SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

(zwana dalej „SIWZ")

W POSTĘPOWANIU O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO PROWADZONYM W TRYBIE PRZETARGU NIEOGRANICZONEGO O WARTOŚCI SZACUNKOWEJ POWYŻEJ RÓWNOWARTOŚCI 135 000 EURO NA:

„Dostawę routerów oraz przełączników sieciowych, przełączników rdzeniowych w Centrali oraz w Oddziałach Instytutu Pamięci Narodowej"

Wspólny Słownik Zamówień (CPV):
32413100-2
32413000-1

ZAMAWIAJĄCY:
INSTYTUT PAMIĘCI NARODOWEJ
KOMISJA ŚCIGANIA ZBRODNI PRZECIWKO NARODOWI POLSKIEMU
UL. WOŁOSKA 7
02 – 675 WARSZAWA

I. INFORMACJE O ZAMAWIAJĄCYM (art. 36 ust. 1 pkt 1 Pzp)

1. Nazwa Zamawiającego: **Instytut Pamięci Narodowej – Komisja Ścigania Zbrodni przeciwko Narodowi Polskiemu**
2. Adres Zamawiającego: **ul. Wołoska 7, 02-675 Warszawa**
3. NIP Zamawiającego: **525-21-80-487**
4. Strona internetowa Zamawiającego: **http://www.ipn.gov.pl/**
5. Oznaczenie niniejszego postępowania: **BAG-11/17**

II. TRYB UDZIELENIA ZAMÓWIENIA (art. 36 ust. 1 pkt 2 Pzp)

1. Niniejsze postępowanie prowadzone jest w trybie **przetargu nieograniczonego** na podstawie art. 39 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r., poz. 2164 z późn. zm), zwaną dalej Pzp.
2. Wartość szacunkowa zamówienia przekracza kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 Pzp.

III. OPIS PRZEDMIOTU ZAMÓWIENIA (art. 36 ust. 1 pkt 3 Pzp)

1. Przedmiotem zamówienia jest zakup, dostawa oraz wsparcie usługi wdrożenia 26 szt. routerów, 81 przełączników sieciowych oraz 3 przełączników rdzeniowych w Centrali oraz w Oddziałach Instytutu Pamięci Narodowej.
2. Szczegółowe określenie przedmiotu zamówienia zawarte jest w załączniku nr 4 do Specyfikacji Istotnych Warunków Zamówienia – *Opis przedmiotu zamówienia*.
3. Zamawiający wymaga aby realizacja przedmiotu zamówienia nastąpiła na warunkach i zasadach określonych we wzorze umowy oraz zgodnie z opisem przedmiotu zamówienia.

IV. TERMIN WYKONANIA ZAMÓWIENIA (art. 36 ust. 1 pkt 4 Pzp)

Dostawa będzie realizowana jednorazowo (do Centrali IPN w Warszawie), **nie później niż do 60 dni kalendarzowych od dnia podpisania umowy.**

V. OPIS CZĘŚCI ZAMÓWIENIA (art. 36 ust. 2 pkt 1 Pzp)

Zamawiający nie dopuszcza możliwości składania ofert częściowych.

VI. ZAMÓWIENIA WARIANTOWE (art. 36 ust. 2 pkt 4 Pzp)

Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

VII. WARUNKI UCZESTNICTWA W POSTĘPOWANIU (art. 36 ust. 1 pkt 5 Pzp)

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
   1) posiadają doświadczenie, tj. wykonali w okresie ostatnich trzech (3) lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, **co najmniej dwie (2) dostawy routerów lub aktywnych urządzeń sieciowych, każda dostawa o wartości nie mniejszej niż 1 milion zł brutto,**
   2) nie podlegają wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 24 ust. 1 Pzp oraz ust. 5 pkt 1 ustawy Pzp.
2. Ocena spełnienia warunków udziału w postępowaniu zostanie dokonana w oparciu o informacje zawarte we właściwych dokumentach wyszczególnionych w rozdz. IX siwz. Z treści przedstawionych dokumentów musi jednoznacznie wynikać, że stawiane warunki Wykonawca spełnił. Niespełnienie warunków określonych w ust. 1 skutkować będzie wykluczeniem z postępowania.

   Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

3. 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 technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych. 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.
4. Zamawiający informuje, iż na podstawie art. 24 aa ustawy Pzp najpierw dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona jako najkorzystniejsza, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu.

VIII. PODSTAWY WYKLUCZENIA (art. 36 ust. 1 pkt 5 a Pzp)

1. Z postępowania o udzielenie zamówienia Zamawiający wykluczy Wykonawcę na podstawie art. 24 ust. 1 oraz ust. 5 pkt 1 Pzp tj. - Wykonawcę w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2015 r. poz. 978, 1259, 1513, 1830 i 1844 oraz z 2016 r. poz. 615) lub którego upadłość ogłoszono, z wyjątkiem Wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2015 r. poz. 233, 978, 1166, 1259 i 1844 oraz z 2016 r. poz. 615),
2. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16–20 lub ust. 5, ustawy Pzp może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu wykonawcy. Przepisu zdania pierwszego nie stosuje się, jeżeli wobec wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.

   Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu wykonawcy, uzna za wystarczające dowody przedstawione na podstawie art. 24 ust. 8 ustawy Pzp.
3. W przypadkach, o których mowa w art. 24 ust. 1 pkt 19 ustawy Pzp, przed wykluczeniem Wykonawcy, Zamawiający zapewnia temu Wykonawcy możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji.
4. Wykonawca, w terminie 3 dni od zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5, **przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej**, o której mowa w art. 24 ust. 1 pkt 23. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

IX. WYKAZ OŚWIADCZEŃ LUB DOKUMENÓW, POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW WYKLUCZENIA (art. 36 ust. 1 pkt 6 Pzp)

1. W celu potwierdzenia spełnienia warunków udziału w niniejszym postępowaniu o udzielenie

zamówienia publicznego Wykonawca dołącza do **Formularza ofertowego** (załącznik nr 1 do SIWZ) **oświadczenie o spełnianiu warunków z art. 22 ust. 1 pkt 2 Pzp w formie jednolitego dokumentu JEDZ sporządzonego zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE oraz art. 80 ust. 3 dyrektywy 2014/25/UE.**

2. W celu wykazania braku podstaw do wykluczenia z postępowania w okolicznościach, o których mowa w art. 24 ust. 1 oraz ust. 5 pkt 1 i 8 ustawy Pzp, Wykonawca dołącza do **Formularza ofertowego** (załącznik nr 1 do SIWZ) **oświadczenie o braku podstaw do wykluczenia z postępowania w formie jednolitego dokumentu JEDZ sporządzonego zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE oraz art. 80 ust. 3 dyrektywy 2014/25/UE.**

3. **W celu potwierdzenia braku podstaw do wykluczenia wykonawcy z udziału w postępowaniu Zamawiający wezwie Wykonawcę, którego oferta zostanie najwyżej oceniona do złożenia następujących dokumentów:**

   1) **odpisu z właściwego rejestru,** lub z centralnej ewidencji i informacji o działalności gospodarczej jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 5 pkt 1 Pzp. Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3, jeżeli zamawiający posiada oświadczenia lub dokumenty dotyczące tego wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352).Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu potwierdzenia braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu zamieszcza informacje o niepodleganiu wykluczeniu podwykonawców w dokumentach, o których mowa w ust. 1 i 2.

   2) **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;

   3) **zaświadczenia właściwego naczelnika urzędu skarbowego** potwierdzającego, że wykonawca nie zalega z opłacaniem podatków, wystawionego nie wcześniej niż 3 miesiące przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, 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.

   4) **zaświadczenie 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;

      Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3, jeżeli

zamawiający posiada oświadczenia lub dokumenty dotyczące tego wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352).

4. **W celu potwierdzenia spełniania warunków udziału w postępowaniu Zamawiający wezwie Wykonawcę, którego oferta zostanie najwyżej oceniona do złożenia: dowodów,** czy dostawy wskazane w wykazie dostaw (patrz. Cześć IV sekcja C pkt 1b JEDZ) zostały wykonane należycie. Dowodami, o których mowa powyżej, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 27 lipca 2016 r., w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy.

5. Dokumenty wchodzące w skład oferty wymienione w ust. 3 oraz w ust. 4 mogą być przedstawione w formie oryginału lub poświadczonej za zgodność z oryginałem kopii, a pozostałe dokumenty w formie oryginałów. Zgodność z oryginałem wszystkich kopii dokumentów wchodzących w skład oferty musi być potwierdzona przez przedstawiciela Wykonawcy lub pełnomocnika (zgodnie z dokumentem określającym status prawny Wykonawcy lub dołączonym do oferty pełnomocnictwem). Wykonawca nie jest zobowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3, jeżeli Zamawiający posiada oświadczenia lub dokumenty dotyczące tego Wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352).

6. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczpospolitej Polskiej zamiast dokumentów, o których mowa w ust. 3 - składa dokumenty wystawione w kraju, w którym ma miejsce zamieszkania lub siedzibę, potwierdzające odpowiednio, że:

    1) nie zalega z opłacaniem podatków, opłat, składek na ubezpieczenie społeczne lub zdrowotne albo że zawarł porozumienie z właściwym organem w sprawie spłat tych należności wraz z ewentualnymi odsetkami lub grzywnami, w szczególności uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu (dokument powinien być wystawiony nie wcześniej niż 3 miesiące przed upływem terminu składania ofert);

    2) nie otwarto jego likwidacji ani nie ogłoszono upadłości (dokument powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert).

    W przypadku dokumentu, o którym mowa w ust. 3 pkt 2 Wykonawca 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 na 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 (dokument powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert)

7. 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 powyżej, zastępuje się je dokumentami zawierającymi 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.

8. Zgodnie z treścią art. 26 ust. 3 oraz 3a Pzp, Zamawiający wzywa Wykonawców, którzy w określonym terminie nie złożyli wymaganych przez Zamawiającego oświadczeń lub dokumentów, o których mowa w art. 25 ust. 1 Pzp, lub którzy nie złożyli pełnomocnictw, albo którzy złożyli wymagane przez Zamawiającego oświadczenia i dokumenty, o których mowa w art. 25 ust. 1 Pzp, zawierające błędy lub którzy złożyli wadliwe pełnomocnictwa, do ich złożenia w wyznaczonym terminie, chyba że mimo ich złożenia oferta Wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania. Złożone na wezwanie Zamawiającego oświadczenia i dokumenty powinny potwierdzać spełnianie przez Wykonawcę warunków udziału w postępowaniu oraz spełnianie przez oferowane dostawy wymagań określonych przez Zamawiającego, nie później niż w dniu, w którym upłynął termin składania ofert.
9. Zamawiający wzywa także, w wyznaczonym przez siebie terminie, do złożenia wyjaśnień dotyczących oświadczeń lub dokumentów, o których mowa powyżej, nie później niż w dniu wyznaczonym przez Zamawiającego jako termin uzupełnienia oświadczeń lub dokumentów.
10. Wykonawca, w terminie 3 dni od zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5, **przekazuje Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej**, o której mowa w art. 24 ust. 1 pkt 23. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

X. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIU OŚWIADCZEŃ I DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI (art. 36 ust. 1 pkt 7 Pzp)

1. Porozumiewanie się Zamawiającego z Wykonawcami odbywa się drogą pisemną z dopuszczeniem możliwości przekazywania oświadczeń, wniosków, zawiadomień i informacji za pomocą faksu lub drogą elektroniczną (e-mail). Nr faksu Zamawiającego: **(22) 581-88-14**, adres e-mail: **wzp@ipn.gov.pl**
2. Każda ze stron na żądanie drugiej niezwłocznie potwierdza pisemnie treść dokumentu przekazanego faksem.
3. Zamawiający wymaga, aby wszelkie pisma związane z udzielanym zamówieniem publicznym były opatrzone numerem sprawy: **BAG-11/17**.
4. Korespondencję uważa się za doręczoną z chwilą, gdy doszła ona do Zamawiającego w taki sposób, że mógł zapoznać się z jej treścią.
5. Osobą uprawnioną do kontaktu z Wykonawcami jest: Wiesława Misior

XI. WYMAGANIA DOTYCZĄCE WADIUM (art. 36 ust. 1 pkt 8 Pzp)

1. Każdy Wykonawca zobowiązany jest wnieść wadium w wysokości **54 000,00 zł brutto** (słownie: pięćdziesiąt cztery tysiące złotych 00/100).
   Forma wadium:

   Wadium może być wniesione wyłącznie w następujących formach:
   1) pieniądzu,
   2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze zobowiązaniem pieniężnym,
   3) gwarancjach bankowych,
   4) gwarancjach ubezpieczeniowych,
   5) w 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 (Dz. U. 2014, poz. 1804 oraz 2015 r., poz. 978 i 1240).

   Wszelkie rozliczenia związane z realizacją zamówienia publicznego którego dotyczy niniejsza SIWZ dokonywane będą wyłącznie w złotych polskich (PLN).
   Wadium wnoszone w innej niż pieniądz formie musi posiadać ważność co najmniej do końca terminu związania Wykonawcy złożoną przez niego ofertą.

2. Miejsce i sposób wniesienia wadium.
   Wadium wnoszone w pieniądzu należy przelać na rachunek Zamawiającego: NBP O/O w Warszawie 26 1010 1010 0092 9213 9120 1000.
   Zaleca się, aby w treści przelewu Wykonawcy wpisali numer NIP.
   Wadium wnoszone w innych dopuszczonych przez Zamawiającego formach należy złożyć w oryginale w pokoju nr 404 Biura Budżetu i Finansów w budynku IPN przy ul. Wołoskiej 7, a do oferty dołączyć kopię dokumentu posiadającą potwierdzenie złożenia dokonane przez osobę przyjmującą dokument.

3. Termin wniesienia wadium.

   Wadium należy wnieść przed upływem terminu składania ofert, przy czym wniesienie wadium w pieniądzu za pomocą przelewu bankowego Zamawiający będzie uważał za **skuteczne tylko wówczas gdy przed upływem terminu składania ofert** kwota wniesionego wadium będzie na koncie bankowym Zamawiającego. Zaleca się, aby kopię dowodu wniesienia wadium załączyć do oferty.

4. Pozostałe informacje dotyczące wadium
   Zamawiający niezwłocznie zwraca wadium zgodnie z zasadami określonymi w art. 46 ust.1, 1a i 2 ustawy Pzp.
   Zamawiający żąda ponownego wniesienia wadium przez Wykonawców, którym zwrócono wadium na podstawie art. 46 ust. 3, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta została wybrana jako najkorzystniejsza. Wykonawca wnosi wadium w terminie określonym przez Zamawiającego.
   Zamawiający zatrzymuje wadium na zasadach określonych w art.46 ust.4a i 5 ustawy Prawo zamówień publicznych.

XII. TERMIN ZWIĄZANIA OFERTĄ (art. 36 ust. 1 pkt 9 Pzp)

1. Wykonawca pozostaje związany złożoną ofertą przez **60 dni**.
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. 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.

XIII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY (art. 36 ust. 1 pkt 10 Pzp)

1. Warunki ogólne:

   1) każdy Wykonawca może złożyć tylko jedną ofertę w języku polskim po dokładnym zapoznaniu się z niniejszą SIWZ - złożenie większej liczby ofert lub oferty zawierającej rozwiązania alternatywne lub oferty wariantowej spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę;

   2) ofertę należy przygotować według wymagań określonych w niniejszej SIWZ oraz zgodnie ze wzorem Formularza ofertowego stanowiącym załącznik nr 1 do SIWZ;

   3) oferta musi być podpisana przez osoby upełnomocnione do reprezentowania Wykonawcy i zaciągania w jego imieniu zobowiązań finansowych w wysokości odpowiadającej co najmniej cenie oferty;

   4) pełnomocnictwo osób podpisujących ofertę do reprezentowania Wykonawcy, zaciągania w jego imieniu zobowiązań finansowych w wysokości odpowiadającej co najmniej cenie oferty oraz podpisania oferty musi bezpośrednio wynikać z dokumentów dołączonych do oferty; oznacza to, że jeżeli pełnomocnictwo takie nie wynika wprost z dokumentu stwierdzającego status prawny Wykonawcy (odpisu z właściwego rejestru), to do oferty należy dołączyć **pełnomocnictwo**, wystawionego na reprezentanta Wykonawcy przez osoby do tego upełnomocnione;

   5) wszelkie pełnomocnictwa załączone do oferty powinny być w formie oryginału lub poświadczonej notarialnie kopii;

6) żadne dokumenty wchodzące w skład oferty, w tym również te przedstawiane w formie oryginałów, nie podlegają zwrotowi przez Zamawiającego;

7) Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty;

8) podana w ofercie cena ofertowa brutto musi zawierać wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej, zgodnej z załączonym wzorem umowy oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia;

9) w przypadku, gdyby oferta zawierała informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r., Nr 153, poz.1503 z późn. zm.), Wykonawca winien w sposób nie budzący wątpliwości zastrzec, które z zawartych w ofercie informacji stanowią tajemnicę przedsiębiorstwa i oznaczyć klauzulą: „DOKUMENTY ZASTRZEŻONE –TAJEMNICA PRZEDSIĘBIORSTWA". Zaleca się wydzielenie tych informacji w złożonej ofercie". **Wykonawca nie później niż w terminie składania ofert musi wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.**

2. Warunki dotyczące Wykonawców wspólnie ubiegających się o zamówienie:

1) oferta musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie;

2) w odniesieniu do wymagań postawionych przez Zamawiającego, każdy z Wykonawców wspólnie składających ofertę musi oddzielnie udokumentować, że nie podlega wykluczeniu na podstawie art. 24 ust. 1 oraz ust. 5 pkt 1 i 8 Pzp, tj. przedstawić **oświadczenie o braku podstaw do wykluczenia z postępowania w formie jednolitego dokumentu JEDZ sporządzonego zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE oraz art. 80 ust. 3 dyrektywy 2014/25/UE.** Ponadto w przypadku gdy oferta Wykonawców wspólnie ubiegających się o zamówienie zostanie najwyżej oceniona, każdy z Wykonawców zostanie wezwany do dostarczenia dokumentów wymienionych w rozdz. IX ust. 3 oraz ust. 4 pkt 1) SIWZ. W odniesieniu do pozostałych dokumentów Wykonawcy wspólnie składający ofertę będą mogli dostarczyć jeden wspólny dokument;

3) wykonawcy występujący wspólnie winni ustanowić pełnomocnika (lidera) do reprezentowania ich w postępowaniu o udzielenie niniejszego zamówienia lub reprezentowania ich w postępowaniu i zawarciu umowy o udzielenie przedmiotowego zamówienia publicznego. Umocowanie może wynikać z dołączonej do oferty umowy konsorcjum lub odrębnego dokumentu (oświadczenia);

4) wszelka korespondencja prowadzona będzie wyłącznie z pełnomocnikiem (liderem);

5) wypełniając formularz ofertowy, składając oświadczenia, jak również wypełniając inne dokumenty powołujące się na „Wykonawcę", w miejscu np. nazwa i adres Wykonawcy należy wpisać dane wszystkich Wykonawców wspólnie ubiegających się o zamówienie.

3. Forma przygotowania oferty:

1) oferta winna być napisana czytelnie i trwałą techniką w języku polskim na maszynie do pisania, komputerze lub ręcznie długopisem lub nieścieralnym atramentem;

2) we wszystkich przypadkach, gdzie jest mowa o pieczątkach, Zamawiający dopuszcza złożenie czytelnego zapisu o treści pieczęci, np.: nazwa Wykonawcy, siedziba lub czytelny podpis w przypadku pieczęci imiennej;

3) wszelkie zmiany w treści oferty (poprawki, przekreślenia, itp.) muszą być parafowane i datowane przez osobę lub osoby podpisujące ofertę;

4) zaleca się, aby wszystkie strony oferty były kolejno ponumerowane i parafowane;

5) zaleca się, aby cała oferta była trwale spięta;

6) ofertę należy złożyć w nieprzezroczystej, zabezpieczonej przed otwarciem kopercie;

7) kopertę należy opisać następująco:

INSTYTUT PAMIĘCI NARODOWEJ
Komisja Ścigania Zbrodni Przeciwko Narodowi Polskiemu
ul. Wołoska 7, 02-675 Warszawa

OFERTA NA:

„Dostawę routerów oraz przełączników sieciowych, przełączników rdzeniowych w Centrali oraz w Oddziałach Instytutu Pamięci Narodowej"

- NIE OTWIERAĆ PRZED DNIEM 4.07.2017 r., godz. 11.00 -

8) opakowanie oferty musi być opatrzone pełną nazwą i dokładnym adresem Wykonawcy składającego ofertę: *(ulica, numer lokalu, miejscowość, numer kodu pocztowego)*.

4. Zmiana lub wycofanie złożonej oferty (art. 84 ust.1 Pzp):
   1) wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę;
   2) zmiany lub wycofanie złożonej oferty są skuteczne tylko wówczas gdy, zostały dokonane przed upływem terminu składania ofert;
   3) zmiany, poprawki lub modyfikacje złożonej oferty muszą być złożone w miejscu i według zasad obowiązujących przy składaniu oferty;
   4) odpowiednio opisaną kopertę zawierającą zmiany należy dodatkowo opatrzyć dopiskiem "ZMIANA";
   5) wycofanie złożonej oferty następuje poprzez złożenie pisemnego powiadomienia podpisanego przez upełnomocnionego przedstawiciela Wykonawcy;
   6) powiadomienie należy złożyć w miejscu i według zasad obowiązujących przy składaniu oferty;
   7) odpowiednio opisaną kopertę zawierającą powiadomienie należy dodatkowo opatrzyć dopiskiem "WYCOFANIE".

XIV. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT (art. 36 ust. 1 pkt 11 Pzp)

1. Ofertę należy złożyć w Centrali Zamawiającego: **ul. Wołoska 7, 02-675 Warszawa – Kancelaria do dnia 4.07.2017 r., godz. 10.00.**
2. W przypadku złożenia oferty po terminie Zamawiający niezwłocznie zawiadomi wykonawcę o złożeniu oferty po terminie oraz zwróci ofertę po upływie terminu do wniesienia odwołania.
3. Publiczne otwarcie ofert nastąpi w Centrali Zamawiającego w Warszawie przy ul. Wołoskiej 7, pok. 223: **4.07.2017 r., godz. 11.00.**
4. Z uwagi na ograniczony wstęp do budynku, osoby które zechcą uczestniczyć w sesji otwarcia ofert, zobowiązane będą okazać dowód tożsamości w celu wystawienia stosownych przepustek – jest to warunek konieczny udziału w sesji otwarcia ofert. Osoby zainteresowane powinny oczekiwać na przedstawiciela Zamawiającego na parterze budynku, w strefie ogólnodostępnej.

XV. OPIS SPOSOBU OBLICZENIA CENY (art. 36 ust. 1 pkt 12 Pzp)

1. Cenę brutto oferty należy wyliczyć zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2016 r., poz. 710)
2. Cena oferty musi wynikać z Formularza ofertowego (wzór formularza stanowi Załącznik nr 1 do SIWZ) i obejmować wszystkie koszty wykonania przedmiotu zamówienia określonego w Opisie przedmiotu zamówienia, w tym: cenę przedmiotu umowy, cenę opakowań, cła, koszty transportu, ubezpieczenia, rozładunku, wniesienia w miejsce wskazane przez Zamawiającego, zysk Wykonawcy, wymagane przepisami prawa obciążenia fiskalne oraz wszystkie koszty związane z realizacją przedmiotu zamówienia.
3. Cena oferty powinna zostać wyrażona cyfrowo i słownie.

4. Cenę oferty należy podać w złotych polskich do dwóch miejsc po przecinku. Wszelkie rozliczenia dotyczące realizacji zamówienia dokonywane będą w złotych polskich.
5. W przypadku Wykonawców zagranicznych składających ofertę w niniejszym postępowaniu Zamawiający doliczy do ceny oferty podatek od towarów i usług, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.
6. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje Zamawiającego, czy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku

XVI. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW I SPOSOBU OCENY OFERT (art. 36 ust. 1 pkt 13 Pzp)

1. Ocenie podlegać będą oferty nieodrzucone.

   Przy wyborze oferty w każdej części zamówienia Zamawiający będzie się kierował następującymi kryteriami:

Kryterium	Wagi %
Cena (brutto)	**60%**
Okres gwarancji i rękojmi	**30%**
Skrócenie terminu realizacji	**10%**

CENA BRUTTO:

Ilość punktów za kryterium **„cena brutto”** ocenianej oferty będzie wyliczana według następującego wzoru:

$$C = \frac{C_{min}}{C_i} \times 60\%$$

C – ilość otrzymanych punktów za kryterium „**cena brutto**”
C_{min} – najniższa cena brutto spośród ofert nieodrzuconych
C_i – cena brutto oferty badanej

OKRES GWARANCJI I RĘKOJMI:

Ocenie będzie podlegać okres gwarancji, który **nie może być krótszy niż 24 miesiące i nie dłuższy niż 60 miesięcy.**

Okres min. 24 miesięcy liczony od daty odbioru – 0 pkt. Za każdy dodatkowy miesiąc 1 pkt. Maksymalna ilość pkt w tym kryterium wynosi - 36 (60 miesięcy okres gwarancji i rękojmi)

Liczba punktów przydzielona w tym kryterium poszczególnym Wykonawcom ustalona zostanie zgodnie z poniższym wzorem:

$$OG = \frac{OGo}{OG\,\max} \times 30\%$$

OG – ilość otrzymanych punktów za kryterium „okres gwarancji i rękojmi”

OGo – ilość punktów za okres gwarancji i rękojmi oferty ocenianej

OGmax. – ilość punktów za najdłuższy okres gwarancji i rękojmi

SKRÓCENIE TERMINU REALIZACJI:

W kryterium odnoszącym się do terminu wykonania przyznane zostaną następujące punkty:
1 pkt za skrócenie terminu, o którym mowa w rozdz. IV SIWZ, o 1 dzień kalendarzowy (**max. skrócenie do 14 dni kalendarzowych**).

$$T = \frac{To}{T\ \max} \times 10\%$$

T – ilość otrzymanych punktów za kryterium „skrócenie terminu realizacji"

To – ilość punktów za skrócenie terminu realizacji oferty ocenianej

Tmax. – ilość punktów za najkorzystniejsze skrócenie terminu realizacji

3. Obliczenia punktów dokonuje się z dokładnością do dwóch miejsc po przecinku.
4. Za najkorzystniejszą ofertę zostanie uznana oferta, która uzyska najwyższą liczbę punktów za wszystkie kryteria łącznie:

$$\Sigma = C + OG + T$$

XVII. INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO (art. 36 ust. 1 pkt 14 Pzp)

1. Zamawiający wezwie Wykonawcę, którego oferta została wybrana jako najkorzystniejsza, do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.
2. Jeżeli Wykonawca, o którym mowa w ust. 1, uchyla się od zawarcia umowy lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, Zamawiający może zbadać, czy nie podlega wykluczeniu oraz czy spełnia warunki udziału w postępowaniu Wykonawca, który złożył ofertę najwyżej ocenioną spośród pozostałych ofert chyba, że zachodzą przesłanki do unieważnienia postępowania o udzielenie zamówienia publicznego, o których mowa w art. 93 ust. 1 Pzp.

XVIII. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY (art. 36 ust. 1 pkt 15 Pzp)

1. Zamawiający żąda zabezpieczenia należytego wykonania umowy w wysokości **10 % ceny ofertowej brutto.**
2. Zabezpieczenie musi być wniesione przez Wykonawcę przed zawarciem umowy w jednej z następujących form:
   1) pieniężnej – przelewem na rachunek Zamawiającego: NBP O/O w Warszawie 26 1010 1010 0092 9213 9120 1000;
   2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze zobowiązaniem pieniężnym;
   3) gwarancjach bankowych;
   4) gwarancjach ubezpieczeniowych;
   5) 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.
3. Gwarancja lub poręczenie muszą być nieodwołalne, bezwarunkowe, zapewniające

płatność na rzecz Zamawiającego na każde żądanie bez konieczności przedkładania dodatkowych dokumentów. Poręczenie musi zawierać rezygnację gwaranta z podnoszenia zarzutów (art. 883 k.c.), włącznie z wykluczeniem możliwości potrącenia oraz zarzutem możliwości uchylenia się od skutków prawnych błędnego oświadczenia, z wyjątkiem uchylenia się od skutków prawnych oświadczenia, zgodnie z art. 86 k.c. Gwarancja lub poręczenie musi obejmować rezygnację z prawa do zdeponowania kwoty gwarancji i poręczenia. Zamawiający zastrzega sobie prawo akceptacji treści gwarancji lub poręczenia.

Wypłata z gwarancji lub poręczenia nie może być uzależniona od zgłoszenia żądania wypłaty za pośrednictwem banku Zamawiającego, który to bank potwierdzi, że podpisy na żądaniu wypłaty zostały złożone przez osoby upoważnione do zaciągania zobowiązań majątkowych w imieniu Zamawiającego.

4. Zabezpieczenie służy zaspokojeniu wszelkich roszczeń Zamawiającego z tytułu nie wykonania lub nienależytego wykonania postanowień umowy przez Wykonawcę, w tym również obowiązku Wykonawcy względem Podwykonawców oraz dalszych Podwykonawców oraz roszczeń Zamawiającego z tytułu udzielonej przez Wykonawcę rękojmi na przedmiot umowy.
5. Zabezpieczenie podlega zwolnieniu przez Zamawiającego w wysokości 70% kwoty zabezpieczenia w terminie 30 dni od dnia podpisania protokołu odbioru końcowego nie zawierającego zastrzeżeń Zamawiającego do wykonanego przedmiotu umowy, a 30 % kwoty zabezpieczenia w terminie nie później niż w 15 dniu po upływie okresu rękojmi za wady.

XIX. INFORMACJE DOTYCZĄCE WZORU UMOWY W SPRAWIE UDZIELENIA ZAMÓWIENIA PUBLICZNEGO – WZÓR UMOWY (art. 36 ust. 1 pkt 16 Pzp)

Istotne dla stron postanowienia związane z realizacją niniejszego zamówienia publicznego zawiera wzór umowy (załącznik nr 7 do SIWZ).

XX. ZASADY DOKONYWANIA ZMIAN ZAWARTEJ UMOWY

1. Zamawiający dopuszcza dokonywanie zmian zawartej umowy na zasadach określonych w art. 144 ustawy Pzp, a ponadto w następujących okolicznościach:
   1) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili zawarcia umowy, niepowodujących zmiany przedmiotu zamówienia,
   2) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań w zakresie modelu/typu sprzętu/oprogramowania w przypadku zakończenia produkcji lub braku dostępności na rynku pod warunkiem że sprzęt /oprogramowanie będzie posiadał parametry nie gorsze od oferowanego modelu/ typu sprzętu/ oprogramowania i nie spowoduje podwyższenia ceny.

XXI. SPOSÓB I TERMIN PŁATNOŚCI

Sposób i termin płatności zostały określone we wzorze umowy stanowiącym załącznik nr 4 do SIWZ.

XXII. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA. (art. 36 ust. 1 pkt 17 Pzp)

Wykonawcy w toku postępowania o udzielenie zamówienia publicznego przysługują środki ochrony prawnej przewidziane w ustawie z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164 z póź. zm.).

XXIII. INNE INFORMACJE DOTYCZĄCE POSTĘPOWANIA (art. 36 ust. 2 pkt 2, 3, 7, 8 Pzp)

Zamawiający nie przewiduje: zawarcia umowy ramowej, zamówień uzupełniających, aukcji elektronicznej, zwrotu kosztów udziału w postępowaniu.

XXIV. ZAŁĄCZNIKI DO SIWZ

1. **Załącznik nr 1** - wzór formularza ofertowego,
2. **Załącznik nr 2 -** wzór jednolitego dokumentu JEDZ sporządzonego zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE oraz art. 80 ust. 3 dyrektywy 2014/25/UE.
3. **Załącznik nr 3** – opis przedmiotu zamówienia,
4. **Załącznik nr 4 –** wzór umowy.

Załącznik nr 1 do SIWZ
(Załącznik nr 1 do umowy)

……
(pieczęć Wykonawcy)

OFERTA
(FORMULARZ OFERTOWY)

WYKONAWCA:

Nazwa Wykonawcy: .....
Adres siedziby:.....
……
Telefon: .....
Fax: .....
Adres poczty elektronicznej (e-mail): .....
(Wszelką korespondencję dotyczącą przedmiotowego postępowania Zamawiający przesyłał będzie na ww. adres, nr faxu lub e-mail)
NIP: .....

ZAMAWIAJĄCY:

INSTYTUT PAMIĘCI NARODOWEJ-
KOMISJA ŚCIGANIA ZBRODNI
PRZECIWKO NARODOWI POLSKIEMU
ul. Wołoska 7, 02-675 Warszawa

Składamy ofertę na:

„Dostawę routerów oraz przełączników sieciowych, przełączników rdzeniowych w Centrali oraz w Oddziałach Instytutu Pamięci Narodowej"

Oferujemy wykonanie przedmiotu zamówienia, zgodnie z opisem przedmiotu zamówienia i określonymi w SIWZ warunkami oraz z uwzględnieniem postanowień wzoru umowy, stanowiącym załącznik do SIWZ, za **całkowitą cenę :**…….. **zł brutto**

(słownie:.....)

wraz z obowiązującym podatkiem VAT, a w tym:

Lp.	Przedmiot zamówienia	J.m.	Ilość	Cena jednostkowa netto (zł)	Łączna wartość netto (zł)	Stawka podatku VAT	Łączna wartość brutto(zł)
1	2	3	4	5	6	7	
1.	**Przełącznik I**	**szt.**	**25**			**23 %**	
2	**Przełącznik II**	**szt.**	**56**			**23 %**	

3	**Przełącznik rdzeniowy**	**szt.**	**3**			**23 %**	
4	**Router I Centrala**	**szt.**	**1**			**23 %**	
5	**Router II**	**szt.**	**25**			**23 %**	
RAZEM		**X**	**X**	**X**		**X**	

Termin realizacji zostanie skrócony o……dni (nie więcej niż 14 dni kalendarzowych).

Okres gwarancji i rękojmi wynosi …….miesięcy od daty podpisania protokołu odbioru (nie krótszy niż 24 miesiące i nie dłuższy niż 60 miesięcy).

Zgodnie z poniższymi tabelami:

Przełącznik I 25 szt.

Oferowany model: …… producent: ……

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	Możliwość montażu w szafie rack 19", wysokość urządzenia nie może przekraczać 1 RU	
		Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne. Przełącznik powinien być wyposażony w zasilacz podstawowy.	
		Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów.	
		Urządzenie musi być sprzętowo przygotowane do obsługi standardu IEEE 802.3az Energy-Efficient Ethernet (EEE).	
		Przełącznik Gigabit Ethernet wyposażony w 48 portów 10/100/1000BaseT oraz min. 4 porty uplink w tym min. 2 10Gigabit Ethernet SFP+.	
		Wszystkie porty muszą obsługiwać standard 802.1AE (szyfrowanie ruchu)	
		Porty uplink muszą umożliwiać obsadzenie modułami Gigabit Ethernet SFP (co najmniej 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX,	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		1000Base-BX-D/U) oraz 10Gigabit Ethernet (co najmniej 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER) zależnie od potrzeb Zamawiającego.	
		Wkładki optyczne (SFP, SFP+) przeznaczone do instalacji w przełączniku muszą pochodzić od tego samego producenta co oferowany przełącznik.	
		Przełącznik musi zapewniać możliwość rozbudowy o możliwość łączenia w stos z zapewnieniem następujących parametrów: a) Przepustowość w ramach stosu min. 40Gb/s b) Min. 8 urządzeń w stosie c) Zarządzanie poprzez jeden adres IP d) Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych urządzeń w stosie) zgodnie z 802.3a	
		Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree.	
		Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)	
		Wydajność przełączania minimum 100 Mpps dla pakietów 64-bajtowych.	
		Przepustowość przełącznika minimum 160 Gbps	
		Minimum 1GB pamięci flash	
		Obsługa minimum a) 1000 sieci VLAN b) 16 000 adresów MAC c) 8 000 tras IPv4	
		Obsługa protokołu NTP	
		Obsługa IGMPv1/2/3 i MLDv1/2 Snooping	
		Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: a) IEEE 802.1w Rapid Spanning Tree b) IEEE 802.1s Multi-Instance Spanning Tree	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		c) Obsługa minimum 128 instancji protokołu STP	
		Obsługa protokołu LLDP i LLDP-MED lub podobnego (np. CDP)	
		Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego	
		Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: a) Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. b) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN c) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL d) Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X e) Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC f) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X g) Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem h) Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 i) Minimum 1000 wpisów dla list kontroli dostępu (ACE)	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		j) Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard k) Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+ l) Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)	
		Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: a) Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi b) Implementacja algorytmu Shaped Round Robin lub Weighted Round Robin lub Deficit Round Robin lub podobnego dla obsługi kolejek c) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) d) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP e) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi f) Kontrola sztormów dla ruchu broadcast/multicast/unicast g) Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP	
		Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak:	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania.	
		Wbudowane reflektometry (TDR) dla portów 10/100/1000	
		Urządzenie musi zapewniać wsparcie routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP). Urządzenie musi zapewniać możliwość rozszerzenia funkcjonalności o wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP) i IPv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM)	
		Obsługa protokołu HSRP lub VRRP lub mechanizmu równoważnego dla usług redundancji bramy	
		Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)	
		Urządzenie musi zapewniać możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne)	
		Dedykowany port Ethernet do zarządzania out-of-band	
		Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi być wyposażone w port konsoli USB	
		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 nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją	
		Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6	
		zarządzanie urządzeniem przez HTTPS, SNMPv2, SNMPv3 i SSHv2,	
		Przełącznik musi być zgodny z normami środowiskowymi, bezpieczeństwa oraz kompatybilności elektromagnetycznej: a) EN 60950-1 b) EN 55022 klasa A c) EN300386 d) EN61000-4-2, EN61000-4-4, EN61000-4-5, EN61000-4-6 e) Reduction of Hazardous Substances (RoHS)	
		Przełącznik musi być w pełni kompatybliny z dostarczonym systemem uwierzytelnienia i profilowania użytkowników będącym przedmiotem postępowania.	

Przełącznik II 56 szt.

Oferowany model: …… producent: ……

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje lotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	Możliwość montażu w szafie rack 19", wysokość urządzenia nie może przekraczać 1 RU	
		Urządzenie musi posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V	
		Urządzenie musi być sprzętowo przygotowane do obsługi standardu IEEE 802.3az Energy-Efficient Ethernet (EEE).	
		Przełącznik Gigabit Ethernet wyposażony w 48 portów 10/100/1000BaseT oraz min. 4 porty uplink 1Gigabit Ethernet SFP.	
		Porty uplink muszą umożliwiać obsadzenie modułami Gigabit Ethernet SFP co najmniej 1000BaseT, 1000Base-SX, 1000BaseLX/LH, 1000BaseEX, 1000Base-BX-D/U i modułami CWDM zależnie od potrzeb Zamawiającego.	
		Wkładki optyczne (SFP, SFP+) przeznaczone do instalacji w przełączniku muszą pochodzić od tego samego producenta co oferowany przełącznik.	
		Przełącznik musi zapewniać możliwość rozbudowy o możliwość łączenia w stos z zapewnieniem następujących parametrów: e) Przepustowość w ramach stosu min. 40Gb/s f) Min. 8 urządzeń w stosie g) Zarządzanie poprzez jeden adres IP h) Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych urządzeń w stosie) zgodnie z 802.3ad	
		Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree.	
		Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)	
		Wydajność przełączania minimum 100 Mpps dla pakietów 64-bajtowych.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje lotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Przepustowość przełącznika minimum 160 Gbps (full duplex)	
		Obsługa minimum: a) 1000 sieci VLAN jednocześnie oraz obsługa 802.1Q b) 16 000 adresów MAC	
		Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów	
		Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów bezpieczeństa typu Port Security i IP Source Guard na interfejsach link aggregation	
		Obsługa protokołu NTP	
		Musi zapewniać obsługę min. 16 statycznych tras dla routingu IPv4 i IPv6	
		Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping	
		Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 128 instancji protokołu STP	
		Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC	
		Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa: a) Minimum 5 poziomów dostępu administracyjnego poprzez konsolę b) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL c) Obsługa funkcji Guest VLAN d) Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC e) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje lotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		f) Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www g) Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie h) Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 i) Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6 j) Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6 k) Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard l) Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego m) Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow LITE, J-Flow lub równoważne) n) Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+	
		Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: a) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje lotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP b) Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub Weighted Round Robin lub Deficit Round Robin lub podobnego dla obsługi tych kolejek c) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) d) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi.	
		Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP)	
		Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli	
		Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB	
		Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)	
		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 nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje lotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania.	
		Przełącznik musi być zgodny z normami środowiskowymi, bezpieczeństwa oraz kompatybilności elektromagnetycznej: a) EN 60950-1 b) EN 55022 klasa A c) EN300386 d) EN61000-4-2, EN61000-4-4, EN61000-4-5, EN61000-4-6 e) Reduction of Hazardous Substances (RoHS)	
		Przełącznik musi być w pełni kompatybliny z dostarczonym systemem uwierzytelnienia i profilowania użytkowników będącym przedmiotem postępowania.	

Przełącznik rdzeniowy 3 szt.

Oferowany model: …… producent: ……

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	Urządzenie o architekturze modularnej – o wysokości max. 11RU dedykowane do zamontowania w szafie rack 19”pozwalające na instalację kart liniowych i redundantnych modułów zarządzająco-przełączających działających w trybie active-standby lub active-active	
		Wymagane niezbędne wyposażenie urządzenia: a) Moduł zarządzająco-przełączający. b) Min dwa zasilacze AC (zapewniające redundancję zasilania w trybie 1:1) o mocy pozwalającej zasilić urządzenie wraz z kartami liniowymi oraz posiadające min. 20% mocy zapasu. c) Urządzenie powinno umożliwiać rozbudowę zasilaczy, mogących pracować w trybie redundancji n+1 d) Cztery moduły minimum 48-portowe 10/100/1000 Gigabit Ethernet e) 32 porty 10G Ethernet SFP/SFP+. Wszystkie porty muszą obsługiwać standard 802.1AE (szyfrowanie ruchu) z pełną wydajnością łącza 10GE.	
		Porty SFP muszą obsługiwać minimum wkładki typu: SX, LH, T (RJ45). Porty SFP+ muszą obsługiwać minimum wkładki typu: SR, LR	
		Dla każdego portu możliwość bezpośredniego zaadresowania portu (IP) (przełączenie portu w tryb L3).	
		Urządzenie, które producent oficjalnie pozycjonuje jako rozwiązanie dla rdzenia sieci kampusowych.	
		Wspiera technologię wirtualizacji, umożliwiającą zbudowanie z co najmniej dwóch urządzeń fizycznych jednego logicznego urządzenia zarządzanego z jednego miejsca (poprzez jeden adres IP).	
		Wydajność przełączania matrycy min. 3,5Tb/s	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Obsługa minimum: a) min. 100 000 wpisów w tablicy adresów MAC b) min. 250 000 wpisów w tablicy routingowej IPv4 c) min. 125 000 wpisów w tablicy routingowej IPv6 d) min. 125 000 tras multicast e) min. 64 000 wpisów na potrzeby realizacji polityk QoS i bezpieczeństwa (listy kontroli dostępu)	
		Obsługa protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4	
		Obsługa protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), MP-BGP	
		Obsługuje sprzętowo ruch multicastowy w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD	
		Urządzenie musi umożliwiać rozszerzenie funkcjonalności o wsparcie dla MPLS, LDP, L2 i L3 VPN, VPLS, MPLS TE, MPLS traceruote poprzez zakup odpowiedniej licencji lub wymianę oprogramowana bez konieczności modernizacji sprzętowej urządzenia	
		Sprzętowa obsługa tunelowania GRE	
		Obsługa IGMPv1/2/3 i MLDv2 for IP	
		Urządzenie wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: a. mechanizm BFD (Bidirectional Forwarding Detection) co najmniej dla protokołu OSPFv2 i OSPFv3 b. IEEE 802.1D Spanning Tree Protocol c. IEEE 802.1w Rapid Spanning Tree d. IEEE 802.1s Multiple Spanning Tree e. Spanning Tree loop guard f. Spanning Tree root guard g. Spanning Tree BPDU filtering h. Obsługa protokołu LLDP (IEEE 802.1AB) i. Obsługa Private VLAN	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		j. Obsługa 802.1q k. IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów z wykorzystaniem portów znajdujących się na różnych kartach liniowych l. pozwala na wymianę kart liniowych oraz modułu fantray bez wyłączania zasilania (tzw. Hot-Swap)	
		Obsługa wirtualnych instancji routingu (VRF) - co najmniej 20 instancji VRF	
		W obrębie VRF musi istnieć możliwość uruchomienia niezależnej instancji protokołu dynamicznego routingu (minimum wsparcie dla OSPF)	
		Możliwość przypisywania interfejsów do VRF (odizolowania interfejsów od globalnej tablicy routingu).	
		Obsługa NTP	
		Obsługa protokołu Hot Standby Router Protocol (HSRP) lub Virtual Router Redundancy Protocol (VRRP)	
		Urządzenie wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS): a. Obsługa min. 4 kolejek sprzętowych b. Obsługa co najmniej jednej kolejki ze statusem strict priority c. Implementacja algorytmu dla obsługi kolejek typu Shaped Round Robin, lub WRR lub DRR lub równoważnego. d. Możliwość ograniczania pasma dostępnego na danym porcie (policing, rate limiting). e. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP f. Możliwość zmiany przez	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		g. urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP h. Definiowanie polityk QoS per port i per VLAN i. Obsługa protokołu RSVP	
		Urządzenie wspiera następujące mechanizmy związane z bezpieczeństwem: a. Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend b. Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x z możliwością przydziału listy kontroli dostępu (ACL) i VLANu c. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X d. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC e. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X f. Wsparcie dla możliwości uwierzytelniania (802.1X) wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem. g. Możliwość obsługi żądań Change of Authorization (CoA) h. Możliwość takiej konfiguracji mechanizmów 802.1X, żeby dostęp do sieci był możliwy również w przypadku wykrycia braku komunikacji z serwerem uwierzytelniającym (tryb awaryjny) i. Obsługa co najmniej	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		j. następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Gurad k. Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP l. Listy kontroli dostępu także dla IPv6 m. Mechanizmy ochrony warstwy kontrolnej np. CoPP	
		Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem: a. Ma możliwość zarządzania przez SNMPv3 oraz SSH v2 b. Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Gigabit Ethernet c. Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+ d. Pamięć flash minimum 2GB e. Umożliwia stworzenie wirtualnego systemu złożonego z min. 2 urządzeń będących przedmiotem opisu, zarządzanego jako całość. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów SFP+ mieszczących się na module zarządzająco-przełączającym jak również na 32 portowym module SFP/SFP+ f. Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN g. Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow lub odpowiednik). Konieczna jest obsługa/buforowanie minimum 256 000 wpisów (per moduł zarządzający/karta liniowa).	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		h. Funkcjonalność ta musi być obsługiwana sprzętowo i wspierać IPv6 oraz multicast'y i. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC j. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych	
		Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame)	
		Przełącznik musi być w pełni kompatybliny z dostarczonym systemem uwierzytelnienia i profilowania użytkowników będącym przedmiotem postępowania.	

Router I centrala 1 szt.

Oferowany model: …… producent: ……

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	Urządzenie o architekturze modularnej, wyposażone w co najmniej 6 portów Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP, a także w min. 2 porty 10 Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP+. W chwili dostarczenia urządzenia zamawiający wymaga dostarczenia urządzenia z dostępnymi i aktywnymi 4 portami 1000BASE-T oraz 2 portami 1000BASE SX-MM, nie wymaga się aktywnych portów 10GE.	
		Urządzenie musi umożliwiać rozszerzenie m.in. o następujące porty: a) 1 port 10 GigabitEthernet b) 8 portów Gigabit Ethernet	
		Musi posiadać zasoby sprzętowe zapewniające wydajność przełączania min. 19 Mpps oraz min. 15 Gbps ruchu	
		Musi posiadać wydajność szyfrowania min. 5,5 Gbps dla ruchu IMIX (encryption+decryption).	
		Musi być wyposażone w minimum 4 GB pamięci RAM.	
		Obsługa minimum 800 000 prefiksów w tablicach rutingu dla IPv4.	
		Obsługa minimum 150 000 prefiksów w tablicach rutingu dla IPv6.	
		Musi obsługiwać następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP.	
		Musi obsługiwać następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP.	
		Obsługa Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja.	
		Urządzenie musi umożliwiać uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Forwarding), umożliwiając m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci.	
		Musi obsługiwać 500 instancji wirtualnych tablic routingu.	
		Musi obsługiwać funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.	
		Musi obsługiwać funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF.	
		Musi obsługiwać multicast, w szczególności: PIM sparse/dense/SSM, IGMP, Multicast VPN.	
		Musi obsługiwać protokół NHRP (ang. Next Hop Resolution Protocol)	
		Urządzenie musi posiadać następujące funkcjonalności związane z niezawodnością pracy: a) BFD dla OSPF, BGP, ISIS b) IP FRR c) Graceful Restart dla OSPF, BGP, ISIS, d) funkcjonalność VRRP lub równoważny e) redundantne zasilacze AC 230V zintegrowane w obudowie urządzenia f) możliwość wymiany modułów w trakcie pracy (ang. hot swap)	
		Urządzenie musi obsługiwać MPLS, w szczególności: a) LDP b) MPLS L2 VPN, VPLS c) MPLS L3 VPN d) MPLS TE e) MPLS FRR w trybach protekcji łącza oraz węzła	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi obsługiwać następujące mechanizmy jakości usług (QoS): a) klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN dla kart L2, zarówno dla IPv4 jak i IPv6 b) hierarchiczny QoS (H-QoS) - 3 poziomy c) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP. d) dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek e) algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek lub równoważny f) możliwość obsługi jednej kolejki z priorytetem w stosunku do innych g) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP h) możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting) i) mechanizm WRED j) możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS	
		Urządzenie musi obsługiwać następujące funkcje i elementy bezpieczeństwa: a) ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu b) Unicast RPF (Reverse Path Forwarding) c) listy kontroli dostępu w oparciu o adresy IP źródłowe i	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		docelowe, protokoły IP, porty TCP/UDP, flagi TCP, d) min. 30 000 wpisów IPv4 na wszystkich listach kontroli dostępu (ACL), e) dostęp administracyjny oparty o role z przypisanymi uprawnieniami f) urządzenie ma realizować funkcjonalności zapory ogniowej typu statefull (ang. statefull firewall), przy czym zapora ogniowa: • umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji). • obsługuje ruch IPv4 oraz IPv6 • umożliwia konfigurację polityk per wirtualna tablica routingu (VRF) • umożliwia obsługę 2 000 000 równoczesnych sesji • umożliwia zestawienie 200 000 nowych połączeń TCP na sekundę g) zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością min. 5,5 Gbps (AES256+SHA512) (encryption+decryption), h) sieci VPN typu site-2-site oparte o IPSec i) dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP (lub równoważny) w relacji spoke to spoke w celu optymalizacji transmsji danych pomiędzy oddziałami. j) bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast	
		Musi obsługiwać bezpieczne algorytmy IPSec, w szczególności: a) Elliptic Curve Diffie-	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Hellman (ECDH) z modulo Prime 521-bit b) Diffie-Hellman, z kluczem 2048 bitów c) Advanced Encryption Standard (AES), z kluczem 256 bitów d) RSA, z kluczem 4096 bitów e) SHA2, z kluczem 512 bitów	
		Konfigurację tuneli IPSec VPN w oparciu o protokół IKEv2 a) IKEv2 dla VPN typu site-2-site b) IKEv2 zarówno dla ruchu IPv4 jak i IPv6	
		funkcjonalność VPN per VRF	
		ochronę centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU	
		Urządzenie musi wspierać usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, klasyfikacja ta powinna udostępniać co najmniej 3 atrybuty opisujące daną aplikację/protokół atrybuty mają ułatwić konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji/protokołów (na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji). Włączenie usługi nie może powodować konieczności rozbudowy sprzętowej urządzenia, co najwyżej zakup licencji pozwalającej na korzystanie z powyższej funkcjonalności.	
		Urządzenie musi obsługiwać zestawianie tuneli GRE.	
		Urządzenie musi posiadać możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE.	
		Urządzenie musi umożliwiać ochronę kryptograficzną tuneli GRE.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		W ramach funkcjonalności zarządzania, urządzenie musi: a) umożliwiać zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3 b) obsługiwać język skryptowy c) obsługiwać protokół Netflow lub Netstream lub równoważny d) posiadać narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP e) posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania z wykorzystaniem protokołów RADIUS lub TACACS+ f) posiadać dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet g) posiadać port USB h) posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona i) posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów	
		Urządzenie musi umożliwiać montaż w szafie 19″.	
		Musi być wykonane z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.	

Routery 25 szt.

Oferowany model: …… producent: ……

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	Musi być urządzeniem pełniącym rolę wielousługowego routera modularnego gotowego do obsługi mechanizmów bezpiecznej i niezawodnej sieci WAN w oparciu o Internet oraz MPLS	
		Musi pozwalać na instalację co najmniej: jednego modułu rozszerzeń takich jak moduły przełącznika, 2 kart z interfejsami sieciowymi	
		Musi posiadać zintegrowaną sprzętową akcelerację szyfrowania DES/3DES/AES	
		Musi posiadać wszystkie interfejsy „aktywne”. Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.	
		Sloty urządzenia przewidziane pod rozbudowę muszą mieć możliwość obsadzenia modułami: z interfejsami szeregowymi WAN, przełącznika Ethernet (funkcje L2 i L3), oczekiwana liczba portów przełącznika nie może być mniejsza niż 8 dla jednego modułu; z portem VDSL2 / ADSL2+ over POTS / Annex M;	
		Urządzenie musi oferować możliwość zwiększenia wydajności do co najmniej 300Mbps dla ruchu IMIX bez rozbudowy o dodatkowe moduły sprzętowe – np. licencyjnie przez odblokowanie wbudowanych zasobów sprzętowych lub jako większa wydajność początkowa routera;	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi oferować dla pakietów IMIX przy włączonych usługach szyfrowania z IPSec, szczegółowej analizy aplikacji, kontroli jakości usługi QoS o przepustowość minimum 200Mbps;	
		Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i SSM) oraz routing statyczny;	
		Protokół BGP musi posiadać obsługę 4 bajtowych ASN;	
		Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v1/v2, IGMP Snooping, PIMv2, Bi-directional PIM;	
		Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)	
		Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q, urządzenie musi obsługiwać co najmniej 1000 sieci VLAN	
		Musi obsługiwać IPv6 w tym ICMP dla IPv6	
		Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, flagi TCP	
		Urządzenie musi posiadać wbudowany mechanizm logowania zdarzeń systemowych a także liczników pokazujących ilość pakietów i bajtów odrzuconych/przepuszczonych przez wybraną regułę listy kontroli dostępu. Musi istnieć możliwość wysyłania logów systemowych na zewnętrzny serwer.	
		Musi posiadać obsługę NAT dla ruchu IP unicast oraz PAT dla ruchu IP unicast	
		Mechanizm NAT musi zapewniać wsparcie dla H.245 lub SIP	
		Musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 64 instancji VRF	
		Musi posiadać obsługę mechanizmu DiffServ	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.	
		Musi zapewniać obsługę mechanizmów kolejkowania ruchu: z obsługą kolejki absolutnego priorytetu ze statyczną alokacją pasma dla typu ruchu WFQ	
		Musi obsługiwać mechanizm WRED	
		Musi obsługiwać mechanizm Traffic Shaping	
		Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu	
		Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.	
		Musi obsługiwać protokół NTP	
		Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP lub GLBP lub VRRP)	
		Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+	
		Musi obsługiwać protokół MPLS (funkcje LER i LSR)	
		Musi obsługiwać MPLS over GRE	
		Musi wspierać QoS dla MPLS	
		Musi obsługiwać MPLS Traffic Engineering	
		Musi obsługiwać MPLS L2 i L3 VPN oraz VPLS	
		Musi obsługiwać funkcjonalność Bidirectional Forwarding Detection (BFD) lub równoważna	
		Funkcjonalność BFD musi być dostępna dla intefejsów skonfigurowanych do współpracy z VRF	
		Musi obsługiwać funkcjonalność BFD Echo Mode lub równoważna	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Funkcjonalność BFD (lub równoważna) musi posiadać wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego oraz HSRP lub VRRP lub równoważne.	
		Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (np. Embedded Event Manager – EEM lub Tcl lub równoważny)	
		Funkcjonalność EEM lub równoważna musi pozwalać na generowanie akcji: a. Wykonanie komendy z poziomu linii poleceń urządzenia b. Wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej c. Wykonanie skryptu d. Wygenerowanie SNMP trap	
		Musi posiadać możliwość sterowania ruchem wyjściowym, niezależnie od tablicy routingu, poprzez wskazanie routera docelowego (next-hop) dla konkretnego ruchu, określonego adresami/podsieciami źródłowymi i docelowymi. Musi istnieć możliwość takiej konfiguracji, żeby powyższa polityka kierowania konkretnego ruchu na konkretny router przestała automatycznie obowiązywać kiedy router docelowy przestaje być osiągalny (przestaje odpowiadać na zawołanie ICMP-echo wysłane z konkretnego interfejsu lub IP źródłowego). W takim przypadku ruch powinien zostać obsłużony zgodnie z tablicą routingu.	
		Urządzenie musi posiadać możliwość integracji z centralnym systemem zarządzania, monitorowania, konfiguracji jak również troubleshootingu	
		Urządzenie musi umożliwiać obsługę przez zcentralizowany system zarządzania w celu zmiany wersji systemu operacyjnego.	
		Musi oferować zaawansowane funkcjonalności bezpieczeństwa takie jak:	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		a) Filtr pakietów oparty o strefy bezpieczeństwa (np. Zone Based Firewall ZBF lub równoważny), b) IPSec VPN, c) Dynamiczny VPN oparty o otwarte protokoły NHRP i mGRE (Dynamic Multipoint VPN DMVPN lub Dynamic Smart VPN lub równoważny).	
		Musi obsługiwać bezpieczne algorytmy IPSec, w szczególności: a) Elliptic Curve Diffie-Hellman (ECDH) z modulo Prime 521-bit b) Diffie-Hellman, z kluczem 2048 bitów c) Advanced Encryption Standard (AES), z kluczem 256 bitów d) RSA, z kluczem 4096 bitów e) SHA2, z kluczem 512 bitów	
		Musi posiadać funkcjonalność sterowania ruchem i jego rozkładu na łącza różnych operatorów na bazie konfigurowalnych polityk uwzględniających SLA (np. dopuszczalny poziom strat w pakietach, bajtach, dopuszczalne opóźnienia, dopuszczalna zmienność opóźnień - tzw. "jitter").	
		Musi być zarządzalne za pomocą SNMPv3	
		Urządzenie musi umożliwiać identyfikowanie aplikacji oraz w ich oparciu budować polityki QoS.	
		Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow lub JFlow lub równoważnego	
		Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI) jak również interfejsu graficznego (GUI)	
		Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.	
		Musi być wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej	
		Musi mieć możliwość montażu w szafie 19” i musi zostać dostarczone z umożliwiającym to zestawem montażowy	
		Urządzenie musi posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V	
		Urządzenie musi być wyposażone w minimum 2 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci WAN/LAN	
		Urządzenie musi być wyposażone w minimum 3 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci WAN/LAN. W chwili dostarczenia urządzenie musi posiadać aktywne minimum 3 interfejsy z portami 1000BASE-T	
		Urządzenie musi być wyposażone w minimum 512MB pamięci Flash	
		Urządzenie musi być wyposażone w minimum 1GB pamięci RAM	
		Urządzenie musi być wyposażone w minimum jeden port USB. Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.	
		Urządzenie musi być wyposażone w port konsolowy szeregowy RJ45 i USB	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie zarówno konsoli USB jak i szeregowej, jak również kablami zasilającymi.	

System zarządzania

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Wymagania	zarządzanie i zbieranie statystyk z wykorzystaniem co najmniej SNMP	
		narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci: możliwość manualnego dodawania urządzeń oraz automatycznego za pośrednictwem protokołów takich jak: LLDP,	
		narzędzia wyświetlania urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu	
		mapa topologii urządzeń z połączeniami oraz wizualizacja alarmów na urządzeniach	
		narzędzia do konfiguracji urządzeń w zakresie przynajmniej interfejsów, list kontroli dostępu, wybranych protokołów routingu na routerach	
		wbudowane przykładowe wzorce konfiguracji urządzeń, takie jak: konfiguracja usług bezpieczeństwa, agregacji linków, konfiguracji NTP, SNMP, NAT, itp.	
		narzędzie do tworzenia wzorców konfiguracji na urządzenia	
		funkcje archiwizacji konfiguracji, przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń	
		narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych	
		narzędzie do zarządzania obrazami oprogramowania urządzeń	
		narzędzie umożliwiające zbieranie informacji o parametrach urządzeń, przynajmniej takich jak: zajętość CPU, zajętość pamięci, dostępność, ilość portów, utylizacja portów, itp.	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		zbieranie statystyk z urządzeń sieciowych za pomocą Netflow lub równoważnego	
		monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania pozwalające na analizę (np.: ilość ruchu, czas odpowiedzi, czas transakcji oraz opóźnienie)	
		monitoring, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie	
		narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku	
		narzędzie do zbierania alarmów pochodzących z urządzeń, kategoryzacji alarmów	
		informowanie o alarmach/incydentach przez notyfikację email	
		narzędzie do konfiguracji, monitoringu (technologia VPN, polityka routingu oraz polityka QoS z podziałem na aplikacje)	
		praca w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci	
		budowanie widoków przez użytkownika	
		hierarchizacja zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów lub zewnętrznego serera uwierzytelniającego	
		narzędzia pozwalające na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy	
		współpraca z serwerami czasu (NTP)	
		wbudowane formularze do konfiguracji usług na nowych urządzeniach	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		wbudowane formularze do weryfikacji możliwości urządzeń pod kątem uruchomienia nowych usług (np. IEEE 802.1X)	
		narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku	
		tworzenie raportów dotyczących urządzeń sieciowych, urządzeń klienckich oraz wydajności sieci	
		narzędzie pozwalające na monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania, pozwalające na analizę, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie, itp.	
		narzędzie pozwalające na diagnostykę działania urządzenia przez wykonanie ping, traceroute, połączenie się z urządzeniem przez telnet, ssh, http, https	
		wyświetlanie wykresów korelujących zmiany w konfiguracji ze zdarzeniami na urządzeniu w celu lepszej i szybszej diagnostyki problemów	
		narzędzie pozwalające na analizę połączenia urządzeń klienckich i użytkowników podłączonych w sposób przewodowy do infrastruktury; narzędzie powinno pozwalać na m.in.: zbieranie informacji o parametrach podłączenia i umożliwiać administratorowi szybką analizę problemów związanych z podłączeniem urządzenia do infrastruktury	
		współpraca z systemem od uwierzytelniania i autoryzacji urządzeń klienckich i użytkowników w celu zbierania informacji o polityce dostępowej nałożonej na urządzenie oraz w celu generowania raportów dotyczących statystyk	
		API REST do integracji z innymi narzędziami/systemami	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		dostarczona wersja musi posiadać licencje na zarządzanie urządzeniami będącymi przedmiotem przetargu z możliwością rozbudowy do przynajmniej 300, ponadto musi umożliwiać dostęp oraz prawo do użytkowania nowych wersji oprogramowania, przez min. 3 lata.	
		system zarządzania musi pochodzić od producenta dostarczonego sprzętu.	
		system musi być dostarczony w najnowszej dostępnej wersji	
		wspiera wysoką dostępność i pracę w trybie active-standby, (nie wymaga się dostarczania systemu w wysokiej dostępności)	
		umożliwia synchronizację danych między systemami redundantnymi	
		instalacja w formie maszyny wirtualnej lub na serwerach fizycznych wspieranych przez producenta systemu	
		wymaga się dostarczenia w formie maszyny wirtualnej pracującej pod VMware ESXi	
		Zamawiający nie wymaga dostarczenia platformy sprzętowej pod system do zarządzania.	

System uwierzytelnienia

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
1.	Podstawowe cechy systemu	System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.	
		System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla bazowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.	
		System musi umożliwiać wsparcie co najmniej 5 000 urządzeń końcowych dołączonych do sieci oraz zapewniać skalowalność do przynajmniej 10 000 urządzeń poprzez rozbudowę istniejącego wdrożenia.	
		System musi zostać dostarczony w formie maszyny wirtualnej.	
		System powinien umożliwiać instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym: a) na hypervisorze VMWare ESXi 5.x i 6.x b) na hypervisorze VMware vSphere Client 5.x and 6.x c) na serwerach fizycznych	
		System musi umożliwiać wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym: a) Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie b) Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z: i. przełączników dostępowych ii. sesji uwierzytelniania 802.1X iii. zdarzeń kontroli dostępu (autoryzacji) iv. zdarzeń związanych z błędami	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		v. zdarzeń związanych z alarmami systemowymi c) Wydzielenie serwerów usługowych realizujących funkcje: i. serwera RADIUS dla infrastruktury sieciowej ii. serwera polityk uwierzytelniania i kontroli dostępu 802.1X iii. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego iv. serwera profilowania stacji końcowych	
		System musi zapewniać realizację wysokiej dostępności elementów funkcjonalnych, w tym: a) zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu b) zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych	
		System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS	
		System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).	
		System musi umożliwiać tworzenie kopii zapasowej na życzenie i w regularnych odstępach czasowych.	
		System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.	
		System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni	
		System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora: a) dostęp do interfejsu konfiguracji	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		usług tożsamości 802.1X b) dostęp do interfejsu konfiguracji urządzeń sieciowych c) dostęp do interfejsu konfiguracji polityk d) dostęp do interfejsu konfiguracji kontroli dostępu gościnnego e) dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania	
		System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.	
2.	Mechanizmy uwierzytelniania 802.1x	System musi wspierać następujące protokoły uwierzytelniania i standardy: a) RADIUS, zgodnie z dokumentami: i. RFC 2138 — Remote Authentication Dial In User Service (RADIUS) ii. RFC 2139 — RADIUS Accounting iii. RFC 2865 — Remote Authentication Dial In User Service (RADIUS) iv. RFC 2866 — RADIUS Accounting v. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support vi. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support vii. RFC 2869 — RADIUS Extensions b) RADIUS Proxy dla zewnętrznego serwera RADIUS	
		System musi wspierać protokół Windows Active Directory, w tym co najmniej następujące repozytoria AD: a) Microsoft Windows Active Directory 2008 32bit i 64bit b) Microsoft Windows Active Directory 2008 R2 64bit c) Microsoft Windows Active Directory 2012 d) Microsoft Windows Active Directory 2012 R2	
		System musi wspierać serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865	
		System musi wspierać następujące protokoły uwierzytelniania: a) PAP/ASCII b) CHAP	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		c) MS-CHAPv1 d) MS-CHAPv2 e) EAP-MD5 f) LEAP g) EAP-TLS h) Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi: i. EAP-MS-CHAPv2 ii. EAP-GTC iii. EAP-TLS i) System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect	
		System musi wspierać implementację 802.1X z przynajmniej następującymi suplikantami: a) wbudowanym klientem 802.1X dla Windows 7, 8, 8.1, 10 b) Apple Mac OS X Supplicant c) Apple iOS Supplicant d) Google Android Supplicant	
		System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based).	
		System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.	
		System musi umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.	
		System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)	
		System musi posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych musi być tworzona per stacja końcowa na podstawie unikalnego adresu MAC.	
		System musi wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC	
		System musi wspierać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym: a) tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		per port b) tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia c) tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym d) mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny e) mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA. f) mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X g) mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X h) obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki i) mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych j) współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN k) możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web l) możliwość uwierzytelnienia przełącznika dostępowego do	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika	
		System musi wspierać uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X)	
		System wspiera przynajmniej następujące urządzenia sieciowe, jako klientów RADIUS (NAD - Network Access Device): Przełączniki sieciowe: Cisco WS-C2960S-48FPD-L Cisco WS-C2960S-24TS-L Cisco WS-C6509-E (M8572) Cisco WS-3850-48P-L Cisco WS-3650-48FD-L	
		System musi zawierać funkcjonalność serwera TACACS+ do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej	
3.	Dostęp gościnny	System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, co najmniej dla: a) Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7 b) Apple Mac OS X 10.x c) Apple iOS 8.0, 7.x, 6.1, 6, 5.1, 5.0.1 d) Google Android dla 2.2 i nowszych e) Linux	
		System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsor).	
		System musi zapewniać uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o: a) wewnętrzną bazę użytkowników b) zewnętrzne repozytorium użytkowników	
		System musi umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do: a) logowania się do systemu b) tworzenia pojedynczego konta gościnnego c) tworzenia wielu kont gościnnych	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		d) importowania kont gościnnych z pliku CSV e) wysyłania wiadomości email po utworzeniu konta gościnnego f) wysyłania wiadomości SMS po utworzeniu konta gościnnego g) wyświetlenia hasła konta gościnnego h) wydrukowania danych konta gościnnego i) wyświetlenia danych stworzonych kont gościnnych j) zawieszenia (suspend) i reinicjacji kont gościnnych	
		System musi umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym: a) zmianę logo strony logowania b) zmianę obrazu tła strony logowania c) zmianę logo bannera d) zmianę obrazu tła bannera e) zmianę koloru tła strony z treścią	
		System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS	
		System musi umożliwiać zmianę adresu URL i FQDN strony sponsora.	
		System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie.	
		System musi posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim,	
		System musi umożliwiać stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.	
		System musi umożliwiać wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora: a) Imienia b) Nazwiska c) Firmy d) adresu e-mail e) numeru telefonu f) danych opcjonalnych	
		System musi umożliwiać konfigurację dla użytkowników gościnnych:	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		a) wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP) b) zezwolenia gościom na zmianę hasła c) samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora	
		System musi umożliwiać honorowanie ustawień local przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.	
		System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.	
		System musi umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługiwać co najmniej 6 urządzeń per konto gościnne.	
		System musi umożliwiać konfigurację czasu ważności hasła w dniach w przedziale zadanym przedziale w dniach.	
		System musi umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny	
		System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych	
		System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika	
		System musi umożliwiać tworzenie portalu gościnnego bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.	
		System musi umożliwiać przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.	
		System musi umożliwiać udostepnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS,	
		System musi wspierać API dla masowych operacji CRUD (Create, Read, Update,	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Delete) na kontach gościnnych.	
4.	Profilowanie urządzeń	System musi umożliwiać dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.	
		System musi umożliwiać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności musi zapewniać stworzenie polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc.	
		System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł: a) DHCP b) http c) RADIUS d) DNS e) SNMP f) Network Scan (NMAP lub inne narzędzie profilowania aktywnego)	
		System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.	
		System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.	
		System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla: a) Stacji roboczych pracujących z systemami Linux, Macintosh, Microsoft Windows, b) Urządzeń mobilnych: Android, Apple, Blackberry c) Drukarek sieciowych d) Routerów	
		System musi umożliwiać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		a) reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci b) reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt	
		System musi umożliwiać włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie.	
		System musi wspierać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.	
5.	Analiza stacji końcowej (Posture Assessment)	System umożliwia pobranie bazy wiedzy reguł analizy stacji końcowej (Posture) dla wspieranych systemów Antywirusowych (AV) i Antispyware (AS) ze strony producenta.	
		System umożliwia kontrolę zachowania dla stacji końcowych, które nie posiadają zainstalowanego agenta głębokiej analizy stacji końcowej (Posture).	
		System umożliwia regularne ponawianie głębokiej analizy stacji końcowej (periodic reassessment) w przedziale od 1 do 24 godzin.	
		System umożliwia przedstawienie użytkownikowi dokumentu Polityki Akceptowalnego Użycia (AUP). Polityka AUP jest prezentowana w postaci strony web po procesie głębokiej analizy stacji. Zawartość dokumentu AUP jest konfigurowalna.	
		System umożliwia głęboką analizę stacji końcowej Windows pod kątem plików (File Condition), w tym: a) istnienia pliku na stacji końcowej b) wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż) c) daty utworzenia i modyfikacji pliku na stacji końcowej (równa,	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		d) wcześniej niż, później niż)	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10 pod kątem wpisów w rejestrze (Registry Condition), w tym: kluczy rejestru z kluczem root: HKCR, HKCU, HKLM, HKU, HKCC z zadanym podkluczem pod kątem: a) istnienia lub nieistnienia klucza b) wartości klucza rejestru c) istnienia i wartości domyślnej wartości klucza rejestru typu Number, String, Version	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, pod kątem uruchomionych aplikacji (Application Condition), w tym: a) nazwy uruchomionego lub nieuruchomionego procesu	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, pod kątem uruchomionych usług systemowych (Service Condition), w tym: a) nazwy uruchomionej lub nieuruchomionej procesu	
		System umożliwia tworzenie słownika prostych i złożonych warunków (Simple i Compound Condition) dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT, w tym z uwzględnieniem: a) parametrów dostępu do sieci, w tym: b) lokalizacji stacji końcowej c) nazwy użytkownika d) adresu IP stacji e) metody uwierzytelnienia f) statusu uwierzytelnienia g) repozytorium użytkowników użytych dla uwierzytelnienia h) atrybutów RADIUS, w tym: i. Calling-Station-ID ii. Framed-IP-Address iii. NAS-Identifier i) NAS-IP-Address j) NAS-Port-Type k) Service-Type l) User-Name m) parametrów sesji w tym:	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		i. typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment) ii. architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit) iii. adresu URL, z którego nastąpiło przekierowanie	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, Mac OS-X, pod kątem zainstalowanych aplikacji Antywirusowych (AV Compound Condition), w tym: a) stwierdzenia czy system AV jest obecny na stacji b) stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od: i. daty ostatniego pliku definicji ii. aktualnego czasu systemowego	
		System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, Mac OS-X pod kątem zainstalowanych aplikacji AntiSpyware (AS Compound Condition), w tym: a) stwierdzenia czy system AS jest obecny na stacji b) stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni od: i. daty ostatniego pliku definicji ii. aktualnego czasu systemowego	
6.	Obsługa serwerów certyfikatów CA.	System musi posiadać funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.	
		Funkcja CA musi umożliwiać wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.	
		System musi wspierać hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		certyfikatów.	
		Funkcja CA musi zapewniać przynajmniej następujące funkcjonalności: a) Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS b) Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym c) Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji d) Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA	
7.	Raportowanie	System musi umożliwiać generowanie raportów dla protokołów AAA: a) diagnostyki protokołów AAA b) trendów uwierzytelnienia 802.1X c) accountingu RADIUS d) uwierzytelniania RADIUS	
		System musi umożliwiać generowanie raportów dozwolonych protokołów a) sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym: i. uwierzytelnień pomyślnych ii. uwierzytelnień nieudanych iii. „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym: uwierzytelnień pomyślnych i nieudanych	
		System musi umożliwiać generowanie raportów dla poszczególnych instancji serwerów systemu, w tym: a) uwierzytelnień RADIUS per serwer b) Top „N"uwierzytelnień per serwer c) monitorowania Online Certificate	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		d) Status Protocol (OCSP) e) administratorów systemu i ich uprawnień f) logowania administratorów do systemu g) zmian konfiguracji serwera dokonanych przez administratorów h) stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS) i) zmian operacyjnych serwera dokonanych przez administratorów j) zmian haseł przez użytkowników	
		System musi umożliwiać generowanie raportów dla stacji końcowych, w tym: a) uwierzytelnień typu MAC Authentication b) Top „N”uwierzytelnień per adres MAC stacji c) Top „N” uwierzytelnień per maszyna d) Top „N”uwierzytelnień per RADIUS Calling Station ID e) działań podsystemu profilera per adres MAC f) czasu wymaganego na sprofilowanie stacji per adres MAC	
		System musi umożliwiać generowanie raportów dla błędów, w tym: a) błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił b) sumarycznych przyczyn nieudanych uwierzytelnień c) Top „N” uwierzytelnień per rodzaj błędu	
		System musi umożliwiać generowanie raportów dla urządzeń sieciowych: a) sumarycznych uwierzytelnień dla urządzeń sieciowych b) Top „N” uwierzytelnień per urządzenie sieciowe c) niedostępności serwera AAA dla urządzenia sieciowego d) wiadomości logowanych przez urządzenia sieciowe e) stanu portów i sesji urządzenia sieciowego widocznych przez SNMP	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		f)	
		System musi umożliwiać generowanie raportów użytkowników: a) sumarycznych uwierzytelnień użytkowników b) Top „N”uwierzytelnień per użytkownik c) sesji użytkowników gościnnych d) aktywności użytkowników gościnnych e) sumarycznych uwierzytelnień sponsorów dostępu gościnnego f) uwierzytelnień per unikalny użytkownik	
		System musi umożliwiać generowanie raportów katalogu sesji a) aktywnych sesji RADIUS b) historii sesji RADIUS c) zaterminowanych sesji RADIUS	
8.	Alarmy	System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: a) wiadomości e-mail b) syslog	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		Alarmy muszą być generowane w następujących sytuacjach: a) ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu b) opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego c) status krytycznych procesów będzie niepożądany, w tym status: i. procesu wewnętrznej bazy danych systemu ii. serwera aplikacyjnego systemu iii. bazy danych sesji iv. kolektora i procesora wiadomości log v. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej) vi. stan obciążenia systemu oraz zajętości pamięci wzrośnie powyżej zadanego poziomu	
		System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: a) badanie łączności IP za pomocą ping, nslookup, traceroute b) wyszukiwanie zdarzeń RADIUS z uwzględnieniem: i. nazwy użytkownika ii. adresu MAC iii. statusu uwierzytelnienia (udana lub nieudana) iv. powodu, jeżeli uwierzytelnienie nieudane v. zakresu czasowego, co do dnia, godziny i minuty c) wykonanie zdalnego polecenia na urządzeniu sieciowym d) ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem: i. definicji serwerów AAA	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
		ii. protokołu RADIUS iii. odkrywania urządzeń iv. logowania v. uwierzytelniania Web vi. konfiguracji trybu 802.1X e) wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu	
9.	Dopuszczalne sposoby realizacji rozwiązania	Zamawiający wymaga spełnienia następujących warunków realizacji systemu uwierzytelnienia dostępu do sieci: a) Zamawiający dopuszcza stosowanie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów. b) W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców Zamawiający oczekuje, iż system będzie zapewniał pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia) c) W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców	
		d) Zamawiający oczekuje iż system będzie serwisowany przez jednego producenta tzn. zgłoszenia serwisowe będą kierowane do jednego dostawcy. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia). e) W przypadku zastosowania serwera CA jako dedykowanego rozwiązania Zamawiający będzie traktował to rozwiązanie jako integralną część systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia)	

Lp.	Nazwa elementu, parametru, funkcjonalności, wymagania	Wymagania minimalne	Parametry techniczne, informacje dotyczące oferowanego sprzętu oraz sposobu spełnienia wymagań. Wykonawca zobowiązany jest podać konkretne dane (informacje, parametry techniczne, nazwę producenta, model oferowanego sprzętu) potwierdzające spełnianie wymagań Zamawiającego
[1]	[2]	[3]	[4]
	Licencje	Wykonawca dostarczy min. 4500 licencji bazowych do systemu uwierzytelnienia i profilowania użytkowników.	
		System musi być w pełni kompatybilny z urządzeniami dostarczonymi przez Wykonawcę.	

OŚWIADCZAMY, ŻE

1. **Jestem / nie jestem * Wykonawcą z sektora małych i średnich przedsiębiorstw.**

2. Pozostajemy związani niniejszą ofertą przez 30 dni licząc od dnia, w którym upłynął termin składania ofert.

3. Oświadczamy, że podane w niniejszej ofercie ceny za wykonanie przedmiotu zamówienia w czasie trwania umowy nie ulegną zmianie.

4. W cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia i realizacji przyszłego świadczenia umownego.

5. Zawarty w Specyfikacji Istotnych Warunków Zamówienia wzór umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku udzielenia nam zamówienia do zawarcia umowy w miejscu i terminie wyznaczonym przez Zamawiającego.

6. Wykonawca oświadcza, że posiada autoryzację producenta sprzętu oraz dysponuje własnym działem serwisu (wsparcia).

7. Wadium wniesione w pieniądzu należy zwrócić na poniższy rachunek bankowy:

   .....

8. Osobą upoważnioną do realizacji przedmiotu zamówienia jest: ……, tel. ……., e-mail: ……

……dnia ……

…….....
(podpis i pieczątka imienna przedstawiciela Wykonawcy/Pełnomocnika)

Podpisy i pieczątki imienne osób upełnomocnionych do reprezentowania Wykonawcy zgodnie z zapisami w dokumencie stwierdzającym status prawny.

Załącznik nr 3 do SIWZ
(Załącznik nr 2 do umowy)

OPIS PRZEDMIOTU ZAMÓWIEN

Przełącznik 25 szt.

Wymagania:

1. Możliwość montażu w szafie rack 19", wysokość urządzenia nie może przekraczać 1 RU
2. Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowanie zewnętrzne systemy zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne. Przełącznik powinien być wyposażony w zasilacz podstawowy.
3. Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów.
4. Urządzenie musi być sprzętowo przygotowane do obsługi standardu IEEE 802.3az Energy-Efficient Ethernet (EEE).
5. Przełącznik Gigabit Ethernet wyposażony w 48 portów 10/100/1000BaseT oraz min. 4 porty uplink w tym min. 2 10Gigabit Ethernet SFP+.
6. Wszystkie porty muszą obsługiwać standard 802.1AE (szyfrowanie ruchu)
7. Porty uplink muszą umożliwiać obsadzenie modułami Gigabit Ethernet SFP (co najmniej 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U) oraz 10Gigabit Ethernet (co najmniej 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER) zależnie od potrzeb Zamawiającego.
8. Wkładki optyczne (SFP, SFP+) przeznaczone do instalacji w przełączniku muszą pochodzić od tego samego producenta co oferowany przełącznik.
9. Przełącznik musi zapewniać możliwość rozbudowy o możliwość łączenia w stos z zapewnieniem następujących parametrów:
    a) Przepustowość w ramach stosu min. 40Gb/s
    b) Min. 9 urządzeń w stosie
    c) Zarządzanie poprzez jeden adres IP
    d) Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych urządzeń w stosie) zgodnie z 802.3ad
10. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree.
11. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
12. Wydajność przełączania minimum 100 Mpps dla pakietów 64-bajtowych.
13. Przepustowość przełącznika minimum 160 Gbps
14. Minimum 1GB pamięci flash
15. Obsługa minimum
    a) 1000 sieci VLAN
    b) 16 000 adresów MAC
    c) 8 000 tras IPv4
16. Obsługa protokołu NTP
17. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
18. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a) IEEE 802.1w Rapid Spanning Tree
    b) IEEE 802.1s Multi-Instance Spanning Tree
    c) Obsługa minimum 128 instancji protokołu STP

19. Obsługa protokołu LLDP i LLDP-MED lub podobnego (np. CDP)
20. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
21. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a) Minimum 5 poziomów dostępu administracyjnego poprzez konsolę.
    b) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
    c) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
    d) Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    e) Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    f) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    g) Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
    h) Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
    i) Minimum 1000 wpisów dla list kontroli dostępu (ACE)
    j) Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
    k) Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
    l) Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
22. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a) Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
    b) Implementacja algorytmu Shaped Round Robin lub Weighted Round Robin lub Deficit Round Robin lub podobnego dla obsługi kolejek
    c) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    d) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    e) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi
    f) Kontrola sztormów dla ruchu broadcast/multicast/unicast
    g) Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
23. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania.
24. Wbudowane reflektometry (TDR) dla portów 10/100/1000

25. Urządzenie musi zapewniać wsparcie routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP). Urządzenie musi zapewniać możliwość rozszerzenia funkcjonalności o wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP) i IPv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM)
26. Obsługa protokołu HSRP lub VRRP lub mechanizmu równoważnego dla usług redundancji bramy
27. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)
28. Urządzenie musi zapewniać możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne)
29. Dedykowany port Ethernet do zarządzania out-of-band
30. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
31. Urządzenie musi być wyposażone w port konsoli USB
32. 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 nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją
33. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
34. zarządzanie urządzeniem przez HTTPS, SNMPv2, SNMPv3 i SSHv2,

35. Przełącznik musi być zgodny z normami środowiskowymi, bezpieczeństwa oraz kompatybilności elektromagnetycznej:
    a) EN 60950-1
    b) EN 55022 klasa A
    c) EN300386
    d) EN61000-4-2, EN61000-4-4, EN61000-4-5, EN61000-4-6
    e) Reduction of Hazardous Substances (RoHS)
36. Przełącznik musi być w pełni kompatybliny z dostarczonym systemem uwierzytelnienia i profilowania użytkowników będącym przedmiotem postępowania.

Przełącznik 56 szt.

Wymagania:

1. Możliwość montażu w szafie rack 19”, wysokość urządzenia nie może przekraczać 1 RU
2. Urządzenie musi posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V
3. Urządzenie musi być sprzętowo przygotowane do obsługi standardu IEEE 802.3az Energy-Efficient Ethernet (EEE).
4. Przełącznik Gigabit Ethernet wyposażony w 48 portów 10/100/1000BaseT oraz min. 4 porty uplink 1Gigabit Ethernet SFP.
5. Porty uplink muszą umożliwiać obsadzenie modułami Gigabit Ethernet SFP co najmniej 1000BaseT, 1000Base-SX, 1000BaseLX/LH, 1000BaseEX, 1000Base-BX-D/U i modułami CWDM zależnie od potrzeb Zamawiającego.
6. Wkładki optyczne (SFP, SFP+) przeznaczone do instalacji w przełączniku muszą pochodzić od tego samego producenta co oferowany przełącznik.
7. Przełącznik musi zapewniać możliwość rozbudowy o możliwość łączenia w stos z zapewnieniem następujących parametrów:
    a) Przepustowość w ramach stosu min. 40Gb/s
    b) Min. 8 urządzeń w stosie
    c) Zarządzanie poprzez jeden adres IP
    d) Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych urządzeń w stosie) zgodnie z 802.3ad
8. Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree.
9. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
10. Wydajność przełączania minimum 100 Mpps dla pakietów 64-bajtowych.
11. Przepustowość przełącznika minimum 160 Gbps (full duplex)
12. Obsługa minimum:
    a) 1000 sieci VLAN jednocześnie oraz obsługa 802.1Q
    b) 16 000 adresów MAC
13. Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów
14. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów bezpieczeństa typu Port Security i IP Source Guard na interfejsach link aggregation
15. Obsługa protokołu NTP
16. Musi zapewniać obsługę min. 16 statycznych tras dla routingu IPv4 i IPv6
17. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping
18. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 128 instancji protokołu STP
19. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
20. Przełącznik musi obsługiwać następujące mechanizmy bezpieczeństwa:
    a) Minimum 5 poziomów dostępu administracyjnego poprzez konsolę
    b) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL
    c) Obsługa funkcji Guest VLAN
    d) Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

e) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
f) Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www
g) Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie
h) Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
i) Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6
j) Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6
k) Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
l) Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
m) Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow LITE, J-Flow lub równoważne)
n) Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+

21. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    b) Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub Weighted Round Robin lub Deficit Round Robin lub podobnego dla obsługi tych kolejek
    c) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
    d) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi.
22. Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP)
23. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli
24. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB
25. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN)
26. 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 nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych
27. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych

pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania.

28. Przełącznik musi być zgodny z normami środowiskowymi, bezpieczeństwa oraz kompatybilności elektromagnetycznej:
    a) EN 60950-1
    b) EN 55022 klasa A
    c) EN300386
    d) EN61000-4-2, EN61000-4-4, EN61000-4-5, EN61000-4-6
    e) Reduction of Hazardous Substances (RoHS)
29. Przełącznik musi być w pełni kompatybliny z dostarczonym systemem uwierzytelnienia i profilowania użytkowników będącym przedmiotem postępowania.

Przełącznik rdzeniowy 3 szt.

Wymagania:

1. Urządzenie o architekturze modularnej – o wysokości max. 11RU dedykowane do zamontowania w szafie rack 19”pozwalające na instalację kart liniowych i redundantnych modułów zarządzająco-przełączających działających w trybie active-standby lub active-active
2. Wymagane niezbędne wyposażenie urządzenia:
    a) Moduł zarządzająco-przełączający.
    b) Min dwa zasilacze AC (zapewniające redundancję zasilania w trybie 1:1) o mocy pozwalającej zasilić urządzenie wraz z kartami liniowymi oraz posiadające min. 20% mocy zapasu.
    c) Urządzenie powinno umożliwiać rozbudowę zasilaczy, mogących pracować w trybie redundancji n+1
    d) Cztery moduły minimum 48-portowe 10/100/1000 Gigabit Ethernet
    e) 32 porty 10G Ethernet SFP/SFP+. Wszystkie porty muszą obsługiwać standard 802.1AE (szyfrowanie ruchu) z pełną wydajnością łącza 10GE.
3. Porty SFP muszą obsługiwać minimum wkładki typu: SX, LH, T (RJ45). Porty SFP+ muszą obsługiwać minimum wkładki typu: SR, LR
4. Dla każdego portu możliwość bezpośredniego zaadresowania portu (IP) (przełączenie portu w tryb L3).
5. Urządzenie, które producent oficjalnie pozycjonuje jako rozwiązanie dla rdzenia sieci kampusowych.
6. Wspiera technologię wirtualizacji, umożliwiającą zbudowanie z co najmniej dwóch urządzeń fizycznych jednego logicznego urządzenia zarządzanego z jednego miejsca (poprzez jeden adres IP).
7. Wydajność przełączania matrycy min. 3,5Tb/s
8. Obsługa minimum:
    a) min. 100 000 wpisów w tablicy adresów MAC
    b) min. 250 000 wpisów w tablicy routingowej IPv4
    c) min. 125 000 wpisów w tablicy routingowej IPv6
    d) min. 125 000 tras multicast
    e) min. 64 000 wpisów na potrzeby realizacji polityk QoS i bezpieczeństwa (listy kontroli dostępu)
9. Obsługa protokołów warstwy 3 dla IPv4: Open Shortest Path First (OSPF), BGPv4
10. Obsługa protokołów warstwy 3 dla IPv6: Open Shortest Path First (OSPFv3), MP-BGP
11. Obsługuje sprzętowo ruch multicastowy w tym PIM Sparse i Dense Mode, SSM, IGMP/MLD
12. Urządzenie musi umożliwiać rozszerzenie funkcjonalności o wsparcie dla MPLS, LDP, L2 i L3 VPN, VPLS, MPLS TE, MPLS traceruote poprzez zakup odpowiedniej licencji lub wymianę oprogramowana bez konieczności modernizacji sprzętowej urządzenia
13. Sprzętowa obsługa tunelowania GRE
14. Obsługa IGMPv1/2/3 i MLDv2 for IP
15. Urządzenie wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a) mechanizm BFD (Bidirectional Forwarding Detection) co najmniej dla protokołu OSPFv2 i OSPFv3
    b) IEEE 802.1D Spanning Tree Protocol
    c) IEEE 802.1w Rapid Spanning Tree
    d) IEEE 802.1s Multiple Spanning Tree
    e) Spanning Tree loop guard
    f) Spanning Tree root guard
    g) Spanning Tree BPDU filtering
    h) Obsługa protokołu LLDP (IEEE 802.1AB)
    i) Obsługa Private VLAN
    j) Obsługa 802.1q
    k) IEEE 802.3ad (Link Aggregation Control Protocol) umożliwiający grupowanie portów z wykorzystaniem portów znajdujących się na różnych kartach liniowych

l) pozwala na wymianę kart liniowych oraz modułu fantray bez wyłączania zasilania (tzw. Hot-Swap)

16. Obsługa wirtualnych instancji routingu (VRF) - co najmniej 20 instancji VRF
17. W obrębie VRF musi istnieć możliwość uruchomienia niezależnej instancji protokołu dynamicznego routingu (minimum wsparcie dla OSPF)
18. Możliwość przypisywania interfejsów do VRF (odizolowania interfejsów od globalnej tablicy routingu).
19. Obsługa NTP
20. Obsługa protokołu Hot Standby Router Protocol (HSRP) lub Virtual Router Redundancy Protocol (VRRP)
21. Urządzenie wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci (QoS):
    a) Obsługa min. 4 kolejek sprzętowych
    b) Obsługa co najmniej jednej kolejki ze statusem strict priority
    c) Implementacja algorytmu dla obsługi kolejek typu Shaped Round Robin, lub WRR lub DRR lub równoważnego.
    d) Możliwość ograniczania pasma dostępnego na danym porcie (policing, rate limiting).
    e) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez nadawanie wartości 802.1p (CoS) oraz IP Precedence/DSCP w ramkach Ethernet oraz pakietach IP. Wykorzystanie następujących parametrów w klasyfikacji: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
    f) Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet oraz pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP Precedence/DSCP
    g) Definiowanie polityk QoS per port i per VLAN
    h) Obsługa protokołu RSVP
22. Urządzenie wspiera następujące mechanizmy związane z bezpieczeństwem:
    a) Wiele poziomów dostępu administracyjnego poprzez konsolę - autoryzacja dostępu do przełącznika w oparciu o mechanizmy AAA – min. 5 poziomów uprawnień z możliwością określenia zakresu z dokładnością do poszczególnych komend
    b) Autoryzacja użytkowników/portów w oparciu o IEEE 802.1x z możliwością przydziału listy kontroli dostępu (ACL) i VLANu
    c) Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
    d) Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
    e) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
    f) Wsparcie dla możliwości uwierzytelniania (802.1X) wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem.
    g) Możliwość obsługi żądań Change of Authorization (CoA)
    h) Możliwość takiej konfiguracji mechanizmów 802.1X, żeby dostęp do sieci był możliwy również w przypadku wykrycia braku komunikacji z serwerem uwierzytelniającym (tryb awaryjny)
    i) Obsługa co najmniej następujących mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Gurad
    j) Możliwość filtrowania ruchu na poziomie portu oraz VLANu w oparciu o adresy MAC, IP, porty TCP/UDP
    k) Listy kontroli dostępu także dla IPv6
    l) Mechanizmy ochrony warstwy kontrolnej np. CoPP
23. Urządzenie musi wspierać następujące mechanizmy związane z zarządzaniem:
    a) Ma możliwość zarządzania przez SNMPv3 oraz SSH v2
    b) Umożliwia zarządzanie poprzez interfejs CLI (konsolę) oraz poprzez dedykowany port Gigabit Ethernet
    c) Umożliwia identyfikację i uwierzytelnianie w oparciu o serwer RADIUS lub TACACS+
    d) Pamięć flash minimum 2GB

e) Umożliwia stworzenie wirtualnego systemu złożonego z min. 2 urządzeń będących przedmiotem opisu, zarządzanego jako całość. Urządzenia pracujące w takiej konfiguracji muszą umożliwiać połączenie w system z wykorzystaniem standardowych portów SFP+ mieszczących się na module zarządzająco-przełączającym jak również na 32 portowym module SFP/SFP+
f) Umożliwia lokalną/zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu lub poprzez dedykowaną sieć VLAN
g) Posiada możliwość raportowania do systemów zarządzających z wykorzystaniem statystyk typu flow (J-Flow, NetFlow lub odpowiednik). Konieczna jest obsługa/buforowanie minimum 256 000 wpisów (per moduł zarządzający/karta liniowa). Funkcjonalność ta musi być obsługiwana sprzętowo i wspierać IPv6 oraz multicast'y
h) Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
i) Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych

24. Obsługuje ramki Ethernet o wielkości nie mniejszej niż 9216 bajtów (tzw. Jumbo Frame)
25. Przełącznik musi być w pełni kompatybliny z dostarczonym systemem uwierzytelnienia i profilowania użytkowników będącym przedmiotem postępowania.

Router Centrala 1 szt.

Wymagania:

1. Urządzenie o architekturze modularnej, wyposażone w co najmniej 6 portów Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP, a także w min. 2 porty 10 Gigabit Ethernet przeznaczone dla modułów optycznych typu SFP+. W chwili dostarczenia urządzenia zamawiający wymaga dostarczenia urządzenia z dostępnymi i aktywnymi 4 portami 1000BASE-T oraz 2 portami 1000BASE SX-MM, nie wymaga się aktywnych portów 10GE.
2. Urządzenie musi umożliwiać rozszerzenie m.in. o następujące porty:
    a) 1 port 10 GigabitEthernet
    b) 8 portów Gigabit Ethernet
3. Musi posiadać wydajność przełączania min. 19 Mpps oraz min. 15 Gbps ruchu
4. Musi posiadać wydajność szyfrowania min. 5,5 Gbps dla ruchu IMIX (encryption+decryption).
5. Musi być wyposażone w minimum 4 GB pamięci RAM.
6. Obsługa minimum 800 000 prefiksów w tablicach rutingu dla IPv4.
7. Obsługa minimum 150 000 prefiksów w tablicach rutingu dla IPv6.
8. Musi obsługiwać następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP.
9. Musi obsługiwać następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP.
10. Obsługa Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter) z możliwością definiowania polityk per aplikacja.
11. Urządzenie musi umożliwiać uruchomienie wydzielonych wirtualnych instancji (przestrzeni) routingowych w oparciu o mechanizm VRF (Virtual Routingu Forwarding), umożliwiając m.in. wykreowanie wydzielonej logicznej sieci na potrzebę obsługi ruchu określonej aplikacji lub wydzielonego fragmentu sieci.
12. Musi obsługiwać 2000 instancji wirtualnych tablic routingu.
13. Musi obsługiwać funkcjonalność Bidirectional Forwarding Detection (BFD), zapewniając przy tym wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego.
14. Musi obsługiwać funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF.
15. Musi obsługiwać multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN.
16. Musi obsługiwać protokół NHRP (ang. Next Hop Resolution Protocol)
17. Urządzenie musi obsługiwać protokół GDOI (RFC 6407).
18. Urządzenie musi posiadać następujące funkcjonalności związane z niezawodnością pracy:
    a) BFD dla OSPF, BGP, ISIS
    b) IP FRR
    c) Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP
    d) funkcjonalność VRRP lub równoważny
    e) redundantne zasilacze AC 230V zintegrowane w obudowie urządzenia
    f) możliwość wymiany modułów w trakcie pracy (ang. hot swap)
19. Urządzenie musi obsługiwać MPLS, w szczególności:
    a) LDP
    b) EoMPLS, VPLS
    c) MPLS L3 VPN
    d) MPLS TE
    e) MPLS FRR w trybach protekcji łącza oraz węzła
20. Urządzenie musi obsługiwać następujące mechanizmy jakości usług (QoS):
    a) klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN dla kart L2, zarówno dla IPv4 jak i IPv6
    b) hierarchiczny QoS (H-QoS) - 3 poziomy

c) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: adres MAC, adres IP, port TCP, VLAN ID, MPLS EXP, 802.1p (CoS), IP ToS/DSCP.
d) dynamiczna alokacja kolejek sprzętowych, dostępne min. 16 000 kolejek
e) algorytm Round Robin (Shaped Round Robin) dla obsługi kolejek lub równoważny
f) możliwość obsługi jednej kolejki z priorytetem w stosunku do innych
g) mechanizm ograniczania ilości ruchu w kolejce priorytetowej
h) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP
i) możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting)
j) mechanizm WRED
k) możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS

21. Urządzenie musi obsługiwać następujące funkcje i elementy bezpieczeństwa:
a) ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu
b) Unicast RPF (Reverse Path Forwarding)
c) listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, flagi TCP,
d) min. 30 000 wpisów IPv4 na wszystkich listach kontroli dostępu (ACL),
e) dostęp administracyjny oparty o role z przypisanymi uprawnieniami
f) urządzenie ma realizować funkcjonalności zapory ogniowej typu statefull (ang. statefull firewall), przy czym zapora ogniowa:
g) umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji).
h) obsługuje ruch IPv4 oraz IPv6
i) umożliwia konfigurację polityk per wirtualna tablica routingu (VRF)
j) zasoby sprzętowe realizujące funkcjonalności szyfrowania VPN z wydajnością min. 5,5 Gbps (AES256+SHA512) (encryption+decryption),
k) sieci VPN typu site-2-site oparte o IPSec
l) dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP (lub równoważny) w relacji spoke to spoke w celu optymalizacji transmsji danych pomiędzy oddziałami.
m) bez-tunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast

22. Musi obsługiwać bezpieczne algorytmy IPSec, w szczególności:
a) Elliptic Curve Diffie-Hellman (ECDH) z modulo Prime 521-bit
b) Diffie-Hellman, z kluczem 2048 bitów
c) Advanced Encryption Standard (AES), z kluczem 256 bitów
d) RSA, z kluczem 4096 bitów
e) SHA2, z kluczem 512 bitów
f) konfigurację tuneli IPSec VPN w oparciu o protokół IKEv2
- IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych
- IKEv2 zarówno dla ruchu IPv4 jak i IPv6

g) funkcjonalność VPN per VRF
h) ochronę centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU

23. Urządzenie musi wspierać usługi klasyfikacji ruchu w oparciu o głęboką analizę pakietów, klasyfikacja ta powinna udostępniać co najmniej 3 atrybuty opisujące daną aplikację/protokół atrybuty

mają ułatwić konfigurowanie QoS na urządzeniu poprzez grupowanie podobnych aplikacji/protokołów (na przykład wszystkie aplikacje typu p2p mają taką samą wartość atrybutu określającego typ aplikacji). Włączenie usługi nie może powodować konieczności rozbudowy sprzętowej urządzenia, co najwyżej zakup licencji pozwalającej na korzystanie z powyższej funkcjonalności.

24. Urządzenie musi obsługiwać do 2000 tuneli GRE.
25. Urządzenie musi posiadać możliwość tunelowania przesyłanych danych w postaci tuneli GRE typu punkt-punkt oraz punkt-wielopunkt z możliwością uruchomienia protokołów routingu dynamicznego pomiędzy urządzeniami połączonymi za pomocą tuneli GRE.
26. Urządzenie musi umożliwiać ochronę kryptograficzną tuneli GRE.
27. W ramach funkcjonalności zarządzania, urządzenie musi:
    a) umożliwiać zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3
    b) obsługiwać język skryptowy
    c) obsługiwać protokół Netflow lub Netstream lub równoważny
    d) posiadać narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP
    e) posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania z wykorzystaniem protokołów RADIUS lub TACACS+
    f) posiadać dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45), port Ethernet oraz port AUX
    g) posiadać port USB
    h) posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona
    i) posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów
28. Urządzenie musi umożliwiać montaż w szafie 19”.
29. Musi być wykonane z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.

Routery oddziały 25 szt.

Wymagania:

1. Musi być urządzeniem pełniącym rolę wielousługowego routera modularnego gotowego do obsługi mechanizmów bezpiecznej i niezawodnej sieci WAN w oparciu o Internet oraz MPLS
2. Musi pozwalać na instalację co najmniej:
    a) jednego modułu rozszerzeń takich jak moduły przełącznika,
    b) 2 kart z interfejsami sieciowymi
3. Musi posiadać zintegrowaną sprzętową akcelerację szyfrowania DES/3DES/AES
4. Musi posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
5. Sloty urządzenia przewidziane pod rozbudowę muszą mieć możliwość obsadzenia modułami:
    a) z interfejsami szeregowymi WAN,
    b) przełącznika Ethernet (funkcje L2 i L3), oczekiwana liczba portów przełącznika nie może być mniejsza niż 8 dla jednego modułu;
    c) z portem VDSL2 / ADSL2+ over POTS / Annex M;
6. Urządzenie musi oferować możliwość zwiększenia wydajności do co najmniej 300Mbps dla ruchu IMIX bez rozbudowy o dodatkowe moduły sprzętowe – np. licencyjnie przez odblokowanie wbudowanych zasobów sprzętowych lub jako większa wydajność początkowa routera;
7. Urządzenie musi oferować dla pakietów IMIX przy włączonych usługach szyfrowania z IPSec, szczegółowej analizy aplikacji, kontroli jakości usługi QoS o przepustowość minimum 200Mbps;
8. Musi posiadać obsługę protokołów routingu IP BGPv4, OSPFv3, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i SSM) oraz routing statyczny;
9. Protokół BGP musi posiadać obsługę 4 bajtowych ASN;
10. Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMP v1/v2, IGMP Snooping, PIMv2, Bi-directional PIM;
11. Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF)
12. Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q, urządzenie musi obsługiwać co najmniej 1000 sieci VLAN
13. Musi obsługiwać IPv6 w tym ICMP dla IPv6
14. Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, flagi TCP
15. Urządzenie musi posiadać wbudowany mechanizm logowania zdarzeń systemowych a także liczników pokazujących ilość pakietów i bajtów odrzuconych/przepuszczonych przez wybraną regułę listy kontroli dostępu. Musi istnieć możliwość wysyłania logów systemowych na zewnętrzny serwer.
16. Musi posiadać obsługę NAT dla ruchu IP unicast oraz PAT dla ruchu IP unicast
17. Mechanizm NAT musi zapewniać wsparcie dla H.245 lub SIP
18. Musi posiadać obsługę wirtualnych instancji routingu (VRF) - co najmniej 64 instancji VRF
19. Musi posiadać obsługę mechanizmu DiffServ
20. Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
21. Musi zapewniać obsługę mechanizmów kolejkowania ruchu:
    a) z obsługą kolejki absolutnego priorytetu
    b) ze statyczną alokacją pasma dla typu ruchu
    c) WFQ

22. Musi obsługiwać mechanizm WRED
23. Musi obsługiwać mechanizm Traffic Shaping
24. Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu
25. Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.
26. Musi obsługiwać protokół NTP
27. Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP lub GLBP lub VRRP)
28. Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+
29. Musi obsługiwać protokół MPLS (funkcje LER i LSR)
30. Musi obsługiwać MPLS over GRE
31. Musi wspierać QoS dla MPLS
32. Musi obsługiwać MPLS Traffic Engineering
33. Musi obsługiwać MPLS L2 i L3 VPN oraz VPLS
34. Musi obsługiwać funkcjonalność Bidirectional Forwarding Detection (BFD) lub równoważna
35. Funkcjonalność BFD musi być dostępna dla intefejsów skonfigurowanych do współpracy z VRF
36. Musi obsługiwać funkcjonalność BFD Echo Mode lub równoważna
37. Funkcjonalność BFD (lub równoważna) musi posiadać wsparcie dla protokołów BGP, OSPF, IS-IS, routingu statycznego oraz HSRP lub VRRP lub równoważne.
38. Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (np. Embedded Event Manager – EEM lub Tcl lub równoważny)
39. Funkcjonalność EEM lub równoważna musi pozwalać na generowanie akcji:
    a. Wykonanie komendy z poziomu linii poleceń urządzenia
    b. Wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej
    c. Wykonanie skryptu
    d. Wygenerowanie SNMP trap
40. Musi posiadać możliwość sterowania ruchem wyjściowym, niezależnie od tablicy routingu, poprzez wskazanie routera docelowego (next-hop) dla konkretnego ruchu, określonego adresami/podsieciami źródłowymi i docelowymi. Musi istnieć możliwość takiej konfiguracji, żeby powyższa polityka kierowania konkretnego ruchu na konkretny router przestała automatycznie obowiązywać kiedy router docelowy przestaje być osiągalny (przestaje odpowiadać na zawołanie ICMP-echo wysłane z konkretnego interfejsu lub IP źródłowego). W takim przypadku ruch powinien zostać obsłużony zgodnie z tablicą routingu.
41. Urządzenie musi posiadać możliwość integracji z centralnym systemem zarządzania, monitorowania, konfiguracji jak również troubleshootingu
42. Urządzenie musi umożliwiać obsługę przez zcentralizowany system zarządzania w celu zmiany wersji systemu operacyjnego.
43. Musi oferować zaawansowane funkcjonalności bezpieczeństwa takie jak:
    a) Filtr pakietów oparty o strefy bezpieczeństwa (np. Zone Based Firewall ZBF lub równoważny),
    b) IPSec VPN,
    c) Dynamiczny VPN oparty o otwarte protokoły NHRP i mGRE (Dynamic Multipoint VPN DMVPN lub Dynamic Smart VPN lub równoważny).
44. Musi obsługiwać bezpieczne algorytmy IPSec, w szczególności:
    a) Elliptic Curve Diffie-Hellman (ECDH) z modulo Prime 521-bit
    b) Diffie-Hellman, z kluczem 2048 bitów
    c) Advanced Encryption Standard (AES), z kluczem 256 bitów
    d) RSA, z kluczem 4096 bitów

e) SHA2, z kluczem 512 bitów

45. Musi posiadać funkcjonalność sterowania ruchem i jego rozkładu na łącza różnych operatorów na bazie konfigurowalnych polityk uwzględniających SLA (np. dopuszczalny poziom strat w pakietach, bajtach, dopuszczalne opóźnienia, dopuszczalna zmienność opóźnień - tzw. "jitter").
46. Musi być zarządzalne za pomocą SNMPv3
47. Urządzenie musi umożliwiać identyfikowanie aplikacji oraz w ich oparciu budować polityki QoS.
48. Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow lub JFlow lub równoważnego
49. Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI) jak również interfejsu graficznego (GUI)
50. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
51. Musi być wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej
52. Musi mieć możliwość montażu w szafie 19” i musi zostać dostarczone z umożliwiającym to zestawem montażowym
53. Urządzenie musi posiadać wbudowany zasilacz umożliwiający zasilanie prądem przemiennym 230V
54. Urządzenie musi być wyposażone w minimum 3 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci WAN/LAN
55. W chwili dostarczenia urządzenie musi posiadać aktywne minimum 3 interfejsy z portami 1000BASE-T
56. Urządzenie musi być wyposażone w minimum 512MB pamięci Flash
57. Urządzenie musi być wyposażone w minimum 1GB pamięci RAM
58. Urządzenie musi być wyposażone w minimum jeden port USB. Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.
59. Urządzenie musi być wyposażone w port konsolowy szeregowy RJ45 i USB
60. Urządzenie musi być dostarczone z kablami pozwalającymi na podłączenie zarówno konsoli USB jak i szeregowej, jak również kablami zasilającymi.

System zarządzania infrastrukturą sieciową
Wymagania:

- zarządzanie i zbieranie statystyk z wykorzystaniem co najmniej SNMP
- narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci: możliwość manualnego dodawania urządzeń oraz automatycznego za pośrednictwem protokołów takich jak: LLDP,
- narzędzia wyświetlania urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu
- mapa topologii urządzeń z połączeniami oraz wizualizacja alarmów na urządzeniach
- narzędzia do konfiguracji urządzeń w zakresie przynajmniej interfejsów, list kontroli dostępu, wybranych protokołów routingu na routerach
- wbudowane przykładowe wzorce konfiguracji urządzeń, takie jak: konfiguracja usług bezpieczeństwa, agregacji linków, konfiguracji NTP, SNMP, NAT, itp.
- narzędzie do tworzenia wzorców konfiguracji na urządzenia
- funkcje archiwizacji konfiguracji, przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń
- narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych
- narzędzie do zarządzania obrazami oprogramowania urządzeń
- narzędzie umożliwiające zbieranie informacji o parametrach urządzeń, przynajmniej takich jak: zajętość CPU, zajętość pamięci, dostępność, ilość portów, utylizacja portów, itp.
- zbieranie statystyk za pomocą Netflow lub równoważny
  monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania pozwalające na analizę (np.: ilość ruchu, czas odpowiedzi, czas transakcji oraz opóźnienie)
- monitoring, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie
- narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku
- narzędzie do zbierania alarmów pochodzących z urządzeń, kategoryzacji alarmów
- informowanie o alarmach/incydentach przez notyfikację email
- narzędzie do konfiguracji, monitoringu (technologia VPN, polityka routingu oraz polityka QoS z podziałem na aplikacje)

Ogólny zakres funkcjonalności:

- praca w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci
- budowanie widoków przez użytkownika
- hierarchizacja zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów lub zewnętrznego serwera uwierzytelniającego
- narzędzia pozwalające na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy
- współpraca z serwerami czasu (NTP)
- wbudowane formularze do konfiguracji usług na nowych urządzeniach
- wbudowane formularze do weryfikacji możliwości urządzeń pod kątem uruchomienia nowych usług (np. IEEE 802.1X)

- narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku
- tworzenie raportów dotyczących urządzeń sieciowych, urządzeń klienckich oraz wydajności sieci
- zbieranie Netflow (lub równoważny) z urządzeń sieciowych
- narzędzie pozwalające na monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania, pozwalające na analizę, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie, itp.
- narzędzie pozwalające na diagnostykę działania urządzenia przez wykonanie ping, traceroute, połączenie się z urządzeniem przez telnet, ssh, http, https
- wyświetlanie wykresów korelujących zmiany w konfiguracji ze zdarzeniami na urządzeniu w celu lepszej i szybszej diagnostyki problemów
- narzędzie pozwalające na analizę połączenia urządzeń klienckich i użytkowników podłączonych w sposób przewodowy do infrastruktury; narzędzie powinno pozwalać na m.in.: zbieranie informacji o parametrach podłączenia i umożliwiać administratorowi szybką analizę problemów związanych z podłączeniem urządzenia do infrastruktury
- współpraca z systemem od uwierzytelniania i autoryzacji urządzeń klienckich i użytkowników w celu zbierania informacji o polityce dostępowej nałożonej na urządzenie oraz w celu generowania raportów dotyczących statystyk
- API REST do integracji z innymi narzędziami/systemami
- dostarczona wersja musi posiadać licencje na zarządzanie urządzeniami będącymi przedmiotem przetargu z możliwością rozbudowy do przynajmniej 300, ponadto musi umożliwiać dostęp oraz prawo do użytkowania nowych wersji oprogramowania, przez min. 3 lata.
- system zarządzania musi pochodzić od producenta dostarczonego sprzętu.

Platforma pod system do zarządzania:

- system musi być dostarczony w najnowszej dostępnej wersji
- wspiera wysoką dostępność i pracę w trybie active-standby (nie wymaga się dostarczania systemu w wysokiej dostępności)
- umożliwia synchronizację danych między systemami redundantnymi
- instalacja w formie maszyny wirtualnej lub na serwerach fizycznych wspieranych przez producenta systemu
- wymaga się dostarczenia w formie maszyny wirtualnej pracującej pod VMware ESXi
- Zamawiający nie wymaga dostarczenia platformy sprzętowej pod system do zarządzania.

System uwierzytelnienia dostępu do sieci LAN

Podstawowe cechy systemu

1. System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.
2. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji dla bazowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.
3. System musi umożliwiać wsparcie co najmniej 5 000 urządzeń końcowych dołączonych do sieci oraz zapewniać skalowalność do przynajmniej 10 000 urządzeń poprzez rozbudowę istniejącego wdrożenia.
4. System musi zostać dostarczony w formie maszyny wirtualnej.
5. System powinien umożliwiać instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym:
    a) na hypervisorze VMWare ESXi 5.x i 6.x
    b) na hypervisorze VMware vSphere Client 5.x and 6.x
    c) na serwerach fizycznych

6. System musi umożliwiać wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:
    a) Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie
    b) Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:
        i. przełączników dostępowych
        ii. sesji uwierzytelniania 802.1X
        iii. zdarzeń kontroli dostępu (autoryzacji)
        iv. zdarzeń związanych z błędami
        v. zdarzeń związanych z alarmami systemowymi
    c) Wydzielenie serwerów usługowych realizujących funkcje:
        i. serwera RADIUS dla infrastruktury sieciowej
        ii. serwera polityk uwierzytelniania i kontroli dostępu 802.1X
        iii. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego
        iv. serwera profilowania stacji końcowych
7. System musi zapewniać realizację wysokiej dostępności elementów funkcjonalnych, w tym:
    a) zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu
    b) zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych
8. System musi umożliwiać aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS
9. System musi umożliwiać zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
10. System musi umożliwiać tworzenie kopii zapasowej na życzenie i w regularnych odstępach czasowych.
11. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
12. System musi umożliwiać wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System musi wymuszać hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni
13. System musi umożliwiać kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
    a) dostęp do interfejsu konfiguracji usług tożsamości 802.1X
    b) dostęp do interfejsu konfiguracji urządzeń sieciowych
    c) dostęp do interfejsu konfiguracji polityk
    d) dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
    e) dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
14. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.

Mechanizmy uwierzytelniania 802.1x

1. System musi wspierać następujące protokoły uwierzytelniania i standardy:
    a) RADIUS, zgodnie z dokumentami:
        i. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
        ii. RFC 2139 — RADIUS Accounting
        iii. RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
        iv. RFC 2866 — RADIUS Accounting
        v. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
        vi. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
        vii. RFC 2869 — RADIUS Extensions
    b) RADIUS Proxy dla zewnętrznego serwera RADIUS

2. System musi wspierać protokół Windows Active Directory, w tym co najmniej następujące repozytoria AD:
    a) Microsoft Windows Active Directory 2008 32bit i 64bit
    b) Microsoft Windows Active Directory 2008 R2 64bit
    c) Microsoft Windows Active Directory 2012
    d) Microsoft Windows Active Directory 2012 R2
3. System musi wspierać serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865
4. System musi wspierać następujące protokoły uwierzytelniania:
    a) PAP/ASCII
    b) CHAP
    c) MS-CHAPv1
    d) MS-CHAPv2
    e) EAP-MD5
    f) LEAP
    g) EAP-TLS
    h) Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
        i. EAP-MS-CHAPv2
        ii. EAP-GTC
        iii. EAP-TLS
    i) System musi umożliwiać konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect
5. System musi wspierać implementację 802.1X z przynajmniej następującymi suplikantami:
    a) wbudowanym klientem 802.1X dla Windows 7, 8, 8.1, 10
    b) Apple Mac OS X Supplicant
    c) Apple iOS Supplicant
    d) Google Android Supplicant
6. System musi umożliwiać tworzenie polityk uwierzytelniania 802.1X opartych o złożone reguły (rule-based).
7. System musi umożliwiać uwierzytelnianie 802.1X maszyn i użytkowników.
8. System musi umożliwiać tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.
9. System musi posiadać lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym)
10. System musi posiadać lokalną bazę stacji końcowych. Lokalna baza stacji końcowych musi być tworzona per stacja końcowa na podstawie unikalnego adresu MAC.
11. System musi wspierać uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC
12. System musi wspierać zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:
    a) tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port
    b) tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia
    c) tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym
    d) mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny
    e) mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA.
    f) mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X
    g) mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X
    h) obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki
    i) mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych

j) współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN
k) możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web
l) możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika

13. System musi wspierać uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X)
14. System wspiera przynajmniej następujące urządzenia sieciowe, jako klientów RADIUS (NAD - Network Access Device):
15. Przełączniki sieciowe:
    Cisco WS-C2960S-48FPD-L
    Cisco WS-C2960S-24TS-L
    Cisco WS-C6509-E (M8572)
    Cisco WS-3850-48P-L
    Cisco WS-3650-48FD-L
16. System musi zawierać funkcjonalność serwera TACACS+ do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej

Realizacja dostępu gościnnego

1. System musi umożliwiać realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, co najmniej dla :
   a) Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7
   b) Apple Mac OS X 10.x
   c) Apple iOS 8.0, 7.x, 6.1, 6, 5.1, 5.0.1
   d) Google Android dla 2.2 i nowszych
   e) Linux
2. System musi umożliwiać dodawanie kont gościnnych przez wybrane osoby (sponsor).
3. System musi zapewniać uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o:
   a) wewnętrzną bazę użytkowników
   b) zewnętrzne repozytorium użytkowników
4. System musi umożliwiać konfigurację uprawnień sponsora, w tym uprawnienia do:
   a) logowania się do systemu
   b) tworzenia pojedynczego konta gościnnego
   c) tworzenia wielu kont gościnnych
   d) importowania kont gościnnych z pliku CSV
   e) wysyłania wiadomości email po utworzeniu konta gościnnego
   f) wysyłania wiadomości SMS po utworzeniu konta gościnnego
   g) wyświetlenia hasła konta gościnnego
   h) wydrukowania danych konta gościnnego
   i) wyświetlenia danych stworzonych kont gościnnych
   j) zawieszenia (suspend) i reinicjacji kont gościnnych
5. System musi umożliwiać personalizację wyglądu portalu sponsora i gościa, w tym:
   a) zmianę logo strony logowania
   b) zmianę obrazu tła strony logowania
   c) zmianę logo bannera
   d) zmianę obrazu tła bannera
   e) zmianę koloru tła strony z treścią
6. System musi umożliwiać zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS
7. System musi umożliwiać zmianę adresu URL i FQDN strony sponsora.
8. System musi umożliwiać automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie.

9. System musi posiadać wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim,
10. System musi umożliwiać stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.
11. System musi umożliwiać wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:
    a) Imienia
    b) Nazwiska
    c) Firmy
    d) adresu e-mail
    e) numeru telefonu
    f) danych opcjonalnych
12. System musi umożliwiać konfigurację dla użytkowników gościnnych:
    a) wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)
    b) zezwolenia gościom na zmianę hasła
    c) samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora
13. System musi umożliwiać honorowanie ustawień local przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
14. System musi umożliwiać konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.
15. System musi umożliwiać konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługiwać co najmniej 6 urządzeń per konto gościnne.
16. System musi umożliwiać konfigurację czasu ważności hasła w dniach w przedziale zadanym przedziale w dniach.
17. System musi umożliwiać określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny
18. System musi umożliwiać konfigurację polityki złożoności haseł użytkowników gościnnych
19. System musi umożliwiać konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika
20. System musi umożliwiać tworzenie portalu gościnnego bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.
21. System musi umożliwiać przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.
22. System musi umożliwiać udostepnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS,
23. System musi wspierać API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

Profilowanie urządzeń

1. System musi umożliwiać dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
2. System musi umożliwiać wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności musi zapewniać stworzenie polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc.
3. System musi umożliwiać dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:
    a) DHCP
    b) http
    c) RADIUS
    d) DNS
    e) SNMP
    f) Network Scan (NMAP lub inne narzędzie profilowania aktywnego)
4. System musi umożliwiać wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.

5. System musi umożliwiać dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
6. System musi posiadać dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:
    a) Stacji roboczych pracujących z systemami Linux, Macintosh, Microsoft Windows,
    b) Urządzeń mobilnych: Android, Apple, Blackberry
    c) Drukarek sieciowych
    d) Routerów
7. System musi umożliwiać subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:
    a) reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci
    b) reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt
8. System musi umożliwiać włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie.
9. System musi wspierać raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.

Analiza stacji końcowej (Posture Assessment)

1. System umożliwia pobranie bazy wiedzy reguł analizy stacji końcowej (Posture) dla wspieranych systemów Antywirusowych (AV) i Antispyware (AS) ze strony producenta.
2. System umożliwia kontrolę zachowania dla stacji końcowych, które nie posiadają zainstalowanego agenta głębokiej analizy stacji końcowej (Posture).
3. System umożliwia regularne ponawianie głębokiej analizy stacji końcowej (periodic reassessment) w przedziale od 1 do 24 godzin.
4. System umożliwia przedstawienie użytkownikowi dokumentu Polityki Akceptowalnego Użycia (AUP). Polityka AUP jest prezentowana w postaci strony web po procesie głębokiej analizy stacji. Zawartość dokumentu AUP jest konfigurowalna.
5. System umożliwia głęboką analizę stacji końcowej Windows pod kątem plików (File Condition), w tym:
    a) istnienia pliku na stacji końcowej
    b) wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż)
    c) daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż)
6. System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10 pod kątem wpisów w rejestrze (Registry Condition), w tym:
    kluczy rejestru z kluczem root: HKCR, HKCU, HKLM, HKU, HKCC z zadanym podkluczem pod kątem:
    a) istnienia lub nieistnienia klucza
    b) wartości klucza rejestru
    c) istnienia i wartości domyślnej wartości klucza rejestru typu Number, String, Version
7. System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, pod kątem uruchomionych aplikacji (Application Condition), w tym:
    a) nazwy uruchomionego lub nieuruchomionego procesu
8. System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, pod kątem uruchomionych usług systemowych (Service Condition), w tym:
    a) nazwy uruchomionej lub nieuruchomionej procesu
9. System umożliwia tworzenie słownika prostych i złożonych warunków (Simple i Compound Condition) dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT, w tym z uwzględnieniem:
    a) parametrów dostępu do sieci, w tym:
    b) lokalizacji stacji końcowej
    c) nazwy użytkownika
    d) adresu IP stacji

e) metody uwierzytelnienia
f) statusu uwierzytelnienia
g) repozytorium użytkowników użytych dla uwierzytelnienia
h) atrybutów RADIUS, w tym:
   i. Calling-Station-ID
   ii. Framed-IP-Address
   iii. NAS-Identifier
i) NAS-IP-Address
j) NAS-Port-Type
k) Service-Type
l) User-Name
m) parametrów sesji w tym:
   i. typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment)
   ii. architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit)
   iii. adresu URL, z którego nastąpiło przekierowanie

10. System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, 10, Mac OS-X, pod kątem zainstalowanych aplikacji Antywirusowych (AV Compound Condition), w tym:
    a) stwierdzenia czy system AV jest obecny na stacji
    b) stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od:
       i. daty ostatniego pliku definicji
       ii. aktualnego czasu systemowego
11. System umożliwia głęboką analizę stacji końcowej z systemami Windows 7, 8, 8.1, Mac OS-X pod kątem zainstalowanych aplikacji AntiSpyware (AS Compound Condition), w tym:
    a) stwierdzenia czy system AS jest obecny na stacji
    b) stwierdzenia czy definicje sygnatur AS są nie starsze niż zadana ilość dni od:
       i. daty ostatniego pliku definicji
       ii. aktualnego czasu systemowego

Obsługa serwerów certyfikatów CA.

1. System musi posiadać funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.
2. Funkcja CA musi umożliwiać wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.
3. System musi wspierać hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów.
4. Funkcja CA musi zapewniać przynajmniej następujące funkcjonalności:
   a) Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS
   b) Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym
   c) Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji
   d) Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA

Raportowanie

System musi umożliwiać generowanie przynajmniej następujących raportów:

1. raportów dla protokołów AAA:
   a) diagnostyki protokołów AAA
   b) trendów uwierzytelnienia 802.1X
   c) accountingu RADIUS
   d) uwierzytelniania RADIUS

2. raportów dozwolonych protokołów
    a) sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:
        i. uwierzytelnień pomyślnych
        ii. uwierzytelnień nieudanych
        iii. „N" największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym: uwierzytelnień pomyślnych i nieudanych
3. raportów dla poszczególnych instancji serwerów systemu, w tym:
    a) uwierzytelnień RADIUS per serwer
    b) Top „N"uwierzytelnień per serwer
    c) monitorowania Online Certificate Status Protocol (OCSP)
    d) administratorów systemu i ich uprawnień
    e) logowania administratorów do systemu
    f) zmian konfiguracji serwera dokonanych przez administratorów
    g) stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
    h) zmian operacyjnych serwera dokonanych przez administratorów
    i) zmian haseł przez użytkowników
4. raportów dla stacji końcowych, w tym:
    a) uwierzytelnień typu MAC Authentication
    b) Top „N"uwierzytelnień per adres MAC stacji
    c) Top „N" uwierzytelnień per maszyna
    d) Top „N"uwierzytelnień per RADIUS Calling Station ID
    e) działań podsystemu profilera per adres MAC
    f) czasu wymaganego na sprofilowanie stacji per adres MAC
5. raportów dla błędów, w tym:
    a) błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
    b) sumarycznych przyczyn nieudanych uwierzytelnień
    c) Top „N" uwierzytelnień per rodzaj błędu
6. raportów dla urządzeń sieciowych:
    a) sumarycznych uwierzytelnień dla urządzeń sieciowych
    b) Top „N" uwierzytelnień per urządzenie sieciowe
    c) niedostępności serwera AAA dla urządzenia sieciowego
    d) wiadomości logowanych przez urządzenia sieciowe
    e) stanu portów i sesji urządzenia sieciowego widocznych przez SNMP
7. raportów użytkowników:
    a) sumarycznych uwierzytelnień użytkowników
    b) Top „N"uwierzytelnień per użytkownik
    c) sesji użytkowników gościnnych
    d) aktywności użytkowników gościnnych
    e) sumarycznych uwierzytelnień sponsorów dostępu gościnnego
    f) uwierzytelnień per unikalny użytkownik
8. raportów katalogu sesji
    a) aktywnych sesji RADIUS
    b) historii sesji RADIUS
    c) zaterminowanych sesji RADIUS

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
    a) wiadomości e-mail
    b) syslog
2. Alarmy muszą być generowane w następujących sytuacjach:
    a) ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
    b) opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego
    c) status krytycznych procesów będzie niepożądany, w tym status:
        i. procesu wewnętrznej bazy danych systemu

ii. serwera aplikacyjnego systemu
iii. bazy danych sesji
iv. kolektora i procesora wiadomości log
v. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)
vi. stan obciążenia systemu oraz zajętości pamięci wzrośnie powyżej zadanego poziomu

3. System musi posiadać zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
   a) badanie łączności IP za pomocą ping, nslookup, traceroute
   b) wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
      i. nazwy użytkownika
      ii. adresu MAC
      iii. statusu uwierzytelnienia (udana lub nieudana)
      iv. powodu, jeżeli uwierzytelnienie nieudane
      v. zakresu czasowego, co do dnia, godziny i minuty
   c) wykonanie zdalnego polecenia na urządzeniu sieciowym
   d) ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
      i. definicji serwerów AAA
      ii. protokołu RADIUS
      iii. odkrywania urządzeń
      iv. logowania
      v. uwierzytelniania Web
      vi. konfiguracji trybu 802.1X
   e) wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

Dopuszczalne sposoby realizacji rozwiązania

1. Zamawiający wymaga spełnienia następujących warunków realizacji systemu uwierzytelnienia dostępu do sieci
    a) Zamawiający dopuszcza stosowanie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów.
    b) W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców Zamawiający oczekuje, iż system będzie zapewniał pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia)
    c) W przypadku zastosowania rozwiązań złożonych z kilku komponentów różnych dostawców Zamawiający oczekuje iż system będzie serwisowany przez jednego producenta tzn. zgłoszenia serwisowe będą kierowane do jednego dostawcy. Zamawiający będzie traktował to rozwiązanie jako integralne części systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia).
    d) W przypadku zastosowania serwera CA jako dedykowanego rozwiązania Zamawiający będzie traktował to rozwiązanie jako integralną część systemu uwierzytelnienia (tzn. jako system tego samego producenta co system uwierzytelnienia)

Licencje

1. Wykonawca dostarczy min. 4500 licencji bazowych do systemu uwierzytelnienia i profilowania użytkowników.
2. System musi być w pełni kompatybilny z urządzeniami dostarczonymi przez Wykonawcę.

Moduły światłowodowe 62 szt.

10 szt. – SFP+ LR 10G (jednomodowe)
40 szt. – SFP+ SR 10G (wielomodowe)
12 szt. – SFP SX 1G (wielomodowe)

Wszystkie moduły światłowodowe muszą być fabrycznie nowe i pochodzić od producenta dostarczonego sprzętu.

Wsparcie, wdrożenie:

Zakres usługi wdrożenia:

a. Przygotowanie dokumentacji wdrożeniowej:
   i. Analiza obecnej konfiguracji sieci
   ii. Przygotowanie koncepcji podstawowej konfiguracji urządzeń oraz systemu zarządzania, kanałów VPN, mechanizmów QoS.
   iii. Optymalizacja konfiguracji pod nowe urządzenie
   iv. Ustalenie harmonogramu wymiany urządzeń w centrali oraz oddziałach
   v. Opracowanie dokumentacji
b. Wstępne przygotowanie urządzeń sieciowych:
   i. Podstawowa konfiguracja urządzenia centralnego oraz urządzeń oddziałowych
   ii. Weryfikacja poprawności konfiguracji urządzeń
   iii. Instalacja oraz konfiguracja systemu zarządzania infrastrukturą sieciową w środowisku wirtualnym
c. Instalacja urządzeń sieciowych w centrali oraz w oddziałach:
   i. Optymalizacja podstawowej konfiguracji urządzenia
   ii. Konfiguracja szyfrowanych połączeń VPN
   iii. Konfiguracja mechanizmów QoS
   iv. Integracja dostarczonych urządzeń z urządzeniami posiadanymi przez Zamawiającego.
   v. Włączenie dostarczonych oraz posiadanych przez Zamawiającego urządzeń do systemu zarządzania siecią. Lista sprzętu posiadanego przez Zamawiającego, koniecznego do włączenia do systemu zarzadzania:
      Cisco WS-C2960S-48FPD-L – 14 szt.
      Cisco WS-C2960S-24TS-L – 6 szt.
      Cisco WS-3850-48P-L – 1 szt.
      Cisco WS-3650-48FD-L – 3 szt.
      Cisco 3925-SEC/K9 – 1 szt.
      Cisco 2951/K9 – 1 szt.
      Cisco 3945/K9 – 1 szt.
      Cisco 2921/K9 – 2 szt.

   vi. Weryfikacja konfiguracji oraz sprawdzenie komunikacji pomiędzy centralą a oddziałami
d. Przygotowanie dokumentacji powdrożeniowej.
e. 3 – miesięczna opieka powdrożeniowa (nie dotyczy zgłoszeń podlegających pod kontrakty serwisowe świadczone przez producentów sprzętu):
   i. Kontakt e-mail/telefon w trybie 24x7 z dedykowanym inżynierem Wykonawcy
   ii. W przypadku problemów z rozwiązaniem usterki, przez 4h od zgłoszenia, przyjazd inżyniera na miejsce awarii.

Gwarancja, serwis, pochodzenie sprzętu:

1. oferowane urządzenie musi posiadać minimum 24 miesięczną gwarancję oraz wsparcie techniczne świadczone przez producenta sprzętu. Serwis gwarancyjny musi być oparty na świadczeniach gwarancyjnych producenta urządzeń. Czas reakcji serwisu dla urządzeń to następny dzień roboczy. Wsparcie powinno być realizowane w systemie 8 godzin / 5 dni roboczych z bezpośrednim dostęp do aktualizacji oprogramowania, wsparcia telefonicznego, poprzez stronę internetową producenta sprzętu – najpóźniej w dniu dostawy należy dostarczyć stosowne oświadczenie producenta sprzętu.

2. oferowane urządzenie sieciowe muszą być fabrycznie nowe, nie mogą posiadać założonych kontraktów serwisowych na inne podmioty, wyprodukowane zostały nie dawniej niż 9 miesięcy przed terminem dostarczenia,
3. oświadczenie producenta sprzętu, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy, przejmie on na siebie wszelkie zobowiązania związane z serwisem gwarancyjnym dostarczonego urządzenia – najpóźniej w dniu dostawy należy dostarczyć stosowne oświadczenie producenta sprzętu.
4. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający, że oprogramowanie zawarte w dostarczonym sprzęcie jest licencjonowane na Zamawiającego.
5. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający zarejestrowanie kontraktu serwisowego na dostarczone urządzenia i oprogramowanie. Serwis gwarancyjny musi obejmować prawo do aktualizacji wersji oprogramowania systemowego urządzeń. Wykonawca zapewni Zamawiającemu dostęp do:
   a) nowych wersji oprogramowania;
   b) narzędzi konfiguracyjnych i dokumentacji technicznej;
   c) pomocy technicznej producentów;
   d) prawo bezpośredniego zgłaszania przez Zamawiającego usterek i awarii sprzętu do Producenta
6. Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
7. Wykonawca na żądanie Zamawiającego będzie wykonywał w cyklu kwartalnym aktualizację oprogramowania systemowego (w ramach zakupionej przez Zamawiającego wersji funkcjonalnej) dostarczonych urządzeń, w godzinach wskazanych przez Zamawiającego, w siedzibie Zamawiającego. W przypadku dokonania uaktualnienia oprogramowania przez Wykonawcę, Wykonawca zobowiązany będzie w terminie 14 dni do dostarczenia aktualnej licencji potwierdzonej przez producenta serwisowanego sprzętu lub jego oficjalnego przedstawiciela wystawionej na Zamawiającego
8. Wszystkie wymagania przedstawione w niniejszym dokumencie muszą zostać spełnione w aktualnie dostępnych komercyjnie rozwiązaniach oprogramowania i sprzętu. Nie dopuszcza się możliwości, że wykonawca określi przyszłą wersję oprogramowania lub sprzętu, która będzie spełniać daną wyspecyfikowaną funkcjonalność.
9. Wymagane jest dostarczenie, wraz z dostawą urządzeń, szczegółowej specyfikacji, dokumentacji technicznej producenta oferowanych produktów potwierdzającej spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia (Zamawiający dopuszcza w tym przypadku możliwość złożenia dokumentacji w języku angielskim).
10. W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:
    zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację), oraz zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych.
11. Zamawiający wymaga, aby wszystkie dostarczone urządzenia pochodziły od jednego producenta.

Dodatkowe:

1. Dostarczane urządzenia muszą być w pełni kompatybilne z posiadanym przez Zamawiającego systemem zarządzania Cisco Prime Infrastructure, Zamawiający dopuszcza dostarczenie równoważnego systemu zarzadzania infrastrukturą sieciową zgodnego ze specyfikacją „system zarządzania infrastrukturą sieciową". Równoważny system zarzadzania musi być kompatybilny z urządzeniami posiadanymi przez Zamawiającego:
   Cisco ASR1001-X (1NG)
   Cisco WS-C2960S-48FPD-L
   Cisco WS-C2960S-24TS-L
   Cisco WS-C6509-E (M8572)
   Cisco WS-3850-48P-L
   Cisco WS-3650-48FD-L
   Cisco 3925-SEC/K9
   Cisco 2951/K9
   Cisco 3945/K9
   Cisco 2921/K9

2. Zamawiający wymaga aby wszystkie routery pracujące w WAN pochodziły od jednego producenta. Dostarczone routery muszą być w pełni kompatybilne z posiadanym przez Zamawiającego routerem centralnym Cisco ASR1001-X. Zamawiający dopuszcza wymianę routera centralnego na urządzenie równoważne, zgodne ze specyfikacją „router centralny".
3. Dostarczony system uwierzytelnienia i profilowania musi być kompatybilny z posiadanymi przez Zamawiającego przełącznikami sieciowymi:
   Cisco WS-C2960S-48FPD-L
   Cisco WS-C2960S-24TS-L
   Cisco WS-C6509-E (M8572)
   Cisco WS-3850-48P-L
   Cisco WS-3650-48FD-L
4. Wykonawca zapewni przeprowadzenie autoryzowanego szkolenia dla 2 osób w zakresie konfiguracji i eksploatacji dostarczonego systemu zarządzania infrastrukturą sieciową oraz systemu uwierzytelniania.
5. Wykonawca zapewni przeprowadzenie autoryzowanego szkolenia dla 2 osób w zakresie podstaw konfiguracji i administracji dostarczonych urządzeń.

Załącznik nr 4 do SIWZ

WZÓR UMOWY

W dniu …….2017 r. w Warszawie, pomiędzy:

INSTYTUTEM PAMIĘCI NARODOWEJ – Komisją Ścigania Zbrodni przeciwko Narodowi Polskiemu z siedzibą w Warszawie, przy ul. Wołoskiej 7, zwanym dalej „Zamawiającym", reprezentowanym przez:

……..,

a

……

zwanym w dalszej części Umowy **„Wykonawcą"**,

reprezentowanym przez:

……..……

§ 1
PODSTAWA ZAWARCIA UMOWY

Niniejsza Umowa zawarta jest w wyniku postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na zasadach określonych w ustawie z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (Dz. U. z 2015 r., poz. 2164 z późn. zm.).

§ 2
PRZEDMIOT UMOWY

1. Przedmiotem umowy jest:
   1) dostawa routerów oraz przełączników fabrycznie nowych, nienoszących śladów użytkowania o cechach, funkcjonalności i parametrach technicznych opisanych w *Opisie przedmiotu zamówienia* stanowiącym załącznik nr 2 oraz kopii *Formularza ofertowego* Wykonawcy stanowiącego załącznik nr 1 do niniejszej umowy wraz z wykonaniem wszelkich czynności, opisanych w załączniku nr 1 i załączniku nr 2, koniecznych do prawidłowej realizacji przedmiotu umowy,
   2) wdrożenie routerów oraz przełączników, podłączenie ich do centralnego systemu zarządzania infrastrukturą sieciową w lokalizacjach wymienionych w załączniku nr 4 w wierszach 1-5, urządzenia do pozostałych lokalizacji zostaną dostarczone do centrali IPN (lokalizacja w załączniku nr 4 wiersz 1) i tam skonfigurowane,
   3) dostawa i wdrożenie systemu uwierzytelnienia dostępu do sieci LAN wraz z licencjami.

§ 3
TERMIN REALIZACJI

1. Termin realizacji umowy – nie później niż do …. dni kalendarzowych od dnia podpisania umowy.
2. Za dzień realizacji umowy uznany będzie dzień podpisania przez Wykonawcę oraz wyznaczonego

pracownika Zamawiającego protokołu odbioru, którego wzór stanowi załącznik nr 3 do umowy, stwierdzającego należyte wykonanie całości przedmiotu zamówienia.

3. Zamawiający w terminie 14 dni roboczych od zgłoszenia gotowości do odbioru wykona wspólnie z Wykonawcą testy przedodbiorowe, potwierdzające prawidłowe wykonanie Zamówienia. W przypadku wykrycia przez Zamawiającego wad uniemożliwiających odbiór przedmiotu umowy, przekazuje on informację o nich Wykonawcy wyznaczając termin ich usunięcia. W przypadku trzykrotnej odmowy dokonania odbioru przedmiotu umowy przez Zamawiającego ze względu na wady dostarczonych urządzeń lub wykonanych usług Zamawiający ma prawo odstąpić od umowy.
4. Za dzień realizacji umowy uznany będzie dzień, w którym:
   1) Wykonawca dokonał wdrożenia routerów oraz przełączników w lokalizacjach w Warszawie wskazanych w załączniku nr 4 w wierszach 1-5,
   2) Wykonawca zakończył dostawę i konfigurację pozostałych urządzeń w Centrali IPN, ul. Wołoska 7 w Warszawie,
   3) Dostarczone urządzenia pomyślnie przeszły testy przedodbiorowe,

§ 4
WYNAGRODZENIE WYKONAWCY

1. Wynagrodzenie podane w ofercie jest stałe, nie podlega waloryzacji i będzie obowiązywać dla wszelkich rozliczeń w trakcie całego okresu trwania Umowy.
2. Łączne maksymalne wynagrodzenie z tytułu wykonania niniejszej Umowy wynosi ……..zł brutto (słownie:……..), w tym należny podatek VAT.
3. Wynagrodzenie określone w ust. 2 obejmuje wszelkie koszty jakie poniesie Wykonawca w związku z należytym, zgodnym z obowiązującymi przepisami, wykonaniem przedmiotu Umowy.

§ 5
WARUNKI DOSTAWY

1. Ze strony Zamawiającego osobą uprawnioną do kontaktów z Wykonawcą w sprawach dotyczących realizacji przedmiotu umowy jest Dyrektor Biura Informatyki lub osoba przez niego wskazana.
2. Ze strony Wykonawcy osobą uprawnioną do kontaktów z Zamawiającym w sprawach dotyczących realizacji przedmiotu umowy jest ……. tel. ……..……., tel. kom. …….
3. Wykonawca zobowiązuje się uzgodnić z osobą wymienioną w ust. 1 termin dostawy z wyprzedzeniem co najmniej 3-dniowym.
4. Zamawiający, bez jakichkolwiek roszczeń finansowych ze strony Wykonawcy z tym związanych, może odmówić Wykonawcy przystąpienia do wykonywania jego obowiązków, jeżeli:
   1) ich termin nie był z nim uprzednio uzgodniony,
   2) pracownicy Wykonawcy odmówią rozładunku przedmiotu dostawy w miejscu wskazanym przez Zamawiającego.
5. Prowadzone prace wdrożeniowe i instalacyjne nie mogą zakłócać prawidłowej pracy istniejącej infrastruktury sieciowej. Wszystkie konieczne przerwy w pracy systemu informatycznego muszą być zgłoszone Zamawiającemu najpóźniej na 24 godziny przed planowaną przerwą i powinny mieć miejsce poza godzinami pracy (tj. poza 8:15 -16:15 w dni robocze).
6. Wszelkie dokumenty dotyczące dostaw przygotowuje Wykonawca. Do faktury Wykonawca dołącza oryginał potwierdzonego protokołu odbioru.

§ 6
GWARANCJA

1. Wykonawca zobowiązuje się dostarczyć urządzenia wyłącznie fabrycznie nowe i wolne od wad.
2. Wykonawca udziela gwarancji i rękojmi na dostarczone urządzenia na okres **……. miesięcy** od daty podpisania protokołu odbioru.
3. Wykonawca udziela na dostarczone urządzenia gwarancji na warunkach określonych w niniejszej umowie i określonych przez producenta, obowiązującej przez okres, o którym mowa w ust. 2.
4. Wykonawca jest obowiązany do usunięcia ujawnionych wad fizycznych w dostarczonych urządzeniach, o ile wady te ujawnią się w ciągu okresu gwarancyjnego, o którym mowa w ust. 2.
5. Wymagany czas usunięcia awarii wynosi 48 godzin. Wykonawca zobowiązany jest usuwać awarię 7 dni w tygodniu przez 24 godziny na dobę.
6. Wykonawca zapewni w okresie wskazanym w ust. 2 bezpłatny serwis naprawczy i konserwację sprzętu w miejscu zainstalowania zgodnie z załącznikiem nr 4.
7. W okresie gwarancji, wymienionym w ust. 2 Wykonawca może obciążyć Zamawiającego kosztami serwisu tylko wówczas, gdy uszkodzenie urządzenia nastąpiło z winy Zamawiającego.
8. Wszelkie uwagi i ewentualne reklamacje Zamawiający przekaże bezpośrednio do Wykonawcy na adres: **…….**
9. Powiadomienie o ewentualnej awarii nastąpi telefonicznie na nr…… lub mailowo na adres ……. Wykonawca dokona nieodpłatnie naprawy gwarancyjnej lub wymieni wadliwy sprzęt na nowy. W przypadku awarii sprzętu Wykonawca zapewni do czasu naprawy sprzęt zastępczy o parametrach nie gorszych niż sprzęt który uległ awarii.
10. Wykonawca zobowiązuje się do rozpoczęcia usuwania awarii nie później niż następnego dnia roboczego od momentu otrzymania zgłoszenia.
11. W szczególnych przypadkach strony mogą uzgodnić inny czas usunięcia usterki, przy czym wymagane jest potwierdzenie na piśmie.
12. Nośniki danych nie mogą opuścić siedziby Zamawiającego. W przypadku stwierdzenia awarii dysku twardego, uszkodzony dysk pozostaje własnością Zamawiającego, Wykonawca zobowiązany jest nieodpłatnie dostarczyć nowy dysk w ramach umowy gwarancyjnej.

§ 7
WARUNKI PŁATNOŚCI

1. Płatność wynagrodzenia określonego w § 4 ust. 2 odbędzie się na podstawie faktury, którą Wykonawca wystawi po dokonaniu protokolarnie potwierdzonego odbioru przedmiotu umowy na konto Wykonawcy wskazane w fakturze.
2. Faktura będzie wystawiana na: Instytut Pamięci Narodowej – Komisja Ścigania Zbrodni przeciwko Narodowi Polskiemu, ul. Wołoska 7, 02-675 Warszawa, NIP 525-21-80-487.
3. Wykonawca zobowiązuje się, że do faktury dołączony będzie oryginał podpisanego przez obie strony protokołu odbioru.
4. Faktura, do której nie będzie dołączony odpowiedni i kompletnie wypełniony oraz podpisany przez obie strony protokół odbioru nie zostanie przez Zamawiającego zaakceptowana i będzie odesłana Wykonawcy do uzupełnienia. W takim przypadku brak zapłaty wynagrodzenia przez Zamawiającego nie będzie stanowić podstawy do naliczania odsetek ustawowych ani nie będzie traktowany jako pozostawanie w zwłoce.
5. Płatność wynagrodzenia nastąpi przelewem w ciągu 14 dni od daty otrzymania przez Zamawiającego faktury zgodnej z postanowieniami ust. 4, przy czym za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.

§ 8
ZABEZPIECZNIE NALEŻYTEGO WYKONANIA UMOWY

1. Strony ustalają zabezpieczenie należytego wykonania umowy w wysokości 10% wynagrodzenia określonego w § 4 ust. 2 co stanowi kwotę …….
2. Zabezpieczenie służy pokryciu roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania umowy przez Wykonawcę. W szczególności z zabezpieczenia Zamawiający ma prawo pokryć kary umowne.
3. Zabezpieczenie o którym mowa w ust. 1, podlega zwolnieniu przez Zamawiającego w wysokości 70% sumy zabezpieczenia w terminie 30 dniu od dnia dokonania odbioru, a 30% tej sumy nie później niż w 15 dniu po upływie okresu rękojmi za wady.

§ 9
KARY UMOWNE

1. Strony ustalają odpowiedzialność za niewykonanie lub nienależyte wykonanie umowy w formie kar umownych w następujących wypadkach i wysokości:
   1) Wykonawca zobowiązany jest do zapłaty kary umownej w wysokości 0,2% wynagrodzenia umownego brutto określonego w § 4 ust. 2 umowy, za każdy dzień opóźnienia w realizacji zamówienia o którym mowa w § 3 ust. 1,
   2) Wykonawca zobowiązany jest do zapłaty kary umownej w wysokości 10% wynagrodzenia umownego brutto określonego w § 4 ust. 2 umowy z tytułu odstąpienia lub wypowiedzenia umowy przez Zamawiającego lub Wykonawcę z przyczyn, za które ponosi odpowiedzialność Wykonawca.
   3) Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,1% wynagrodzenia umownego brutto określonego w § 4 ust. 2 umowy, za każdy dzień opóźnienia w przypadku, o którym mowa w § 6 ust. 5 zdanie 1.
2. Zamawiający ma prawo potrącenia wartości naliczonych Wykonawcy kar umownych z należnego Wykonawcy wynagrodzenia bez potrzeby uzyskania akceptacji Wykonawcy.
3. W sytuacji, gdy kary umowne, przewidziane w ust. 1, nie pokrywają rozmiarów szkody, Zamawiającemu przysługuje prawo żądania odszkodowania na zasadach ogólnych.

§ 10

WARUNKI WYPOWIEDZENIA LUB ODSTĄPIENIA OD UMOWY

1. Zamawiającemu przysługuje prawo do odstąpienia od Umowy w terminie 30 dni w przypadku:
   1) wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy;
   2) likwidacji, rozwiązania przedsiębiorstwa Wykonawcy, nakazanego przez organ publiczny zajęcia majątku Wykonawcy;
   3) o którym mowa w § 3 ust. 3 tj. trzykrotnej odmowy dokonania odbioru przedmiotu umowy przez Zamawiającego ze względu na wady dostarczonych urządzeń lub wykonanych usług,
   4) w przypadku niezrealizowania umowy w terminie określonym w § 3 ust. 1.
2. Zamawiającemu przysługuje prawo do natychmiastowego wypowiedzenia Umowy w przypadku:
   1) nieuzasadnionego przerwania przez Wykonawcę wykonywania przedmiotu Umowy i bezskutecznym upływie terminu wyznaczonego przez Zamawiającego na wznowienie jego wykonania;
   2) wykonywania przez Wykonawcę przedmiotu umowy wadliwie lub w sposób sprzeczny z Umową, po bezskutecznym upływie terminu wyznaczonego przez Zamawiającego na dokonanie przez Wykonawcę zmiany sposobu wykonywania przedmiotu umowy;
   3) trzykrotnego zgłoszenia do odbioru przez Wykonawcę systemu i stwierdzenia niezgodności dostarczonego systemu z opisem przedmiotu zamówienia.

3. Wypowiedzenie lub odstąpienie od Umowy powinno nastąpić pod rygorem nieważności na piśmie i zawierać uzasadnienie.
4. W przypadku wypowiedzenia Umowy w terminie 14 dni od daty jej wypowiedzenia, o ile będzie to możliwe w danych okolicznościach przy udziale drugiej strony, zostanie sporządzony protokół inwentaryzacji wykonanych usług i dostaw, zgodnie ze stanem faktycznym na dzień wypowiedzenia Umowy.

§ 12

ZMIANY UMOWY

Zamawiający dopuszcza dokonywanie zmian zawartej umowy na zasadach określonych w art. 144 ustawy Pzp, a ponadto w następujących okolicznościach:

1) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili zawarcia umowy, niepowodujących zmiany przedmiotu zamówienia,
2) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań w zakresie modelu/typu sprzętu/oprogramowania w przypadku zakończenia produkcji lub braku dostępności na rynku pod warunkiem że sprzęt /oprogramowanie będzie posiadał parametry nie gorsze od oferowanego modelu/ typu sprzętu/ oprogramowania i nie spowoduje podwyższenia ceny.

§ 13

KLAUZULA POUFNOŚCI

1. Wykonawca zobowiązuje się do nieujawniania informacji związanych z działalnością Zamawiającego oraz zachowania w tajemnicy wszelkich informacji i danych pozyskanych w trakcie realizacji niniejszej umowy, niezależnie od formy ich przekazania oraz źródła pochodzenia. Obowiązek zachowania tajemnicy ma zastosowanie zarówno w trakcie trwania umowy, jak i po jej zakończeniu.
2. Wykonawca zobowiązuje się do wykorzystywania informacji, o których mowa w ust. 1, wyłącznie w celach określonych przedmiotem niniejszej umowy.
3. Przepisy § 13 mają zastosowanie do Wykonawcy oraz osób przez Niego zatrudnionych.

§ 14
POSTANOWIENIA KOŃCOWE

1. W sprawach nie uregulowanych niniejszą Umową zastosowanie mają odpowiednie przepisy prawa polskiego, w szczególności ustawy Prawa zamówień publicznych w brzmieniu obowiązującym w dacie wszczęcie postepowania o udzielenie zamówienia publicznego i Kodeksu Cywilnego.
2. W przypadku uznania któregokolwiek z postanowień niniejszej Umowy za nieważne, niezgodne z prawem lub nie mające mocy wiążącej w jakimkolwiek zakresie, takie postanowienia uważa się za wyodrębnione od pozostałych postanowień Umowy, które pozostają w mocy w możliwie najszerszym zakresie dopuszczalnym przez prawo. W takim przypadku strony podejmą niezwłocznie wszelkie działania aby cel wynikający z tych postanowień został osiągnięty.
3. Strony dołożą starań, aby wszelkie spory pomiędzy nimi powstałe w związku z realizacją niniejszej Umowy były rozstrzygane polubownie. Gdyby jednak starania te nie przyniosły rozstrzygnięcia w ciągu trzydziestu (30) dni od dnia ich rozpoczęcia - Strony poddadzą spór rozstrzygnięciu właściwego miejscowo dla siedziby Zamawiającego sądu powszechnego.
4. Przeniesienie przez Wykonawcę jakichkolwiek praw związanych z wykonaniem Umowy bez pisemnej uprzedniej zgody Zamawiającego na osobę trzecią jest nieważne.
5. Wykonawca zobowiązany jest do informowania Zamawiającego niezwłocznie o wszystkich zdarzeniach mających lub mogących mieć wpływ na wykonanie Umowy, w szczególności

o wszczęciu wobec niego postępowania egzekucyjnego, naprawczego, likwidacyjnego lub innych istotnych zdarzeniach, w szczególności o złożeniu wniosku o ogłoszenie jego upadłości.

6. Wykonawca może dokonać przelewu wierzytelności powstałych w wyniku wykonania Umowy, tylko za zgodą Zamawiającego wyrażoną na piśmie pod rygorem nieważności.
7. Zamawiający, o ile będzie to możliwe w danej lokalizacji, zapewni pracownikom Wykonawcy wykonującym zadania w lokalizacjach Zamawiającego warunki pracy zgodne z przepisami BHP i o ochronie przeciwpożarowej.
8. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

Załączniki:

- *Załącznik nr 1 –Kopia oferty Wykonawcy;*
- *Załącznik nr 2 – Opis przedmiotu zamówienia*
- *Załącznik nr 3 – Wzór protokołu odbioru.*
- *Załącznik nr 4 – Lista Oddziałów IPN.*

ZAMAWIAJĄCY: **WYKONAWCA:**

Załącznik nr 3 do umowy

Warszawa , dnia ……..

PROTOKÓŁ ODBIORU (wzór)

W dniu dzisiejszym dostarczono do Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu niżej wymieniony przedmiot zamówienia:

Pozycja	Nazwa dostarczonego przedmiotu zamówienia	Ilość

Zamawiający dokonał odbioru przedmiotu zamówienia wymienionego w protokole.

UWAGI……
……
……
……

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 4 do umowy

Lista Oddziałów IPN

L.p.	Lokalizacja
1	Centrala IPN Warszawa, ul. Wołoska 7, 00-675 Warszawa
2	Archiwum IPN Warszawa, ul. Kłobucka 21, 02-699 Warszawa
3	Oddział Warszawa, ul. Pl. Krasińskich 2/4/6, 00-207 Warszawa
4	BL, ul. Żurawia 4A, 00-503 Warszawa
5	Centrala IPN Warszawa ul. Marszałkowska 21/23, 00-626
6	Oddział Warszawa, ul. Stawki 2, 00-193 Warszawa
7	Oddział Białystok, ul. Warsztatowa 1a, 15-637 Białystok
8	Delegatura Olsztyn, ul. Jagiellońska 46, 10-273 Olsztyn
9	Oddział Gdańsk, Al. Grunwaldzka 214-216, 80-266 Gdańsk
10	Delegatura Bydgoszcz, ul. Grudziądzka 9-15, 85-130 Bydgoszcz
11	Oddział Katowice, ul. Józefowska 102, 40-145 Katowice
12	Oddział Kraków, ul. Reformacka 3, 31-012 Kraków
13	Oddział Kraków, ul. Skulimowskiego 1, Wieliczka
14	Oddział Kraków ul. Dunajewskiego 3, 31-133 Kraków
15	Delegatura Kielce, Al. Na Stadion 1, 25-127 Kielce
16	Oddział Lublin, ul. Szewska 2, 20-086 Lublin
17	Delegatura Radom, ul. Żeromskiego 53, 26-600 Radom
18	Oddział Łódź, ul. Orzeszkowej 31/35, 91-479 Łódź
19	Oddział Łódź ul. Piotrkowska 149, 90-440 Łódź
20	Oddział Poznań, ul. Rolna 45a, 61-487 Poznań
21	Oddział Rzeszów, ul. Słowackiego 18, 35-060 Rzeszów
22	Oddział Rzeszów, ul. Chopina 23, 35-055 Rzeszów

L.p.	Lokalizacja
23	Oddział Szczecin, ul. K. Janickiego 30, 71-270 Szczecin
24	Oddział Szczecin al. Wojska Polskiego 9, 70-470 Szczecin
25	Oddział Wrocław, ul. Sołtysowicka 21a, 51-168 Wrocław
26	Oddział Wrocław, ul. Paprotna 14, 51-117 Wrocław
27	Delegatura Opole ul. Piastowska 17, 45-081 Opole