SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

1. Nazwa oraz adres zamawiającego

Lubelski Oddział Wojewódzki Narodowego Funduszu Zdrowia
20-124 Lublin, ul. Szkolna 16, tel. (0-81) 53-105-11, fax (0-81) 53-105-28

2. Tryb udzielenia zamówienia

Postępowanie o udzielenie zamówienia prowadzone jest na zasadach określonych w ustawie z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j.Dz.U.2017.1579 ze zm.) - dalej „Pzp", o wartości zamówienia przekraczającej kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 ww. ustawy, **w trybie przetargu nieograniczonego.**

3. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest modernizacja sieci LAN.
Szczegółowy opis przedmiotu zamówienia zawarty jest w załączniku nr 5 do specyfikacji.

4. Termin wykonania zamówienia
Zamawiający wymaga aby zamówienie zostało wykonane w terminie nie dłuższym niż 60 dni kalendarzowych od podpisania umowy.

5. Warunki udziału w postępowaniu o udzielenie zamówienia.

O udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy:

1. nie podlegają wykluczeniu na podstawie art. 24 ust. 1 pkt 12 – 23 oraz art. 24 ust. 5 pkt 1 ustawy pzp,

2. spełniają warunki udziału w postępowaniu dotyczące:

   1) posiadania kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów;
   Zamawiający nie stawia szczególnych wymagań w zakresie spełnienia tego warunku.

   2) sytuacji ekonomicznej lub finansowej;
   Zamawiający nie stawia szczególnych wymagań w zakresie spełnienia tego warunku.

   3) zdolności technicznych lub zawodowych;

   Wykonawca musi wykazać, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał, a w przypadku świadczeń okresowych lub ciągłych również wykonuje co najmniej dwie (2) modernizacje sieci LAN o wartości nie mniejszej niż 300 000,00 zł (słownie: trzysta tysięcy złotych) każda..
   Ocena spełnienia warunku nastąpi na podstawie wykazu usług zgodnie z Załącznikiem nr 4 do specyfikacji oraz załączonych dokumentów potwierdzających, że usługi te zostały lub są wykonywane należycie.

3. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, warunki określone punkcie 5.2 winien spełniać, co najmniej jeden Wykonawca wspólnie ubiegający się o zamówienie. Warunek określony w punkcie 5.1 powinien spełniać każdy z Wykonawców indywidualnie.

4. Wykonawca może, w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach oraz w odniesieniu do konkretnego zamówienia, lub jego części, polegać na zdolnościach ekonomicznych lub finansowych innych podmiotów, jak również na ich zdolnościach technicznych lub zawodowych, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić zamawiającemu, że realizując zamówienie będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.

6. Wykaz oświadczeń lub dokumentów, jakie należy załączyć do oferty, w celu wstępnego potwierdzenia, że Wykonawca nie podlega wykluczeniu oraz spełniania warunki udziału w postępowaniu i kryteria selekcji:

1. Oświadczenie własne Wykonawcy złożone w postaci Jednolitego Europejskiego Dokumentu Zamówienia (JEDZ) – wg. Załącznika nr 2 do SIWZ.

1.1 JEDZ należy przesłać w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym. Oświadczenia podmiotów składających ofertę/wniosek wspólnie oraz podmiotów udostępniających potencjał składane na formularzu JEDZ powinny mieć formę dokumentu elektronicznego, podpisanego kwalifikowanym podpisem elektronicznym przez każdego z nich w zakresie w jakim potwierdzają okoliczności, o których mowa w treści art. 22 ust. 1 ustawy Pzp. Analogiczny wymóg dotyczy JEDZ składanego przez podwykonawcę, na podstawie art. 25a ust. 5 pkt 1 ustawy Pzp.

1.2 Środkiem komunikacji elektronicznej, służącym złożeniu JEDZ przez wykonawcę, jest poczta elektroniczna. **UWAGA!** Złożenie JEDZ wraz z ofertą na nośniku danych (np. CD, pendrive) jest niedopuszczalne, nie stanowi bowiem jego złożenia przy użyciu środków komunikacji elektronicznej w rozumieniu przepisów ustawy z dnia 18 lipca 2002 o świadczeniu usług drogą elektroniczną.

JEDZ należy przesłać na adres email: jolanta.pietrasinska@nfz-lublin.pl

a) Zamawiający dopuszcza w szczególności następujący format przesyłanych danych: .pdf, .doc, .docx, .rtf,.xps, .odt.
b) Wykonawca wypełnia JEDZ, tworząc dokument elektroniczny. Może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu elektronicznego, w szczególności w jednym z ww. formatów.
c) Po stworzeniu lub wygenerowaniu przez wykonawcę dokumentu elektronicznego JEDZ, wykonawca podpisuje ww. dokument kwalifikowanym podpisem elektronicznym, wystawionym przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne - podpis elektroniczny, spełniające wymogi bezpieczeństwa określone w ustawie.
d) Podpisany dokument elektroniczny JEDZ powinien zostać zaszyfrowany, tj. opatrzony hasłem dostępowym. W tym celu wykonawca może posłużyć się narzędziami oferowanymi przez oprogramowanie, w którym przygotowuje dokument oświadczenia (np. Adobe Acrobat), lub skorzystać z dostępnych na rynku narzędzi na licencji open-source (np.: AES Crypt, 7-Zip i Smart Sign) lub komercyjnych.

e) Wykonawca zamieszcza hasło dostępu do pliku JEDZ w treści swojej oferty/wniosku (wybrać właściwe), składanej/składanego w formie pisemnej. Treść oferty/wniosku może zawierać, jeśli to niezbędne, również inne informacje dla prawidłowego dostępu do dokumentu, w szczególności informacje o wykorzystanym programie szyfrującym lub procedurze odszyfrowania danych zawartych w JEDZ.
f) Wykonawca przesyła zamawiającemu zaszyfrowany i podpisany kwalifikowanym podpisem elektronicznym JEDZ na wskazany adres poczty elektronicznej w taki sposób, aby dokument ten dotarł do zamawiającego przed upływem terminu składania ofert. W treści przesłanej wiadomości należy wskazać oznaczenie i nazwę postępowania, którego JEDZ dotyczy oraz nazwę wykonawcy albo dowolne oznaczenie pozwalające na identyfikację wykonawcy (np. JEDZ do oferty 658 – w takim przypadku numer ten musi być wskazany w treści oferty).
g) Wykonawca, przesyłając JEDZ, żąda potwierdzenia dostarczenia wiadomości zawierającej JEDZ.
h) Datą przesłania JEDZ będzie potwierdzenie dostarczenia wiadomości zawierającej JEDZ z serwera pocztowego zamawiającego.
i) Obowiązek złożenia JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym w sposób określony powyżej dotyczy również JEDZ składanego na wezwanie w trybie art. 26 ust. 3 ustawy Pzp; w takim przypadku Zamawiający nie wymaga szyfrowania tego dokumentu.

2. Formularz Oferta – wg załącznika nr 1 do specyfikacji.
   Ofertę składa się pod rygorem nieważności w formie pisemnej.

3. Oświadczenie w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO zgodnie z załącznikiem nr 7 do specyfikacji.

4. Zgodnie z art. 24 ust. 11 ustawy Pzp, Wykonawca, w terminie 3 dni od zamieszczenia na stronie internetowej informacji z otwarcia ofert, o której mowa w art. 86 ust. 5 ustawy Pzp, przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy Pzp. Wykonawca składa niniejsze oświadczenie zgodnie z wzorem określonym w załączniku nr 3 do specyfikacji. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

7. <u>Przed udzieleniem zamówienia</u>, Zamawiający będzie żądał od Wykonawcy, którego oferta została najwyżej oceniona, złożenia w wyznaczonym terminie nie krótszym niż 10 dni (aktualnych na dzień złożenia) oświadczeń lub dokumentów, potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy Pzp tj.

A. dokumentów lub oświadczeń potwierdzających, spełnianie warunków udziału w postępowaniu:

Wykazu wykonanych modernizacji sieci LAN, potwierdzającego spełnienie warunku udziału w postępowaniu, o którym mowa w pkt 5.1.1. SIWZ, wraz z załączonymi dowodami potwierdzającymi, że usługi te zostały wykonane należycie – **wg Załącznika Nr 4 do SIWZ**
Dowodami, o których mowa w pkt 16.A.1) są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz, którego dostawy lub usługi były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3

miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu.

B. dokumentów lub oświadczeń potwierdzających brak podstaw wykluczenia z postępowania w okolicznościach, o których mowa w art. 24 ust. 1 ustawy Pzp (poza oświadczeniem wskazanym w pkt. 6.1 SIWZ), to jest:

1) informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu;
2) zaświadczenia właściwego naczelnika urzędu skarbowego potwierdzającego, że wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem podatkowym w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
3) zaświadczenia właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert, lub innego dokumentu potwierdzającego, że wykonawca zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;
4) odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 5 pkt 1 ustawy;

Dokumenty wymagane od Wykonawców mających siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej:

1. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa:
   1.1. w punkcie B.1 – składa informację z odpowiedniego rejestru albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w art. 24 ust. 1 pkt 13, 14 i 21 ustawy;
   1.2. w punkcie B.2-4 - składa dokument lub dokumenty, wystawione w kraju, w którym ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
      a) nie zalega z uiszczaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu,
      b) nie otwarto jego likwidacji ani nie ogłoszono upadłości
2. Dokumenty, o których mowa w pkt 1.1. i 1.2. lit. b. powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert. Dokument, o którym mowa w pkt 1.2. lit. a) powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
3. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa w ust. 1, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy,

ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby. Przepis ust. 2 stosuje się.

4. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a ustawy Pzp, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w rozdziale 7 pkt B.
5. Zamawiający może żądać od Wykonawcy przedstawienia dokumentów wymienionych rozdziale 7 pkt B, dotyczących podwykonawcy, któremu zamierza powierzyć wykonanie części zamówienia, a który nie jest podmiotem, na którego zdolnościach lub sytuacji Wykonawca polega na zasadach określonych w art. 22a ustawy Pzp.

8. Informacje o sposobie porozumiewania się zamawiającego z wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z wykonawcami.

W niniejszym postępowaniu wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje można przekazywać pisemnie, faxem lub drogą elektroniczną.
Osobą upoważnioną do kontaktowania się z wykonawcami jest:
Jolanta Pietrasińska, tel. 81 53-105-11, e-mail jolanta.pietrasinska@nfz-lublin.pl
Adres strony internetowej, na której zamieszczone jest ogłoszenie o zamówieniu oraz specyfikacja istotnych warunków zamówienia: www.nfz-lublin.pl Na stronie tej zamawiający będzie zamieszczał również inne informacje wymagane prawem zamówień publicznych związane z niniejszym postępowaniem.

9. Wymagania dotyczące wadium

1) Składający ofertę winien wnieść **wadium w wysokości: 15 000,00 zł** (słownie: piętnaście tysięcy złotych),

Wadium może być wnoszone 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. DzU z 2007 Nr 42 poz.275 ze zm.).

2) Dokumenty potwierdzające wniesienie wadium powinny być załączone do oferty.

3) Wadium wnoszone w pieniądzu należy wpłacić przelewem na konto Zamawiającego w BGK, nr 45 1130 1206 0028 9000 1220 0004,

4) Wadium wniesione w formie gwarancji ubezpieczeniowej lub bankowej będzie akceptowane pod warunkiem, że jest zgodne z Prawem zamówień publicznych, a w szczególności:

- gwarancja będzie zawierała wszystkie przypadki utraty wadium przez wykonawcę określone w art. 46 ust. 4 a i 5 Prawa zamówień publicznych
- okres ważności gwarancji będzie nie krótszy niż okres związania ofertą określony w specyfikacji istotnych warunków zamówienia

5) Wadium wniesione w formie poręczenia bankowego, poręczenia spółdzielczej kasy oszczędnościowo-kredytowej lub poręczenia udzielonego przez podmiot, o którym mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości będzie akceptowane pod warunkiem, że jest zgodne z Prawem zamówień publicznych, a w szczególności:

- poręczenie będzie zawierało wszystkie przypadki utraty wadium przez wykonawcę określone w art. 46 ust. 4 a i 5 Prawa zamówień publicznych,

- poręczenie będzie zawierało określony datą termin odpowiedzialności, nie krótszy niż okres związania ofertą określony w specyfikacji istotnych warunków zamówienia.

6) Wadium wnoszone w innej formie niż w pieniądzu, powinno zawierać, bezwarunkowe bezwzględne i nieodwołalne zobowiązanie podmiotu udzielającego do wypłaty kwoty wadium w przypadkach wymienionych w art. 46 ust. 4a i 5 ustawy.

10. Termin związania ofertą.

Wykonawca będzie związany ofertą 60 dni od upływu terminu składania ofert.

11. Opis sposobu przygotowania ofert.

Ofertę należy napisać pismem czytelnym w języku polskim. Poprawki powinny być naniesione czytelnie oraz opatrzone podpisem osoby upoważnionej.

Dokumenty składające się na ofertę powinny być podpisane przez osobę upoważnioną do występowania w imieniu wykonawcy (uprawnioną zgodnie z odpisem z Krajowego Rejestru Sądowego lub z zaświadczeniem o wpisie do ewidencji działalności gospodarczej) albo przez osobę umocowaną przez osobę uprawnioną.

Ofertę należy złożyć w trwale zamkniętej kopercie zaadresowanej: Lubelski Oddział Wojewódzki NFZ, ul. Szkolna 16, 20-124 Lublin, opatrzonej pieczęcią lub danymi adresowymi oferenta oraz posiadającej następujące oznaczenie:

„**Oferta na modernizację sieci LAN**, nie otwierać przed 02.10.2018 r. godz. 14.15".

12. Miejsce oraz termin składania i otwarcia ofert.

Oferty należy składać osobiście lub przesłać pocztą do Lubelskiego Oddziału Wojewódzkiego NFZ, ul. Szkolna 16, 20-124, Lublin, pokój nr 20 w terminie do dnia **02.10.2018 r. do godziny 14.00.**

Decyduje data i godzina wpływu oferty do zamawiającego, a nie data jej wysłania przesyłką pocztową czy kurierską. Oferty złożone po terminie zostaną niezwłocznie zwrócone oferentom. **Otwarcie ofert nastąpi w siedzibie Zamawiającego przy ul. Szkolnej 16 w Lublinie, pokój nr 18 w dniu 02.10.2018 r. o godzinie 14.15.**

13. Opis sposobu obliczenia ceny

Cenę oferty należy obliczyć zgodnie z formularzem kosztorysu ofertowego, według załącznika nr 7 do specyfikacji. Cena powinna zawierać w sobie ewentualne upusty, marże oraz należne podatki.

14. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty wraz z podaniem znaczenia tych kryteriów oraz sposobu oceny ofert.

1. Kryteria oceny ofert

1. Cena zamówienia – 60%
2. Jednorodność rozwiązania – 20%
3. Okres gwarancji -20%

2) Szczegółowe zasady oceny z tytułu kryteriów zostały przedstawione poniżej.

Kryterium C: Cena (60% wagi oceny)

Z tytułu niniejszego kryterium maksymalna ilość punktów wynosi 60.

Oferta o najkorzystniejszej (najniższej) cenie uzyska 60 pkt. Pozostałe ceny obliczone dla badanych ofert zostaną porównane z ofertą o najkorzystniejszej (najniższej) cenie, stosując wzór opisany w punkcie 14.3 SIWZ.

Kryterium J: Jednorodność rozwiązania – 20%

Z tytułu niniejszego kryterium maksymalna liczba punktów wynosi 20.

W przypadku zaoferowania przez Wykonawcę urządzeń i komponentów określonych w punktach 1, 2, 3 i 4 załącznika nr 5, pochodzących od jednego producenta oferta otrzyma maksymalną liczbę punktów (J = 20 pkt)
W przypadku gdy wykonawca zaoferuje rozwiązania kilku producentów dla ww. urządzeń i komponentów, oferta otrzyma 0 punktów (J = 0 pkt)

Kryterium G: Okres gwarancji -20%

Kryterium to będzie rozpatrywane na podstawie zaoferowanego okresu gwarancji na modernizację sieci LAN.
Z tytułu niniejszego kryterium maksymalna liczba punktów **wynosi 20**.
Sposób obliczania wartości punktowej kryterium oferowanego terminu wykonania zamówienia:
Okres gwarancji 24 miesiące = 0 pkt
Okres gwarancji 36 miesięcy = 20 pkt
Zaproponowanie przez Wykonawcę innego okresu gwarancji niż wskazane powyżej spowoduje odrzucenie oferty.

3) Sposób obliczenia wartości punktowej

$$\textbf{Ilość punktów} = \frac{\textit{cena najniższa}}{\textit{cena oferty badanej}} \times \mathbf{60} + \textbf{punkty uzyskane za jednorodność rozwiązania (J = 20 lub 0) + punkty uzyskane za zaoferowany okres gwarancji (G = 20 lub 0)}$$

Zaokrąglenia w obliczeniach końcowych punktacji — do dwóch miejsc po przecinku
Najkorzystniejszą ofertą jest oferta z najwyższą ilością punktów. Maksymalna ilość punktów, która może zostać przyznana ofercie wynosi 100.

15. Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.
Wykonawca, którego oferta zostanie wybrana zobowiązany jest podpisać umowę w miejscu i terminie wskazanym przez zamawiającego.

16. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.
Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

17. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy | w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli zamawiający wymaga od wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach
Istotne postanowienia umowy zawiera załącznik nr 6.

18. Pouczenie o środkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia.
Wykonawcom a także innym osobom, jeżeli ich interes prawny w uzyskaniu zamówienia doznał lub może doznać uszczerbku w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki ochrony prawnej zgodnie z Działem VI ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych.

19. Oferty częściowe
Zamawiający nie dopuszcza składania ofert częściowych.

20. Umowa ramowa
Zamawiający nie przewiduje zawarcia umowy ramowej

21. Oferty wariantowe
Zamawiający nie dopuszcza możliwości składania ofert wariantowych

22. Informacja dotycząca walut obcych
Zamawiający nie przewiduje możliwości prowadzenia rozliczeń w walutach obcych.

23. Informacja dotycząca kosztów postępowania
Zamawiający nie przewiduje możliwości zwrotu kosztów udziału w postępowaniu.

24. Podwykonawcy
Zamawiający dopuszcza udział podwykonawców w wykonaniu zamówienia. W przypadku powierzenia wykonywania części zamówienia podwykonawcom, Wykonawca wskaże w formularzu oferta, stanowiącym załącznik nr 1 do specyfikacji, części zamówienia, które powierzy podwykonawcom oraz nazwy podwykonawców.

Podpisano:

Członkowie Komisji przetargowej.

ZATWIERDZAM

Dyrektor
Lubelskiego Oddziału Wojewódzkiego
Narodowego Funduszu Zdrowia
Karol Tarkowski

Załącznik nr 1

OFERTA

z dnia .....

Dane oferenta:

nazwa.....

siedziba.....

nr telefonu ....., nr faxu .....

e-mail .....

REGON....., NIP ……..

Oferent jest małym lub średnim przedsiębiorcą: TAK / NIE * *(*niepotrzebne skreślić)*

Do:
Lubelski Oddział Wojewódzki Narodowego Funduszu Zdrowia
ul. Szkolna 16, 20-124 Lublin

Oferujemy realizację zamówienia dotyczącego modernizacji sieci LAN, zgodnie ze specyfikacją istotnych warunków zamówienia za kwotę:

brutto ..... zł.

(słownie .....)

w tym kwota netto wynosi ..... zł

(słownie .....)

podatek VAT w wysokości ..... zł

(słownie .....)

2. Szczegółowa charakterystyka przedmiotu oferty (opis oferowanych przez Wykonawcę urządzeń i komponentów z określeniem producenta) stanowi załącznik nr ..... do oferty.

3. Na przeprowadzoną modernizację sieci LAN udzielamy …….. * miesięcy gwarancji. *(*24 miesiące lub 36 miesięcy)*

4. Zamówienie wykonamy w terminie do ..... * dni od podpisania umowy *(*nie dłużej niż 60 dni kalendarzowych)*.

5. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez 60 dni od terminu składania ofert.

6. Oświadczamy, że zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy w miejscu i terminie wyznaczonym przez zamawiającego.

7. Oświadczamy, że w rozliczeniach obowiązywać będzie 21 dniowy termin płatności.

8. Zamierzamy powierzyć podwykonawcom *(wymagane jest wskazanie nazw podwykonawców*)

   następujące części zamówienia: .....

   ……

9. Osobą/osobami upoważnionymi do podpisania umowy są:

.....
(imię nazwisko, stanowisko)

10. Hasło dostępu do pliku JEDZ ……

Podpisano
(upoważniony przedstawiciel oferenta)

Załącznik nr 2

STANDARDOWY FORMULARZ JEDNOLITEGO EUROPEJSKIEGO DOKUMENTU ZAMÓWIENIA

Załącznik nr 3

LISTA PODMIOTÓW
NALEŻĄCYCH DO GRUPY KAPITAŁOWEJ

W związku z ubieganiem się o udzielenie zamówienia publicznego na modernizację sieci LAN:

oświadczam/my, że:

a) należę/my do grupy kapitałowej (w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. 2015 r., poz. 184 z późn. zm.), w skład której wchodzą następujące podmioty: *

1) ……..
2) ……..
3) ……..

b) nie należę/my do żadnej grupy kapitałowej *

* niepotrzebne skreślić

…….. ……..
data imię i nazwisko

……..
podpis wykonawcy lub osoby upoważnionej

Załącznik nr 4

.....
Nazwa Wykonawcy

Wykaz zrealizowanych modernizacji sieci LAN
o wartości nie mniejszej niż 300 000,00 tys. zł

Nazwa Zleceniodawcy	Termin realizacji zamówienia	Opis i wartość dokonanej modernizacji

Do wykazu załączono …….....szt. dokumentów potwierdzających, że świadczone usługi zostały wykonane należycie.

.....
Pieczątka i podpis Wykonawcy

Załącznik nr 5

OPIS PRZEDMIOTU ZAMÓWIENIA

1. PRZEŁĄCZNIK DOSTĘPOWY 24 PORT – 2 sztuki

Wymagania podstawowe

1. Przełącznik posiadający 24 porty 10/100/1000BASE-T POE+
2. Przełącznik posiadający 4 wbudowane porty 10G SFP+
3. Wysokość urządzenia 1U
4. Nieblokująca architektura o wydajności przełączania min. 210 Gb/s
5. Szybkość przełączania min. 150 Milionów pakietów na sekundę
6. Możliwość łączenia do 8 przełączników w stos za pomocą wbudowanego portu stakującego
7. Możliwość łączenia do 8 przełączników w stos za pomocą portów 10G
8. Tablica MAC adresów min. 68k
9. Pamięć operacyjna: min. 1GB pamięci DRAM
10. Pamięć flash: min. 4GB pamięci Flash
11. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
12. Obsługa sieci wirtualnych protokołowych IEEE 802.1v
13. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
14. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
15. Obsługa Q-in-Q IEEE 802.1ad
16. Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
17. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
18. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
19. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
20. Przełącznik musi być wyposażony w redundantny system zasilania.
21. Wbudowany DHCP Serwer i klient
22. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
23. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
24. Możliwość monitorowania zajętości CPU
25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
26. Wbudowany dodatkowy port 10/100/1000BASE-T do zarządzania poza pasmem - out of band management.
27. Wbudowany port USB do łatwego backupu konfiguracji
28. Obsługa CDPv2
29. Sumaryczna moc POE+ nie mniejsza niż 720W

Obsługa Routingu IPv4

30. Sprzętowa obsługa routingu IPv4 – forwarding
31. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów
32. Routing statyczny
33. Obsługa routingu dynamicznego IPv4
    a. RIPv1/v2
    b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania

Obsługa Routingu IPv6

34. Sprzętowa obsługa routingu IPv6 – forwarding
35. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów
36. Routing statyczny
37. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
38. Telnet Serwer/Klient dla IPv6
39. SSH2 Serwer/Klient dla IPv6
40. Ping dla IPv6
41. Tracert dla IPv6
42. Obsługa MLDv1 (Multicast Listener Discovery version 1)

Obsługa Multicastów

43. Filtrowanie IGMP
44. Obsługa Multicast VLAN Registration - MVR
45. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo

46. Obsługa Network Login
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
47. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
48. Możliwość integracji funkcjonalności Network Login z Microsoft NAP
49. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
50. Obsługa Guest VLAN dla IEEE 802.1x
51. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
52. Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication
53. Obsługa Identity Management
54. Wbudowana obrona procesora urządzenia przed atakami DoS
55. Obsługa TACACS+ (RFC 1492)
56. Obsługa RADIUS Authentication (RFC 2138)
57. Obsługa RADIUS Accounting (RFC 2139)
58. RADIUS and TACACS+ per-command Authentication
59. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie (ang. sticky)
    c. możliwość wpisania statycznych MAC adresów na port/vlan
60. Możliwość wyłączenia MAC learning
61. Obsługa SNMPv1/v2/v3
62. Klient SSH2
63. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
64. Listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4

d. Adres MAC źródłowy i docelowy plus maska
e. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
f. Protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
g. Numery portów źródłowych i docelowych TCP, UDP
h. Zakresy portów źródłowych i docelowych TCP, UDP
i. Identyfikator sieci VLAN – VLAN ID
j. Flagi TCP
k. Obsługa fragmentów

65. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
66. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania
67. Obsługa bezpiecznego transferu plików SCP/SFTP
68. Obsługa DHCP Option 82
69. Obsługa IP Security - Gratuitous ARP Protection
70. Obsługa IP Security - Trusted DHCP Server
71. Obsługa IP Security - DHCP Snooping
72. Obsługa IP Security - DHCP Secured ARP/ARP Validation
73. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 64 kb/s

Bezpieczeństwo sieciowe

74. Możliwość konfiguracji portu głównego i zapasowego
75. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
76. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
77. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
78. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
79. Obsługa PVST+
80. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
81. Obsługa G.8032 v1/v2
82. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.
83. Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

84. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
85. Obsługa synchronizacji czasu NTP
86. Zarządzanie przez SNMP v1/v2/v3
87. Zarządzanie przez przeglądarkę WWW – protokół http i https
88. Możliwość zarządzania poprzez protokół XML
89. Telnet Serwer/Klient dla IPv4 / IPv6
90. SSH2 Serwer/Klient dla IPv4 / IPv6
91. Ping dla IPv4 / IPv6
92. Traceroute dla IPv4 / IPv6
93. Obsługa SYSLOG z możliwością definiowania wielu serwerów
94. Sprzętowa obsługa sFlow
95. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
96. Obsługa RMON2 (RFC 2021)

Inne

97. Obsługa skryptów CLI
98. Obsługa funkcji TCL/Tk w skryptach CLI
99. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
100. Obsługa OpenFlow – możliwość rozszerzenia przez licencje
101. Obsługa AVB (Audio Video Bridging)- możliwość rozszerzenia przez licencję oprogramowania
102. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym
103. Oferowane urządzenia muszą umożliwiać integrację z posiadanymi przez Zamawiającego urządzeniami Cisco VoIP w zakresie automatycznego rozpoznania i autoryzacji podłączonych telefonów wraz z auto konfiguracją portu sieciowego poprzez przydzielenie im osobnego VLAN'u oraz QoS.
104. Gwarancja minimum 24 miesiące typu NBD, umożliwiająca naprawę urządzeń, wsparcie techniczne i aktualizację firmware.

2. PRZEŁĄCZNIK DOSTĘPOWY 48 PORT – 10 sztuk

Wymagania podstawowe

1. Przełącznik posiadający 48 portów 10/100/1000BASE-T POE+
2. Przełącznik posiadający 4 wbudowane porty 10G SFP+
3. Wysokość urządzenia 1U
4. Nieblokująca architektura o wydajności przełączania min. 260 Gb/s
5. Szybkość przełączania min. 190 Milionów pakietów na sekundę
6. Możliwość łączenia do 8 przełączników w stos za pomocą wbudowanego portu stakującego
7. Możliwość łączenia do 8 przełączników w stos za pomocą portów 10G
8. Tablica MAC adresów min. 68k
9. Pamięć operacyjna: min. 1GB pamięci DRAM
10. Pamięć flash: min. 4GB pamięci Flash
11. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
12. Obsługa sieci wirtualnych protokołowych IEEE 802.1v
13. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
14. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
15. Obsługa Q-in-Q IEEE 802.1ad
16. Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
17. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
18. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
19. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
20. Przełącznik musi być wyposażony w redundantny system zasilania.
21. Wbudowany DHCP Serwer i klient
22. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
23. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
24. Możliwość monitorowania zajętości CPU
25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
26. Wbudowany dodatkowy port 10/100/1000BASE-T do zarządzania poza pasmem - out of band management.
27. Wbudowany port USB do łatwego backupu konfiguracji
28. Sumaryczna moc POE+ nie mniejsza niż 1440W

Obsługa Routingu IPv4

29. Sprzętowa obsługa routingu IPv4 – forwarding
30. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów
31. Routing statyczny
32. Obsługa routingu dynamicznego IPv4
    a. RIPv1/v2
    b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania

Obsługa Routingu IPv6

33. Sprzętowa obsługa routingu IPv6 – forwarding
34. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów
35. Routing statyczny
36. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
37. Telnet Serwer/Klient dla IPv6
38. SSH2 Serwer/Klient dla IPv6
39. Ping dla IPv6
40. Tracert dla IPv6
41. Obsługa MLDv1 (Multicast Listener Discovery version 1)

Obsługa Multicastów

42. Filtrowanie IGMP
43. Obsługa Multicast VLAN Registration - MVR
44. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo

45. Obsługa Network Login
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
46. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
47. Możliwość integracji funkcjonalności Network Login z Microsoft NAP
48. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
49. Obsługa Guest VLAN dla IEEE 802.1x
50. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
51. Obsługa Identity Management
52. Wbudowana obrona procesora urządzenia przed atakami DoS
53. Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication
54. Obsługa TACACS+ (RFC 1492)
55. Obsługa RADIUS Authentication (RFC 2138)
56. Obsługa RADIUS Accounting (RFC 2139)
57. RADIUS and TACACS+ per-command Authentication
58. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    d. zatrzaśnięcie MAC adresu na porcie
    e. możliwość wpisania statycznych MAC adresów na port/vlan
59. Możliwość wyłączenia MAC learning
60. Obsługa SNMPv1/v2/v3
61. Klient SSH2
62. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
63. Listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4

a. Adres MAC źródłowy i docelowy plus maska
b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
c. Protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
d. Numery portów źródłowych i docelowych TCP, UDP
e. Zakresy portów źródłowych i docelowych TCP, UDP
f. Identyfikator sieci VLAN – VLAN ID
g. Flagi TCP
h. Obsługa fragmentów

64. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
65. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania
66. Obsługa bezpiecznego transferu plików SCP/SFTP
67. Obsługa DHCP Option 82
68. Obsługa IP Security - Gratuitous ARP Protection
69. Obsługa IP Security - Trusted DHCP Server
70. Obsługa IP Security - DHCP Snooping
71. Obsługa IP Security - DHCP Secured ARP/ARP Validation
72. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 64 kb/s

Bezpieczeństwo sieciowe

73. Możliwość konfiguracji portu głównego i zapasowego
74. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
75. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
76. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
77. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
78. Obsługa PVST+
79. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
80. Obsługa G.8032 v1/v2
81. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.
82. Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.

Zarządzanie

83. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
84. Obsługa synchronizacji czasu NTP
85. Zarządzanie przez SNMP v1/v2/v3
86. Zarządzanie przez przeglądarkę WWW – protokół http i https
87. Możliwość zarządzania poprzez protokół XML
88. Telnet Serwer/Klient dla IPv4 / IPv6
89. SSH2 Serwer/Klient dla IPv4 / IPv6
90. Ping dla IPv4 / IPv6
91. Traceroute dla IPv4 / IPv6
92. Obsługa SYSLOG z możliwością definiowania wielu serwerów
93. Sprzętowa obsługa sFlow
94. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
95. Obsługa RMON2 (RFC 2021)

Inne

96. Obsługa skryptów CLI
97. Obsługa funkcji TCL/Tk w skryptach CLI
98. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
99. Obsługa OpenFlow – możliwość rozszerzenia przez licencje
100. Obsługa AVB (Audio Video Bridging)- możliwość rozszerzenia przez licencję oprogramowania
101. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym
102. Oferowane urządzenia muszą umożliwiać integrację z posiadanymi przez Zamawiającego urządzeniami Cisco VoIP w zakresie automatycznego rozpoznania i autoryzacji podłączonych telefonów wraz z auto konfiguracją portu sieciowego poprzez przydzielenie im osobnego VLAN'u oraz QoS
103. Gwarancja minimum 24 miesiące typu NBD, umożliwiająca naprawę urządzeń, wsparcie techniczne i aktualizację firmware.

3. PRZEŁĄCZNIK SZKIELETOWY – 2 sztuki

Wymagania podstawowe

1. Przełącznik posiadający 48 portów 10Gigabit Ethernet SFP+, mogących pracować z prędkością 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+
2. 4 porty 40GBASE-X QSFP+
3. Wysokość urządzenia 1U
4. Nieblokująca architektura o wydajności przełączania min. 1280 Gb/s
5. Szybkość przełączania min. 950 Milionów pakietów na sekundę
6. Tablica MAC adresów min. 280k
7. Pamięć operacyjna: min. 2 GB pamięci DRAM
8. Pamięć flash: min. 4 GB pamięci Flash
9. Możliwość stakowania do 8 przełączników
10. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
11. Obsługa sieci wirtualnych protokołowych IEEE 802.1v
12. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
13. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
14. Obsługa Q-in-Q IEEE 802.1ad
15. Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
16. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
17. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
18. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
19. Przełącznik wyposażony w dwa modularne, wewnętrzne zasilacze, które umożliwiają uzyskanie redundancji zasilania. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika
20. Przepływ powietrza w przełączniku: przód-tył
21. Moduł wentylatorów zapewniający ich redundancję
22. Wbudowany DHCP Serwer i klient
23. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
24. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
25. Możliwość monitorowania zajętości CPU
26. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
27. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
28. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
29. Przełączniki wyposażone w niezbędne kable stakujące (o długości 0,5 m)

Obsługa Routingu IPv4

30. Sprzętowa obsługa routingu IPv4 - forwarding
31. Pojemność tabeli routingu min. 16 tys. wpisów
32. Routing statyczny
33. Obsługa routingu dynamicznego IPv4

    a. RIP v1/v2
    b. OSPFv2 - możliwość rozszerzenia przez licencje
    c. BGPv4 - możliwość rozszerzenia przez licencje
    d. IS-IS - możliwość rozszerzenia przez licencje
34. Policy Based Routing dla IPv4

Obsługa Routingu IPv6

35. Sprzętowa obsługa routingu IPv6 - forwarding
36. Pojemność tabeli routingu min. 8 tys. wpisów
37. Routing statyczny
38. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. OSPF v3
    c. IS-IS
39. Telnet Serwer/Klient dla IPv6
40. SSH2 Serwer/Klient dla IPv6
41. Ping dla IPv6
42. Tracert dla IPv6
43. Obsługa 6to4 (RFC 3056)
44. Obsługa MLDv1 (Multicast Listener Discovery version 1)
45. Policy Based Routing dla IPv6

Obsługa Multicastów

46. Statyczne przyłączanie do grupy multicast
47. Filtrowanie IGMP
48. Obsługa PIM-SM
49. Obsługa PIM-DM
50. Obsługa PIM-SSM
51. Obsługa PIM snooping
52. Obsługa Multicast VLAN Registration - MVR
53. Obsługa IGMP v1 - RFC 1112
54. Obsługa IGMP v2 - RFC 2236
55. Obsługa IGMP v3 - RFC 3376
56. Obsługa IGMP v1/v2/v3 snooping
57. Możliwość konfiguracji statycznych tras dla Routingu Multicastów

Bezpieczeństwo

58. Obsługa Network Login
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
59. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
60. Możliwość integracji funkcjonalności Network Login z Microsoft NAP
61. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
62. Obsługa Guest VLAN dla IEEE 802.1x
63. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
64. Obsługa Identity Management
65. Wbudowana obrona procesora urządzenia przed atakami DoS

66. Obsługa TACACS+
67. Obsługa RADIUS Authentication (RFC 2138)
68. Obsługa RADIUS Accounting (RFC 2139)
69. RADIUS and TACACS+ per-command Authentication
70. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
71. Możliwość wyłączenia MAC learning
72. Obsługa SNMPv1/v2/v3
73. Klient SSH2
74. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
75. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    a. Adres MAC źródłowy i docelowy plus maska
    b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    d. Numery portów źródłowych i docelowych TCP, UDP
    e. Zakresy portów źródłowych i docelowych TCP, UDP
    f. Identyfikator sieci VLAN - VLAN ID
    g. Flagi TCP
    h. Obsługa fragmentów
76. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
77. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
78. Obsługa bezpiecznego transferu plików SCP/SFTP
79. Obsługa DHCP Option 82
80. Obsługa IP Security - Gratuitous ARP Protection
81. Obsługa IP Security – Trusted DHCP Server
82. Obsługa IP Security – DHCP Secured ARP/ARP Validation
83. Ograniczanie przepustowości (rate limiting) na portach wyjściowych

Bezpieczeństwo sieciowe

84. Możliwość konfiguracji portu głównego i zapasowego
85. Obsługa redundancji routingu VRRP - RFC 2338
86. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
87. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
88. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
89. Obsługa PVST+
90. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
91. Obsługa G.8032 v1/v2
92. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
93. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników

Zarządzanie

94. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
95. Obsługa synchronizacji czasu NTP
96. Zarządzanie przez SNMP v1/v2/v3
97. Zarządzanie przez przeglądarkę WWW – protokół http i https
98. Możliwość zarządzania przez protokół XML
99. Telnet Serwer/Klient dla IPv4 / IPv6
100. SSH2 Serwer/Klient dla IPv4 / IPv6
101. Ping dla IPv4 / IPv6
102. Traceroute dla IPv4 / IPv6
103. Obsługa SYSLOG z możliwością definiowania wielu serwerów
104. Sprzętowa obsługa sFlow
105. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
106. Obsługa RMON2 (RFC 2021)

Inne

107. Zakres temperatury pracy 0-45 °C
108. Możliwość rozszerzenia funkcjonalności o MPLS poprzez wymianę oprogramowania lub licencję. Wymagane wsparcie dla następujących funkcjonalności: MPLS/VPLS, MPLS/VPWS, LDP, RSVP-TE, Fast Reroute
109. Obsługa skryptów CLI
110. Obsługa funkcji TCL/Tk w skryptach CLI
111. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
112. Obsługa OpenFlow – możliwość rozszerzenia przez licencje
113. Obsługa AVB (Audio Video Bridging) - możliwość rozszerzenia przez licencje
114. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym
115. Oferowane urządzenia muszą umożliwiać integrację z posiadanymi przez Zamawiającego urządzeniami Cisco VoIP w zakresie automatycznego rozpoznania i autoryzacji podłączonych telefonów wraz z auto konfiguracją portu sieciowego poprzez przydzielenie im osobnego VLAN'u oraz QoS
116. Gwarancja minimum 24 miesiące typu NBD, umożliwiająca naprawę urządzeń, wsparcie techniczne i aktualizację firmware.

4. SYSTEM ZARZĄDZANIA

1. Aplikacja musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera
   a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, Windows oraz jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare
   b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.
2. Aplikacja musi zarządzać siecią przewodową i bezprzewodową
3. Aplikacja zarządzająca musi obsługiwać minimum 25 urządzeń (adresów IP)
4. Aplikacja zarządzająca musi pozwalać na zarządzanie siecią dla minimum 25 jednoczesnych użytkowników.
5. Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego
6. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
7. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
8. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
9. Aplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
10. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
11. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
12. Aplikacja musi posiadać wbudowaną przeglądarkę SNMP MIB
13. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
14. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
15. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla danych urządzeń sieciowych.
16. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
17. Aplikacja musi posiadać wbudowany Syslog serwer
18. Aplikacja musi posiadać wbudowany BootP serwer
19. Aplikacja musi wspierać protokół IPv4 oraz IPv6
20. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
21. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
22. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
23. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
   a. połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości
   b. stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów

c. konfiguracji sieci VLAN
d. konfiguracji protokołu routingu OSPF

24. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/https
25. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
    a. adres IP urządzenia
    b. adresu MAC urządzenia
    c. nazwy urządzenia
    d. wersji oprogramowania
    e. wersji bootrom
    f. lokalizacji urządzenia
    g. danych kontaktowych administratora
    h. numeru seryjnego
26. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
    a. możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
    b. możliwość odtworzenia wskazanej konfiguracji urządzenia
    c. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych
    d. możliwość obsługi urządzeń sieciowych różnych producentów
27. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
28. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
29. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
30. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd itp.
31. Tworzona polityka musi zawierać możliwość:
    a. blokowania lub zezwalania ruchu na podstawie
        i) źródłowy i docelowy adres MAC
        ii) źródłowy i docelowy adres IP
        iii) źródłowy i docelowy adres IP podsieci
        iv) źródłowy i docelowy port TCP/UDP
        v) źródłowy i docelowy zakres portów TCP/UDP
        vi) typ protokołu
        vii) pole IP TOS
    b. przydziału parametrów QoS
        i) priorytety
        ii) ograniczenia przepustowości
    c. przydziału użytkownika do wskazanej sieci VLAN
    d. przekierowania ruchu do zewnętrznego systemu analizującego pakiety
32. Aplikacja musi mieć możliwość wdrażania polityk bezpieczeństwa w całej sieci, dla urządzeń przewodowych i bezprzewodowych za pomocą jednego kliknięcia.
33. Aplikacja musi pozwalać na łatwą modyfikację i ponowne wdrożenie na wszystkich urządzeniach przewodowych i bezprzewodowych
34. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
    a. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności

korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).

b. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
c. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
d. generowanie raportów

35. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.
    a. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
    b. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac
    c. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
        i) adres IP kontrolera
        ii) liczba obsługiwanych klientów
        iii) szczytowe wartości zajmowanego pasma
        iv) wersja oprogramowania
    d. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
        i) adres IP punktu dostępowego
        ii) MAC adres punktu dostępowego
        iii) wersja oprogramowania
        iv) typ punktu dostępowego
        v) kanały pracy poszczególnych interfejsów radiowych
        vi) szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
    e. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
        i) adres IP klienta
        ii) MAC adres klienta
        iii) nazwa użytkownika
        iv) nazwa punktu dostępowego, do którego dołączony jest użytkownik
        v) BSSID, do którego dołączony jest użytkownik
        vi) SSID, do którego dołączony jest użytkownik
    f. Musi być zapewniona możliwość tworzenia map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
        i) zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
        ii) zaznaczenie kanałów pracy urządzeń
        iii) lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych
36. Aplikacja zarządzająca musi być zintegrowana z systemem zapewniającym widoczność zautoryzowanych klientów w sieci z zapewnieniem widzialności następujących informacji:
    a. adresu MAC
    b. adresu IP
    c. nazwy komputera
    d. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7,10, iPhone / IOS itp.
    e. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
    f. adres IP urządzenia, do którego dołączony jest klient.

g. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
h. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
i. nazwa przydzielonej polityki bezpieczeństwa.

37. System zapewniający widoczność zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.
38. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
39. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List
40. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
41. System zapewniający widoczność zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
    a. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
    b. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
    c. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
    d. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
    e. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
42. System zapewniający widoczność zautoryzowanych klientów jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 1500 urządzeń klienckich (adresów IP). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 250 punktów dostępowych oraz min. 25 przełączników sieciowych. System musi umożliwiać w przyszłości rozbudowę do minimum 250 urządzeń sieciowych i 1000 punktów dostępowych.
43. System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na analizę ruchu w sieci do warstwy 7.
44. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów.
45. System powinien umożliwiać integrację z posiadanymi, przez Zamawiającego, urządzeniami Fortinet na poziomie automatycznej dystrybucji zautoryzowanych użytkowników przez oferowany system zarządzania do firewalla brzegowego oraz podejmowanie automatycznej reakcji na zaistniałe incydenty. W celu wdrożenia funkcjonalności Wykonawca musi posiadać inżyniera z ważnym certyfikatem Fortinet Security Expert 7.
46. System zarządzania musi być objęty minimum 24 miesięcznym wsparciem umożliwiającym wsparcie techniczne i aktualizację oprogramowania.

5. DODATKOWE WYPOSAŻENIE

W ramach realizacji zamówienia należy dostarczyć:

1. Kable 40Gb QSFP+ służące do połączenia przełączników szkieletowych w stos o długości 0,5m – szt. **2**
2. Kable umożliwiające łącznie przełączników dostępowych w stos po dedykowanych do tego celu portach o długości 0,5m – szt. **10**
3. Kable umożliwiające łącznie przełączników dostępowych w stos po dedykowanych do tego celu portach o długości 3m – szt. **2**
4. Moduł optyczny 10Gb SFP+ dla światłowodu wielomodowego zgodny z oferowanymi przełącznikami - szt. **36**
5. Moduł optyczny 10Gb SFP+ dla światłowodu wielomodowego **zgodny z urządzeniami HP** - szt. **2**
6. Moduł optyczny 1Gb SFP dla światłowodu wielomodowego zgodny z oferowanymi przełącznikami - szt. **4**
7. Moduł umożliwiający zamianę portu SFP przełącznika na port typu 10/100/1000BASE-T zgodny z oferowanymi przełącznikami – szt. 4
8. Moduł optyczny 1Gb SFP dla światłowodu wielomodowego **zgodny z urządzeniami Fortinet** - szt. 4
9. W ramach postępowania należy dostarczyć trzy stacje zarządzające typu laptop wyposażone w dysk SSD o wielkości co najmniej 200GB, co najmniej w 16GB RAM, co najmniej dwurdzeniowy procesor, wyświetlacz maksymalnie 14 cala o rozdzielczości WQHD, kartę sieciową przewodową i bezprzewodową, zintegrowany modem GSM dla sieci 3G i 4G, moduł TPM, licencja Microsoft Windows 10 Professional PL, system operacyjny w wersji dla procesorów 64-bitowych w polskiej wersji językowe. Maksymalna waga: 1,5kg

6. Urządzenie sieciowe SSL-VPN

1. Urządzenie musi być oparte o dedykowaną platformę sprzętową oraz zapewniać obsługę co najmniej 25 jednoczesnych sesji SSL VPN z możliwością rozbudowy do 200 jednoczesnych sesji.
2. Urządzenie musi posiadać min 2 porty 1 GbE
3. Urządzenie musi posiadać dedykowany port zarządzający 1 GbE.
4. Urządzenie musi posiadać przepustowości 200 Mb/s
5. Urządzenie musi być wyposażone w dysk twardy o pojemności min 500 GB
6. Urządzenie musi mieć możliwość montażu w szafie 19", a jego wysokość nie może być większa niż 1U.
7. Urządzenie musi oferować zróżnicowane metody dostępu do zasobów:
   a. dostęp podstawowy (min. aplikacje Web; standardowe protokoły pocztowe – IMAP, POP3,SMTP; współdzielenie plików – NETBIOS, NFS; usługi terminalowe – telnet, SSH),
   b. dostęp do aplikacji klient-serwer (enkapsulacja dowolnej aplikacji TCP w protokół HTTPS) be konieczności zastosowania dodatkowych licencji,
   c. pełen dostęp sieciowy bez konieczności zastosowania dodatkowych licencji - praca w trybie wysokiej dostępności (SSL) oraz wysokiej wydajności (ESP wraz z kompresją treści). Możliwość automatycznego przełączania z trybu wysokiej wydajności do trybu wysokiej dostępności.
8. Rozwiązanie musi umożliwiać autentykację użytkowników w oparciu o:
   - serwery RADIUS,
   - usługi katalogowe LDAP, Microsoft Active Directory, Novell NDS/eDirectory,
   - lokalna baza danych użytkowników,
   - system RSA SecurID,
   - certyfikaty X.509,
   - serwery NIS
9. Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (hasło statyczne plus certyfikat, hasło dynamiczne plus certyfikat). Musi istnieć możliwość rozdzielenia serwera autentykacji użytkowników od serwera autoryzacji dostępu do zasobów.
10. Urządzenie musi umożliwiać obsługę CRL poprzez http.
11. Urządzenie musi umożliwiać dynamiczne przyznawanie praw dostępu do zasobów w zależności od: spełnienia określonych warunków przez użytkownika zdalnego, węzeł zdalny, parametry sieci oraz parametry czasowe.
12. Urządzenie musi umożliwiać szczegółową weryfikację stanu bezpieczeństwa węzła zdalnego. Musi istnieć możliwość:
    - sprawdzenia obecności konkretnego procesu, pliku, wpisu w rejestrze Windows
    - sprawdzenia czy włączono odpowiednie usługi zabezpieczeń zarówno w momencie logowania jak w trakcie trwania sesji,
    - sprawdzenia czy wszystkie pobierane pliki pośrednie i pliki tymczasowe instalowane w czasie logowania są usuwane w momencie wylogowania,
    - sprawdzenia przed zalogowaniem takich atrybutów jak adres IP, typ przeglądarki, certyfikaty cyfrowe,
    - integracji z systemami weryfikacji stanu bezpieczeństwa firm trzecich,
13. Urządzenie musi umożliwiać budowanie konfiguracji odpornych na awarię w trybie Aktywny/Aktywny oraz Aktywny/Pasywny. Musi istnieć możliwość tworzenia konfiguracji nadmiarowej, w której węzły klastra zlokalizowane są w LAN bądź w odległych graficznie sieciach i komunikują się poprzez sieć WAN.
14. System musi umożliwiać spójne zarządzanie z jednej konsoli administracyjnej wieloma urządzeniami w przypadku budowania konfiguracji nadmiarowych.
15. Urządzenie musi być zarządzane poprzez przeglądarkę Web

16. Urządzenie musi umożliwiać wykonywanie lokalnych kopi zapasowych konfiguracji lub na zewnętrznym serwerze FTP oraz SCP .
17. Urządzenie musi umożliwiać integrację z zewnętrznymi serwerami SNMP v.2 oraz SYSLOG
18. Urządzenie musi przechowywać dwie wersje oprogramowania oraz umożliwiać reset do wersji fabrycznej.
19. Wraz z produktem wymagane jest dostarczenie opieki technicznej ważnej przez okres minimum 24 miesięcy. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

7. SZKOLENIA, WDROŻENIE, WSPARCIE TECHNICZNE

W ramach realizacji zamówienia należy dostarczyć vouchery na szkolenia z możliwością zdania egzaminu po ich ukończeniu:

1. Autoryzowane przez producenta oferowanych przełączników szkolenie z ich zarządzania i konfiguracji, czas trwania minimum 3 dni – 4 vouchery
2. Autoryzowane przez producenta oferowanego systemu zarządzania przełączników z jego administracji, czas trwania minimum 3 dni – 2 vouchery

W przypadku organizacji szkoleń w miejscu oddalonym o ponad 30 km od siedziby Zamawiającego Wykonawca zobowiązany jest zapewnić nocleg dla uczestników.

W ramach realizacji zamówienia należy wykonać wdrożenie oferowanych urządzeń i systemu zarządzania w siedzibie Zamawiającego. Zamawiający wymaga, aby wszystkie prace, które mogą spowodować przestoje w pracy sieci produkcyjnej, były przeprowadzane w godzinach 16.30 – 7.30. Zamawiający dopuszcza prowadzanie prac wdrożeniowych w dni wolne od pracy po wcześniejszym uzgodnieniu terminu. W ramach wdrożenia należy: wykonać montaż urządzeń, instalację sytemu zarządzania, konfigurację połączeń oraz stosy, konfigurację polityk dostępowych i innych zgodnych z SIWZ. Po wykonaniu wdrożenia należy dostarczyć dokumentację powykonawczą.
Po wykonaniu wdrożenia należy świadczyć na rzecz Zamawiającego wsparcie techniczne do oferowanych rozwiązań przez okres gwarancji. W tym celu wykonawca musi posiadać co najmniej dwóch inżynierów posiadających aktualny certyfikat techniczny (lub certyfikaty) wystawione przez producenta oferowanych przełączników sieciowych i systemu zarządzania potwierdzające wiedzę z ich zakresu.

Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 4 miesiące przed ich dostarczeniem) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym Wykonawca jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem).

Załącznik nr 6

Projekt umowy

zawarta w dniu
pomiędzy

§ 1

W wyniku przeprowadzenia przetargu nieograniczonego Zamawiający zleca, a Wykonawca zobowiązuje się do modernizacji sieci LAN, zgodnie ze specyfikacją istotnych warunków zamówienia i ofertą Wykonawcy z dnia ..... stanowiącą załącznik nr ..... do niniejszej umowy.

§ 2

Wynagrodzenie z tytułu realizacji przedmiotu umowy wynosi: Netto: ..... zł (słownie: .....) Podatek VAT: ..... zł (słownie: .....) Brutto: ..... zł (słownie: .....).

§ 3

1. Strony ustalają termin realizacji zamówienia na …… dni od podpisania umowy.

§ 4

1. Wykonawca na dokonaną modernizację sieci LAN, dostarczone urządzenia i materiały udziela gwarancji na okres ……. miesięcy, liczony od dnia podpisania protokołu odbioru.
2. Zamawiającemu, niezależnie od uprawnień z tytułu gwarancji, określonych w niniejszej umowie, przysługują uprawnienia z tytułu rękojmi.
3. W przypadku ujawnienia się w okresie gwarancji wad fizycznych Sprzętu lub zużycia świadczącego o niższej jakości niż zapewniana, Wykonawca zobowiązuje się do nieodpłatnego usunięcia tych wad w terminie wyznaczonym przez zamawiającego poprzez naprawę Sprzętu lub wymianę elementów, które uległy pogorszeniu.

§ 5

Wykonawca oświadcza, że sprzedany, dostarczony i zainstalowany Sprzęt nie posiada wad fizycznych, ani prawnych i jest najwyższej jakości oraz zobowiązuje się wykonać całość prac zgodnie z obowiązującymi przepisami prawa.

§ 6

1. Rozliczenie wynagrodzenia z tytułu realizacji umowy nastąpi w oparciu o fakturę VAT wystawioną po podpisaniu przez upoważnionych przedstawicieli stron protokołu odbioru.

2. Zamawiający dokona płatności faktury w formie przelewu na rachunek Wykonawcy nr …….. w ciągu 21 dni od daty otrzymania faktury wystawionej po realizacji zamówienia.
3. Zamawiający upoważnia Wykonawcę do wystawiania faktur VAT bez podpisu Zamawiającego.
4. Faktury powinna zawierać następujące dane:

Nabywca	Odbiorca i płatnik dowodu:
Narodowy Fundusz Zdrowia w Warszawie	Lubelski Oddział Wojewódzki w Lublinie
ul. Grójecka 186, 02-390 Warszawa	ul. Szkolna 16, 20-124 Lublin

NIP 1070001057

5. Strony przyjmują, że za dzień dokonania zapłaty uważają datę obciążenia rachunku bankowego Zamawiającego.

§ 7

1. Zamawiający może rozwiązać umowę w terminie 14 dni od dnia stwierdzenia nienależytego jej wykonania, wykonania w sposób sprzeczny z ofertą lub opóźniania się Wykonawcy z realizacją umowy powyżej 20 dni.

2. W przypadku zaistnienia sytuacji określonej w ust. 1 Wykonawcy przysługuje wyłącznie wynagrodzenie za wykonane i odebrane na podstawie protokołu odbioru prace.

§ 8

1. Wykonawca zapłaci Zamawiającemu karę umowną:
   1) za odstąpienie od umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, w wysokości 5% wartości umowy brutto określonej w § 2,
   2) za odstąpienie od umowy przez Wykonawcę, w wysokości 5% wartości umowy brutto określonej w § 2,
   3) za zwłokę w dostawie w wysokości 0,5% wartości umowy brutto określonej w § 2, za każdy dzień zwłoki,
   4) za zwłokę w usunięciu wad stwierdzonych przy odbiorze, w wysokości 0,5% wartości umowy brutto określonej w § 2 za każdy dzień zwłoki liczony od dnia wyznaczonego na usunięcie wad.
   5) za nieterminową naprawę Sprzętu w wysokości 500 zł brutto za każdy dzień opóźnienia po dniu ustalonym jako termin naprawy.
2. Wykonawca może obciążyć Zamawiającego odsetkami ustawowymi w przypadku zwłoki w dokonaniu zapłaty należności.
3. Strony mają prawo dochodzić odszkodowania uzupełniającego na zasadach Kodeksu Cywilnego, jeżeli szkoda przewyższa wartość kar umownych.

§ 9

1. Zamawiający wyznacza do nadzorowania prac związanych z realizacją niniejszej umowy oraz od podpisania protokołu odbioru następujące osoby:
……

2. Wykonawca wyznacza do nadzorowania prac związanych z realizacją niniejszej umowy oraz od podpisania protokołu odbioru następujące osoby:
……

§ 10

1. Strony oświadczają, że będą dążyć aby wszelkie ewentualne spory odnośnie treści lub wykonania umowy uzgadniać polubownie. Jeżeli rozwiązanie polubowne nie będzie możliwe, spór zostanie rozstrzygnięty przez właściwy sąd w Lublinie.
2. Wszelkie ustalenia związane z realizacją niniejszą umową strony wymagają formy pisemnej w postaci protokołów uzgodnień.
3. W sprawach nieuregulowanych niniejszą umową stosuje się przepisy ustawy z dnia 29 stycznia 2004 r. prawo zamówień publicznych oraz Kodeksu Cywilnego
4. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, dwa dla Zamawiającego, jeden dla Wykonawcy.

Wykonawca Zamawiający

Załącznik nr 7

Oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO

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

Podpisano
(upoważniony przedstawiciel oferenta)

[1)] rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

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