różnych producentów, zintegrowanych na pojedynczym urządzeniu przy pomocy technologii wykorzystującej zaawansowane techniki analizy składni obiektów i streamingu w celu uniknięcia opóźnień i problemów ze skalowalnością przy skanowaniu przez np. dwa silniki. Mechanizm ten powinien chronić przed szerokim wachlarzem zagrożeń - od reklam, programów zmieniających stronę startową, ataków typu phishing czy pharming, aż do bardziej złośliwych ataków, takich jak rootkity, konie trojańskie, wirusy, robaki, monitory systemu i keyloggery.
19) Rozwiązanie musi posiadać dedykowany mechanizm skanujący wszystkie porty TCP/IP z prędkością transmisji, w celu wykrywania i blokowania próby wysyłania danych przez programy szpiegujące w sieci wewnętrznej (proces "phone-home"). Śledzenie wszystkich 65 535 portów sieciowych, ma mieć na celu zatrzymywanie złośliwego oprogramowania, które próbuje ominąć port 80 przy komunikacji z Internetem.
20) Rozwiązanie musi obsługiwać wyżej wymienione mechanizmy reputacji i filtrowania adresów URL przy podejmowaniu decyzji o deszyfrowaniu HTTPs. Na przykład, witryna banku może zostać pominięta przy deszyfrowaniu HTTPs, chyba że ocena jej reputacji internetowej jest niska. W takim przypadku połączenie HTTPs powinno być deszyfrowane w celu przeskanowania treści pod kątem złośliwego oprogramowania.
21) Proponowane rozwiązanie powinno mieć licencje dla 500 użytkowników w sieci korporacyjnej na okres co najmniej 3 lat, z możliwością przedłużenia, na kolejne lata. Licencje powinny zawierać wszystkie wyżej wymienione funkcjonalności.
22) Rozwiązanie powinno być w konfiguracji sprzętowej zapewniającej redundancję między pojedynczymi urządzeniami.
23) Rozwiązanie powinno posiadać dodatkową, zewnętrzną, dedykowaną platformę sprzętową do zcentralizowanego zarządzania konfiguracjami zaproponowanego kompletu o następujących parametrach:

    a) Możliwość centralnego zarządzania konfiguracjami do 50 urządzeń zabezpieczających protokół HTTP oraz HTTPS
    b) Urządzenie musi być przystosowane do montażu w 19” szafie rackowej i mieć wysokość nie większa niż 2U.
    c) Urządzenie musi posiadać redundantne, zasilacze o mocy 750 wat
    d) Urządzenie musi posiadać dyski twarde o łącznej pojemności co najmniej 3TB typu hot swap pracujące w technologii RAID 1+0
    e) Urządzenie musi posiadać co najmniej dwa, wielordzeniowe procesory.
    f) Urządzenie musi posiadać co najmniej 6 interfejsów typu GigabitEth
    g) Urządzenie musi posiadać port szeregowy typu RS-232 (DB-9)

1.6 Urządzenia systemu ochrony ruchu Web dla Oddziałów Wojewódzkich

1) Dostarczane rozwiązanie musi być dedykowaną, sprzętową platformą zawierającą:
    a) Mechanizmy filtrowania adresów WWW (ang.URL filtering).
    b) Mechanizmy filtrujące bazujące na ocenie reputacji adresów IP i nazw domen do których nawiązywane są połączenia HTTP z sieci wewnętrznej. Reputacja musi być ustalana za pomocą danych gromadzonych w globalnej bazie reputacji o parametrach opisanych w dalszej części Specyfikacji.
    c) Mechanizmy antywirusowe dla protokołu HTTP realizowane za pomocą dwóch niezależnych silników skanujących dostarczanych przez dwóch różnych producentów.
    d) Mechanizmy wykrywające podejrzane połączenia z sieci wewnętrznej, do adresów IP, bądź domen o złej reputacji, na wszystkich 65535 portach TCP/IP (wykrywanie tzw. Procesu „call-home”).
    e) Mechanizmy proxy, obejmujące deszyfrowanie i szyfrowanie sesji HTTPS w celu umożliwienia inspekcji ruchu nieszyfrowanego przez silniki antywirusowe.
2) Wszystkie wymienione powyżej funkcjonalności, muszą być wykonywane przez pojedyncze urządzenie z dedykowanym systemem operacyjnym, które można replikować w celu zapewnienia redundancji.
3) Rozwiązanie musi być dedykowanym serwerem proxy dla protokołu WWW działającym w trybie transparent proxy oraz forwarding proxy.
4) Rozwiązanie musi posiadać oddzielne fizyczne porty ethernetowe umożliwiające pasywne monitorowanie całego ruchu sieciowego, zarówno wchodzącego jak i wychodzącego z sieci chronionej.

5) Rozwiązanie powinno umożliwiać integrację z innymi serwerami proxy za pomocą obsługi nagłowka X-Forward-For w przypadku trybu pracy forward proxy oraz w trybie transparent proxy, za pomocą podszywania się (ang. IP spoofingu) pod oryginalne adresy IP użytkowników w celu ich przesyłania do innych serwerów proxy.
6) Rozwiązanie musi mieć możliwość integracji z infrastrukturą sieciową za pomocą protokołu WCCP.
7) Urządzenie musi być przystosowane do montażu w 19" szafie rackowej i mieć wysokość nie większa niż 2U.
8) Urządzenie musi posiadać redundantne, zasilacze o mocy 750 wat, typu hot swap
9) Urządzenie musi posiadać dyski twarde o łącznej pojemności co najmniej 1.2TB pracujące w technologii RAID 1+0
10) Urządzenie musi posiadać co najmniej jeden, wielordzeniowy procesor CPU
11) Urządzenie musi posiadać co najmniej 4GB pamięci RAM
12) Urządzenie musi posiadać co najmniej 6 interfejsów typu GigabitEth
13) Urządzenie musi posiadać port szeregowy typu RS-232 (DB-9)
14) Platforma musi bazować na dedykowanym systemie operacyjnym, opartym na systemie z rodziny BSD.
15) Konfiguracja urządzenia musi być przetrzymywana w pliku opartym o XML
16) Filtry URL powinny porównywać żądania wysyłane do internetu przez użytkowników z zasadami ustalonymi przez administratora w co najmniej 52 wstępnie zdefiniowanych kategoriach (bez ograniczeń ilościowych w przypadku własnych kategorii),
17) Baza stron WWW filtra URL musi zawierać co najmniej 20 milionów witryn (przyjmuje się, że odpowiada ponad 3 miliardom stron internetowych).
    Rozwiązanie musi posiadać dwustopniową ochronę przed złośliwym kodem przenoszonym w protokole HTTP (nie licząc Filtrowania URL).
    Pierwszą warstwą ochrony musi być sprawdzenie reputacji adresu IP bądź domeny, z którymi łączą się użytkownicy strefy chronionej, za pomocą danych zgromadzonych w globalnej bazie reputacji, która ustala reputacje w zakresie od -1 do 10, gdzie 10 jest wynikiem obarczonym najmniejszym zagrożeniem.
    Wynik ustalany powinien być na podstawie analizy co najmniej 50 różnych parametrów dotyczących adresów WWW między innymi, takich jak:

    a) • Czy strona znajduje się na tzw. internetowych „Czarnych listach" stron WWW
    b) • Czy strona znajduje się na tzw. Internetowych „Białych listach" stron WWW
    c) • W jakiej kategorii jest skatalogowana
    d) • Jaką zawartość ma HTML
    e) • Jak zachowuje się URL podczas połączenia
    f) • Dane dotyczące globalnego ruchu sieciowego dotyczącego tej strony
    g) • Dane podmiotu na który domena jest zarejestrowana
    h) • Czy adres IP strony jest z puli adresów przydzielanych dynamicznie
    i) • Czy adres nie znajduje się na liście serwerów na które się włamano
    j) • Dane dotyczące właścicieli sieci, w których strona jest hostowana

18) Baza, która gromadzi dane do analizy musi zbierać informacje z co najmniej 120 000 źródeł na świecie i musi znajdować się w internecie nie krócej niż 5 lat.
19) Mechanizm filtrowania w zależności od reputacji powinien być wsparty drugą warstwą ochrony protokołu HTTP - dodatkowym mechanizmem skanowania zawartości tego protokołu za pomocą silników skanujących dostarczanych przez co najmniej dwóch różnych producentów, zintegrowanych na pojedynczym urządzeniu przy pomocy technologii wykorzystującej zaawansowane techniki analizy składni obiektów i streamingu w celu uniknięcia opóźnień i problemów ze skalowalnością przy skanowaniu przez np. dwa silniki. Mechanizm ten powinien chronić przed szerokim wachlarzem zagrożeń - od reklam, programów zmieniających stronę startową, ataków typu phishing czy pharming, aż do bardziej złośliwych ataków, takich jak rootkity, konie trojańskie, wirusy, robaki, monitory systemu i keyloggery.
20) Rozwiązanie musi posiadać dedykowany mechanizm skanujący wszystkie porty TCP/IP z prędkością transmisji, w celu wykrywania i blokowania próby wysyłania danych przez programy szpiegujące w sieci wewnętrznej (proces "phone-home"). Śledzenie wszystkich 65 535 portów sieciowych, ma mieć na celu zatrzymywanie złośliwego oprogramowania, które próbuje ominąć port 80 przy komunikacji z Internetem.
21) Rozwiązanie musi obsługiwać wyżej wymienione mechanizmy reputacji i filtrowania adresów URL przy podejmowaniu decyzji o deszyfrowaniu HTTPs. Na przykład, witryna banku może zostać pominięta przy deszyfrowaniu HTTPs, chyba że ocena jej reputacji internetowej jest niska. W takim przypadku połączenie HTTPs powinno być deszyfrowane w celu przeskanowania treści pod kątem złośliwego oprogramowania.
22) Proponowane rozwiązanie powinno mieć licencje dla 4500 użytkowników (dla wszystkich oddziałów – detaliczny podział zostanie określony przed dostawą) w sieci korporacyjnej na okres co najmniej 3 lat, z możliwością przedłużenia, na kolejne lata. Licencje powinny zawierać wszystkie wyżej wymienione funkcjonalności.
23) Rozwiązanie powinno być w konfiguracji sprzętowej zapewniającej redundancję między pojedynczymi urządzeniami. (min. dwa węzły w każdym oddziale)

1.7 Urządzenia systemu ochrony ruchu pocztowego

1) Dostarczane rozwiązanie musi być dedykowaną, sprzętową platformą zawierającą mechanizmy antyspamowe, antywirusowe (także te zwalczające inny niż wirusy, złośliwy kod) i filtrujące zawartość treści dla poczty elektronicznej oraz mechanizmy kryptograficzne umożliwiające m.in uwierzytelnienie i szyfrowanie zawartości poczty elektronicznej w sposób opisany poniżej.
2) Rozwiązanie musi być dedykowanym MTA (Mail Transfer Agent) pracującym w trybie bramy dla wchodzącego i wychodzącego ruchu SMTP.
3) Urządzenie musi być przystosowane do montażu w 19" szafie rackowej i mieć wysokość nie większą niż 1U.
4) Urządzenie musi posiadać co najmniej dwa dyski twarde o łącznej pojemności 500GB pracujące w technologii Raid 1
5) Urządzenie musi posiadać co najmniej 4GB pamięci RAM
6) Urządzenie musi posiadać 2 interfejsy 10/100/1000 BaseT
7) Urządzenie musi posiadać port szeregowy typu RS-232 (DB-9)
8) Proponowane rozwiązanie musi składać się z co najmniej dwóch redundantnych urządzeń potrafiących pracować zarówno w trybie aktywny-zapasowy jak i aktywny-aktywny bez dodatkowych licencji wymaganych do uruchomienia tych funkcjonalności.
9) Platforma musi bazować na dedykowanym systemie operacyjnym ze specjalnie przygotowanym systemem plików do obsługi dużych ilości małych plików
10) System operacyjny musi umożliwiać tworzenie wątków bez alokowania dedykowanego stosu pamięci dla każdego z nich, w celu obsłużenia powyżej 1000 jednoczesnych połączeń SMTP.
11) System operacyjny musi posiadać specjalnie zaprojektowany mechanizm do obsługi I/O, zoptymalizowany do obsługi poczty elektronicznej.
12) System operacyjny musi przeznaczać co najmniej 10GB powierzchni dyskowych na kolejkowanie poczty.
13) System operacyjny musi umożliwiać zarządzanie grupą proponowanych urządzeń centralnie z jednego urządzenia, przy czym powinno być to za każdym razem dowolne urządzenie z zarządzanej grupy. (ang. multi-root management cluster). Zarządzanie grupą urządzeń nie może być wymogiem do dokupienia dodatkowego rozwiązania zarządzającego.
14) Konfiguracja urządzenia musi być przetrzymywana w pliku XML
15) Mechanizm antyspamowy musi być realizowany dwufazowo.
16) Pierwsza faza musi opierać się na sprawdzeniu reputacji adresu IP nadawcy w ogólnoświatowej bazie reputacji, która musi posiadać następujące parametry:

    a) Musi otrzymywać dane z co najmniej 120.000 źródeł z całego świata
    b) Musi analizować co najmniej 150 parametrów dotyczących ruchu poczty elektronicznej i protokołu WWW (W tym co najmniej 90 dla poczty)
    c) Musi używać do komunikacji z rozwiązaniem protokołu DNS
    d) Musi zwracać wynik reputacji dla adresu IP w skalo od -10 do 10, gdzie 10 stanowi najmniejsze zagrożenie spamem.
    e) Baza powinna ustalać rezultat reputacji jedynie na podstawie zbieranych danych, nie dopuszczając jednorazowych interwencji ze strony wysyłających pocztę mających na celu manualne podwyższenie ich reputacji.
    f) Baza musi istnieć od co najmniej 5 lat.

17) Druga faza ma następować jeżeli wiadomość przejdzie pomyślnie fazę pierwszą i musi opierać się silniku antyspamowym, korzystającym z reguł wysyłanych od producenta.

    a) Reguły muszą być tworzone dynamicznie na podstawie informacji z co najmniej trzech źródeł – ogólnoświatowej bazy danych reputacji o parametrach jak w fazie pierwszej, informacji zwrotnych od użytkowników proponowanego rozwiązania oraz informacji od dedykowanych analityków bezpieczeństwa pracujących 24h na dobę, 7 dni w tygodniu, 365 dni w roku dla producenta proponowanego rozwiązania.
    b) Reguły muszą weryfikować , informację na temat adresów IP pojawiających się w mailach jako linki do stron, strukturę wiadomości, czyli sposób w jaki została wysłana, treść wiadomości ; oraz reputację nadawcy.
    c) Reguły powinny być uaktualniane, automatycznie, nie rzadziej niż co 20 minut przez internet.

18) Mechanizm antywirusowy musi mieć możliwość korzystania z co najmniej dwóch komercyjnych silników antywirusowych (na pojedyńczej platformie sprzętowej).
19) Silniki antywirusowe muszą korzystać z następujących metod skanowania wiadomości:
    a) Dopasowanie wzorców binarnych do sygnatur antywirusowych
    b) Analiza heurystyczna
    c) Emulacja uruchomienia kodu (w celu zapobiegania infekcji wirusami polimorficznymi)
20) Mechanizm musi mieć do dyspozycji oddzielną od dedykowanej dla spamu, kwarantannę do ktorej dostęp ma tylko administrator.

21) Wiadomości oznaczone jako spam, przez mechanizm antyspamowy, zeskanowane także przez silnik antywirusowy, muszą trafiać do kwarantanny antywirusowej, a nie antyspamowej. (W przypadku wybrania akcji kwarantanny wiadomości.)
22) Mechanizm antywirusowy musi posiadać technologię umożliwiająca automatyczną kwarantannę wiadomości, które pomimo, że nie są wskazane przez powyższe metody skanowania (z powodu np. braku odpowiednich sygnatur antywirusowych), mogą jednak zawierać złośliwy kod. Informacje o takim podejrzeniu powinny być wysyłane przed bazę reputacji, o parametrach opisanych w wymogach modułu antyspamowego. Podejrzane wiadomości powinny pozostać w kwarantannie, aż do wypuszczenia przez producentów silników antywirusowych odpowiednich sygnatur i automatycznie wypuszczane i skanowane ponownie po ściągnięciu odpowiednich sygnatur.
23) Proponowane rozwiązanie musi posiadać mechanizmy analizy i flitrowania oraz zarządzania treścia wiadomości poczty elektronicznej, zarówno treści samej wiadomości jak i jej załączników.
24) Mechanizm musi mieć możliwość zdefinjowania polityki zarządzania treścia wiadomości w oparciu o wynik reputacji pobrany z bazy reputacji o parametrach opisanych w module antyspamowym.
25) Mechanizm musi mieć możliwość zdefiniowania polityki zarządzania treścia wiadomości w oparciu o wynik uwierzytelnienia DKIM, funkcjnalności opisanej w wymaganiach dotyczących zastosowania kryptografii w proponowanym urządzeniu
26) Mechanizm musi mieć możliwość filtrowania treści za pomocą integracji z zewnętrznymi słownikami. Proponowane rozwiązanie musi mieć zainstalowane co najmniej trzy różne słowniki.
27) Oferowane rozwiązanie musi posiadać mechanizmy oznaczania poczty wychodzącej (Bounce Address Tag Validation (BATV)) oraz weryfikacji tego oznaczenia w przypadku otrzymania wiadomosci odbitej od odbiorcy (tzw. Bounce) w celu ochrony przed atakmi typu „misdirected bounce spam"
28) Oferowane rozwiązanie musi obsługiwać standart DKIM (Domain Keys Identified Messages) używany w celu uwierzytelnienia poczty, za pomocą szyfrowania asymetrycznego.
29) Oferowane rozwiązanie musi umożliwiać opcjonalnie, oddzielnie licencjonowane, szyfrowanie symetryczne poczty dla wybranych wiadomości, wykonywane bez potrzeby jakiejkolowiek ingerencji w klienta pocztowego oraz bez potrzeby implementacji PKI. Rozwiązanie powinno udostępniać szyfrowanie za pomocą algorytmów AES oraz ARC4.
30) Proponowane rozwiązanie powinno mieć licencje na czas nieokreślony na następujące funkcjonalności: MTA, DKIM, BATV, Filtrowania treści
31) Proponowane rozwiązanie powinno mieć licencje dla 4500 skrzynek pocztowych (łącznie wszystkie oddziały – detaliczny podział zostanie określony przed dostawą) na czas 3 lat z możliwością przedłużenia, na nastepujące funkcjonalności: Antyspam, Antywirus oparty o co najmniej dwa silniki różnych producentów, z dodatkową obsługą ochrony przed epidemią złośliwego kodu.
32) Licencje powinny umożliwiać centralne zarządzanie proponowanym rozwiązaniem.

1.8. System zarządzania ochroną aplikacyjną i raportowania

1) system umożliwiający centralne zarządzanie i raportowanie dla systemów ochrony ruchu pocztowego,
2) dedykowany, zoptymalizowany system operacyjny
3) centralne raportowanie
    a) konsolidacja danych z poszczególnych węzłów oddziałowych
    b) personalizacja raportów
    c) możliwość planowego lub na żądanie generowania raportów
    d) możliwość eksportu raportów do plików PDF, CSV, wysyłania przez e-mail
4) śledzenie wiadomości
5) centralna kwarantanna wiadomości podejrzewanych o spam
    a) możliwość integracji uwierzytelnienia użytkowników z LDAP
6) redundancja rozwiązania (min. dwa węzły)
7) platforma sprzętowa
    a) obudowa 19" rack, maks. 2U
    b) redundantne zasilacze 230V AC
    c) min. 4 dyski 300GB SCSI, hot-swap
    d) min. dwa porty 10/100/1000BaseT

1.9 Rozbudowa systemu zarządzania elementami bezpieczeństwa

1) rozszerzenie posiadanego przez Zamawiającego systemu Cisco Security Manager Pro o możliwość zarządzania dodatkowymi 100-ma urządzeniami sieciowymi,
2) w przypadku oferowania rozwiązania równoważnego, wymagane spełnienie poniższych wymogów
    a) niezależny dedykowany pakiet do zarządzania bezpieczeństwem sieci
    b) obsługa min. 150 urządzeń z możliwością późniejszego rozszerzenia do min. 1000
    c) zarządzanie elementami bezpieczeństwa w następującym zakresie:
        - funkcjonalność VPN
        - funkcjonalność Firewall
        - funkcjonalność IPS
    d) zarządzanie posiadanymi przez NFZ urządzeniami bezpieczeństwa:
        - firewalle Cisco PIX
        - urządzenia wielofunkcyjne Cisco ASA
        - routery Cisco serii 7200, 2600, 2800, 3800
        - oferowane sondy IPS
    e) współpraca z oferowanym systemem korelacji zdarzeń
    f) obrazowanie stanu sieci na podstawie widoków:
        - urządzeń
        - polityk
        - topologii w tym topologii sieci VPN
    g) grupowanie urządzeń
    h) narzędzia hierarchizacji i dziedzieczenia polityk bezpieczeństwa np. polityka firmowa stanowi integralną część każdej polityki tworzonej przez administratora.
    i) narzędzia workflow w zakresie:
        - tworzenia, edycji i zatwierdzania polityki bezpieczeństwa
        - generowania, zatwierdzania oraz wdrażania działań związanych z zatwierdzoną polityką bezpieczeństwa
    j) tworzenie makr umożliwiających wprowadzanie szeregu komend/działań konfiguracyjnych i wykonywanie ich jedną operacją.
    k) narzędzia archiwizacji i porównywania konfiguracji poszczególnych urządzeń
    l) zbieranie statystyk co najmniej z wykorzystaniem SNMP
    m) kontrola dostepu na bazie roli (Role-Based Access Control)
    n) narzędzia zarządzania firewallami umożliwiające conajmniej:
        - definiowanie przez użytkownika grup urządzeń dla przypisania reguł,
        - kontrolę dostępu do urzadzeń zależnie od funkcji pracownika (role-based access control)
        - obligatoryjne i automatyczne dziedziczenie podstawowych ustawień konfiguracyjnych dla nowych urządzeń w sieci
        - możliwość przeglądania wszystkich reguł dotyczących firewalli w jednej tabeli z możliwością wykrywania sprzeczności
        - możliwość dziedziczenia polityk bezpieczeństwa pomiędzy firewallami
        - możliwość zarządzania firewallami wirtualnymi konfigurowanymi na urządzeniach wraz z przypisywaniem zasobów sprzętowych per firewall
        - możliwość zarządzania firewallami L2 (transparentnymi)
        - możliwość zarządzania funkcjami QoS na firewallach
        - możliwość zarządzania funkcją failover
    o) narzędzia zarzadzania systemami network IDS/IPS umożliwiające conajmniej:
        - zbieranie informacji o zaistniałych atakach sieciowych
        - możliwość informowania administratora o atakach z wykorzystaniem np, poczty elektronicznej
        - używanie kreatorów dla typowo wykonywanych zadań
        - zarządzanie wieloma sondami z jednej konsoli
        - automatyczne aktualizowanie sygnatur, patchy, zestawów serwisowych (service pack) systemu IPS
        - dziedziczenie polityk i konfiguracji przez urządzenia dodawane do systemu IPS
    p) narzędzia zarządzania systemami VPN umożliwiające co najmniej:
        - konfiguracja sieci VPN site-to-site i sieci RA VPN (zdalny dostęp) za pomocą kreatorów
        - informowanie o zasobach systemów VPN takich jak wykorzystanie pamięci, obciążenie procesora, aktywnych tunelach i sesjach VPN
        - możliwość obserwacji obecnego i długoterminowego obciążenia urządzeń
        - graficzne przedstawienie topologii sieci VPN
        - możliwość inwentaryzacji sieci
        - zarządzanie informacjami o urządzeniach aktywnych w sieci
        - monitorowanie i raportowanie o zmianach w obrębie sprzętu, oprogramowania

- możliwość zarządzania i wprowadzania zmian konfiguracyjnych i update'ów image oprogramowania do wielu urządzeń sieciowych
- możliwość szybkiej identyfikacji urządzeń, które mogą być wykorzystane do stworzenia sieci VPN po upgrade do odpowiedniego image oprogramowania systemowego urządzenia.
- wykrywanie, które urządzenia sieciowe są wyposażone w dedykowany moduł wsparcia szyfrowania
- graficzne porównanie konfiguracji urządzeń VPN

q) platforma sprzętowa zgodna z zaleceniami producenta systemu (montaż w rack 19", nie więcej niż 1U, redundantne zasilacze i wentylatory)

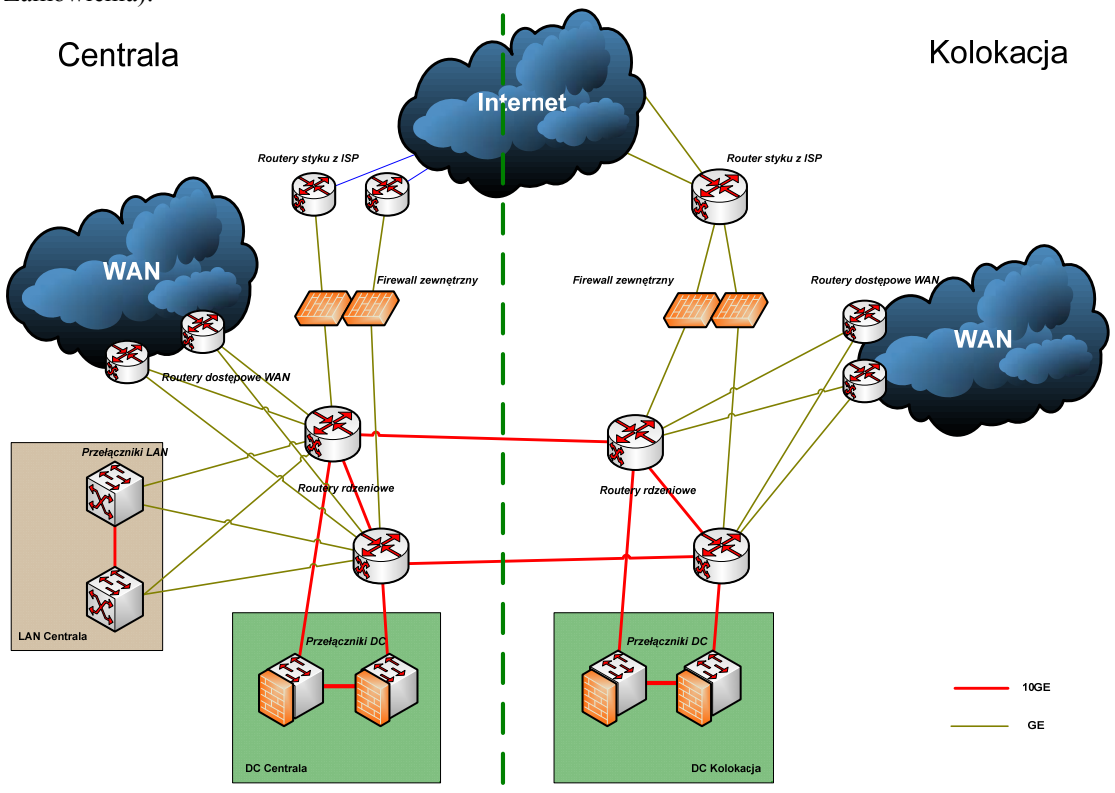
III. Warunki gwarancji i serwisu

Zamawiający wymaga, by Wykonawca udzielił na dostarczone urządzenia 36 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. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych telefonicznie w godzinach pracy Zamawiającego, oraz przez całą dobę - faxem, e-mailem lub WWW; Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań.
W przypadku urządzeń, dla których jest wymagany dłuższy czas na usunięcie awarii, Zamawiający dopuszcza podstawienie na ten czas sprzętu o nie gorszych parametrach funkcjonalnych. Usunięcie awarii w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki.
Przez cały okres trwania gwarancji:
1) Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w godzinach pracy Zamawiającego w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń.
2) Zamawiający uzyska dostęp do części chronionych stron internetowych producentów urządzeń (min. 18 kont dostępowych), umożliwiający:

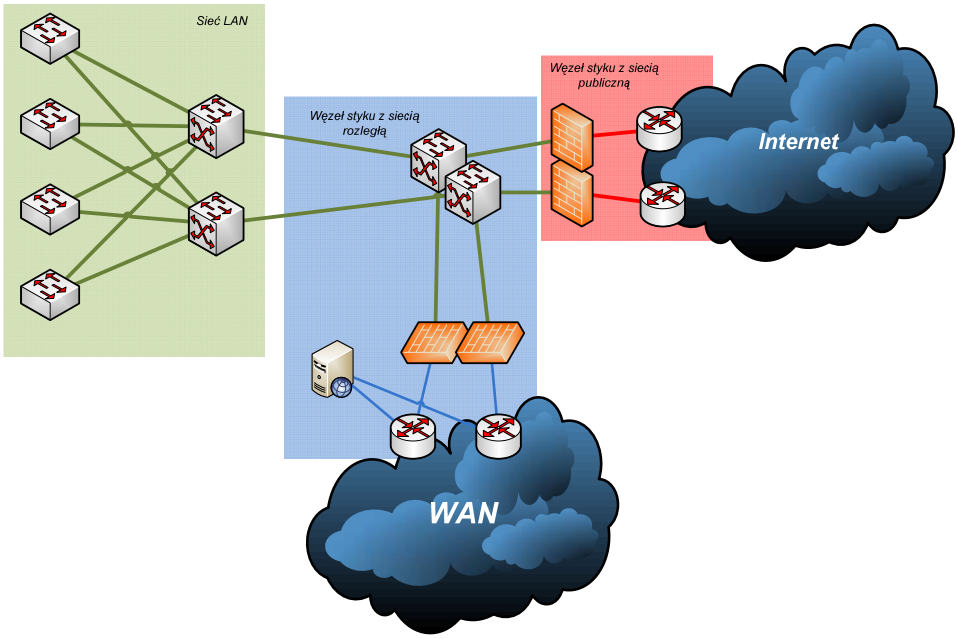
- pobieranie nowych wersji oprogramowania,
- dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
- dostęp do pomocy technicznej producentów.

IV. Projekt techniczny

Docelową strukturę węzła centralnego obrazuje poniższy diagram (nie wszystkie pokazane elementy wchodzą w zakres Zamówienia):



Oczekiwana struktura węzłów oddziałowych przedstawiona jest na poniższym diagramie (nie wszystkie pokazane elementy wchodzą w zakres Zamówienia):



1) Po podpisaniu umowy Wykonawca otrzyma od Zamawiającego dokumentację aktualnie eksploatowanej infrastruktury telekomunikacyjnej. Na jej podstawie Wykonawca zobowiązany jest do przygotowania projektu technicznego wdrożenia systemu.

2) Opracowany projekt techniczny musi być dostarczony w terminie realizacji umowy.

3) Projekt techniczny musi zawierać precyzyjne wytyczne konfiguracyjne urządzeń oraz procedury instalacyjne.

4) Projekt musi uwzględniać integrację rozwiązania z posiadaną przez Zamawiającego infrastrukturą.

5) Dostarczony projekt musi zawierać przynajmniej:
   a) mapę topologii połączeń fizycznych i logicznych
   b) procedurę instalacji i podłączenia urządzeń
   c) wytyczne dotyczące zastosowania oprogramowania w odpowiedniej wersji
   d) szablony konfiguracji urządzeń sieci LAN uwzględniające: konfigurację VLAN, konfigurację zabezpieczeń i zarządzania, konfigurację QoS
   e) szablony konfiguracyjne urządzeń sieci WAN uwzględniające: konfigurację zabezpieczeń i zarządzania, konfigurację QoS, konfigurację szyfrowania wielopunktowego lub grupowego, konfigurację routingu, procedurę postępowania a przypadku awarii
   f) szablony konfiguracyjne urządzeń zapory ogniowej uwzględniające: konfigurację zabezpieczeń i zarządzania, konfigurację redundancji urządzeń, konfigurację filtrowania ruchu
   g) szablony konfiguracji systemu ochrony poczty elektronicznej i ruchu Web uwzględniające: konfigurację zabezpieczeń i zarządzania, konfigurację integracji urządzeń z posiadaną infrastrukturą dostępu do Internetu, konfigurację polityk bezpieczeństwa implementowanych na urządzeniach

6) Projekt musi być dostarczony w wersji papierowej oraz w wersji elektronicznej umożliwiającej edycję.

V. Asysta techniczna powdrożeniowa

1) W okresie sześciu miesięcy od podpisania protokołu odbioru Wykonawca zobowiązany będzie do świadczenia Zamawiającemu asysty technicznej, której celem będzie wsparcie Zamawiającego we wdrożeniu oraz w pierwszym okresie użytkowania rozwiązania.

2) W ramach asysty Wykonawca zobowiązany będzie do:
   a) - bezpośredniej asysty podczas uruchamiania urządzeń w lokalizacjach Zamawiającego
   b) - analizy zgłoszeń serwisowych
   c) - pomocy w rekonfiguracji sieci

d) - analizy możliwości rozwoju i zmian w sieci
e) - cykliczny (raz na 3 mc-e) przegląd stanu sieci (logi)
f) - rekomendacji aktualizacji software

3) W ramach asysty Wykonawca przeprowadzi 2 szkolenia 5-dniowe dla personelu Zamawiającego w zakresie odpowiadającym zrealizowanemu zamówieniu. Każde szkolenie musi być zrealizowane dla dwóch 20 osobowych grup pracowników Zamawiającego. Minimalny zakres szkoleń dla każdej z grup:
    a) Routing & Switching - podstawowe zagadnienia budowy sieci LAN/WAN, zasady funkcjonowania sieci, rola routerów i switchy w sieciach TCP/IP, podstawowe zagadnienia związane z protokołami routingu dynamicznego oraz routingiem statycznym. Zagadnienia protokołów używanych w LAN z szczególnym uwzględnieniem konfiguracji i diagnostyki protokołu STP (Spanning Tree Protocol). Konfiguracja i diagnostyka urządzeń.
    b) Bezpieczeństwo - zagadnienia polityki bezpieczeństwa oraz jej wpływu na bezpieczne funkcjonowanie sieci, omówienie zagadnień kompleksowej polityki bezpieczeństwa sieci ze szczególnym uwzględnieniem konfiguracji dostarczonych urządzeń (realizujących funkcje bezpieczeństwa): zapora ogniowa (firewall), urządzenia ochrony ruchu pocztowego i Web, systemy zarządzania urządzeniami bezpieczeństwa.

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 z późn. zm.), zawarto umowę następującej treści:

§ 1

1. Przedmiotem umowy jest **dostawa zespołu urządzeń dla systemu redundantnych węzłów sieci rozległej**. W ramach zamówienia Wykonawca będzie zobowiązany do dostawy komponentów systemu, przygotowania projektu technicznego obejmującego szczegóły implementacyjne rozwiązań i świadczenia powykonawczej asysty technicznej zgodnie z załącznikiem nr 1 do umowy.
2. Zamawiający dopuszcza zmianę komponentów systemu na spełniające warunki opisane w załączniku nr 1 w przypadku gdy:
   1) z przyczyn niezależnych od WYKONAWCY nie będzie możliwe dostarczenie wskazanych w ofercie komponentów,
   2) zostanie wyprodukowana nowsza wersja urządzenia.
3. 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 komponentów systemu, przygotowanie projektu technicznego obejmującego szczegóły implementacyjne rozwiązań systemu redundantnych węzłów sieci rozległej nastąpi w terminie 8 tygodni od daty zawarcia umowy.
2. Termin, o którym mowa w ust. 1 może ulec zmianie w przypadku zaistnienia okoliczności niezależnych od Wykonawcy. Za okoliczności niezależne od Wykonawcy, Zamawiający uzna w szczególności:
   1) siłę wyższą,
   2) nieprzewidywalne warunki fizyczne dotyczące transportu.
3. Strony ustalają, że świadczenie powykonawczej asysty technicznej będzie realizowane w terminie 6 miesięcy od daty dostawy zespołu urządzeń.
4. Wykonawca dostarczy przedmiot umowy do siedziby Zamawiającego, miejsca wskazanego prze Zamawiającego na terenie m. st. Warszawy oraz do Oddziałów Wojewódzkich zgodnie z załącznikiem nr 1 do umowy.
5. Odbiór przedmiotu umowy w zakresie dostawy komponentów systemu i przygotowania projektu technicznego potwierdzony zostanie protokołem odbioru.
6. Protokół odbioru, o którym mowa w ust. 5, ze strony Zamawiającego podpisuje osoba pełniąca funkcję Naczelnika Wydziału Eksploatacji w Centrali.
7. Wykonawca zobowiąże pisemnie wskazanych swoich pracowników i pracowników podwykonawców wyznaczonych do realizacji przedmiotu umowy (zgodnie z załącznikiem nr 3), do zachowania tajemnicy przez podpisanie zobowiązań według wzoru określonego w załączniku nr 4 i zobowiązuje się dostarczyć takie dokumenty Zamawiającemu, przed przystąpieniem do praktycznej realizacji niniejszej umowy przez danego pracownika Wykonawcy lub pracownika podwykonawcy.

§ 3

1. Ustala się łączne wynagrodzenie 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. 5, 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.
7. Wierzytelności przysługujące z tytułu realizacji niniejszej umowy nie podlegają przenoszeniu na osoby trzecie bez zgody Zamawiającego.

§ 4

1. Wykonawca zobowiązuje się do świadczenia powykonawczej asysty technicznej - w terminie 6 miesięcy od daty dostawy oferowanego systemu.
2. W ramach asysty Wykonawca zobowiązany jest do:
   1) bezpośredniej asysty podczas uruchamiania urządzeń w lokalizacjach Zamawiającego,
   2) analizy zgłoszeń serwisowych,
   3) pomocy w rekonfiguracji sieci,
   4) analizy możliwości rozwoju i zmian w sieci,
   5) cyklicznego (raz na 3 mc-e) przeglądu stanu sieci (logi),
   6) rekomendacji aktualizacji software.
3. W ramach asysty Wykonawca przeprowadzi 2 szkolenia 5-dniowe dla personelu Zamawiającego w zakresie odpowiadającym zrealizowanemu zamówieniu. Każde szkolenie musi być zrealizowane dla dwóch 20 osobowych grup pracowników Zamawiającego. Minimalny zakres szkoleń dla każdej z grup:
   1) Routing & Switching - podstawowe zagadnienia budowy sieci LAN/WAN, zasady funkcjonowania sieci, rola routerów i switchy w sieciach TCP/IP, podstawowe zagadnienia związane z protokołami routingu dynamicznego oraz routingiem statycznym. Zagadnienia protokołów używanych w LAN z szczególnym uwzględnieniem konfiguracji i diagnostyki protokołu STP (Spanning Tree Protocol). Konfiguracja i diagnostyka urządzeń,
   2) Bezpieczeństwo - zagadnienia polityki bezpieczeństwa oraz jej wpływu na bezpieczne funkcjonowanie sieci, omówienie zagadnień kompleksowej polityki bezpieczeństwa sieci ze szczególnym uwzględnieniem konfiguracji dostarczonych urządzeń (realizujących funkcje bezpieczeństwa): zapora ogniowa (firewall), urządzenia ochrony ruchu pocztowego i Web, systemy zarządzania urządzeniami bezpieczeństwa.
4. Wszystkie koszty związane ze świadczeniem powykonawczej asysty technicznej ponosi Wykonawca.
5. Wykonawca na dostarczone, zamontowane i uruchomione urządzenia udziela 36 miesięcznej gwarancji. Okres gwarancji liczony jest od daty podpisania protokołu odbioru, o którym mowa w § 2 ust. 5, przy czym serwis będzie realizowany przez producenta (lub zlecony przez producenta autoryzowanemu partnerowi serwisowemu).
6. Strony ustalają, że:
   1) serwis gwarancyjny świadczony będzie w miejscu instalacji sprzętu,
   2) czas usunięcia awarii w okresie gwarancji nie będzie przekraczał 24 godzin od momentu zgłoszenia, Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon w godzinach pracy Zamawiającego, oraz przez całą dobę - faxem, e-mail lub WWW; Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań,
   3) w przypadku urządzeń, dla których jest wymagany dłuższy czas usunięcia awarii, Zamawiający dopuszcza podstawienie na ten czas sprzętu o nie gorszych parametrach funkcjonalnych. Usunięcie awarii w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia serwisowego.
7. Przez cały okres trwania gwarancji, Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w godzinach pracy Zamawiającego w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych urządzeń.
8. Przez cały okres trwania gwarancji, Zamawiający uzyska dostęp do części chronionych stron internetowych producentów urządzeń (min. 18 kont dostępowych), umożliwiający:
   1) pobieranie nowych wersji oprogramowania,
   2) dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
   3) dostęp do pomocy technicznej producentów.
9. Wszystkie koszty związane ze świadczeniem gwarancji ponosi Wykonawca.

§ 5

Zamawiający może odstąpić od umowy w terminie 7 dni od dnia stwierdzenia nienależytego jej wykonania lub wykonania jej w sposób sprzeczny z 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% wynagrodzenia brutto określonego w § 3 ust. 1 pkt 3,
   2) za opóźnienie w oddaniu przedmiotu umowy w wysokości 0,2% wynagrodzenia brutto określonego w § 3 ust. 1 pkt 3 za każdy dzień opóźnienia.
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. 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.

§ 7

1. Wykonawca wnosi zabezpieczenie należytego wykonania umowy w wysokości 5% wynagrodzenia brutto, o którym mowa w § 3 ust. 1 pkt 3 tj. ..... (słownie: .....złotych).
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

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.

§ 9

Wszelkie dopuszczalne zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 10

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

§ 11

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

§ 12

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

ZAMAWIAJĄCY WYKONAWCA

ZAŁACZNIK DO UMOWY NR ….

ZOBOWIĄZANIE
DO ZACHOWANIA TAJEMNICY

Nazwisko (-ka) :

…….....

Imię (imiona): 1. .....

2. .....

Numer identyfikacyjny PESEL: |___|___|___|___|___|___|___|___|___|___|___|

Dowód tożsamości: Seria |__|__|__|Nr |__|__|__|__|__|__|__|__|__|__|__|__|__|__|

wydany przez

…….....

Ja niżej podpisany, potwierdzając zgodność moich danych osobowych ze stanem faktycznym, oświadczam, że :

1. Zapoznałem się z treścią ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) i wynikających z niej przepisów prawnych,
2. Zostałem uprzedzony, iż dane osobowe i medyczne przetwarzane w Systemie Informatycznym NFZ podlegają ustawowej ochronie prawnej na podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych w związku z ustawą z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. Nr 210, poz. 2135 z późn. zm.).
3. Zostałem poinformowany, iż informacje związane z technologią i metodyką ich przetwarzania w Systemie Informatycznym NFZ, ze względu na ważny interes NFZ, jak również osób w niej ubezpieczonych, podlegają szczególnej ochronie prawnej, w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.).
4. Zobowiązuję się do zachowania w tajemnicy i nie ujawniania wszelkich danych osobowych, medycznych oraz innych danych uzyskiwanych i przetwarzanych przez Narodowy Fundusz Zdrowia w zakresie i trybie objętym ustawą z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. Nr 210, poz. 2135 z późn. zm.), ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.)
5. Zobowiązuję się do nie ujawniania – w ramach wykonywania prac związanych z realizacją umowy zawartej pomiędzy …… informacji objętych tajemnicą służbową w rozumieniu ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 z późn. zm.).
6. Zobowiązuję się do nie rozpowszechniania nabytej informacji o charakterze technicznym, technologicznym, organizacyjnym i handlowym, stanowiących tajemnicę NFZ pod rygorem odpowiedzialności cywilnej i karnej.
7. Obowiązek zachowania w tajemnicy informacji dotyczących wyżej wymienionych danych uzyskanych w związku z realizacją zadań wynikających z przedmiotu umowy zawartej pomiędzy NFZ a …… ciąży na mnie nawet po wygaśnięciu stosunku o pracę.

Powyższe zobowiązanie zachowuje ważność w przypadku danych osobowych i medycznych bezterminowo, a w przypadku pozostałych danych przez cały okres trwania umowy, oraz przez okres 3-lat po jego zakończeniu.

..... dnia ..... Podpis pracownika : .....

pieczęć Wykonawcy

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

Oferta

Nazwa Wykonawcy .....

.....

Adres Wykonawcy .....

.....

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

REGON…….. NIP……

składa ofertę na dostawę zespołu urządzeń dla systemu redundantnych węzłów sieci rozległe

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 przedstawione przez Zamawiającego terminy realizacji zamówienia określone w pkt 1.2 SIWZ

3. Oświadczenie o spełnianiu przez oferowane urządzenia wymagań określających przedmiot zamówienia:

Oświadczam, że oferowane urządzenia spełniają wszystkie wymagania określone w załączniku do Specyfikacji „Opis przedmiotu zamówienia".

4. Oświadczenie o akceptacji warunków płatności:

Oświadczam, że bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki płatności za realizację zamówienia określone w pkt. 1.3.

5. 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.

6. Oświadczenie o akceptacji warunków gwarancji

Oświadczam, że bez zastrzeżeń przyjmuję przedstawione przez Zamawiającego warunki gwarancji określone we wzorze umowy załączonym do Specyfikacji

.....

Podpis i pieczęć Wykonawcy

7. 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.

8. 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 ..... .

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

Oświadczamy, że realizację przedmiotu zamówienia:

☐ wykonamy sami *

☐ powierzymy wykonanie części zamówienia podwykonawcom zgodnie z poniższym zestawieniem *

** właściwe zaznaczyć*

Lp.	Części zamówienia, której wykonanie Wykonawca powierzy podwykonawcom

10. 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)

Przystępując do postępowania o udzielenie zamówienia publicznego na:

dostawa zespołu urządzeń dla systemu redundantnych węzłów sieci rozległej.

niniejszym oświadczam, że spełniamy warunki określone w art. 22 ust. 1

.....

podpis i pieczęć Wykonawcy *

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

....., dnia ..... ZAŁĄCZNIK NR 5 DO SPECYFIKACJI

pieczęć Wykonawcy

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

WYKAZ WYKONANYCH DOSTAW

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. co najmniej 1 dostawę polegającą na dostawie routerów i/lub urządzeń zapory ogniowej (firewall) oraz co najmniej 1 dostawę polegającą na dostawie urządzeń służących ochronie stron www i/lub poczty elektronicznej o łącznej wartości (dla obu dostaw) co najmniej 5 mln. zł brutto (słownie: pięć milionów złotych)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.

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

Wykaz osób, które będą wykonywać zamówienie

Wykonawca winien przedstawić pisemny wykaz osób, które będą wykonywać zamówienie wraz z **aktualnymi upoważnieniami dostępu do informacji niejawnych oznaczonych klauzulą „Poufne**”

UWAGA – należy załączyć dokumenty potwierdzające uprawnienia tych osób aktualne na dzień otwarcia ofert oraz przez cały okres trwania umowy.

lp.	Imię i nazwisko osoby	Ew. uwagi
1.		
2.		
3.		
4.		
5.		
6.		
7		
8		
9		
10		
11		
12		
…		

.....
Podpis i pieczęć Wykonawcy

Nazwa Wykonawcy: .....

Adres Wykonawca: .....

OŚWIADCZENIE O POSZCZEGÓLNYCH CENACH JEDNOSTKOWYCH *

Lp.	Oznaczenie urządzenia	Cena jednostkowa netto (zł)	Jednostka miary	Zapotrzebowanie Zamawiającego	Cena łączna netto (zł)	Podatek VAT (zł)	Cena łączna brutto (zł)
1	**Routery dostępowe dla Centrali NFZ**		Szt.	3			
2	**Routery dostępowe dla Oddziałów Wojewódzkich**		Szt.	16			
3	**Urządzenia ochrony styku z siecią WAN**		Szt.	32			
4	**Przełączniki do obsługi węzła styku z siecią WAN**		Szt.	32			
5	**Urządzenia systemu ochrony ruchu Web dla Centrali NFZ**		Szt.	2			
6	**Urządzenia systemu ochrony ruchu Web dla Oddziałów Wojewódzkich**		Szt.	32			
7	**Urządzenia systemu ochrony ruchu pocztowego**		Szt.	32			
8	**System zarządzania ochroną aplikacyjną i raportowania**		Szt.	2			
9	**Rozbudowa systemu zarządzania elementami bezpieczeństwa**		Szt.	1			
				RAZEM			

* podane ceny powinny obejmować wartość dostawy urządzeń, koszt przygotowania projektu i świadczenia powykonawczej asysty technicznej w odniesieniu do poszczególne rodzajów urządzeń wymienionych w kolumnie „oznaczenie urządzenia”

.....
podpis i pieczęć Wykonawcy