**Załącznik nr 1 do SIWZ**

**Szczegółowy Opis Przedmiotu Zamówienia (OPZ)**

Świadczenie usług

transmisji danych w Sieci WAN

oraz dostępu do Internetu

**SPIS TREŚCI**

1. Cel zamówienia publicznego 5

2. Słownik użytych pojęć 6

3. Roboty budowlane 8

3.1. Informacje wstępne 8

3.2. Właściwości stosowanych wyrobów budowlanych 9

3.3. Kontrola robót budowlanych 9

3.4. Informacje dotyczące Lokalizacji 10

3.5. Zabezpieczenie i powykonawcze porządkowanie pomieszczeń 10

3.6. Adresy Lokalizacji 11

4. Specyfikacja parametrów technicznych łączy telekomunikacyjnych przeznaczonych dla transmisji danych w Sieci WAN 13

4.1. Struktura fizyczna łączy telekomunikacyjnych 13

4.2. Parametry Łączy IP VPN MPLS 14

4.3. Wymagania dotyczące Routerów CE 16

4.4. Wymagania dotyczące Routerów CPE 16

4.5. Wymagania dotyczące Routerów PE 17

4.6. Wymagania dotyczące Węzłów Dostępowych 17

5. Specyfikacja Funkcjonalności usługi transmisji danych w Sieci WAN 18

5.1. Informacje podstawowe 18

5.2. Podział logiczny 18

5.3. Routing statyczny i dynamiczny 18

5.4. Szyfrowanie transmisji danych 18

5.5. QoS 19

5.6. Przełączanie transmisji danych pomiędzy głównym, a zapasowym Łączem IP VPN MPLS 19

5.7. Eliminacja pojedynczego punktu awarii Routera CE obsługującego Sieć WAN w siedzibie Zamawiającego w Warszawie 20

5.8. Transmisja danych w technologii IP Multicast 20

5.9. Zabezpieczenie Routerów CE 20

5.10. Kopie zapasowe konfiguracji Routerów CE 20

6. Specyfikacja parametrów łączy telekomunikacyjnych przeznaczonych dla usługi dostępu do Internetu 21

6.1. Struktura fizyczna łączy telekomunikacyjnych 21

6.2. Parametry łączy telekomunikacyjnych 22

6.3. Wymagania dotyczące Routerów CE 23

6.4. Wymagania dotyczące Routerów CPE 23

7. Specyfikacja Funkcjonalności usługi dostępu do Internetu 24

7.1. Informacje podstawowe 24

7.2. Eliminacja pojedynczego punktu awarii Routera CE obsługującego usługę dostępu do Internetu w siedzibie Zamawiającego w Warszawie 24

7.3. Adresacja IP i kierowanie ruchu w siedzibie Zamawiającego w Warszawie 24

7.4. Serwery nazw 24

7.5. AntyDDoS 25

8. Specyfikacja parametrów technicznych Routerów CE 28

8.1. Informacje podstawowe 28

8.2. Specyfikacja istniejących u Zamawiającego Routerów CE 28

8.3. Dostawa nowych Routerów CE 31

9. Usługa Serwisu Producenta 33

9.1. Informacje ogólne 33

9.2. Zakres usługi Serwisu Producenta 33

10. Topologia Sieci WAN, dostępu do Internetu 34

11. System monitoringu 35

11.1. Informacje wstępne 35

11.2. Wykrywanie zdarzeń i automatyczne informowanie o zdarzeniach 35

11.3. Korelacja zdarzeń 36

11.4. Kolekcjonowanie danych historycznych 36

11.5. Kopie zapasowe konfiguracji Routerów CE 37

11.6. Parametry fizyczne serwera systemu monitoringu 37

12. Testy akceptacyjne 38

12.1. Informacje wstępne 38

12.2. Pierwsza część testów akceptacyjnych 39

12.3. Druga część testów akceptacyjnych 40

13. Usługi instalacyjno-konfiguracyjne 42

13.1. Uruchomienie głównych i zapasowych Łączy IP VPN MPLS 42

13.2. Instalacja Routerów CPE 42

13.3. Uruchomienie głównych i zapasowych łączy dla dostępu do Internetu 42

13.4. Konfiguracja Routerów CE 42

13.5. Uruchomienie usługi transmisji danych w Sieci WAN 42

13.6. Uruchomienie usługi dostępu do Internetu 42

13.7. Uruchomienie systemu monitoringu 42

13.8. Uruchomienie transmisji IP Multicast 43

14. Instruktaż powdrożeniowy 45

14.1. Informacje ogólne 45

14.2. Zakres instruktażu 45

15. Instruktaż techniczny 47

15.1. Informacje ogólne 47

15.2. Zakres i podział tematyczny instruktażu przewidzianego dla Routerów CE firmy CISCO 48

15.3. Zakres i podział tematyczny instruktażu przewidzianego dla Routerów CE innej firmy niż CISCO 54

16. Dokumentacja powykonawcza 62

16.1. Informacje wstępne 62

16.2. Dokumentacja robót budowlanych 62

16.3. Pozostała dokumentacja 62

17. Współpraca Stron Umowy 64

17.1. Plan komunikacji Wykonawcy z Zamawiającym 64

17.2. Zasady współpracy 64

17.3. Sposób realizacji zdalnego dostępu spoza siedziby Zamawiającego 64

17.4. Lista upoważnionych w Lokalizacjach pracowników Zamawiającego 65

17.5. Harmonogram wykonywania prac 65

17.6. Zasady postępowania Wykonawcy na placu budowy 67

17.7. Odbiory prac 69

17.8. Protokoły odbioru oraz protokół odbioru końcowego 70

17.9. Serwis Wykonawcy 71

17.10. Gwarancja i rękojmia Wykonawcy 72

17.11. Serwis pogwarancyjny Routerów CE świadczony przez Wykonawcę 74

17.12. Klasyfikacja Awarii 75

17.13. Zmiana klasyfikacji Awarii 77

17.14. Bieg czasu trwania Awarii 77

17.15. Zawieszenie biegu czasu trwania Awarii 78

17.16. Rejestracja Awarii i potwierdzanie zdarzeń dla Awarii 78

17.17. Zasady usuwania Awarii 79

17.18. Czasy graniczne na usunięcie Awarii 80

17.19. SLA 81

18. Załącznik 84

19. Wzory protokołów 85

# Cel zamówienia publicznego

Przedmiotem postępowania jest zapewnienie usług transmisji danych pomiędzy Lokalizacjami Zamawiającego w oparciu o technologię IP VPN MPLS, przy wykorzystaniu wydzielonej infrastruktury telekomunikacyjnej Wykonawcy, a także zapewnienie usługi dostępu do Internetu.

W ramach postępowania przewidziano także dostawę nowych routerów brzegowych Zamawiającego niezbędnych do zestawienia szyfrowanych połączeń między Lokalizacjami, routera brzegowego niezbędnego do obsługi dostępu do Internetu, przeprowadzenie instruktażu technicznego niezbędnego do zapoznania się z obsługą Routerów CE, zapewnienie przez Wykonawcę serwisu w ramach zasobów własnych, a także zapewnienie wsparcia producenta na nowe i istniejące routery brzegowe (Routery CE).

# Słownik użytych pojęć

| Pojęcie | Opis pojęcia |
| --- | --- |
| **Awaria** | jakiekolwiek zdarzenie uniemożliwiające korzystanie przez Zamawiającego z którejkolwiek z Funkcjonalności Routerów CE lub innych urządzeń, w szczególności systemu monitoringu, w zakresie obsługi Sieci WAN Zamawiającego oraz Internetu, a także jakiekolwiek zdarzenie uniemożliwiające bądź ograniczające korzystanie z usług transmisji danych w Sieci WAN lub usługi dostępu do Internetu, lub ograniczające Funkcjonalność tych usług |
| **Dni Robocze** | dni od poniedziałku do piątku, z wyłączeniem przypadających w dni wolne od pracy określone w art. 1 ust. 1 Ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz. U. z 2015 r., poz.90) |
| **Funkcjonalność** | zespół parametrów: Routerów CE, transmisji danych w Sieci WAN oraz dostępu do Internetu widocznych od strony Routerów CE, np.: automatyczne przełączanie transmisji danych pomiędzy głównym, a zapasowym Łączem IP VPN MPLS, określonej jakości komunikacja ze stronami dostępnymi w Internecie i nie znajdującymi się w infrastrukturze Wykonawcy |
| **Internet** | ogólnoświatowa sieć komputerowa. W sensie logicznym, Internet to przestrzeń adresowa zrealizowana przy wykorzystaniu protokołu komunikacyjnego IP, działająca w oparciu o specjalistyczny sprzęt sieciowy oraz istniejącą światową infrastrukturę telekomunikacyjną |
| **IMIX** | ciąg ramek Ethernet, dla których udział ramek poszczególnej długości, w całkowitej liczbie ramek przesyłanych, odpowiada charakterystyce IMIX (ang. Internet MIX według IETF RFC 6985 „IMIX Genome: Specification of Variable Packet Sizes for Additional Testing”) |
| **Jitter** | zmienność opóźnienia pakietów przychodzących z lub wychodzących do określonej Lokalizacji |
| **Jednostka Terenowa** | oznacza każdą siedzibę Zamawiającego z wyłączeniem siedziby w Warszawie |
| **Lokalizacja** | oznacza każdą siedzibę Zamawiającego |
| **IP VPN MPLS** | technologia transmisji danych w wewnętrznej sieci telekomunikacyjnej Wykonawcy gwarantująca logiczną separację ruchu danych od innych klientów Wykonawcy na poziomie warstwy 3 modelu ISO/OSI, umożliwiająca rezerwację pasma dla określonego ruchu, gwarantująca rozróżnienie wymagań QoS i implementowanie VPN |
| **IP Multicast** | technologia optymalizacji przesyłania danych polegająca na redukcji ruchu IP w Sieci WAN poprzez przesyłanie jednego strumienia danych równocześnie do wielu odbiorców |
| **Łącze IP VPN MPLS** | główne lub zapasowe łącze zrealizowane w technologii IP VPN MPLS przeznaczone dla świadczenia usług transmisji danych w Sieci WAN |
| **Miesiąc Rozliczeniowy** | oznacza okres rozliczeniowy za świadczone w ramach Umowy określone usługi transmisji danych i dostępu do Internetu, przy czym jest to okres od pierwszego do ostatniego dnia danego miesiąca |
| **Miesięczna Dostępność** | oznacza dostępność rozliczaną w cyklu miesięcznym począwszy od pierwszego do ostatniego dnia danego miesiąca, z zastrzeżeniem, że przerwa w świadczeniu usług transmisji danych w Sieci WAN z wykorzystaniem głównych lub zapasowych Łączy IP VPN MPLS i przerwa w świadczeniu usługi dostępu do Internetu poprzez główne lub zapasowe łącze dla usługi dostępu do Internetu, która rozpoczęła się w jednym Miesiącu Rozliczeniowym, a zakończyła w kolejnym rozliczana jest w całości w tym Miesiącu Rozliczeniowym, w którym się zakończyła |
| **Roczna Dostępność** | oznacza dostępność rozliczaną w cyklu rocznym począwszy od pierwszego do ostatniego dnia danego roku kalendarzowego, z zastrzeżeniem, że przerwa w świadczeniu usług transmisji danych w Sieci WAN z wykorzystaniem głównych lub zapasowych Łączy IP VPN MPLS i przerwa w świadczeniu usługi dostępu do Internetu poprzez główne lub zapasowe łącze dla usługi dostępu do Internetu, która rozpoczęła się w jednym roku kalendarzowym, a zakończyła w kolejnym rozliczana jest w całości w tym roku kalendarzowym i Miesiącu Rozliczeniowym, w którym się zakończyła |
| **Router PE** | brzegowy router Wykonawcy znajdujący się w infrastrukturze telekomunikacyjnej sieci IP VPN MPLS Wykonawcy (zgodnie z wymaganiami RFC 2547), zarządzany przez niego i będący jego własnością. Zadaniem routera jest terminowanie łącza dostępowego, tj. głównego lub zapasowego Łącza IP VPN MPLS, wychodzącego z węzła Wykonawcy do Lokalizacji Zamawiającego |
| **Router CPE** | brzegowy router Wykonawcy znajdujący się w Lokalizacji Zamawiającego, zarządzany przez niego i będący jego własnością. Zadaniem routera jest terminowanie łącza dostępowego, tj. głównego lub zapasowego Łącza IP VPN MPLS, przychodzącego z węzła Wykonawcy oraz kierowanie zaszyfrowanych danych do określonych klas QoS sieci IP VPN MPLS Wykonawcy na podstawie widocznego pola DSCP oznaczonego przez Router CE. Router CPE musi posiadać co najmniej interfejs Gigabit Ethernet 10/100/1000 służący do podłączenia do infrastruktury Zamawiającego (do Routerów CE) w Jednostkach Terenowych, a w siedzibie Zamawiającego w Warszawie interfejs Ethernet 100/1000/10000 |
| **Router CE** | brzegowy router Zamawiającego, zarządzany przez niego i będący jego własnością, który służy do podłączenia Routerów CPE Wykonawcy (dla Sieci WAN) oraz usługi dostępu do Internetu poprzez interfejs przyłączeniowy typu Ethernet |
| **RTD** | czas wymagany do przesłania danych w obu kierunkach, na przykład w Sieci WAN od Routera CE w siedzibie Zamawiającego w Warszawie do Routera CE w danej Jednostce Terenowej, a następnie od Routera CE w tej Jednostce Terenowej do Routera CE w siedzibie Zamawiającego w Warszawie |
| **Serwerownia** | Serwerownia Zamawiającego znajdująca się w danej Lokalizacji, i w której muszą być zainstalowane Routery CPE |
| **SLA** | utrzymanie ustalonego między Zamawiającym, a Wykonawcą poziomu jakości i dostępności świadczonych usług |
| **Sieć WAN** | spójna, wewnętrzna sieć komputerowa Zamawiającego, bez żadnych ograniczeń w przesyłaniu danych, łączącą wszystkie Jednostki Terenowe z siedzibą Zamawiającego w Warszawie, przy czym komunikacja między dwoma Jednostkami Terenowymi z założenia odbywa się poprzez urządzenia brzegowe. Urządzeniami brzegowymi Sieci WAN są Routery CE |
| **Szczegółowy harmonogram prac** | ogólny harmonogram prac z ustalonymi przez Strony Umowy datami wykonania poszczególnych zadań |
| **Węzeł Dostępowy** | miejsce, w którym Wykonawca posiada w swojej infrastrukturze urządzenie sieciowe, do którego podłączone jest fizycznie dane łącze telekomunikacyjne przeznaczone dla transmisji danych w Sieci WAN i zapewniające redundantne połączenie w górę sieci Wykonawcy |

# Roboty budowlane

## Informacje wstępne

### Wykonawca jest zobowiązany wykonać wszystkie roboty budowlane niezbędne do wykonania Przedmiotu Zamówienia, tj. wszelkie prace budowlane, które w sposób oczywisty są potrzebne do tego, aby Przedmiot Zamówienia osiągnął wymagane cele, nawet jeżeli prace takie nie są wyraźnie wyszczególnione w niniejszym dokumencie, w Umowie i pozostałych załącznikach do niej. W razie wątpliwości za prace takie, a także możliwe dostawy uznać należy te, których wykonanie nierozerwalnie wiąże się z realizacją Przedmiotu Zamówienia i bez wykonania których Przedmiot Zamówienia nie może zostać prawidłowo zrealizowany.

### Planowane roboty budowlane i ich zakres przed wykonaniem muszą zostać uzgodnione z dyrekcją każdej Lokalizacji Zamawiającego pośrednio, przez upoważnionego w danej Lokalizacji pracownika Zamawiającego po wcześniejszym uzyskaniu opinii inspektorów nadzoru inwestorskiego w branżach budowlano-konstrukcyjnej i elektrycznej.

### Wszelkie dokumenty formalne, w szczególności zgłoszenia, opisy sytuacyjne, wnioski budowlane i inne w danej Lokalizacji, zobowiązany jest przygotować i uzyskać Wykonawca w imieniu Zamawiającego, a dyspozycje w tym zakresie muszą być załatwiane z dyrekcją każdej Lokalizacji Zamawiającego pośrednio, poprzez upoważnionego w danej Lokalizacji pracownika Zamawiającego po wcześniejszym uzyskaniu opinii inspektorów nadzoru inwestorskiego w branżach budowlano-konstrukcyjnej i elektrycznej.

### Wszystkie prace i roboty budowlane, a także instalacje, w szczególności trasy kablowe, prowadzone poza terenem Zamawiającego dla każdej Lokalizacji, nie mogą obciążać kosztami prawnymi i ekonomicznymi Zamawiającego.

### Wykonawca musi zapewnić pracowników robót budowlanych z odpowiednimi uprawnieniami budowlanymi, tj. konstrukcyjno-budowlanymi lub architektonicznymi do wykonywania robót związanych z elementami budowlano-konstrukcyjnymi, a także elektrycznymi do wykonywania robót w zakresie instalacji i urządzeń elektrycznych i elektroenergetycznych. Weryfikacja uprawnień zostanie przeprowadzona przez Zamawiającego na etapie prowadzenia postępowania przetargowego na podstawie dostarczonych kserokopii stosownych uprawnień dla osób przewidzianych do realizacji Przedmiotu Zamówienia. Osoby wskazane podczas postępowania przetargowego zostaną wpisane do Umowy jako osoby odpowiedzialne za realizację Przedmiotu Zamówienia.

### Wykonawca jest zobowiązany do zabezpieczania terenu Zamawiającego w miejscu wykonywania robót w okresie trwania realizacji Przedmiotu Zamówienia, sukcesywnie w trakcie wykonywania robót.

### Wykonawca jest zobowiązany do ponoszenia odpowiedzialności od następstw związanych z realizacją Przedmiotu Zamówienia w zakresie:

#### organizacji robót budowlanych;

#### zabezpieczenia interesów osób trzecich;

#### ochrony środowiska;

#### warunków bezpieczeństwa i higieny pracy;

#### zabezpieczenia terenu Zamawiającego w miejscu wykonywania robót przed dostępem osób trzecich;

#### ochrony mienia związanego z wykonywaniem Przedmiotu Zamówienia i jego zabezpieczeniem przed zniszczeniem;

#### ochrony urządzeń w udostępnianych pomieszczeniach, w szczególności ochrony urządzeń w Serwerowniach.

### Wykonawca jest zobowiązany do systematycznego wywozu materiałów nadmiarowych i ewentualnych odpadów powstałych w trakcie realizacji Przedmiotu Zamówienia, zgodnie z obowiązującymi przepisami prawa. Strony Umowy ustalają, że Wykonawca jest właścicielem wszelkich odpadów powstałych w trakcie realizacji Przedmiotu Zamówienia.

### Wykonawca jest zobowiązany do udostępnienia dokumentów potwierdzających utylizację odpadów lub przekazanie do utylizacji odpadów na każde żądanie Zamawiającego.

### Wykonawca jest zobowiązany do zabezpieczenia przed ewentualnym zanieczyszczeniem i zniszczeniem dróg komunikacyjnych w miejscu wykonywania robót oraz bieżące usuwanie powstałych zanieczyszczeń.

## Właściwości stosowanych wyrobów budowlanych

### Materiały przewidziane do wbudowania muszą spełniać wymagania art. 10 ustawy Prawo budowlane oraz wymagania wynikające z obowiązujących Polskich Norm przenoszących normy europejskie lub norm innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy.

### W przypadku braku Polskich Norm przenoszących normy europejskie lub norm innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy uwzględnia się w kolejności:

#### europejskie aprobaty techniczne;

#### wspólne specyfikacje techniczne;

#### normy międzynarodowe;

#### inne techniczne systemy odniesienia ustanowione przez europejskie organy normalizacyjne.

### W przypadku braku Polskich Norm przenoszących normy europejskie lub norm innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy oraz aprobat, specyfikacji, norm i systemów, o których mowa powyżej, uwzględnia się w kolejności:

#### Polskie Normy;

#### polskie aprobaty techniczne;

#### polskie specyfikacje techniczne.

### Wszystkie materiały muszą być w I gatunku.

### Wykonawca jest zobowiązany na każde żądanie Zamawiającego przedstawić dokumenty świadczące, że wbudowane materiały są dopuszczone do stosowania w budownictwie zgodnie z art. 10 ustawy Prawo budowlane oraz uzyskać przed zastosowaniem wyrobu akceptację inspektora nadzoru inwestorskiego.

## Kontrola robót budowlanych

### Każdy odbiór robót budowlanych łącznie z odbiorami dodatkowymi robót budowlanych nie wymaganymi wprost Umową, oraz odbiór dokumentacji powykonawczej robót budowlanych muszą zostać protokolarnie potwierdzone przez inspektorów nadzoru inwestorskiego oraz Kierownika projektu Zamawiającego, a także upoważnionego pracownika Wykonawcy, pod rygorem nieważności takich protokołów i odbiorów.

### Czynności odbioru zakończą się albo podpisaniem odpowiedniego protokołu odbioru bez uwag, albo odmową odbioru przedmiotu odbioru (protokół odbioru z uwagami) ze wskazaniem przyczyn odmowy odbioru. Jeżeli Zamawiający zgłosi zastrzeżenia do przedmiotu odbioru, obie strony Umowy ustalą protokolarnie zakres i termin bezpłatnego dokonania przez Wykonawcę niezbędnych poprawek. Wykonawca dokona poprawek w wyznaczonym terminie.

### Odbiór robót budowlanych odbywać się musi komisyjnie, przy udziale Wykonawcy, inspektorów nadzoru inwestorskiego i upoważnionych przedstawicieli Zamawiającego. Odbiór odbywać się musi na podstawie:

#### zgłoszenia zakończenia wszystkich naprawczych robót budowlanych przez Wykonawcę;

#### wymagań wskazanych przez inspektorów nadzoru inwestorskiego;

#### obowiązujących przepisów i norm.

### Sprawdzeniu i kontroli będą podlegać:

#### zastosowane wyroby budowlane i instalacje w odniesieniu do dokumentów potwierdzających ich dopuszczenie do obrotu na terenie Rzeczpospolitej Polski oraz zgodności ich parametrów z wymaganiami Zamawiającego;

#### sposób wykonania robót budowlanych, montażu i działania instalacji w aspekcie ich wykonania zgodnie przepisami prawa;

#### jakość wykonania i dokładność prac;

#### wyniki przeprowadzanych prób, badań i pomiarów, jeżeli są wymagane przez odpowiednie przepisy.

## Informacje dotyczące Lokalizacji

### Zamawiający nie posiada podkładów projektowych DWG dla Lokalizacji za wyjątkiem Lokalizacji w Warszawie, Opolu, Katowicach, Olsztynie i Krakowie.

### wszystkie Lokalizacje stanowią własność Skarbu Państwa w trwałym zarządzie Zamawiającego.

### Jednostki Terenowe w Katowicach, Białymstoku, Olsztynie, Łodzi, Bydgoszczy, Lublinie, Poznaniu, Rzeszowie oraz w Goławicach i siedziba Zamawiającego w Warszawie znajdują się w wolnostojących budynkach, które użytkuje tylko Zamawiający i nimi zarządza - przy czym w Jednostce Terenowej w Poznaniu Zamawiający wynajmuje pomieszczenia dla innych podmiotów.

### niewymienione w punkcie powyżej pozostałe Jednostki Terenowe znajdują się w budynkach, w których Zamawiający jest współwłaścicielem i zajmuje od jednego do trzech pięter. Budynki te mają zewnętrznych w stosunku do Zamawiającego zarządców.

### pod ochroną konserwatora zabytków znajduje się elewacja siedziby Zamawiającego w Warszawie oraz całe budynki w Jednostkach Terenowych w Szczecinie, Opolu i Olsztynie.

### dach w siedzibie Zamawiającego w Warszawie został wyremontowany w 2012 r. i podlega dwudziestoletniej gwarancji. Wykonawca jest zobowiązany prowadzić wszelkie prace na tym dachu w taki sposób, żeby Zamawiający nie stracił gwarancji. W tym celu Wykonawca zobowiązany jest do uzgodnienia tych prac z firmą: Andrzej Trzeszczkowski Zakład Konstrukcyjno-Montażowy ASIS 16-070 Choroszcz, Łyski 4A oraz z inspektorem nadzoru inwestorskiego. W przypadku utraty gwarancji przez Zamawiającego w wyniku prac prowadzonych przez Wykonawcę w sposób nie uzgodniony wcześniej z gwarantem dachu, Wykonawca będzie zobowiązany pokryć wszelkie koszty związane z przywróceniem opieki gwarancyjnej, a jeżeli okaże się to niemożliwe, do sprawowania tej opieki na własny koszt.

### W siedzibie Zamawiającego w Warszawie znajdują się dwa maszty telekomunikacyjne. Wykonawca będzie mógł skorzystać z tych masztów, o ile ich parametry graniczne, tj. wytrzymałość, wysokość, instalacja odgromowa, itp. będą dla Wykonawcy wystarczające. W przeciwnym wypadku Wykonawca będzie zobowiązany do budowy własnego masztu. Maszty przygotowane są do montażu anten o średnicy do 1 metra i wadze do 50 kilogramów każda. Wysokość masztu nad pokrycie dachu wynosi 3 metry. Podstawowe obciążenia na konstrukcję określono w oparciu o:

#### PN-80/B-02010/Az1/Z1-1-obciążenie śniegiem (III strefa);

#### PN-77/B-02011/Z1-3-obciążenie wiatrem (I strefa);

#### PN -80/B-02001-obciążenie stałe;

#### PN-80/B-02003-ociążenia zmienne technologiczne.

### Wykonawca nie może zakładać bezwzględnej zgody Zamawiającego na zainstalowanie urządzeń radiowych na dachu, bądź prowadzenia instalacji na budynkach.

### Aktualnie istniejące miejsca, w których są zainstalowane anteny i instalacje nie gwarantują poprawnej pracy dla urządzeń Wykonawcy wybranego w postępowaniu, a instalacja nowych urządzeń w innym miejscu może wymagać dodatkowych pozwoleń od właściwych instytucji, np.: konserwatora zabytków.

## Zabezpieczenie i powykonawcze porządkowanie pomieszczeń

### w czasie wykonywania robót budowlanych miejsce prowadzenia prac należy tak zabezpieczyć, aby uniemożliwić roznoszenie się kurzu (brudu) po czynnej części budynku.

### podłogę w pobliżu miejsca pracy należy zabezpieczyć folią przed zabrudzeniem.

### po zakończeniu pracy codziennie należy sprzątnąć miejsca pracy.

### korytarze, klatki schodowe, które służą do komunikacji, należy w godzinach pracy Zamawiającego utrzymywać w należytym porządku.

### w pomieszczeniach, w których będą prowadzone prace należy zabezpieczyć wyposażenie (np. meble, grzejniki, czujki ppoż., czujki ruchu i kontaktrony), a po zakończeniu robót oczyścić je, po uprzednim po zdjęciu zabezpieczeń przez Zamawiającego.

### w miarę potrzeb przenosić kolidujące z pracami meble i następnie po zakończeniu prac w pomieszczeniu doprowadzić pomieszczenie do stanu pierwotnego.

### prace prowadzić w taki sposób, żeby nie zapylić, ani nie uszkodzić urządzeń zamontowanych w pomieszczeniach.

### w przypadku zapylenia urządzeń, w szczególności przełączników sieciowych, Wykonawca zobowiązany jest na własny koszt je wyczyścić, również wewnątrz obudów.

### po wykonaniu wszelkich prac Wykonawca zobowiązany jest sprzątnąć na mokro pomieszczenia włącznie ze wszystkimi szafami, itp.

### Wykonawca zobowiązany jest do odpowiedzialności za powstałe w toku własnych prac odpady oraz za właściwy sposób postępowania z nimi zgodnie z obowiązującymi przepisami prawa.

### z uwagi na wykonywanie prac w czynnym obiekcie, Wykonawca musi dokonywać wywozu odpadów (np. gruzu) sukcesywnie.

## Adresy Lokalizacji

Adresy Lokalizacji wskazano w *Tabeli nr 1*.

Tabela nr 1

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Nazwa Lokalizacji** | **Adres** | **Telefon miejski** |
|  | Siedziba w Warszawie | 02-056 Warszawa  ul. Filtrowa 57  fax (22) 444-54-10 | (22) 444-50-00 |
|  | Delegatura w Białymstoku | 15-950 Białystok ul. Akademicka 4  fax (85) 874-81-33 | (85) 874-81-00 |
|  | Delegatura w Bydgoszczy | 85-131 Bydgoszcz ul. Wały Jagiellońskie 12  fax (52) 567-58-60 | (52) 567-58-00 |
|  | Delegatura w Gdańsku | 80-853 Gdańsk   ul. Wały Jagiellońskie 36  fax (58) 768-36-05 | (58) 768-36-00 |
|  | Delegatura w Katowicach | 40-039 Katowice  ul. Powstańców 29  fax (32) 784-42-31 | (32) 784-42-00 |
|  | Delegatura w Kielcach | 25-955 Kielce Al. Tysiąclecia Państwa Polskiego nr 4  fax (41) 249-91-05 | (41) 249-91-00 |
|  | Delegatura w Krakowie | 30-038 Kraków  ul. Łobzowska 67  fax (12) 342-34-44 | (12) 342-34-00 |
|  | Delegatura w Lublinie | 20-001 Lublin  ul. Okopowa 7  fax (81) 461-31-11 | (81) 461-31-00 |
|  | Delegatura w Łodzi | 93-106 Łódź  ul. Kilińskiego 210  fax (42) 239-32-90 | (42) 239-32-00 |
|  | Delegatura w Olsztynie | 10-165 Olsztyn  ul. Artyleryjska 3e  fax (89) 678 82 30 | (89) 678-82-00 |
|  | Delegatura w Opolu | 45-075 Opole  ul. Krakowska 28  fax (77) 449-70-99 | (77) 449-70-00 |
|  | Delegatura w Poznaniu | 61-662 Poznań  ul. Dożynkowa 9H  fax (61) 655-62-01 | (61) 655-62-00 |
|  | Delegatura w Rzeszowie | 35-016 Rzeszów  ul. Kraszewskiego 8  fax (17) 780-23-06 | (17) 780-23-00 |
|  | Delegatura w Szczecinie | 71-420 Szczecin  ul. Jacka Odrowąża 1  fax (91) 831-39-66 | (91) 831-39-00 |
|  | Delegatura we Wrocławiu | 50-044 Wrocław  ul. Piłsudskiego 15/17  fax (71) 711-83-50 | (71) 711-83-00 |
|  | Delegatura w Zielonej Górze | 65-213 Zielona Góra  ul. Podgórna 9a  fax (68) 410-66-39 | (68) 410-66-00 |
| 17. | Ośrodek Szkoleniowy w Goławicach | Goławice Drugie  05-180 Pomiechówek  fax (22) 451 23 00 | (22) 451-22-00 |

# Specyfikacja parametrów technicznych łączy telekomunikacyjnych przeznaczonych dla transmisji danych w Sieci WAN

## Struktura fizyczna łączy telekomunikacyjnych

Do serwerowni Zamawiającego w każdej Lokalizacji Wykonawca doprowadzi dwa łącza telekomunikacyjne w technologii IP VPN MPLS, tzw. główne Łącze IP VPN MPLS przeznaczone dla usługi transmisji danych w sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS i zapasowe Łącze IP VPN MPLS przeznaczone dla usługi transmisji danych w sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS. Szczegółowy schemat połączeń przedstawiony jest w części: *Topologia Sieci WAN, dostępu do Internetu*.

### Dopuszcza się wykonanie Łączy IP VPN MPLS za pomocą następujących mediów:

#### światłowodu jednomodowego;

#### bezprzewodowego łącza telekomunikacyjnego typu punkt-punkt pracującego w paśmie koncesjonowanym;

#### z następującymi zastrzeżeniami:

#### główne Łącze IP VPN MPLS w danej Lokalizacji nie może być zrealizowane za pomocą tego samego fizycznego łącza, na którym zrealizowane będzie zapasowe Łącze IP VPN MPLS w tej Lokalizacji;

#### główne Łącze IP VPN MPLS w siedzibie Zamawiającego w Warszawie nie może być zrealizowane za pomocą fizycznego łącza, na którym zrealizowane będzie łącze dla usługi głównego dostępu do Internetu w siedzibie Zamawiającego w Warszawie.

### Oba Łącza IP VPN MPLS Wykonawca wprowadzi do wskazanej przez upoważnionego w danej Lokalizacji pracownika Zamawiającego szafy typu rack 19" w serwerowni i zakończy w montowanym przez Wykonawcę w tej szafie patchpanelem – w przypadku światłowodu – patchpanelem światłowodowym typu SC, w przypadku łącza miedzianego – patchpanelem przynajmniej kat.6 z gniazdami typu RJ 45.

### Ze względu na wysokie pożądane SLA dotyczące dostępności usługi transmisji danych w Sieci WAN Zamawiający będzie dodatkowo premiował tych Wykonawców , którzy jednocześnie spełnią następujące dwa warunki:

#### we wszystkich Lokalizacjach zaoferują realizację głównego Łącza IP VPN MPLS za pomocą światłowodu jednomodowego. Z warunku tego wyłącza się Jednostkę Terenową w Goławicach z uwagi na szczególne położenie geograficzne;

#### we wszystkich Jednostkach Terenowych zaoferują realizację zapasowego Łącza IP VPN MPLS za pomocą bezprzewodowego łącza telekomunikacyjnego typu punkt-punkt pracującego w paśmie koncesjonowanym.

### W przypadku realizacji Łączy IP VPN MPLS za pomocą światłowodu należy stosować światłowód o ilości włókien nie mniejszej niż osiem.

### Ze względu na możliwe utrudnienia budowlane Zamawiający dopuszcza, aby światłowody zostały doprowadzone w okresie do **4 miesięcy** od dnia podpisania Umowy, przy czym do okresu tego nie wlicza się dni od **1 listopada do 30 kwietnia**, kiedy wykonywanie robót ziemnych zazwyczaj jest wstrzymane ze względu na zimowe warunki atmosferyczne. Do momentu doprowadzenia światłowodu, warunkowo w danej Lokalizacji dopuszcza się wykorzystanie bezprzewodowego łącza telekomunikacyjnego typu punkt-punkt pracującego w paśmie koncesjonowanym.

### Zamawiający obligatoryjnie wymaga wykonania głównego Łącza IP VPN MPLS w siedzibie Zamawiającego w Warszawie za pomocą światłowodu jednomodowego.

### W przypadku, jeżeli Wykonawca zdecyduje o instalacji w danej Lokalizacji dwóch światłowodów, to w takim wypadku pierwszy taki światłowód przeznaczony dla głównego Łącza IP VPN MPLS musi być ciągnięty fizycznie innymi studzienkami telekomunikacyjnymi na odcinku od węzła Wykonawcy do siedziby Zamawiającego niż światłowód przeznaczony dla zapasowego Łącza IP VPN MPLS. Zniszczenie (awaria) ciągu komunikacyjnego (studzienki telekomunikacyjnej) dla jednego światłowodu nie może powodować awarii drugiego z tych światłowodów. Mapy projektowe (inwentaryzacyjne) wskazujące trasy obu światłowodów muszą być dołączone do dokumentacji powykonawczej.

### W przypadku, jeżeli Wykonawca zdecyduje o instalacji w danej Lokalizacji dwóch bezprzewodowych łączy telekomunikacyjnych typu punkt-punkt, to w takim wypadku pierwsze takie łącze przeznaczone dla głównego Łącza IP VPN MPLS musi być skierowane w innym kierunku niż drugie łącze przeznaczone dla zapasowego Łącza IP VPN MPLS. Awaria w węźle dostępowym Wykonawcy obsługującym główne Łącze IP VPN MPLS nie może powodować awarii węzła dostępowego Wykonawcy obsługującego zapasowe Łącza IP VPN MPLS, i odwrotnie. Mapy projektowe (inwentaryzacyjne) wskazujące lokalizacje węzłów dostępowych muszą być dołączone do dokumentacji powykonawczej.

### W celu zapewnienia prywatności i odpowiedniego bezpieczeństwa transmisji danych w Sieci WAN, główne i zapasowe Łącza IP VPN MPLS nie mogą być budowane z wykorzystaniem:

#### infrastruktury znajdującej się poza terytorium RP;

#### zasobów sieci Internet;

#### łączy asymetrycznych w technologii xDSL;

#### łączy satelitarnych;

#### łączy technologii radiowych w paśmie nie podlegającym koncesjonowaniu;

#### łączy technologii radiowych typu punkt – wielopunkt;

#### komutowanych łączy telefonicznych;

#### technologii WiFi;

#### w oparciu o sieci komórkowe, tj. w szczególności technologii GPRS, EDGE, UMTS, HSPA, HSDPA, CDMA, LTE, LTE+, 5G.

### Główne i zapasowe Łącza IP VPN MPLS przeznaczone dla usług transmisji danych w Sieci WAN na odcinku od węzła Wykonawcy do Routera CPE (tzw. ostatnia mila) nie mogą być wykorzystywane do świadczenia przez Wykonawcę jakichkolwiek usług dla klientów innych niż Zamawiający. Od węzła Wykonawcy do Routera PE ruch musi być odseparowany przynajmniej logicznie, na przykład za pomocą VLAN lub PVC.

### W celu wykonania instalacji Wykonawca zobowiązany jest dla każdej Lokalizacji zdobyć w imieniu Zamawiającego wymagane pozwolenia, decyzje i zgody, w szczególności konserwatora zabytków jeżeli są wymagane, oraz wykonać konieczne projekty, roboty budowlane, w tym prace wykończeniowe, porządkowe i inne. Dokumentacja projektowa oraz prace podlegają kontroli i odbiorom przez inspektora nadzoru inwestorskiego.

### Infrastruktura fizyczna Wykonawcy zamontowana na terenie Zamawiającego (za wyjątkiem urządzeń Wykonawcy wskazanych w dokumentacji powykonawczej) nie ulega demontażowi po zakończeniu Umowy. Z dniem zakończenia realizacji Umowy przechodzi ona na własność Zamawiającego.

### Wszystkie prace i roboty budowlane, a także instalacje, w szczególności trasy kablowe, prowadzone poza terenem Zamawiającego dla każdej Lokalizacji, nie mogą obciążać kosztami prawnymi i ekonomicznymi Zamawiającego.

## Parametry Łączy IP VPN MPLS

### Technologia łącza telekomunikacyjnego: IP VPN MPLS. Zamawiający wymaga skonfigurowania dwóch oddzielnych, niezależnych od siebie chmur IP VPN MPLS. Jedną obsługującą wszystkie główne łącza IP VPN MPLS, a drugą wszystkie zapasowe łącza IP VPN MPLS. Pomiędzy tymi chmurami IP VPN MPLS nie może być zestawiony routing, także w infrastrukturze wewnętrznej sieci operatora.

### Zarówno główne jak i zapasowe Łącza IP VPN MPLS w każdej Lokalizacji muszą być łączami bez jakichkolwiek ograniczeń przesyłanych danych oraz łączami symetrycznymi, tj. o jednakowej, minimalnej gwarantowanej wskazanej w *Tabeli nr* 2 szybkości transmisji danych w obu kierunkach, mierzonej na interfejsie Routera CE podłączonym poprzez Router CPE do danego Łącza IP VPN MPLS.

Tabela nr 2

|  |  |
| --- | --- |
| **Lokalizacje** | **minimalna szybkość transmisji danych dla głównych i zapasowych Łączy IP VPN MPLS mierzona w warstwie transportowej modelu ISO/OSI** |
| siedziba Zamawiającego w Warszawie | 1100 Mb/s |
| Jednostki Terenowe z wyłączeniem Jednostki Terenowej w Goławicach | 60 Mb/s |
| Jednostka Terenowa w Goławicach | 120Mb/s |

### Wymagane szybkości transmisji danych (dalej zamiennie: przepustowości) są to gwarantowane przez Wykonawcę **minimalne** szybkości transmisji danych **dostępne w Sieci WAN w warstwie transportowej TCP/IP modelu ISO/OSI dla ruchu typu IMIX** (charakterystyka ruchu zamieszczona w *Tabeli nr 11*), tj. pomiędzy siedzibą w Warszawie, a jednocześnie każdą Jednostką Terenową, przy założeniu jednoczesnej komunikacji z Routera CE w stronę Routera CPE i odwrotnie.

### Szybkość transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS będzie sprawdzana pomiędzy interfejsem Routera CE od strony Sieci WAN w siedzibie Zamawiającego w Warszawie, a Routerem CE w każdej Jednostce Terenowej przy zastosowaniu protokołu komunikacyjnego FTP. Niedotrzymanie parametru minimalnej gwarantowanej szybkości transmisji danych przez strony Umowy traktowane jest jako Awaria.

### Szybkość transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS będzie sprawdzana pomiędzy interfejsem Routera CE od strony Sieci WAN w siedzibie Zamawiającego w Warszawie, a Routerem CE w każdej Jednostce Terenowej przy zastosowaniu protokołu komunikacyjnego FTP. Niedotrzymanie parametru minimalnej gwarantowanej szybkości transmisji danych przez strony Umowy traktowane jest jako Awaria.

### Każde główne i zapasowe Łącze IP VPN MPLS musi być zakończone dedykowanym dla tego Łącza IP VPN MPLS Routerem CPE, będącym stykiem infrastruktury fizycznej Wykonawcy z infrastrukturą fizyczną Zamawiającego, tj. Routerem CE.

### Zamawiający wymaga skonfigurowania priorytetyzacji ruchu na każdym głównym i zapasowym Łączu IP VPN MPLS. W tym celu Wykonawca musi zastosować dla głównych i zapasowych Łączy IP VPN MPLS usługę QoS. Wartości graniczne parametrów dla poszczególnych klas ruchu QoS dla każdego głównego i zapasowego Łącza IP VPN MPLS, pomiędzy siedzibą Zamawiającego w Warszawie, a odpowiednio daną Jednostką Terenową, na poziomie interfejsu przyłączeniowego Routera CE i przy założeniu obciążenia do 90% dostępnej przepustowości Łącza IP VPN MPLS, wskazano *w Tabeli nr 3*.

Tabela nr 3

|  |  |  |  |
| --- | --- | --- | --- |
| **klasa ruchu QoS**  **(nazwy umowne)** | **utrata pakietów** | **opóźnienie (RTD)** | **Jitter** |
| Klasa głos (voice) | < 0,1 % | <30 ms | <15 ms |
| Klasa wideo (video) | < 0,1 % | <35 ms | <15 ms |
| Klasa aplikacje (data) | < 0,2 % | <50 ms | - |
| Klasa reszta ruchu (best effort ) | < 0,5% | <50 ms | - |
| Klasa kontroli sieci (network control) | < 0,5% | <60 ms | - |

przy czym klasa *voice* musi być typu LLQ (Low Latency Queueing), a *video,* *data*, *network* *control* i *best* *effort* muszą być typu WFQ (Weighted Fair Queuing) lub CBWFQ (Class Based Weighted Fair Queuing) lub innego równoważnego.

### Podane wyżej wartości parametrów QoS nie mogą zostać przekroczone w ramach oferowanej usługi. Ich przekroczenie traktowane jest przez strony Umowy jako Awaria.

### Podział procentowy do każdej z klas ruchu, w ramach przepustowości Łącza IP VPN MPLS, zostanie uzgodniony z Wykonawcą podczas wdrożenia, przy czym wstępnie Zamawiający przyjmuje, że:

#### suma gwarantowanych pasm przepustowości poszczególnych klas QoS nie będzie przekraczać 75% założonej przepustowości Łącza IP VPN MPLS;

#### pojedyncza gwarantowana klasa ruchu będzie zajmować do 33% dostępnej przepustowości Łącza IP VPN MPLS;

#### klasy *voice* i *video* będą zajmować łącznie nie więcej niż 40% przepustowości Łącza IP VPN MPLS.

### Pula adresów IP dostępna dla Zamawiającego w ramach głównego Łącza IP VPN MPLS musi być inna niż dostępna dla zapasowego Łącza IP VPN MPLS. Pomiędzy tymi pulami nie może być zestawionego routingu.

### Główne i zapasowe Łącza IP VPN MPLS w ramach swojej chmury IP VPN MPLS muszą być wykonane w technologii *full-mesh*.

### Zamawiający wymaga kontroli jakości wykonanych Łączy IP VPN MPLS poprzez przeprowadzenie przez Wykonawcę pierwszej części testów akceptacyjnych. Sposób wykonania testów jest wskazany przez Zamawiającego w części *Testy akceptacyjne*.

### Główne Łącza IP VPN MPLS muszą umożliwiać transmisję danych w Sieci WAN w czasie kiedy zapasowe Łącza IP VPN MPLS ulegną Awarii. Oznacza to, że Wykonawca musi zapewnić brak pojedynczego punktu awarii jednocześnie dla obu kanałów transmisji danych w Sieci WAN, tj. dla usługi transmisji danych w Sieci WAN z wykorzystaniem głównego Łącza IP VPN MPLS i dla usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowego Łącza IP VPN MPLS w każdej Lokalizacji Zamawiającego i w swojej infrastrukturze telekomunikacyjnej.

### W trakcie trwania Umowy, utrata pakietów i opóźnienie będą kontrolowane przez Zamawiającego pomiędzy Routerami CE za pomocą aplikacji ping lub równoważnej przy założeniu, że wielkość wysyłanej paczki danych wynosi:

#### 400 bajtów dla klasy *voice*;

#### 1350 bajtów dla pozostałych klas QoS.

Zamawiający uznaje parametry danego Łącza IP VPN MPLS za poprawne jeżeli średnia utrata pakietów oraz średnie opóźnienie za okres minimum pięciu minut nie przekroczy wymaganych wartości.

## Wymagania dotyczące Routerów CE

### W przypadku konieczności Wykonawca, bez naliczania dodatkowych kosztów, zaktualizuje oprogramowanie danego Routera CE (IOS) do wersji umożliwiającej wdrożenie wymaganej Funkcjonalności.

### W przypadku konieczności Wykonawca, bez naliczania dodatkowych kosztów, rozbuduje dany Router CE o konieczne licencje lub moduły fizyczne, w szczególności zwiększy pojemność dostępnej pamięci RAM lub FLASH.

## Wymagania dotyczące Routerów CPE

### Routery CPE są własnością Wykonawcy i podlegają zwrotowi po zakończeniu Umowy, na zasadach wskazanych w Umowie.

### Wykonawca dostarczy łącznie 34 szt. Routerów CPE, tj. po jednym dla każdej Lokalizacji i obsługujących główne Łącze IP VPN MPLS oraz po jednym dla każdej Lokalizacji i obsługujących zapasowe Łącze IP VPN MPLS.

### Zamawiający wymaga, aby Wykonawca wykorzystał jako Routery CPE routery IP dostarczone wraz z niezbędnym okablowaniem, osprzętem i oprogramowaniem umożliwiającym realizowanie założonych Funkcjonalności. Zamawiający nie dopuszcza wykorzystywania jako Routerów CPE wyłącznie mostów lub modemów oraz innych urządzeń pracujących w warstwie drugiej modelu ISO/OSI.

### Router CPE może być wykorzystywany **wyłącznie** do świadczenia przez Wykonawcę usług na rzecz Zamawiającego.

### W serwerowni w każdej Lokalizacji Wykonawca zamontuje, skonfiguruje i uruchomi dwa Routery CPE, które będą stykiem infrastruktury fizycznej Wykonawcy, odpowiednio głównego i zapasowego Łącza IP VPN MPLS z infrastrukturą fizyczną Zamawiającego, tj. Routerem CE w Jednostkach Terenowych lub Routerami CE terminującymi Sieć WAN w siedzibie Zamawiającego w Warszawie.

### Dany Router CPE w każdej Lokalizacji musi zostać zamontowany w szafie typu rack 19" w miejscu wskazanym przez upoważnionego w danej Lokalizacji pracownika Zamawiającego. Jeżeli będzie konieczne, w celu montażu Wykonawca dostarczy i zamontuje szafkę lub półkę typu rack 19".

### Routery CPE muszą komunikować się z wykorzystaniem protokołu TCP/IP z Routerami CE Zamawiającego.

### Routery CPE w Jednostkach Terenowych muszą być połączone bezpośrednio do Routerów CE za pomocą skrętki przynajmniej kat.6 i z wykorzystaniem przynajmniej interfejsu RJ45 GigabitEthernet 10/100 (100Base TX), za wyjątkiem Jednostki Terenowej w Ośrodku Szkoleniowym w Goławicach, gdzie wymaga się zastosowania interfejsu RJ45 10/100/1000 (1000Base TX). Wszystkie kable połączeniowe muszą być oznaczone i opisane przez Wykonawcę.

### Routery CPE i CE w siedzibie Zamawiającego w Warszawie muszą być połączone bezpośrednio ze sobą za pomocą patchcordu światłowodowego wielomodowego typu LC-LC MM-50/125µm OM4 do interfejsu Ten GigabitEthernet 100/1000/10000 typu SFP+ wyposażonego we wkładkę GBIC wielomodowy 10Gb/s, typ SR, długość fali 850nm. Wszystkie kable połączeniowe muszą być oznaczone i opisane przez Wykonawcę.

## Wymagania dotyczące Routerów PE

### Wykonawca zapewni łącznie 17 szt. Routerów PE w swojej infrastrukturze telekomunikacyjnej. W wypadku, jeżeli Wykonawca stosuje mechanizmy mające zapewnić nieprzerwaną ciągłość działania Routerów PE poprzez zbudowanie ich w układzie zapewniającym wysoką dostępność, tj. minimum dwóch fizycznych urządzeń, z których jedno pracujące jako podstawowe, a drugie jako zapasowe oraz jednocześnie zapewniona jest konfiguracja mechanizmów odpowiedzialnych za natychmiastowe przełączenie ruchu na urządzenie zapasowe w przypadku wystąpienia Awarii urządzenia podstawowego, Zamawiający dopuszcza zapewnienie minimum 5 szt. takich Routerów PE. W przypadku stosowania obu rodzajów Routerów PE, w celu spełnienia wymogu technicznego należy przyjąć następujący przelicznik: 1 Router PE w układzie zapewniającym wysoką dostępność jest równoważny 4 szt. Routerów PE bez tego układu

### Ze względu na pożądane SLA dany Router PE może obsługiwać tylko główne Łącze IP VPN MPLSw danej Lokalizacji, a inny Router PE tylko zapasowe Łącze IP VPN MPLS w tej Lokalizacji.

### Ze względu na pożądane SLA dany Router PE nie posiadający układu zapewniającego wysoką dostępność może obsługiwać jednocześnie co najwyżej jedno główne Łącze IP VPN MPLS w danej Lokalizacji oraz co najwyżej jedno zapasowe Łącze IP VPN MPLS w dowolnej innej Lokalizacji.

### Ze względu na pożądane SLA dany Router PE posiadający układ zapewniający wysoką dostępność może obsługiwać jednocześnie główne Łącza IP VPN MPLS maksymalnie w czterech Lokalizacjach i zapasowe Łącza IP VPN MPLS maksymalnie w czterech innych Lokalizacjach.

## Wymagania dotyczące Węzłów Dostępowych

### Wykonawca zapewni łącznie 34 szt. Węzłów Dostępowych w swojej infrastrukturze telekomunikacyjnej.

### Ze względu na pożądane SLA każdy Węzeł Dostępowy może obsługiwać co najwyżej jedno główne Łącze IP VPN MPLS, albo jedno zapasowe Łącze IP VPN MPLS. Awaria pojedynczego Węzła Dostępowego nie może powodować Awarii więcej niż jednego Łącza IP VPN MPLS.

# Specyfikacja Funkcjonalności usługi transmisji danych w Sieci WAN

## Informacje podstawowe

### Transmisja danych w Sieci WAN realizowana musi być wyłącznie poprzez główne lub zapasowe Łącza IP VPN MPLS o właściwościach i parametrach technicznych wskazanych w części: *Specyfikacja parametrów technicznych łączy telekomunikacyjnych przeznaczonych dla transmisji danych w Sieci WAN*.

### Rolę urządzenia brzegowego, tj. urządzenia będącego stykiem pomiędzy Siecią WAN, a łączami Wykonawcy w każdej Lokalizacji pełni Router CE. Szczegółowy opis Routerów CE znajduje się w części *Specyfikacja parametrów technicznych Routerów CE*.

### Wykonawca wykona wszystkie prace projektowe i konfiguracyjne niezbędne w celu uzyskania minimalnej wymaganej Funkcjonalności Sieci WAN oraz odtworzenia Funkcjonalności jak przed rozpoczęciem robót nawet, jeżeli prace te nie zostały wprost wskazane w Umowie i niniejszym opracowaniu.

### Minimalna wymagana Funkcjonalność Sieci WAN, którą Wykonawca uzyska poprzez odpowiednią konfigurację Routerów CE, została opisana poniżej.

## Podział logiczny

### Sieć WAN jest podzielona logicznie na niezależne sieci przy wykorzystaniu mechanizmu VRF (Virtual Routing and Forwarding), z możliwością zwiększania przez Zamawiającego ilości tych sieci (aktualnie do czterdziestu) niezależnie do każdej Lokalizacji, wyłącznie poprzez rekonfigurację Routerów CE.

### Konfiguracja i działanie mechanizmu VRF muszą być całkowicie przezroczyste względem infrastruktury telekomunikacyjnej Wykonawcy, tj. nie mogą być uzależnione od wcześniejszej rekonfiguracji przez Wykonawcę Routerów PE, Routerów CPE, Łączy IP VPN MPLS, routingu w sieci MPLS i innych koniecznych elementów składowych infrastruktury telekomunikacyjnej. Konieczne zmiany w tej infrastrukturze muszą zachodzić w sposób dynamiczny (automatyczny) po dodaniu i skonfigurowaniu kolejnej sieci w ramach mechanizmu VRF w Routerach CE przez upoważnionych pracowników Zamawiającego.

### Niezależna sieć w ramach Sieci WAN, zwana dalej w skrócie VRF, musi umożliwiać obsługę tej samej puli adresacji IP co obsługiwana jednocześnie w innym VRF. Ruch z każdego VRF skierowany jest za pomocą interfejsu z funkcjonalnością TRUNK do określonego VLAN na przełącznikach (JUNIPER, CISCO) obsługujących Sieć WAN w każdej Lokalizacji.

## Routing statyczny i dynamiczny

### Transmisja danych w Sieci WAN w ramach każdego VRF pomiędzy Jednostkami Terenowymi musi odbywać się zawsze poprzez Router lub Routery CE w siedzibie Zamawiającego w Warszawie pomiędzy skonfigurowanymi tunelami typu GRE over IPSEC. Szczegóły dotyczące tego rozwiązania do ustalenia w trakcie wdrożenia.

### W celu automatycznej aktualizacji tras routingu w Sieci WAN aktualnie jest wykorzystywany protokół EIGRP obsługujący mechanizm VRF.

### W celu automatycznej aktualizacji tras routingu, w wydzielonej na potrzeby Zamawiającego sieci operatora wykorzystywany musi być protokół BGP (iBGP, eBGP) lub równoważny. W ramach tego mechanizmu Zamawiający musi mieć możliwość definiowania sieci obsługujących tunele dla VRF.

### W momencie przełączenia transmisji danych z głównego Łącza IP VPN MPLS na zapasowe i odwrotnie protokół routingu dynamicznego zdefiniowany na Routerach CE musi automatycznie aktualizować trasy routingu i propagować w całej Sieci WAN, niezależnie w każdym VRF.

### Protokół routingu dynamicznego musi umożliwiać propagację określonych tras statycznych w szczególności routingu zerowego niezależnie dla każdego VRF.

## Szyfrowanie transmisji danych

### Transmisja danych w Sieci WAN musi być szyfrowana sprzętowo w czasie rzeczywistym w Routerach CE i realizowana za pomocą dwóch tuneli GRE over IPSEC, oddzielnie dla każdego VRF, skonfigurowanych pomiędzy Routerem CE w każdej Jednostce Terenowej, a odpowiednio dwoma Routerami CE w siedzibie Zamawiającego w Warszawie obsługującymi pierwszy główne, a drugi zapasowe Łącze IP VPN MPLS. Szczegóły dotyczące tego rozwiązania bądź możliwe inne rozwiązanie szyfrujące transmisję sposobem wskazanym poniżej do ustalenia w trakcie wdrożenia.

### Pierwszy tunel GRE over IPSEC (szyfrowanie typu AES o długości klucza minimum 256, funkcja skrótu typu SHA-1 lub SHA-2) musi być skonfigurowany poprzez główne Łącze IP VPN MPLS.

### Drugi tunel GRE over IPSEC (szyfrowanie typu AES o długości klucza minimum 256, funkcja skrótu typu SHA-1 lub SHA-2) musi być skonfigurowany poprzez zapasowe Łącze IP VPN MPLS.

### Uwierzytelnianie IPSEC odbywa się poprzez współdzielone hasło inne dla każdego Łącza IP VPN MPLS dla każdej Lokalizacji.

## QoS

### Przy konfiguracji każdego tunelu GRE over IPSEC Wykonawca musi skorzystać z metody qos pre-classify tak, aby możliwe było przekazywanie do Routerów CPE Wykonawcy niezaszyfrowanej informacji z pola DSCP w nagłówku pakietu, celem skierowania ruchu w określony kanał QoS danego Łącza IP VPN MPLS. Ustawienia liczbowe pola DSCP zostaną ustalone z Wykonawcą na etapie wdrożenia.

### Zamawiający wymaga, aby były możliwe przynajmniej następujące ustawienia:

#### skonfigurowanie kolejki typu LLQ dla klasy *voice*;

#### skonfigurowanie kolejek WFQ lub CBWFQ lub innych równoważnych dla pozostałych klas QoS (z wyjątkiem *best effort*);

### Aktualnie wykorzystywana jest nw. Funkcjonalność:

#### kierowanie całego ruchu z danego VRF do jednej klasy QoS;

#### kierowanie ruchu wydzielonego za pomocą ACL (listy dostępu) do konkretnej klasy QoS, a za pomocą innej ACL do innej klasy QoS;

#### obsługa w ramach jednej klasy QoS ruchu skierowanego za pomocą ACL jednocześnie z różnych VRF;

#### kierowanie domyślnego ruchu z każdego VRF do klasy *best effort*;

#### kierowanie nadmiarowego ruchu w klasie *data* lub *network control* do klasy *best effort*;

### Ruch generowany przez protokół routingu dynamicznego oraz zdalny dostęp typu SSH do Routerów CE muszą być kierowane przez klasę *network control*.

## Przełączanie transmisji danych pomiędzy głównym, a zapasowym Łączem IP VPN MPLS

### Wykonawca musi umożliwić transmisję danych w Sieci WAN (dla dowolnych VRF) pomiędzy siedzibą Zamawiającego w Warszawie, a każdą Jednostką Terenową z wykorzystaniem obu usług transmisji danych w Sieci WAN, tj. obu Łączy IP VPN MPLS jednocześnie (głównego i zapasowego), w zależności od potrzeb Zamawiającego. Zamawiający przyjmuje, że konfiguracja podziału ruchu pomiędzy Łączami IP VPN MPLS będzie realizowana na poziomie definicji routingu domyślnego dla każdego zdefiniowanego tunelu GRE over IPSEC.

### W momencie utraty łączności w medium transmisyjnym (Awaria w Lokalizacji lub inny powód, w szczególności Awaria usługi transmisji danych w Sieci WAN z wykorzystaniem danego Łącza IP VPN MPLS w Lokalizacji lub Awaria Routera CE w siedzibie Zamawiającego w Warszawie) Router CE w Lokalizacji musi bez zbędnej zwłoki, w sposób automatyczny przełączyć transmisję danych w całości na usługę transmisji danych w Sieci WAN z wykorzystaniem Łącza IP VPN MPLS, które nie uległo Awarii. Po ustaniu Awarii sposób transmisji danych musi ponownie, bez zbędnej zwłoki, wrócić do stanu pierwotnego, tj. zbalansowanego obciążenia przy wykorzystaniu obu usług transmisji danych w Sieci WAN z wykorzystaniem obu Łączy IP VPN MPLS jednocześnie.

### Przełączanie transmisji danych w Routerze CE nie może wymagać i pociągać za sobą zmiany adresacji IP w jakimkolwiek VRF dla urządzeń podłączanych do Routera CE od strony Sieci WAN w każdej Lokalizacji.

### Przełączenie transmisji danych na jedno Łącze IP VPN MPLS powinno równolegle uruchomić zestaw reguł ACL niezależnie dla każdego VRF, dotyczący ograniczenia ilości transmitowanych danych, który m.in. blokuje określony, mniej istotny ruch w każdej klasie QoS w Sieci WAN Zamawiającego.

## Eliminacja pojedynczego punktu awarii Routera CE obsługującego Sieć WAN w siedzibie Zamawiającego w Warszawie

### W celu eliminacji pojedynczego punktu awarii dla Routera CE w siedzibie w Warszawie aktualnie zainstalowano dwa identyczne Routery CE, z których jeden bezpośrednio obsługuje główne, a drugi zapasowe Łącze IP VPN MPLS. W ramach niniejszej Umowy routery te podlegają wymianie na nowe. Oba Routery CE od strony Sieci WAN są widoczne dla prawie każdego VRF pod jednym wirtualnym adresem dzięki metodzie HSRP. Metody tej Wykonawca użyje również do skonfigurowania trzeciej grupy interfejsów skierowanych w stronę łącz dla dostępu do Internetu. W niektórych VRF połączenie do dalszej sieci zrealizowano w warstwie trzeciej modelu ISO/OSI wykorzystując protokół routingu dynamicznego EIGRP (Zamawiający posiada przełączniki CISCO). Blokowy schemat Sieci WAN przedstawiony jest w części: *Topologia Sieci WAN, dostępu do Internetu*.

## Transmisja danych w technologii IP Multicast

### W ramach transmisji danych w Sieci WAN Zamawiający wymaga uruchomienia transmisji danych w technologii IP Multicast dla dowolnych wybranych VRF pomiędzy wszystkimi lokalizacjami. Szczegółowe wymagania dotyczące wykonania projektu oraz implementacji rozwiązania przedstawione są w części: *Uruchomienie transmisji IP Multicast*.

## Zabezpieczenie Routerów CE

### Zamawiający wymaga bezpiecznego skonfigurowania Routerów CE, tj. takiej jego konfiguracji, która zabezpieczy dostęp do zarządzania routerami przez nieuprawnionych pracowników Zamawiającego zarówno od strony Sieci WAN od strony interfejsów podłączonych do Routerów CPE, jak i interfejsów terminalowych samych routerów oraz przez pracowników Wykonawcy od strony interfejsów podłączonych do Routerów CPE. Ponadto, w celu zachowania stabilnego działania Sieci WAN Zamawiający wymaga, aby sygnały sterujące, w szczególności transmisja danych routingowych, wykorzystywały specjalnie przeznaczoną do tego klasę QoS, tj. *network control*.

## Kopie zapasowe konfiguracji Routerów CE

### Zamawiający wymaga skonfigurowania automatycznego wysyłania kopii zapasowej każdego z Routerów CE na serwer monitoringu, o którym mowa w części: *System monitoringu*. Kopia zapasowa musi być wysyłana raz na tydzień, w piątek w godzinach popołudniowych. Nazwa pliku kopii zapasowej musi wskazywać na konkretny router, datę i godzinę wykonania kopii zapasowej. Ponadto musi być możliwe wykonanie takiej kopii zapasowej ręcznie z poziomu CLI routera w dowolnej chwili.

# Specyfikacja parametrów łączy telekomunikacyjnych przeznaczonych dla usługi dostępu do Internetu

## Struktura fizyczna łączy telekomunikacyjnych

Do serwerowni Zamawiającego w siedzibie w Warszawie Wykonawca doprowadzi dwa niezależne łącza telekomunikacyjne, tzw. główne i zapasowe łącze dla usługi dostępu do Internetu. Szczegółowy schemat połączeń przedstawiony jest w części: *Topologia Sieci WAN, dostępu do Internetu*.

### Dopuszcza się wykonanie łączy dla usługi dostępu do Internetu za pomocą następujących mediów:

#### światłowodu jednomodowego;

#### bezprzewodowego łącza telekomunikacyjnego typu punkt-punkt pracującego w paśmie koncesjonowanym;

#### z następującym zastrzeżeniem:

#### łącze dla usługi głównego dostępu do Internetu w siedzibie Zamawiającego w Warszawie nie może być zrealizowane za pomocą fizycznego łącza, na którym zrealizowana będzie główne Łącze IP VPN MPLS w siedzibie Zamawiającego w Warszawie.

### Łącza Wykonawca wprowadzi do wskazanej przez upoważnionego w danej Lokalizacji pracownika Zamawiającego szafy typu rack 19" w serwerowni i zakończy w montowanym przez Wykonawcę w tej szafie patchpanelem – w przypadku światłowodu – patchpanelem światłowodowym typu SC, w przypadku łącza miedzianego – patchpanelem przynajmniej kat.6 z gniazdami typu RJ 45.

### Ze względu na wysokie pożądane SLA dotyczące dostępności usługi dostępu do Internetu Zamawiający obligatoryjnie wymaga wykonania przynajmniej jednego, tj. głównego lub zapasowego łącza dla dostępu do Internetu w siedzibie Zamawiającego w Warszawie za pomocą światłowodu jednomodowego.

### W przypadku realizacji łącza za pomocą światłowodu należy stosować światłowód o ilości włókien nie mniejszej niż osiem.

### Ze względu na możliwe utrudnienia budowlane Zamawiający dopuszcza, aby światłowód został doprowadzony w okresie do **4 miesięcy** od dnia podpisania Umowy, przy czym do okresu tego nie wlicza się dni od **1 listopada do 30 kwietnia**, kiedy wykonywanie robót ziemnych zazwyczaj jest wstrzymane ze względu na zimowe warunki atmosferyczne. Do momentu doprowadzenia światłowodu warunkowo dopuszcza się wykorzystanie bezprzewodowego łącza telekomunikacyjnego typu punkt-punkt pracującego w paśmie koncesjonowanym.

### W przypadku, jeżeli Wykonawca zdecyduje o instalacji dwóch światłowodów przeznaczonych odpowiednio dla głównego i zapasowego łącza dla usługi dostępu do Internetu w siedzibie Zamawiającego w Warszawie, ze względu na wysokie pożądane SLA dotyczące dostępności usługi dostępu do Internetu, Zamawiający wymaga, aby ciągnięte były one fizycznie innymi studzienkami telekomunikacyjnymi na odcinku od węzła Wykonawcy do siedziby Zamawiającego. Zniszczenie (awaria) ciągu komunikacyjnego (studzienki telekomunikacyjnej) dla jednego światłowodu nie może powodować awarii drugiego z tych światłowodów i odwrotnie. Mapy projektowe (inwentaryzacyjne) wskazujące trasy obu światłowodów muszą być dołączone do dokumentacji powykonawczej.

### W przypadku, tymczasowej instalacji dwóch bezprzewodowych łączy telekomunikacyjnych typu punkt-punkt, ze względu na wysokie pożądane SLA dotyczące dostępności usługi dostępu do Internetu, muszą być one skierowane w różnych kierunkach, w stronę dwóch różnych węzłów dostępowych. Awaria w węźle dostępowym Wykonawcy obsługującym zapasowe łącze dla usługi dostępu do Internetu nie może powodować awarii węzła dostępowego Wykonawcy obsługującego główne łącze dostępowe dla usługi dostępu do Internetu, i odwrotnie. Mapy projektowe (inwentaryzacyjne) wskazujące lokalizacje węzłów dostępowych muszą być dołączone do dokumentacji powykonawczej.

### W celu zapewnienia odpowiedniej jakości, spójności i bezpieczeństwa transmisji danych łącza dla usługi dostępu do Internetu nie mogą być budowane z wykorzystaniem:

#### łączy asymetrycznych w technologii xDSL;

#### łączy satelitarnych;

#### łączy technologii radiowych w paśmie nie podlegającym koncesjonowaniu;

#### łączy technologii radiowych typu punkt – wielopunkt;

#### komutowanych łączy telefonicznych;

#### technologii WiFi;

#### w oparciu o sieci komórkowe, tj. w szczególności technologii GPRS, EDGE, UMTS, HSPA, HSDPA, CDMA, LTE, LTE+, 5G.

### W celu wykonania instalacji Wykonawca zobowiązany jest zdobyć w imieniu Zamawiającego wymagane pozwolenia, decyzje i zgody, w szczególności konserwatora zabytków jeżeli są wymagane, oraz wykonać konieczne projekty, roboty budowlane, w tym prace wykończeniowe, porządkowe i inne. Dokumentacja projektowa oraz prace podlegają kontroli i odbiorom przez inspektora nadzoru inwestorskiego.

### Infrastruktura fizyczna Wykonawcy zamontowana na terenie Zamawiającego (za wyjątkiem urządzeń Wykonawcy wskazanych w dokumentacji powykonawczej) nie ulega demontażowi po zakończeniu Umowy. Z dniem zakończenia realizacji Umowy przechodzi ona na własność Zamawiającego.

### Wszystkie prace i roboty budowlane, a także instalacje, w szczególności trasy kablowe, prowadzone poza terenem Zamawiającego nie mogą obciążać kosztami prawnymi i ekonomicznymi Zamawiającego.

## Parametry łączy telekomunikacyjnych

### Łącza muszą być łączami bez jakichkolwiek ograniczeń przesyłanych danych oraz łączami symetrycznymi, tj. o jednakowej, wskazanej w *Tabeli nr 4* gwarantowanej szybkości transmisji danych w obu kierunkach, mierzonej na interfejsie Routera CE od strony sieci Zamawiającego.

Tabela nr 4

|  |  |
| --- | --- |
| **Lokalizacja** | **minimalna szybkość transmisji danych** |
| siedziba Zamawiającego w Warszawie – łącze główne | 900 Mb/s |
| siedziba Zamawiającego w Warszawie – łącze zapasowe | 900 Mb/s |

### Wymagana szybkość transmisji danych (dalej zamiennie: przepustowość) dla łącza dla usługi dostępu do Internetu to gwarantowana przez Wykonawcę **minimalna** szybkość transmisji danych w warstwie transportowej modelu ISO/OSI dla ruchu typu IMIX (charakterystyka ruchu zamieszczona w *Tabeli nr 11*) dostępna **w sieci Internet**, przy założeniu komunikacji z wykorzystaniem protokołów TCP/IP dla transmisji z Routera CE w stronę sieci Wykonawcy i odwrotnie.

### Szybkość transmisji danych będzie sprawdzana na interfejsie każdego Routerów CE od strony sieci Zamawiającego, w stosunku do serwera referencyjnego udostępniającego co najmniej usługę FTP umiejscowionego wewnątrz głównej infrastruktury telekomunikacyjnej Wykonawcy i wskazanego w momencie przeprowadzania testów akceptacyjnych. Dane serwera referencyjnego będą wpisane do dokumentacji powykonawczej. Serwer referencyjny będzie dostępny dla Zamawiającego przez cały okres świadczenia usług. Zmiana serwera referencyjnego musi być protokolarnie potwierdzona przez obie strony Umowy i wymaga bezpłatnego wykonania przez Wykonawcę modyfikacji dokumentacji powykonawczej w terminie **10 Dni Roboczych** od dnia spisania protokołu.

### Niedotrzymanie parametru minimalnej gwarantowanej szybkości transmisji danych lub brak możliwości pomiaru danego łącza przez strony Umowy traktowane jest jako Awaria tego łącza.

### Utrata pakietów i opóźnienie będą kontrolowane przez Zamawiającego za Routerami CE, od strony wewnętrznej sieci Zamawiającego, przy wykorzystaniu aplikacji ping lub równoważnej przy założeniu, że wielkość wysyłanej paczki danych wynosi 400 bajtów, przy czym Zamawiający zastrzega sobie prawo do zgłoszenia Awarii usługi dostępu do Internetu poprzez dane łącze dla usługi dostępu do Internetu również w przypadku, jeżeli system monitoringu będzie wskazywał, że łącze to nie dotrzymuje wymaganych parametrów. Zamawiający uznaje utratę pakietów oraz opóźnienie dla każdego łącza dla usługi dostępu do Internetu za poprawne jeżeli średnia utrata pakietów oraz średnie opóźnienie za okres minimum pięciu minut, przy założeniu obciążenia do 90% dostępnej przepustowości, nie przekroczy wartości podanych w *Tabeli nr 5*.

Tabela nr 5

|  |  |  |  |
| --- | --- | --- | --- |
| **Lokalizacja** | **utrata pakietów** | **opóźnienie (RTD)** | **Jitter** |
| siedziba Zamawiającego w Warszawie – łącze główne | < 0,1 % | <40 ms | - |
| siedziba Zamawiającego w Warszawie – łącze zapasowe | < 0,1 % | <40 ms | - |

w stosunku do przynajmniej jednocześnie dwóch serwerów referencyjnych. W przypadku ustalenia większej ilości serwerów referencyjnych Zamawiający uznaje, ze łącze działa prawidłowo, jeżeli przynajmniej 50% + 1 serwerów referencyjnych wskazuje wymagane parametry tego łącza. W rozumieniu Zamawiającego serwery referencyjne to serwery nie umiejscowione w infrastrukturze telekomunikacyjnej Wykonawcy, posiadające publiczne, stałe adresy IP i nie będące w sieci jednego operatora (właściciela).

### Ilość i adresy IP serwerów referencyjnych zostaną uzgodnione z Wykonawcą na etapie wdrożenia i zostaną wpisane do dokumentacji powykonawczej. W czasie obowiązywania Umowy lista serwerów referencyjnych może zostać zmodyfikowana za zgodą obu stron Umowy, w następujących przypadkach:

#### serwer referencyjny zostanie wyłączony;

#### serwer referencyjny ulegnie awarii trwającej dłużej niż **10 dni**;

#### serwer referencyjny w sposób powtarzalny będzie generował błędne odczyty, a odczyty z pozostałych serwerów referencyjnych nie będą wykazywały odchyłek od wymaganych w Umowie parametrów.

### Zmiana serwerów referencyjnych musi być protokolarnie potwierdzona w siedzibie Zamawiającego w Warszawie przez kierowników projektu wskazanych w Umowie i wymaga bezpłatnego wykonania przez Wykonawcę modyfikacji dokumentacji powykonawczej w terminie **10 Dni Roboczych** od dnia spisania protokołu.

### Niedotrzymanie parametrów, brak możliwości ich pomiaru jak i brak odpowiedzi dla danego łącza dla usługi dostępu do Internetu przez strony Umowy traktowane są jako Awaria tego łącza.

### Zamawiający wymaga kontroli jakości wykonanych łączy telekomunikacyjnych poprzez przeprowadzenie przez Wykonawcę pierwszej części testów akceptacyjnych. Sposób wykonania testów jest wskazany przez Zamawiającego w części *Testy akceptacyjne*.

## Wymagania dotyczące Routerów CE

### W przypadku konieczności Wykonawca, bez naliczania dodatkowych kosztów, zaktualizuje oprogramowanie danego Routera CE (IOS) do wersji umożliwiającej wdrożenie wymaganej Funkcjonalności.

### W przypadku konieczności Wykonawca, bez naliczania dodatkowych kosztów, rozbuduje dany Router CE o konieczne licencje lub moduły fizyczne, w szczególności zwiększy pojemność dostępnej pamięci RAM lub FLASH.

### Routery CE w siedzibie Zamawiającego w Warszawie muszą być podłączone za pomocą patchcordu światłowodowego wielomodowego typu LC-LC MM-50/125µm OM4 do interfejsu Ten GigabitEthernet 100/1000/10000 typu SFP+ wyposażonego we wkładkę GBIC wielomodowy 10Gb/s, typ SR, długość fali 850nm bezpośrednio do urządzeń Wykonawcy. Wszystkie kable połączeniowe muszą być oznaczone i opisane przez Wykonawcę.

## Wymagania dotyczące Routerów CPE

### Zamawiający nie wymaga stosowania przez Wykonawcę Routerów CPE dla łączy dla usługi dostępu do Internetu. Zamawiający przyjmuje, że punktem styku z infrastrukturą Wykonawcy, tj. łączem dla usługi dostępu do Internetu w danej Lokalizacji, są w tym przypadku Routery CE.

# Specyfikacja Funkcjonalności usługi dostępu do Internetu

## Informacje podstawowe

### Usługa dostępu do Internetu świadczona musi być wyłącznie z wykorzystaniem łączy telekomunikacyjnych o właściwościach i parametrach technicznych wskazanych w niniejszym dokumencie.

### Usługa dostępu do Internetu jest usługą łączącą Sieć WAN z siecią Internet.

### Rolę urządzeń brzegowych, tj. urządzeń będących stykiem pomiędzy wewnętrzną siecią Zamawiającego, a łączami Wykonawcy w siedzibie Zamawiającego w Warszawie pełnią Routery CE. Szczegółowy opis Routerów CE znajduje się w części *Specyfikacja parametrów technicznych Routerów CE.*

### Wykonawca wykona wszystkie prace projektowe i konfiguracyjne niezbędne w celu uzyskania minimalnej wymaganej Funkcjonalności usługi dostępu do Internetu nawet jeżeli prace te nie zostały wprost wskazane w Umowie i niniejszym opracowaniu.

### Minimalna wymagana Funkcjonalność usługi dostępu do Internetu, którą Wykonawca uzyska poprzez odpowiednią konfigurację Routerów CE, została opisana poniżej.

## Eliminacja pojedynczego punktu awarii Routera CE obsługującego usługę dostępu do Internetu w siedzibie Zamawiającego w Warszawie

### W celu eliminacji pojedynczego punktu awarii dla Routera CE w siedzibie w Warszawie Zamawiający wymaga skonfigurowania dwóch Routerów CE. Jeden Router CE będzie bezpośrednio obsługiwał główne, a drugi zapasowe łącze dla usługi dostępu do Internetu.

### Wymaga się konfiguracji Routerów CE od strony sieci Zamawiającego w taki sposób, żeby były widoczne pod jednym wirtualnym publicznym adresem IP. Funkcjonalność można uzyskać dzięki metodzie HSRP lub innej równoważnej obsługiwanej przez posiadany przez Zamawiającego Router CE aktualnie obsługujący usługę dostępu do Internetu i nowy Router CE dostarczony przez Wykonawcę.

### Szczegółowy schemat przedstawiony jest w części *Topologia Sieci WAN, dostępu Internetu.*

## Adresacja IP i kierowanie ruchu w siedzibie Zamawiającego w Warszawie

### Zamawiający wymaga dostarczenia podsieci z przynajmniej **128 stałymi publicznymi adresami IPv4** (maska o maksymalnej wartości 25), przy czym adresy te nie mogą zostać wykorzystane w celu konfiguracji łączy dla usługi dostępu do Internetu od strony Wykonawcy.

### Zamawiający wymaga skonfigurowania dwóch fizycznie oddzielnych łączy dla usługi dostępu do Internetu, tj. głównego i zapasowego łącza dla usługi dostępu do Internetu. Ruch do i z sieci Internet musi być realizowany jednocześnie przez oba łącza w trybie zrównoważenia obciążenia. W celu umożliwienia wdrożenia ww. usługi Wykonawca skonfiguruje do swojej sieci routing BGP (iBGP, eBGP) lub równoważny, możliwy do uzyskania w Routerze CE, oraz nada numer ASN.

### Minimalna gwarantowana łączna szybkości transmisji danych dla jednej sesji dostępu do Internetu musi wynosić tyle ile **minimalna** szybkość transmisji danych dla dowolnego z łączy dla usługi dostępu do Internetu.

### Minimalna gwarantowana łączna szybkości transmisji danych dla dwóch sesji dostępu do Internetu musi wynosić tyle ile **minimalna** szybkość transmisji danych każdego z łączy dla usługi dostępu do Internetu.

### W przypadku Awarii głównego łącza dla usługi dostępu do Internetu albo zapasowego łącza dla usługi dostępu do Internetu, cały ruch do Internetu musi zostać niezwłocznie i w sposób automatyczny przejęty przez odpowiednio: zapasowe łącze dla usługi dostępu do Internetu albo główne łącze dla usługi dostępu do Internetu.

### W przypadku usunięcia Awarii, niezwłocznie i w sposób automatyczny ruch musi zostać ponownie zrównoważony, przy jednoczesnym wykorzystaniu obu łączy dla usługi dostępu do Internetu.

### Kierowanie ruchu przez jedno lub dwa łącza dla dostępu do Internetu nie może powodować zmian publicznej adresacji IP przydzielonej Zamawiającemu.

## Serwery nazw

### Usługa serwerów nazw jest elementem składowym usługi dostępu do Internetu.

### Zamawiający wymaga, aby Wykonawca skonfigurował w swojej infrastrukturze przynajmniej dwa publiczne serwery DNS:

#### typu master dla domen: prostej i odwrotnej dla nik.gov.pl oraz nik.eu, wraz ze zdalnym systemem dostępowym umożliwiającym Zamawiającemu pełną modyfikację stref 24 godziny na dobę 7 dni w tygodniu;

#### typu slave dla domen: prostej odwrotnej dla nik.gov.pl oraz nik.eu.

### Serwery muszą być skonfigurowane w trybie wskazującym dodatkowo na serwer pracujący w trybie slave dla domen: prostej i odwrotnej znajdujący się w infrastrukturze wewnętrznej Zamawiającego. Wykonawca odpowiednio skonfiguruje strefy tego serwera DNS.

### Publiczne serwery DNS dla domeny nik.gov.pl Zamawiającego muszą mieć wdrożone zabezpieczenie DNSSEC, czyli ochronę domen Zamawiającego przed przekierowaniem na fałszywe adresy IP. W przypadku konieczności Wykonawca odpowiednio zaktualizuje konfigurację DNS znajdującego się w infrastrukturze wewnętrznej Zamawiającego.

### Zmiana wpisu dla domeny prostej lub odwrotnej dokonana przez Zamawiającego musi spowodować automatyczną aktualizację wpisów w serwerach typu slave oraz rozpropagowanie się aktualizacji domen w całej sieci Internet.

### Na wniosek Wykonawcy Zamawiający we własnym zakresie i na swój koszt zleci firmie zewnętrznej, w której zaparkowane są jego domeny, dokonanie zmian adresacji IP wskazujących na serwery DNS na adresację IP przydzieloną przez Wykonawcę. Koszty drugiej i kolejnych zmian w tym zakresie refinansuje Wykonawca.

### Serwery DNS Zamawiającego oraz Wykonawcy muszą mieć możliwość konfigurowania nazw dla adresacji IP przeznaczonej dla siedziby Zamawiającego w Warszawie.

### Zamawiający wymaga udostępnienia panelu zdalnego dostępu dla klienta poprzez dedykowaną stronę internetową. Panel klienta musi umożliwiać przynajmniej:

#### konfigurację i zmianę wpisów w domenie prostej dla przynajmniej następujących rekordów: A, PTR, MX, NS, CNAME, TXT, SPF, SRV;

#### konfigurację i zmianę wpisów w domenie odwrotnej dla przynajmniej następujących rekordów: PTR;

#### wprowadzenie opisu słownego dla każdego z rekordów.

## AntyDDoS

AntyDDoS czyli usługa przeciwdziałania atakom typu DDoS (Distributed Denial of Service) jest elementem składowym usługi dostępu do Internetu. AntyDDoS musi być świadczony bez żadnych ograniczeń w ilości analizowanych danych i bez naliczania dodatkowych kosztów. Wymagany czas reakcji na zdarzenia nie może być dłuższy niż 1 minutę od wykrycia zdarzenia.

### W celu poprawnego świadczenia usługi AntyDDoS Wykonawca musi posiadać we własnej infrastrukturze i strukturze organizacyjnej:

#### system monitorowania w czasie rzeczywistym Routerów PE lub innych urządzeń w infrastrukturze, w celu sporządzenia profilu typowego ruchu w kierunkach od i do Zamawiającego;

#### system wykrywania anomalii ruchu przynajmniej za pomocą sygnatur, przekroczenia zdefiniowanych progów ruchu dla określonego typu pakietów i protokołów, analizy profilu ruchu w oparciu o profil standardowego ruchu;

#### system usuwania ataku (filtrowania) przy możliwie jak najmniejszym wpływie na pozostały ruch w kierunkach od i do Zamawiającego;

#### panel zdalnego dostępu dla klienta poprzez dedykowaną stronę internetową umożliwiający dostęp dla minimum 3 pracowników Zamawiającego. Panel klienta musi umożliwiać przynajmniej sprawdzenie:

##### statystyki aktualnego ruchu w kierunkach od i do klienta wraz z wartościami ekstremalnymi;

##### aktualnego stanu wykrytych ataków i aktualnego stanu działań zabezpieczających;

##### ustawień progów alarmowych oraz progów rozpoczęcia mitygacji ruchu;

##### ustawień reguł zabezpieczających;

##### raportów dziennych/miesięcznych z wykrytych ataków i podjętych działań, także raportów historycznych.

#### specjalistów dedykowanych do obsługi AntyDDoS w sposób ciągły, przez 24 godziny na dobę, w każdym dniu dowolnego tygodnia i roku.

### System wykrywania anomalii ruchu musi obejmować przynajmniej:

#### wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu w sieci Internet, w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS;

#### wyznaczanie oczekiwanej wartości ruchu w kierunkach do i od Zamawiającego, o danej porze dnia w danym dniu tygodnia;

#### wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanych tego ruchu

#### ochronę przed nasyceniem łączy telekomunikacyjnych przeznaczonych dla usługi dostępu do Internetu.

### System usuwania ataku musi obejmować przynajmniej:

#### filtrowanie ruchu z błędnymi nagłówkami IP/TCP/UDP;

#### odrzucanie lub przepuszczanie na bazie zdefiniowanych dla Zamawiającego filtrów operujących na informacjach w nagłówkach L3 i L4 modelu ISO/OSI;

#### filtrowanie ruchu na określonych portach UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne;

#### filtrowanie ruchu na określonych portach TCP na podstawie zawartości pola danych w oparciu o wyrażenia regularne;

#### ochronę przed atakami z udawanymi adresami źródłowymi IP (spoofing) poprzez autentykację sesji TCP, zapytań DNS oraz zapytań http;

#### filtrowanie nieprawidłowych zapytań DNS;

#### ograniczenie zapytań DNS do zadanej wartości zapytań na sekundę;

#### filtrowanie oparte o wyrażenia regularne definiujące zakres stosowania autentykacji DNS oraz ograniczania liczby zapytań DNS;

#### filtrowanie nieprawidłowych zapytań HTTP;

#### blokowanie ruchu do stacji Zamawiającego przekraczających progi dla operacji HTTP na sekundę na dany serwer lub na dany URL;

#### filtrowanie oparte o wyrażenia regularne definiujące zakres stosowania autentykacji HTTP lub ograniczania liczby zapytań http;

#### filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków HTTP;

#### ochronę przez atakami typu Slow Lories poprzez resetowanie połączeń, które pozostają nieaktywne przez zadany okres czasu;

#### ochronę przez atakami typu Slow Lories poprzez resetowanie sesji TCP, której aktywność jest poniżej zadanej liczby bajtów przesyłanej w zadanym okresie czasu;

#### wykrywanie ruchu kierowanego z serwerów CDN proxy i stosowanie algorytmów filtrowania na podstawie oryginalnego źródła ruchu;

#### wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS, które są poza sekwencją;

#### blokowane sesji jeżeli podczas negocjacji SSL/TLS klient zarządza nadmiernej ilości metod kryptograficznych lub rozszerzeń użytkownika. Próg dla tych wartości musi być definiowalny;

#### wykrywanie i rozłączanie sesji jeżeli negocjacja SSL/TLS nie zakończy się w zadanym czasie;

#### blokowanie ruchu ze stacji, dla których występuje nadmierna liczba nieprawidłowych, nadmiarowych lub niekompletnych sesji SSL;

#### monitorowanie negocjacji SSL dla wszystkich portów, na których można stosować aplikacje zabezpieczone protokołem TLS, przynajmniej: HTTPS, SMTP, IMAP4, POP, LDAP, NNTP, TELNET, FTP i SIP;

#### ochronę przed atakami pochodzącymi od sieci botnetowych (komputerów zainfekowanych w sposób umożliwiające zdalne sterowanie przez hackerów) poprzez filtrowanie na podstawie na bieżąco aktualizowanych sygnatur zawierających listę adresów IP;

#### ochronę przed atakami pochodzącymi z sieci botnetowych poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości. Wartości progowe muszą być definiowalne zarówno dla całości ruchu jak i do części ruchu zdefiniowanego za pomocą filtru.

### Ze względu na wymaganą w Umowie poufność monitoring i obróbka ruchu pod kątem ataków DDoS musi odbywać się wyłącznie w infrastrukturze Wykonawcy.

### Specjaliści dedykowani do obsługi AntyDDoS muszą odpowiadać przynajmniej za:

#### analizę ruchu w celu identyfikacji typu i natury ataku;

#### powiadamianie Zamawiającego o podejrzeniu wystąpienia ataku;

#### rozpoczęcie usuwania ataku w porozumieniu z Zamawiającym, przy czym automatycznie musi być uruchamiania obrona dla alarmów o uzgodnionym poziomie zagrożenia;

#### modyfikację zestawu użytych mechanizmów przeciwdziałania tak, aby uzyskać maksymalny poziom filtracji ruchu niepożądanego przy minimalnym wpływie na ruch prawidłowy;

#### klasyfikację alarmów typu DDoS jako: atak prawdziwy - zweryfikowany, atak fałszywy – zweryfikowany, nagły wzrost ruchu – zweryfikowany (pożądany).

### Szczegółowy sposób powiadamiania Zamawiającego, inicjowania, awaryjnego przerwania i zakończenia procedury filtrowania w przypadku wykrycia ataku zostanie uzgodniony na etapie wdrożenia.

### Po zakończeniu operacji filtrowania ruchu po zaistniałym ataku DDoS każdorazowo wymaga się sporządzania przez Wykonawcę i przekazywania Zamawiającemu raportu z wykrytego ataku. Raport musi zawierać przynajmniej następujące informacje:

#### rozmiar ataku, liczniki pakietów, procent całości ruchu wyrażony także w Gb/s;

#### czas trwania ataku;

#### główne źródła ataku wraz z geograficznym położeniem tych źródeł;

#### typ i naturę ataku;

#### wdrożone metody eliminacji ataku;

#### wielkość oczyszczonego ruchu;

#### czasy związane z wykonywaniem usługi AntyDDoS, tj.: godzina początku ataku, godzina powiadomienia Zamawiającego, godzina wdrożenia procedur obronnych, godzina zakończenia ataku, godzina przywrócenia normalnej pracy sieci.

### Wymaga się sporządzania przez Wykonawcę i przekazywania Zamawiającemu raportów zawierających przynajmniej:

#### statystykę ruchu w kierunkach od i do Zamawiającego;

#### maksymalne wartości ruchu;

#### listę zarejestrowanych ataków wraz z ich klasyfikacją;

#### listę usuniętych ataków.

# Specyfikacja parametrów technicznych Routerów CE

## Informacje podstawowe

### Zamawiający obecnie posiada łącznie 20 szt. Routerów CE, tj. po jednym w każdej Jednostce Terenowej obsługującym Sieć WAN, oraz cztery w siedzibie w Warszawie, przy czym dwa routery obsługują Sieć WAN, a dwa usługę dostępu do Internetu.

### Wykonawca dostarczy:

#### 2 szt. Routera CE do siedziby w Warszawie przeznaczone do obsługi Funkcjonalności dla Sieci WAN;

#### 1 szt. Routera CE do siedziby w Warszawie przeznaczonego do obsługi Funkcjonalności dla dostępu do Internetu;

### Nowo dostarczone Routery CE Wykonawca zamontuje zamiennie za istniejące Routery CE i skonfiguruje analogicznie do istniejących tak, aby uzyskać wymaganą Funkcjonalność i odtworzyć pozostałe skonfigurowane w nich Funkcjonalności.

## Specyfikacja istniejących u Zamawiającego Routerów CE

### Aktualnie w siedzibie Zamawiającego w Warszawie zamontowane są 4 Routery CE firmy CISCO serii ASR1000. 3 szt. to model: ASR1001-2.5G-SECK9. Dwa z nich obsługują Łącza IP VPN MPLS przeznaczone dla Sieci WAN, jeden obsługuje jedno łącze dla usługi dostępu do Internetu. Czwarty Router CE to model: ASR1001X-SECK9, obsługuje jedno łącze dla usługi dostępu do Internetu.

### Aktualnie w Jednostkach Terenowych zamontowanych jest 16 szt. Routerów CE. Są to routery firmy CISCO serii 2900, model: CISCO2921-HSEC/K9.

### Rozmieszczenie Routerów CE w Lokalizacjach oraz ich numery seryjne wskazano w *Tabeli nr 6*.

### Routery CE podlegające demontażowi i wymianie na nowo dostarczone przez Wykonawcę zaznaczono kolorem szarym i oznaczono słowem „TAK’ w kolumnie „wymiana na nowe” w *Tabeli nr 6*.

### Router CE podlegający demontażowi i wymianie na jeden ze zdemontowanych przez Wykonawcę w Warszawie zaznaczono kolorem szarym i oznaczono słowem „TAK” w kolumnie „wymiana na zdemontowany w Warszawie” w *Tabeli nr 6*.

### Routery CE firmy CISCO serii 2900, model: CISCO2921-HSEC/K9 nie podlegające wymianie oraz jeden Router CE firmy CISCO serii ASR1000, model: ASR1001-2.5G-SECK9, docelowo zamontowany w Goławicach podlegają serwisowi pogwarancyjnemu, który świadczony będzie przez serwis Wykonawcy.

### Zdemontowane Routery CE pozostaną u Zamawiającego i będą mogły zostać użyte przez serwis Wykonawcy zamiennie na wypadek Awarii sprzętowej danego modelu Routera CE w Jednostkach Terenowych.

Tabela nr 6

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **lokalizacja** | **model** | **numer seryjny** | **demontaż istniejącego** | **wymiana na nowe** | **wymiana na zdemontowany w Warszawie** |
| Warszawa | ASR1001-2.5G-SECK9 | SSI1727082G | TAK | TAK |  |
| Warszawa | ASR1001-2.5G-SECK9 | SSI173306MD | TAK | TAK |  |
| Warszawa | ASR1001-2.5G-SECK9 | SSI172906T0 | TAK | TAK |  |
| Warszawa | ASR1001X-SECK9 | FXS2110Q8UD |  |  |  |
| Wrocław | CISCO2921-HSEC/K9 | FCZ17376032 |  |  |  |
| Białystok | CISCO2921-HSEC/K9 | FCZ1737701Y |  |  |  |
| Bydgoszcz | CISCO2921-HSEC/K9 | FCZ17376030 |  |  |  |
| Lublin | CISCO2921-HSEC/K9 | FCZ17376034 |  |  |  |
| Poznań | CISCO2921-HSEC/K9 | FCZ17376039 |  |  |  |
| Goławice | CISCO2921-HSEC/K9 | FCZ17377020 | TAK |  | TAK |
| Zielona Góra | CISCO2921-HSEC/K9 | FCZ17376037 |  |  |  |
| Opole | CISCO2921-HSEC/K9 | FCZ17376036 |  |  |  |
| Olsztyn | CISCO2921-HSEC/K9 | FCZ17377021 |  |  |  |
| Kielce | CISCO2921-HSEC/K9 | FCZ1737603D |  |  |  |
| Katowice | CISCO2921-HSEC/K9 | FCZ1737603C |  |  |  |
| Łódź | CISCO2921-HSEC/K9 | FCZ1737603B |  |  |  |
| Szczecin | CISCO2921-HSEC/K9 | FCZ17376033 |  |  |  |
| Gdańsk | CISCO2921-HSEC/K9 | FCZ1737701Z |  |  |  |
| Rzeszów | CISCO2921-HSEC/K9 | FJC1911A1N0 |  |  |  |
| Kraków | CISCO2921-HSEC/K9 | FCZ1737603E |  |  |  |

**UWAGA!**

Wskazane w Tabeli nr 6 Routery CE firmy CISCO, model: CISCO2921-HSEC/K9 w ilości 15 szt., oraz 1 szt. Routera CE firmy CISCO serii ASR1000, model: ASR1001-2.5G-SECK9 pozostają w Jednostkach Terenowych na cały okres świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu i podlegają wyłącznie serwisowi Wykonawcy. Zamawiający nie wymaga zapewnienia Serwisu Producenta na te Routery CE.

### Specyfikacja Routerów CE serii 2900, model: CISCO2921-HSEC/K9

Tabela nr 7

|  |  |  |  |
| --- | --- | --- | --- |
| **Opis** | | | |
| NAME: "CISCO2921/K9", DESCR: "CISCO2921/K9 chassis, Hw Revision: 1.0"PID: CISCO2921/K9, VID: V08 | | | |
| NAME: "Internal Services Module - Crypto Engine on Slot 0", DESCR: "Internal Services Module - Crypto Engine"  PID: ISM-VPN-29, VID: V02 | | | |
| NAME: "C2921/C2951 AC Power Supply", DESCR: "C2921/C2951 AC Power Supply" PID: PWR-2921-51-AC, VID: V03 | | | |
| Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.4(3)M5, RELEASE SOFTWARE (fc1) | | | |
| ROM: System Bootstrap, Version 15.0(1r)M16, RELEASE SOFTWARE (fc1) | | | |
| Cisco CISCO2921/K9 (revision 1.0) with 1003520K/45056K bytes of memory  3 Gigabit Ethernet interfaces  2 terminal lines  1 Virtual Private Network (VPN) Module  1 cisco ISM Crypto Engine(s)  DRAM configuration is 64 bits wide with parity enabled.  255K bytes of non-volatile configuration memory.  500472K bytes of ATA System CompactFlash 0 (Read/Write) | | | |
| Licence info:  Technology Package License Information for Module:'c2900' | | | |
| Technology | Technology-package | | Next reboot |
| Current | Type |
| ipbase | ipbasek9 | Permanent | ipbasek9 |
| security | securityk9 | Permanent | securityk9 |
| uc | None | None | None |
| data | datak9 | Permanent | datak9 |
| NtwkEss | None | None | None |
| CollabPro | None | None | None |

### Specyfikacja Routerów CE firmy CISCO serii ASR1000, model: ASR1001-2.5G-SECK9

Tabela nr 8

|  |
| --- |
| **Opis** |
| NAME: "Chassis", DESCR: "Cisco ASR1001 Chassis w/o IDC", PID: ASR1001, VID: V03 |
| NAME: "Power Supply Module 0", DESCR: "Cisco ASR1001 AC Power Supply", PID: ASR1001-PWR-AC, VID: V02 |
| NAME: "Power Supply Module 1", DESCR: "Cisco ASR1001 AC Power Supply", PID: ASR1001-PWR-AC, VID: V02 |
| NAME: "Fan Tray", DESCR: "Cisco ASR1001 Fan Tray", PID: ASR1001-FANTRAY, VID: |
| NAME: "module 0", DESCR: "Cisco ASR1001 SPA Interface Processor", PID: ASR1001, VID: |
| NAME: "SPA subslot 0/1", DESCR: "5-port Gigabit Ethernet Shared Port Adapter", PID: SPA-5X1GE-V2, VID: V03 |
| NAME: "subslot 0/1 transceiver 0", DESCR: "GE T", PID: SP7041-E, VID: E |
| NAME: "subslot 0/1 transceiver 1", DESCR: "GE T", PID: SP7041-E, VID: E |
| NAME: "subslot 0/1 transceiver 2", DESCR: "GE T", PID: SP7041-E, VID: E |
| NAME: "subslot 0/1 transceiver 3", DESCR: "GE T", PID: SP7041-E, VID: E |
| NAME: "subslot 0/1 transceiver 4", DESCR: "GE T", PID: SP7041-E, VID: E |
| NAME: "SPA subslot 0/0", DESCR: "4-port Gigabit Ethernet Shared Port Adapter", PID: ASR1001, VID: |
| NAME: "subslot 0/0 transceiver 2", DESCR: "GE T", PID: SP7041-E, VID: E |
| NAME: "subslot 0/0 transceiver 3", DESCR: "GE T", PID: SP7041-E, VID: E |
| NAME: "module R0", DESCR: "Cisco ASR1001 Route Processor", PID: ASR1001, VID: V03 |
| NAME: "module F0", DESCR: "Cisco ASR1001 Embedded Services Processor", PID: ASR1001, VID: |
| Cisco IOS XE Software, Version 03.16.04b.S - Extended Support Release |
| Cisco IOS Software, ASR1000 Software (X86\_64\_LINUX\_IOSD-UNIVERSALK9-M), Version 15.5(3)S4b, RELEASE SOFTWARE (fc1) |
| License Level: adventerprise  License Type: Permanent  Next reload license Level: adventerprise |
| cisco ASR1001 (1RU) processor (revision 1RU) with 3729028K/6147K bytes of memory.  Processor board ID SSI172906T0  9 Gigabit Ethernet interfaces  32768K bytes of non-volatile configuration memory.  8388608K bytes of physical memory.  7741439K bytes of eUSB flash at bootflash:. |

### Specyfikacja Routera CE firmy CISCO serii ASR1000, model: ASR1001X-SECK9

Tabela nr 9

|  |
| --- |
| **Opis** |
| NAME: "Chassis", DESCR: "Cisco ASR1001-X Chassis" PID: ASR1001-X, VID: V03 |
| NAME: "Power Supply Module 0", DESCR: "Cisco ASR1001-X AC Power Supply" PID: ASR1001-X-PWR-AC, VID: V01 |
| NAME: "Power Supply Module 1", DESCR: "Cisco ASR1001-X AC Power Supply" PID: ASR1001-X-PWR-AC, VID: V01 |
| NAME: "Fan Tray", DESCR: "Cisco ASR1001-X Fan Tray" PID: ASR1001-X-FANTRAY, VID: |
| NAME: "module 0", DESCR: "Cisco ASR1001-X SPA Interface Processor" PID: ASR1001-X, VID: |
| NAME: "SPA subslot 0/1", DESCR: "5-port Gigabit Ethernet Shared Port Adapter" PID: SPA-5X1GE-V2, VID: V04 |
| NAME: "subslot 0/1 transceiver 0", DESCR: "GE T" PID: GLC-TE, VID: A1 |
| NAME: "subslot 0/1 transceiver 1", DESCR: "GE T" PID: GLC-TE, VID: A1 |
| NAME: "SPA subslot 0/0", DESCR: "Built-in GE SPA with 2 port 10G and 6 port 1G Interfaces"  PID: BUILT-IN-2T+6X1GE, VID: |
| NAME: "subslot 0/0 transceiver 2", DESCR: "GE T" PID: GLC-TE, VID: A1 |
| NAME: "subslot 0/0 transceiver 3", DESCR: "GE T" PID: GLC-TE, VID: A1 |
| NAME: "subslot 0/0 transceiver 4", DESCR: "GE T" PID: GLC-TE, VID: A1 |
| NAME: "module R0", DESCR: "Cisco ASR1001-X Route Processor" PID: ASR1001-X, VID: V03 |
| NAME: "module F0", DESCR: "Cisco ASR1001-X Embedded Services Processor" PID: ASR1001-X, VID: |
| Cisco IOS XE Software, Version 03.16.04b.S - Extended Support Release |
| Cisco IOS Software, ASR1000 Software (X86\_64\_LINUX\_IOSD-UNIVERSALK9-M), Version 15.5(3)S4b, RELEASE SOFTWARE (fc1) |
| License Level: adventerprise  License Type: Permanent  Next reload license Level: adventerprise |
| cisco ASR1001-X (1NG) processor (revision 1NG) with 3729028K/6147K bytes of memory.  Processor board ID FXS2110Q8UD  11 Gigabit Ethernet interfaces  2 Ten Gigabit Ethernet interfaces  32768K bytes of non-volatile configuration memory.  8388608K bytes of physical memory.  6594559K bytes of eUSB flash at bootflash:. |

## Dostawa nowych Routerów CE

Dostarczane Routery CE muszą poprawnie współpracować z istniejącymi u Zamawiającego Routerami CE, podlegającymi usłudze serwisowej. W razie konieczności Wykonawca rozszerzy wymagane minimalne parametry i Funkcjonalności dostarczanych Routerów CE tak, żeby była możliwa poprawna wzajemna współpraca istniejących i dostarczanych Routerów CE.

### Wszystkie dostarczane Routery CE muszą być tego samego producenta.

### Dostarczany Router CE musi być nowy i musi pochodzić z bieżącej produkcji, a jednocześnie nie może być urządzeniem, które mogło być używane w innych projektach i poddane procesowi odnowienia.

### Ze względu na pożądaną pełną kompatybilność oraz zabezpieczenie uprawnień gwarancyjnych Zamawiającego i, po upływie Umowy - uprawnień serwisowych, karty i moduły zainstalowane w Routerze CE muszą być tego samego producenta co Router CE.

### Router CE musi być wyprodukowany nie wcześniej niż sześć miesięcy od daty podpisania Umowy z Wykonawcą i nie może się znajdować na listach: EOS (End of Sale), EOL (End of Life), EOSL (End of Service Life).

### Wykonawca w ramach realizacji Umowy dostarczy wraz z Routerem CE dokument licencji wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela na terenie RP potwierdzający, że oprogramowanie zawarte w dostarczonym Routerze CE jest licencjonowane na Zamawiającego. Licencja będzie udzielona na następujących zasadach:

#### udzielona bezterminowo;

#### ważna na terenie RP;

#### bez ograniczeń w stosunku do minimalnych wymagań na Routery CE określonych w Umowie, w szczególności w ofercie Wykonawcy;

#### zezwoli na wykonywanie Zamawiającemu kopii bezpieczeństwa oprogramowania Routera CE i przechowywania na nośnikach elektronicznych.

### Gwarancja świadczona w ramach realizacji Umowy musi obejmować prawo do bezpłatnej aktualizacji wersji oprogramowania Routera CE. Wykonawca zapewni Zamawiającemu dostęp do:

#### nowych wersji oprogramowania;

#### narzędzi konfiguracyjnych i dokumentacji technicznej.

### Wymagane jest dostarczenie wraz z Routerem CE i dołączenie do dokumentacji powykonawczej oryginału pisemnego potwierdzenia wydanego przez producenta lub przedstawicielstwo producenta sprzętu na terenie RP, poświadczającego datę produkcji sprzętu.

### Wymagane jest dostarczenie do siedziby w Warszawie i dołączenie do dokumentacji powykonawczej szczegółowej dokumentacji technicznej producenta oferowanego Routera CE potwierdzającej spełnianie przez Router CE wymagań technicznych oraz wskazanie miejsc w tej dokumentacji potwierdzających wymagania (Zamawiający dopuszcza w tym przypadku możliwość złożenia dokumentacji w języku angielskim).

### Zamawiający będzie prowadził odbiór techniczny dostarczonego Routera CE poprzez analizę dokumentacji technicznej producenta routera oraz analizę dostarczonego sprzętu z wykorzystaniem CLI Routera CE.

### Brak dokumentacji producenta potwierdzającej spełnianie przez Router CE wymagań technicznych skutkuje brakiem odbioru technicznego Routera CE, a w konsekwencji brakiem odbioru końcowego potwierdzającego gotowość Wykonawcy do produkcyjnego świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu. W takim wypadku odpowiedzialność za opóźnienie w uruchomieniu usług ponosi Wykonawca. Wykonawca przed ponownym zgłoszeniem do odbioru końcowego musi zmienić lub zmodyfikować Router CE do parametrów wymaganych Umową i dostarczyć dokumentację techniczną producenta potwierdzającą te parametry.

### Zamawiający wymaga dostarczenia:

#### do siedziby Zamawiającego w Warszawie dwóch przeznaczonych do obsługi Sieci WAN Routerów CE CISCO serii ASR1001, minimum ASR1001-HX lub routerów równoważnych, przy czym minimalną Funkcjonalność i parametry dostarczanego Routera CE wymieniono w *Tabeli nr 1* w części: *Załącznik*;

#### do siedziby Zamawiającego w Warszawie jednego przeznaczonego do obsługi dostępu do Internetu Routera CE CISCO serii ASR1001, minimum ASR1001-HX lub routera równoważnego, przy czym minimalną Funkcjonalność i parametry dostarczanego Routera CE wymieniono w *Tabeli nr 1* w części: *Załącznik*;

### W związku z faktem, że Zamawiający posiada we własnej infrastrukturze Routery CE oraz przełączniki sieciowe wykorzystujące protokół routingu dynamicznego EIGRP, a także w związku z faktem, że Zamawiający wykorzystuje funkcjonalność TRUSTSEC niezbędną do kontroli przepływu danych pomiędzy podsieciami Sieci WAN, celem zapewnienia jednolitości i spójności konfiguracji Zamawiający będzie premiował Wykonawców, którzy zaoferują Routery CE zapewniające dodatkowo:

#### obsługę protokołu EIGRP oraz mechanizmu uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołu TACACS+;

#### obsługę TRUSTSEC przynajmniej w zakresie SGT (IP to SGT, Subnet to SGT), SXP (speaker, listener), Inline SGT tagging (SGT over Ethernet, SGT over IPsec VPN), SGT Enforcement (SGACL, Monitor mode, Logging, SG Firewall, SGT based QoS, SGT Caching, SGT based PBR),

zgodnie ze wskazaniem dodatkowych Funkcjonalności wyszczególnionych w *Tabeli nr 1* w części: *Załącznik.*

### Do każdego z dostarczanych Routerów CE Wykonawca dostarczy także komplet poniżej wymienionych:

#### 3 szt. modułu AOC CISCO SFP-10G-AOC10M= lub innego równoważnego, tego samego producenta co dostarczane Routery CE, składającego się z kompletu dwóch SFP+ 10Gb/s, typu LC, o długości fali 850nm, funkcje hot-swap i plug&play, autodetekcja prędkości, zintegrowanych ze światłowodem o długości ok. 10mb +- 2mb. W związku z faktem, że dostarczone Routery CE będą podłączane do istniejących u Zamawiającego przełączników firmy CISCO, jedno z dwóch SFP+ w dostarczonym komplecie musi być wskazane przez firmę CISCO jako dopuszczone do współpracy z przełącznikami CISCO, a drugie SFP+ musi być wskazane przez producenta dostarczanego Routera CE jako dopuszczone do współpracy z tym Routerem CE. Odpowiednie dokumenty producentów Wykonawca dostarczy wraz z dokumentacją urządzeń;

#### 1 szt. CISCO SFP-10G-SR-S= lub inne równoważne, tego samego producenta co dostarczane Routery CE, moduły SFP+ 10Gb/s, typu LC-LC, o długości fali 850nm, funkcje hot-swap i plug&play, autodetekcja prędkości;

#### 1 szt. patchcord światłowodowy wielomodowy typu MM OM4 LC-LC o szlifie PC, duplex 50/125µm o długości 10mb;

#### 4 szt. patchcord światłowodowy wielomodowy typu MM OM4 LC-LC o szlifie PC, duplex 50/125µm o długości 5mb;

#### 1 szt. patchcord światłowodowy wielomodowy typu MM OM4 LC-LC o szlifie PC, duplex 50/125µm o długości 3mb.

# Usługa Serwisu Producenta

## Informacje ogólne

### Na każdy dostarczony Router CE wraz z wyposażeniem oraz jeden Router CE ASR1001X-SECK9 wraz z wyposażeniem (dodatkowo należy uwzględnić dwa porty TenGigabitEthernet oraz zwiększenie wydajności przełączania ruchu do 20Gb/s), obsługujący jedno łącze dla usługi dostępu do Internetu w Warszawie, łącznie 4 szt. Routerów CE, Wykonawca jest zobowiązany zapewnić Serwis Producenta na okres **36 miesięcy** licząc od dnia rozpoczęcia świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu, potwierdzonego stosownym protokołem odbioru końcowego bez uwag.

### W przypadku skorzystania przez Zamawiającego z prawa opcji dotyczącego przedłużenia świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu, Wykonawca będzie zobowiązany zapewnić Serwis Producenta na każdy dostarczony Router CE wraz z wyposażeniem oraz jeden Router CE ASR1001X-SECK9 wraz z wyposażeniem (dodatkowo należy uwzględnić dwa porty TenGigabitEthernet oraz zwiększenie wydajności przełączania ruchu do 20Gb/s), łącznie 4 szt. Routerów CE przez okres na jaki zostało przedłużone świadczenie usług.

### Serwis Producenta Wykonawca zapewni jednorazowo z góry i aktywuje u producentów, w urządzeniach i oprogramowaniu przed odbiorem końcowym, przy czym dopuszczalna jest wcześniejsza aktywacja, ale nie może ona spowodować skrócenia wymaganego okresu świadczenia serwisu liczonego od dnia podpisania protokołu odbioru końcowego bez uwag.

### Wykonawca zapewni serwis partnerski umożliwiający zgłaszanie Awarii przez pracowników Zamawiającego pośrednio za pośrednictwem serwisu Wykonawcy. Zgłoszenie takie musi być zrealizowane bez naliczania dodatkowych opłat.

### Wykonawca jest zobowiązany zapewnić usługę Serwisu Producenta obejmującą czas usunięcia Awarii przez Producenta nie dłuższy niż w następnym Dniu Roboczym, tzw. 8x5xNBD.

## Zakres usługi Serwisu Producenta

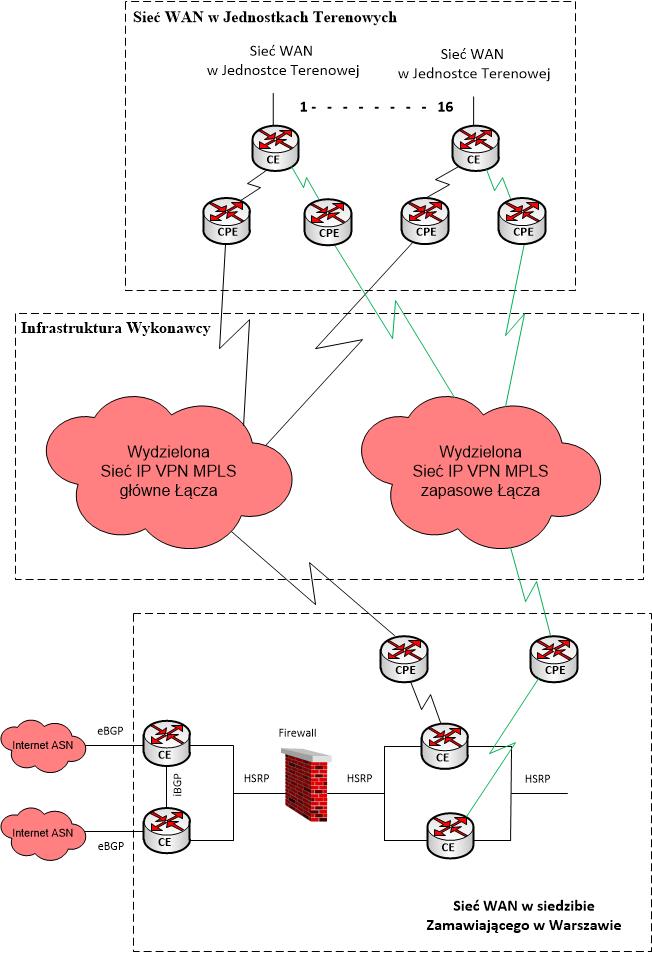
### Nieograniczona pomoc techniczna realizowana przez ulokowany na terenie RP ośrodek pomocy technicznej producenta, świadczona w języku polskim przynajmniej w godzinach od 8:00 do 16:00 w Dni Robocze. Przez pomoc techniczną Zamawiający rozumie przynajmniej przyjmowanie zgłoszeń o Awarii, procesowanie Awarii i jej usuwanie w terminie przewidzianym przez producenta dla tej usługi Serwisu Producenta.

### Dostawa i odbiór Routerów CE lub ich elementów z miejsca aktualnej instalacji, wymianę zepsutych urządzeń lub ich elementów na nowe, nie gorsze, nieregenerowane i nieużywane w przypadku braku możliwości naprawy, w terminie przewidzianym przez producenta dla tej usługi Serwisu Producenta.

### Możliwość legalnego pobierania i użytkowania bez dodatkowych opłat wszystkich uaktualnień i poprawek dla wszystkich objętych Przedmiotem Zamówienia Routerów CE i ich oprogramowania, wydanych przez producenta w trakcie świadczenia usługi Serwisu Producenta.

# Topologia Sieci WAN, dostępu do Internetu

Zamawiający wymaga skonfigurowania przez Wykonawcę dwóch niezależnych, odseparowanych od siebie sieci MPLS wykreowanych w infrastrukturze MPLS Wykonawcy na potrzeby obsługi: pierwsza sieć IP VPN MPLS dla usługi transmisji danych w Sieci WAN z wykorzystaniem wszystkich głównych Łączy IP VPN MPLS, druga sieć IP VPN MPLS dla usługi transmisji danych w Sieci WAN z wykorzystaniem wszystkich zapasowych Łączy IP VPN MPLS. Pomiędzy tymi sieciami nie może być zestawionego routingu, także w infrastrukturze Wykonawcy. Oba rodzaje łączy będą używane przez Zamawiającego jednocześnie.



# System monitoringu

## Informacje wstępne

### System monitoringu w całości jest własnością Wykonawcy i podlega zwrotowi do Wykonawcy zgodnie z warunkami Umowy, przy czym dyski twarde każdego z elementów składowych tego systemu po zakończeniu Umowy zostaną przez serwis Wykonawcy wymontowane i nieodpłatnie przekazane Zamawiającemu w Warszawie.

### Wykonawca zainstaluje i skonfiguruje elementy systemu monitoringu we wszystkich Lokalizacjach, a w siedzibie Zamawiającego w Warszawie we wskazanej szafie typu rack 19" zostanie zainstalowany centralny serwer zarządzający i kolekcjonujący wszystkie dane.

### Zamawiający dopuszcza użycie Routerów CE w Lokalizacjach jako sond dla systemu monitoringu.

### Ze względu na bezpieczeństwo wewnętrzne Zamawiającego i integralność systemu monitoringu dostęp Wykonawcy do tego systemu będzie możliwy lokalnie, z siedziby Zamawiającego w Warszawie.

### Zamawiający nie będzie zarządzał systemem monitoringu, ale musi otrzymać hasła dostępu do niego celem kontroli pod względem bezpieczeństwa urządzeń i danych Zamawiającego. Jest to warunek konieczny do uzyskania przez Wykonawcę odbioru.

### System monitoringu musi monitorować łączność z siedziby Zamawiającego w Warszawie do każdego Routera CE do interfejsów podłączonych pod główne i zapasowe Łącze IP VPN MPLS w każdej Jednostce Terenowej.

### W przypadku dostępu do Internetu na każdym fizycznym łączu system monitoringu musi kontrolować łączność przynajmniej z dwoma referencyjnymi stałymi adresami IP dostępnymi w Internecie i nie będącymi w sieci telekomunikacyjnej należącej do Wykonawcy lub kontrolowanej przez Wykonawcę oraz nie będącymi w sieci jednego operatora (właściciela). Adresy IP zostaną uzgodnione z Wykonawcą na etapie wdrożenia.

## Wykrywanie zdarzeń i automatyczne informowanie o zdarzeniach

### System monitoringu musi wykrywać w czasie rzeczywistym z punktu widzenia Routerów CE przynajmniej następujące zdarzenia, które mają charakter ciągły i nie krótszy niż 10 sekund, oraz rejestrować datę i godzinę (na podstawie serwerów czasu dla instytucji publicznych), w której dane zdarzenie zostało zarejestrowane:

#### status każdego, zarówno głównego jak i zapasowego, Łącza IP VPN MPLS, tj. czy łącze jest aktywne czy uległo Awarii.

#### przekroczenie i powrót do wymaganych parametrów zarówno dla głównego jak i zapasowego Łącza IP VPN MPLS w każdej Lokalizacji dla każdej klasy QoS dla ustawień globalnych VRF, tj.:

1. utraty pakietów;
2. opóźnienia (RTD);
3. jitteru.

Sposób wykonywania pomiarów musi być zgodny ze sposobem opisanym w części: *Specyfikacja parametrów technicznych łączy telekomunikacyjnych przeznaczonych dla transmisji danych w Sieci WAN*. Jeżeli sposób wykonywania danego pomiaru nie został wskazany wówczas podlega on uzgodnieniu w momencie wdrożenia.

#### status każdego łącza dla usługi dostępu do Internetu, tj. czy łącze jest aktywne czy uległo Awarii.

#### przekroczenie i powrót do wymaganych uśrednionych parametrów każdego łącza dla usługi dostępu do Internetu w stosunku do przynajmniej 50% +1 serwerów referencyjnych o stałych adresach IP, tj.:

1. utraty pakietów;
2. opóźnienia (RTD).

Sposób wykonywania pomiarów musi być zgodny ze sposobem opisanym w odpowiednio części *Specyfikacja parametrów technicznych łączy telekomunikacyjnych przeznaczonych dla usługi dostępu do Internetu*. Jeżeli sposób wykonywania danego pomiaru nie został wskazany wówczas podlega on uzgodnieniu w momencie wdrożenia.

#### brak komunikacji poprzez dane łącze dla usługi dostępu do Internetu w przypadku jeżeli przynajmniej 50% +1 serwerów referencyjnych o stałych adresach IP przestanie odpowiadać na zapytanie ICMP lub inne ustalone z Wykonawcą w trakcie wdrożenia.

#### przeciążenie procesora dowolnego z Routerów CE.

### Informacja o każdym zdarzeniu wykrytym przez system monitoringu musi być wysyłana zarówno do Zamawiającego jak i Wykonawcy, przy czym musi być możliwe wysłanie na przynajmniej 10 adresów email nie później niż 1 minutę od chwili wykrycia zdarzenia. Informacje o wybranych zdarzeniach (lub grupie zdarzeń) muszą być także wysyłane poprzez bramkę SMS z możliwością powiadamiania przynajmniej 10 odbiorców nie później niż 10 minut od chwili wykrycia zdarzenia.

### Szczegóły związane z klasyfikacją, ilością zdarzeń i ustaleniem progów po przekroczeniu których wysyłane będą informacje mailem lub SMS podlegają ustaleniu w czasie wdrożenia.

### Bramka SMS musi być fizycznym urządzeniem przeznaczonym do wysyłania takich komunikatów, tj. SMS nie mogą być wysyłane poprzez Internet, Sieć WAN oraz Łącza IP VPN MPLS.

## Korelacja zdarzeń

### Wykonawca musi zaprojektować i wykonać odpowiednią konfigurację korelacji zdarzeń rejestrowanych przez system monitoringu w taki sposób, żeby zminimalizować ilość reakcji na te zdarzenia do niezbędnego minimum, wskazującego pierwotną/najważniejszą przyczynę sekwencji zarejestrowanych zdarzeń. Dla przykładu: włączono monitorowanie dostępności głównego i zapasowego łącza IP VPN MPLS. W przypadku jednoczesnej awarii obu łącz do tej Lokalizacji zarejestrowane zostaną następujące zdarzenia:

#### główne Łącze IP VPN MPLS jest niedostępne;

#### zapasowe Łącze IP VPN MPLS jest niedostępne;

#### brak dostępności Routera CE w Katowicach.

W takim wypadku Zamawiający musi dostać tylko jeden komunikat wskazujący pierwotną przyczynę Awarii, tj. jednoczesny brak dostępności obu łączy IP VPN MPLS do Lokalizacji w Katowicach. Wszystkie inne zdarzenia powinny być zarejestrowane, ale w tym wypadku nie przekazywanie w formie email, ani SMS.

### Ze względu na konieczność korelacji zdarzeń oraz uniknięcia tzw. hazardu Zamawiający dopuszcza niewielkie opóźnienia w przesyłaniu komunikatów email i SMS o zdarzeniach. Szczegóły do ustalenia z Wykonawcą w trakcie wdrożenia.

### W przypadku, gdy wbudowany w system monitoringu układ korelacji zdarzeń nie będzie umożliwiał otrzymania wymaganej Funkcjonalności, Wykonawca jest zobowiązany bez dodatkowych opłat dostarczyć ewentualny sprzęt i odpowiednie oprogramowanie realizujące takie zadania.

## Kolekcjonowanie danych historycznych

### System monitoringu musi umożliwiać, poprzez autoryzowaną stronę WWW, graficzną prezentację zebranych danych w funkcji czasu, w postaci wykresów tygodniowych, miesięcznych, rocznych i z dowolnie wybranego okresu, z możliwością ich wydruku w formacie A4 lub eksportu do pliku CSV. System monitoringu musi kolekcjonować przynajmniej:

#### status każdego, zarówno głównego jak i zapasowego, Łącza IP VPN MPLS, tj. czy łącze jest aktywne czy uległo Awarii.

#### parametry zarówno dla głównego jak i zapasowego Łącza IP VPN MPLS w każdej Lokalizacji dla każdej klasy QoS, tj.:

1. utratę pakietów;
2. opóźnienie (RTD);
3. jitter.

#### obciążenie zarówno dla głównego jak i zapasowego Łącza IP VPN MPLS w każdej Lokalizacji dla każdej klasy QoS.

#### status każdego łącza dla usługi dostępu do Internetu, tj. czy łącze jest aktywne czy uległo Awarii.

#### obciążenie każdego łącza dla usługi dostępu do Internetu.

#### brak komunikacji poprzez dane łącze dla usługi dostępu do Internetu w przypadku jeżeli przynajmniej 50% +1 serwerów referencyjnych o stałych adresach IP przestanie odpowiadać na zapytanie typu ping o wielkości wysyłanej paczki danych równej 123 bajty.

#### obciążenie procesora każdego z Routerów CE.

### Dane historyczne muszą być kolekcjonowane i dostępne przez cały okres trwania Umowy, przy czym Zamawiający wymaga, aby dane były pobierane w odstępach nie większych niż minutowe i dostępne w takiej szczegółowości przynajmniej przez **7 dni**.

### Szczegóły kolekcjonowania danych historycznych do ustalenia z Wykonawcą w trakcie wdrożenia.

## Kopie zapasowe konfiguracji Routerów CE

### System monitoringu musi umożliwiać kolekcjonowanie kopii zapasowych plików konfiguracyjnych każdego z Routerów CE z osobna.

### Kopie zapasowe będą wykonywane automatycznie, raz na tydzień. W tym celu Wykonawca skonfiguruje w systemie monitoringu serwer TFTP, FTP lub SSH lub inne równoważne rozwiązanie, uzgodnione z Zamawiającym w trakcie wdrożenia.

### Kopie zapasowe będą dostępne z poziomu Routerów CE oraz z serwera monitorującego (za pomocą serwera TFTP, FTP, SSH, stron WWW, innych rozwiązań wskazanych przez Wykonawcę i uzgodnionych z Zamawiającym) zarówno dla Wykonawcy jak, i Zamawiającego i będą umożliwiały szybkie przywrócenie ostatniej lub wcześniejszej poprawnej konfiguracji danego Routera CE.

## Parametry fizyczne serwera systemu monitoringu

### W celu poprawnej i bezawaryjnej pracy systemu monitoringu Zamawiający wymaga, aby Wykonawca dostarczył serwer o parametrach nie gorszych od parametrów wskazanych w części: *Załącznik*.

# Testy akceptacyjne

## Informacje wstępne

### Testy akceptacyjne mają potwierdzić wymagane Umową parametry głównych i zapasowych Łączy IP VPN MPLS, wszystkich łączy dla usługi dostępu do Internetu oraz oczekiwaną Funkcjonalność Sieci WAN i dostępu do Internetu.

### Testy akceptacyjne wykonuje Wykonawca w obecności kierowników projektu obu stron Umowy.

### Testy muszą zostać tak przygotowane przez Wykonawcę, aby było możliwe ich przeprowadzenie z siedziby Zamawiającego w Warszawie.

### Testy akceptacyjne dzielą się na dwie części:

#### pierwsza część testów akceptacyjnych;

#### druga część testów akceptacyjnych.

### Każdy test w ramach pierwszej i drugiej części testów akceptacyjnych musi posiadać, tzw. **kartę testu akceptacyjnego**. Przykładowy wzór takiej karty podano w *Tabeli nr 9*.

### Karta testu akceptacyjnego musi zawierać przynajmniej parametry początkowe dla danego łącza, które będzie testowane, jaki parametr będzie testowany, dokładny opis procedury testowej, spodziewane wyniki pomiarowe oraz rzeczywiste wyniki pomiarowe.

### Zamawiający będzie uważał test za zaliczony, jeżeli rzeczywiste wyniki pomiarowe nie będą przekraczały parametrów granicznych wskazanych w spodziewanych wynikach pomiarowych dla tego testu.

### Każdy test musi być przygotowany przez Wykonawcę zarówno teoretycznie jak i sprzętowo w taki sposób, żeby było możliwe jednoznaczne stwierdzenie, czy został on zaliczony, czy nie. Ocena będzie przeprowadzana komisyjnie metodą porównawczą względem spodziewanych wyników pomiarowych. Brak możliwości jednoznacznego ocenienia danego testu będzie traktowany jako brak zaliczenia tego testu.

### Kierownik projektu Wykonawcy w sposób pisemny lub email poinformuje kierownika projektu Zamawiającego o uruchomieniu głównych i zapasowych Łączy IP VPN MPLS we wszystkich Lokalizacjach i o gotowości do przeprowadzenia pierwszej części testów akceptacyjnych.

### Przeprowadzanie pierwszej części testów akceptacyjnych rozpocznie się w terminie uzgodnionym z kierownikiem projektu Zamawiającego jednak nie później niż **5 Dnia Roboczego** od dnia wpłynięcia zawiadomienia od Wykonawcy.

### Kierownik projektu Wykonawcy w sposób pisemny lub email poinformuje kierownika projektu Zamawiającego o przełączeniu lokalnej sieci Zamawiającego do Routerów CE we wszystkich Lokalizacjach i o gotowości do przeprowadzenia drugiej części testów akceptacyjnych.

### Przeprowadzanie drugiej części testów akceptacyjnych rozpocznie się w terminie uzgodnionym z kierownikiem projektu Zamawiającego jednak nie później niż **3 Dnia Roboczego** od dnia wpłynięcia zawiadomienia od Wykonawcy.

### W przypadku jeżeli chociaż jeden test z grupy testów przeprowadzonych przez Wykonawcę w ramach pierwszej lub drugiej części testów akceptacyjnych nie zostanie zaliczony, nie zostaje zaliczona odpowiednio cała pierwsza lub cała druga część testów akceptacyjnych. W takim wypadku Wykonawca bez zbędnej zwłoki usunie przyczyny związane z niepowodzeniem danego testu lub testów, lub odpowiednio zmodyfikuje procedurę prowadzenia samego testu oraz uzyska ponowną akceptację kierownika projektu Zamawiającego i ponownie zgłosi gotowość do przeprowadzenia wszystkich testów. Przeprowadzanie testów rozpocznie się w terminie uzgodnionym z kierownikiem projektu Zamawiającego jednak nie później niż **3 Dnia Roboczego** od dnia wpłynięcia ponownego zawiadomienia od kierownika projektu Wykonawcy.

### Strony Umowy ustalają, że kierownik projektu Zamawiającego oraz Zamawiający nie ponoszą odpowiedzialności w przypadku, jeżeli zatwierdzony przez kierownika projektu Zamawiającego test nie powiedzie się ze względu na złe zaprojektowanie przez Wykonawcę procedury prowadzenia testu lub złe zaprojektowanie układu pomiarowego.

Przykładowa karta testu akceptacyjnego

Tabela nr 10

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **I Część Testów** | **Weryfikacja parametrów głównego Łącza IP VPN MPLS**  **w Lokalizacji Gdańsk** | | | | | |
| **CEL** | Weryfikacja parametrów głównego Łącza IP VPN MPLS | | | | | |
| **OPIS** | Procedura testowa wg ........ | | | | | |
| **Kryterium powodzenia** | Spodziewane wyniki wg tabeli ..... | | | | | |
| **Mierzone parametry** | | | | | | |
| **Przepustowość [Mb/s]** | do Warszawy: | | | z Warszawy: | | |
|  | Klasa ruchowa | | | | | |
| Głos | Wideo | Aplikacje | | Kontrola sieci | Reszta ruchu |
| **Utrata pakietów [%]** |  |  |  | |  |  |
| **Opóźnienie RTD [ms]** |  |  |  | |  |  |
| **Jitter [ms]** |  |  | x | | x | x |
| **Wynik testu** | ⬜ zatwierdzono ⬜ nie zatwierdzono | | | | | |
| **Czytelny podpis Wykonawcy** |  | | | | | |

## Pierwsza część testów akceptacyjnych

### Pierwsza część testów akceptacyjnych dotyczy sprawdzenia parametrów wybudowanych przez Wykonawcę głównych i zapasowych Łączy IP VPN MPLS oraz łączy dla usługi dostępu do Internetu.

### Wykonawca może przystąpić do wykonywania tych testów jeżeli jednocześnie spełni następujące dwa warunki:

#### uzyska odbiór propozycji pierwszej części testów akceptacyjnych;

#### uruchomi główne i zapasowe Łącza IP VPN MPLS we wszystkich Lokalizacjach oraz łącza dla usługi dostępu do Internetu w siedzibie Zamawiającego w Warszawie.

### W ramach pierwszej części testów akceptacyjnych Wykonawca musi zmierzyć przynajmniej:

#### minimalną przepustowość w obu kierunkach pomiędzy głównym oraz zapasowym Łączem IP VPN MPLS w każdej Jednostce Terenowej, a odpowiednio głównym i zapasowym Łączem IP VPN MPLS w siedzibie Zamawiającego w Warszawie zgodnie z warunkami pomiarowymi opisanymi w niniejszym dokumencie;

#### minimalną przepustowość pomiędzy każdym z łączy dla usługi dostępu do Internetu, a serwerem wewnątrz infrastruktury Wykonawcy zgodnie z warunkami pomiarowymi opisanymi w niniejszym dokumencie;

#### maksymalną utratę pakietów dla każdej klasy QoS pomiędzy głównym oraz zapasowym Łączem IP VPN MPLS w każdej Jednostce Terenowej, a odpowiednio głównym i zapasowym Łączem IP VPN MPLS w siedzibie Zamawiającego w Warszawie zgodnie z warunkami pomiarowymi opisanymi w niniejszym dokumencie;

#### maksymalną utratę pakietów pomiędzy każdym z łączy dla usługi dostępu do Internetu, a serwerem wewnątrz infrastruktury Wykonawcy zgodnie z warunkami pomiarowymi opisanymi w niniejszym dokumencie;

#### maksymalne opóźnienie (RTD) dla każdej klasy QoS pomiędzy głównym oraz zapasowym Łączem IP VPN MPLS w każdej Jednostce Terenowej, a odpowiednio głównym i zapasowym Łączem IP VPN MPLS w siedzibie Zamawiającego w Warszawie zgodnie z warunkami pomiarowymi opisanymi w niniejszym dokumencie;

#### maksymalne opóźnienie (RTD) pomiędzy każdym z łączy dla usługi dostępu do Internetu, a serwerem wewnątrz infrastruktury Wykonawcy zgodnie z warunkami pomiarowymi opisanymi w niniejszym dokumencie;

#### maksymalny Jitter dla klas QoS: *voice* i *video* pomiędzy głównym oraz zapasowym Łączem IP VPN MPLS w każdej Jednostce Terenowej, a odpowiednio głównym i zapasowym Łączem IP VPN MPLS w siedzibie Zamawiającego w Warszawie zgodnie z warunkami pomiarowymi opisanymi w niniejszym dokumencie.

### Zamawiający ustala, że testy parametrów łączy, tj. RTD, utratę pakietów i Jitter, a także testy przepustowości głównych i zapasowych Łączy IP VPN MPLS oraz przepustowości łączy dla usługi dostępu do Internetu należy wykonać certyfikowanym miernikiem zgodnie ze standardem RFC 2544, przy następujących założeniach:

#### rodzaj generowanego ruchu - typ IMIX zgodnie z parametrami z *Tabeli nr 11;*

#### parametr „throughput” ustawiony w taki sposób, aby wykonać pomiar dla 100% wymaganej przepustowości łączy;

#### warstwa modelu ISO/OSI: L4;

#### tolerancja pomiaru: nie większa niż 1%;

#### czas prowadzenia każdego testu: minimum 5 minut;

#### ilość prób przeprowadzenia danego testu: 2 próby.

Tabela nr 11

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Długość pakietu IP w Bajtach** | **Proporcja liczby pakietów** | **Udział w liczbie przesyłanych pakietów** | **Udział w ilości przesyłanych bajtów** |
| 1. | 40 | 7 | 58,4% | 6,9% |
| 2. | 576 | 4 | 33,3% | 56,4% |
| 3. | 1500 | 1 | 8,3% | 36,7% |

### Każdy wynik pomiarowy wskazany w raporcie z pomiaru danego łącza należy wpisać do karty przeprowadzenia testu jako wynik tego testu. Test będzie zaliczony jeżeli zmierzona wartość parametru podlegającego weryfikacji będzie, w zależności od wymagań nie mniejsza lub nie większa, niż wskazana w niniejszym dokumencie.

### Miernik pomiarowy użyty do pomiarów łączy musi posiadać certyfikację organu upoważnionego aktualną na dzień prowadzenia pomiaru. Z certyfikacji musi wynikać, że miernik pracuje poprawnie, oraz że został on prawidłowo skalibrowany. Kopię takiego dokumentu Wykonawca zobowiązany jest przedstawić Zamawiającemu do wglądu przed rozpoczęciem wykonywania testów, a także zobowiązany jest dołączyć ją do dokumentacji powykonawczej.

## Druga część testów akceptacyjnych

### Druga część testów akceptacyjnych dotyczy sprawdzenia wymaganej Funkcjonalności Sieci WAN w każdej z Lokalizacji oraz Funkcjonalności dostępu do Internetu w siedzibie Zamawiającego w Warszawie.

### Wykonawca może przystąpić do wykonywania tych testów jeżeli jednocześnie spełni następujące trzy warunki:

#### uzyska odbiór projektu transmisji danych w technologii IP Multicast;

#### uzyska odbiór wyników pierwszej części testów akceptacyjnych;

#### uzyska odbiór propozycji drugiej części testów akceptacyjnych;

#### we wszystkich Lokalizacjach przełączy Sieć WAN Zamawiającego (w tym dostęp do Internetu) do Routerów CE.

### W ramach drugiej części testów akceptacyjnych Wykonawca musi przeprowadzić przynajmniej:

#### weryfikację konfiguracji i działania łączy typu TRUNK pomiędzy Routerem CE, a przełącznikiem obsługującym Sieć WAN w każdej Lokalizacji;

#### weryfikację konfiguracji i działania tunelu dla głównego i dla zapasowego Łącza IP VPN MPLS dla każdego skonfigurowanego VRF;

#### weryfikację poprawności konfiguracji i działania routingu dla każdego VRF na Routerze CE w każdej Lokalizacji;

#### weryfikację poprawności konfiguracji i działania list dostępowych (ACL) na głównym i zapasowym Łączu IP VPN MPLS w każdej Lokalizacji;

#### weryfikację poprawności konfiguracji i kierowania określonego ruchu do danej klasy QoS;

#### weryfikację poprawności konfiguracji i działania HSRP (lub rozwiązania równoważnego) w siedzibie Zamawiającego w Warszawie;

#### weryfikację poprawności konfiguracji i działania automatycznego przełączania ruchu dla każdego VRF pomiędzy głównym, a zapasowym Łączem IP VPN MPLS;

#### weryfikację działania transmisji danych w technologii IP Multicast;

#### weryfikację poprawności konfiguracji i działania automatycznego przełączania ruchu pomiędzy głównym, a zapasowym łączem dla usługi dostępu do Internetu;

#### weryfikację poprawności konfiguracji i działania systemu monitoringu w zakresie wykrywania Awarii, zbierania i eksportowania statystyk, korelacji zdarzeń, wysyłania email i SMS z powiadomieniami o Awariach oraz wykonywania i odtwarzania konfiguracji Routerów CE z kopii zapasowych;

#### weryfikację poprawności konfiguracji i działania głównego oraz zapasowego DNS i revDNS, w tym zapasowego DNS i revDNS znajdującego się w siedzibie Zamawiającego w Warszawie, w tym poprawnego działania zabezpieczeń DNSSEC;

#### weryfikację poprawności konfiguracji i działania ASN oraz routingu BGP (iBGP, eBGP);

#### weryfikację poprawności konfiguracji i działania usługi dostępu do Internetu w siedzibie Zamawiającego w Warszawie;

#### weryfikację poprawności działania Funkcjonalności AntyDDoS.

### Sposób przeprowadzenia testów Wykonawca zaproponuje oraz uzgodni z kierownikiem projektu Zamawiającego.

# Usługi instalacyjno-konfiguracyjne

Wykonawca jest zobowiązany do wykonania wszystkich prac niezbędnych do uruchomienia transmisji danych w Sieci WAN oraz usługi dostępu do Internetu zgodnie z wymaganiami Umowy, nawet jeżeli prace te nie są wyraźnie wyszczególnione w niniejszym dokumencie, w Umowie i pozostałych załącznikach do niej.

## Uruchomienie głównych i zapasowych Łączy IP VPN MPLS

### dostawa, montaż, konfiguracja i uruchomienie w każdej Lokalizacji infrastruktury telekomunikacyjnej Wykonawcy, w szczególności anten, modemów, mostów i innych urządzeń w ramach infrastruktury Wykonawcy.

## Instalacja Routerów CPE

### dostawa, montaż, konfiguracja i uruchomienie w każdej Lokalizacji dwóch Routerów CPE, każdy dedykowany dla osobnego Łącza IP VPN MPLS.

## Uruchomienie głównych i zapasowych łączy dla dostępu do Internetu

### dostawa, montaż, konfiguracja i uruchomienie w siedzibie Zamawiającego w Warszawie infrastruktury telekomunikacyjnej Wykonawcy, w szczególności anten, modemów, mostów i innych urządzeń w ramach infrastruktury Wykonawcy.

## Konfiguracja Routerów CE

### dostawa, montaż, konfiguracja i uruchomienie w siedzibie Zamawiającego w Warszawie nowo dostarczonych Routerów CE i połączenie z siecią Zamawiającego za pomocą funkcjonalności TRUNK (w tym rekonfiguracja przełączników w zakresie łączy TRUNK do Routerów CE), a także połączenie z łączami Wykonawcy. Demontaż istniejących starych Routerów CE i pozostawienie w Lokalizacji;

### demontaż w Jednostce Terenowej w Goławicach istniejącego Routera CE, przywiezienie do siedziby Zamawiającego w Warszawie i pozostawienie w tej Lokalizacji;

### konfiguracja i uruchomienie w Jednostce Terenowej w Goławicach zdemontowanego wcześniej Routera CE przywiezionego z siedziby Zamawiającego w Warszawie i połączenie z siecią Zamawiającego za pomocą funkcjonalności TRUNK (w tym rekonfiguracja przełączników w zakresie łączy TRUNK do Routerów CE), a także połączenie z łączami Wykonawcy;

### konfiguracja i uruchomienie w Jednostkach Terenowych istniejących Routerów CE i połączenie z siecią Zamawiającego za pomocą funkcjonalności TRUNK (w tym rekonfiguracja przełączników w zakresie łączy TRUNK do Routerów CE), a także połączenie z łączami Wykonawcy;

### konfiguracja i uruchomienie w siedzibie Zamawiającego w Warszawie istniejącego Routera CE dedykowanego do obsługi usługi dostępu do Internetu i połączenie z siecią Zamawiającego za pomocą funkcjonalności TRUNK (w tym rekonfiguracja przełączników w zakresie łączy TRUNK do Routerów CE), a także połączenie z łączami Wykonawcy i drugim dostarczonym na potrzeby usługi dostępu do Internetu Routerem CE.

### instalacja i aktywacja licencji odblokowującej użytkowanie portów TenGigabitEthernet w podlegającym serwisowi Routerze CE CISCO serii ASR1001 ASR1001X-SECK9 oraz licencji odblokowującej zwiększenie wydajności przełączania ruchu. Licencje te zostaną dostarczone przez Zamawiającego na etapie wdrożenia.

## Uruchomienie usługi transmisji danych w Sieci WAN

### skonfigurowanie wymaganej Funkcjonalności Sieci WAN i odtworzenie innych wcześniej istniejących na Routerach CE Funkcjonalności.

## Uruchomienie usługi dostępu do Internetu

### skonfigurowanie wymaganej Funkcjonalności dostępu do Internetu i odtworzenie innych wcześniej istniejących, skonfigurowanych na Routerach CE Funkcjonalności.

## Uruchomienie systemu monitoringu

### dostawa, montaż, konfiguracja i uruchomienie systemu monitoringu.

## Uruchomienie transmisji IP Multicast

Prace należy przeprowadzić dwuetapowo. W pierwszym etapie wykonać dokumentacje projektową. W drugim etapie, po uzyskaniu odbioru projektu, na jego podstawie wykonać wdrożenie i uruchomienie transmisji IP Multicast, a następnie przeprowadzić testy akceptacyjne.

### wykonanie projektu wdrożenia transmisji strumieniowej audio/wideo w Sieci LAN i Sieci WAN w technologii IP Multicast.

#### projekt wdrożenia musi obejmować wszystkie konieczne do wykonania prace. Projekt musi zawierać rysunki ideowe oraz szczegółowy opis zaproponowanego rozwiązania. Wykonany projekt wdrożenia musi charakteryzować się wysoką jakością polegającą m.in. na:

##### czytelnej i zrozumiałej strukturze poszczególnych dokumentów i całego projektu, z podziałem odpowiednio na rozdziały, podrozdziały i sekcje;

##### zachowaniu standardów w sposobie pisania, rozumianych jako zachowanie jednolitej i spójnej struktury, formy i sposobu prezentacji treści poszczególnych dokumentów, fragmentów tego samego dokumentu, jak i całego projektu wdrożenia.

#### w trakcie prac projektowych Wykonawca jest zobowiązany na bieżąco prowadzić uzgodnienia z Kierownikiem projektu Zamawiającego w zakresie proponowanych rozwiązań projektowych. Wszelkie rozwiązania nie uzgodnione wcześniej mogą zostać zakwestionowane na etapie odbioru projektu. W takim wypadku Wykonawca będzie zobowiązany dokonać niezbędnych zmian lub poprawek bez naliczania dodatkowych opłat.

#### projekt wdrożenia transmisji strumieniowej musi być oparty na rozwiązaniach dostępnych w istniejących urządzeniach Sieci WAN (bez zakupu dodatkowych urządzeń lub licencji), dla transmisji strumieniowej IPv4, zarówno dla warstwy L2 w ramach jednego VLAN, jak też z uwzględnieniem routingu multicast w sieci IP w warstwie L3 i obejmować w szczególności następujące zagadnienia:

##### wybór i konfigurację trybu dostarczania danych;

##### wybór i konfigurację rodzaju drzewa dystrybucyjnego dla źródeł i odbiorców sygnału multicast i wskazanie jego najkorzystniejszego umiejscowienia w infrastrukturze sieciowej Zamawiającego;

##### wybór i konfigurację mechanizmu kontroli członkostwa w grupach multicast;

##### wybór i konfigurację protokołu routingu dla multicast z uwzględnieniem mechanizmu zapobiegania pętlom w transmisji multicast;

##### wybór i konfigurację mechanizmu dynamicznego rejestrowania użytkowników w odpowiedniej grupie multicast;

##### wybór i konfigurację mechanizmu ograniczającego przesyłanie pakietów multicast tylko do portów w Przełącznikach Dostępowych, także przełącznikach dostępowych w lokalizacjach Zamawiającego, do których podłączeni są odbiorcy multicast;

##### wybór i konfigurację mechanizmów zabezpieczających transmisję multicast, w tym mechanizmów QoS;

##### wybór i opis mechanizmów kontroli (w tym ograniczania) ruchu multicast;

##### projekt i opis testów sprawdzających poprawność wdrożenia nowej Funkcjonalności Sieci WAN polegającej na transmisji strumieniowej w technologii IP Multicast.

#### projekt wdrożenia podlega protokolarnemu odbiorowi w terminie wskazanym w Szczegółowym harmonogramie Prac.

### wykonanie wdrożenia transmisji strumieniowej audio/wideo w Sieci WAN w technologii IP Multicast. Wdrożenie musi obejmować wszystkie konieczne do wykonania prace.

#### wdrożenie Wykonawca może rozpocząć po protokolarnym odebraniu przez Zamawiającego projektu transmisji strumieniowej audio/wideo w Sieci WAN w technologii IP Multicast.

#### prace muszą być prowadzone przez Wykonawcę w taki sposób, aby utrzymać ciągłość działania Sieci WAN w godzinach pracy Zamawiającego. W razie potrzeby część prac będzie prowadzona po godzinach pracy lub w dniu ustawowo wolne od pracy. O tego rodzaju zastrzeżeniu każdorazowo decyduje Zamawiający.

#### po uruchomieniu Wykonawca w obecności Zamawiającego przeprowadzi testy działania transmisji strumieniowej IP Multicast. Sprzęt oraz oprogramowanie niezbędne do przeprowadzenia testów zapewnia Wykonawca.

#### po wykonaniu wdrożenia Wykonawca wykona dokumentację powykonawczą obejmującą w szczególności:

##### szczegółowy opis wykonanej konfiguracji wraz z listingiem konfiguracji każdego Routera CE;

##### szczegółowy opis, rysunki, screeny wykonanych testów sprawdzających nową Funkcjonalność polegającą na transmisji strumieniowej w technologii IP Multicast i wyniki tych testów;

##### szczegółowy opis procedur zarządzania ruchem multicast w środowisku Zamawiającego, w tym ograniczania ruchu do określonych odbiorców/dodawania kolejnych odbiorców;

##### szczegółowy opis procedur analizy ruchu multicast w środowisku Zamawiającego.

# Instruktaż powdrożeniowy

## Informacje ogólne

### Instruktaż powdrożeniowy musi zostać przeprowadzony dla maksymalnie 8 osób w siedzibie Zamawiającego w Warszawie w sali szkoleniowej, przed odbiorem końcowym, w terminie zgodnym z wymaganiami ogólnego harmonogramu prac;

### Instruktaż nie może trwać krócej niż **2 dni** po minimum 4 godziny zegarowe bez wliczania przerw;

### Uczestnicy muszą dostać materiały szkoleniowe zawierające wszystkie informacje i rysunki, które będą omawiane podczas instruktażu;

### Uczestnicy muszą dostać instrukcję obsługi systemu monitoringu w wersji papierowej oraz w wersji elektronicznej w formacie PDF.

## Zakres instruktażu

### Omówienie wykonanej i skonfigurowanej dla Zamawiającego sieci telekomunikacyjnej na podstawie informacji, które musi zawierać dokumentacja powykonawcza, zgodnie z opisem w części: *Dokumentacja powykonawcza*, w szczególności:

#### omówienie wykonanych instalacji związanych z siecią IP VPN MPLS, tj. jakie zastosowano media transmisyjne w każdej z Lokalizacji, w jaki sposób dociągnięto te media do serwerowni, gdzie zostały zainstalowane i jak je zasilono;

#### podział wykonanych instalacji pod względem instalacji dla głównego i zapasowego Łącza IP VPN MPLS ze szczególnym uwzględnieniem rozdziału toru transmisji danych, tj. żeby każde z łączy było zrealizowane za pomocą innego medium transmisyjnego;

#### omówienie schematu ideowego i adresacji IP wykonanej sieci IP VPN MPLS;

#### omówienie schematu połączeń i adresacji IP dla Sieci WAN (w tym Routerów CE).

### Omówienie obsługi Routerów CE w zakresie dotyczącym wymaganej Funkcjonalności, zgodnie z opisem w części: *Specyfikacja Funkcjonalności usługi transmisji danych w Sieci WAN* oraz w części: *Specyfikacja Funkcjonalności usługi dostępu do Internetu*, w szczególności dokładne omówienie na przykładzie Jednostek Terenowych w Gdańsku i Goławicach oraz siedziby Zamawiającego w Warszawie:

#### konfiguracji zabezpieczeń Routerów CE w tym kodów dostępu dla użytkowników;

#### konfiguracji routingu statycznego i dynamicznego;

#### konfiguracji VRF;

#### konfiguracji Multicast;

#### konfiguracji każdej z kolejek QoS wraz z ograniczeniami przeciwko nasyceniu Łączy IP VPN MPLS;

#### konfiguracji szyfrowania transmisji danych;

#### konfiguracji funkcjonalności związanej z przełączaniem transmisji danych pomiędzy głównym a zapasowym Łączem IP VPN MPLS;

#### konfiguracji list ACL;

#### konfiguracji HSRP lub systemu równoważnego;

#### konfiguracji adresacji IP dla usługi dostępu do Internetu dla siedziby Zamawiającego w Warszawie;

#### konfiguracji funkcjonalności związanej z przełączaniem transmisji danych pomiędzy głównym a zapasowym łączem dla usługi dostępu do Internetu;

#### konfiguracji DNS;

#### konfiguracji Routerów CE zarówno dla Sieci WAN jak i dla dostępu do Internetu w zakresie współpracy z systemem monitoringu opisanym w części: *System monitoringu*.

### Omówienie obsługi systemu monitoringu w zakresie dotyczącym wymaganej Funkcjonalności, zgodnie z opisem w części: S*ystem monitoringu,* w szczególności:

#### konfigurowanie adresatów i alertów wysyłanych emailem oraz przez SMS;

#### obsługa danych historycznych;

#### wykonywanie i odtwarzanie kopii zapasowych Routerów CE.

# Instruktaż techniczny

## Informacje ogólne

### Wymagane jest przeprowadzenie instruktażu przez specjalistyczne firmy zajmujące się świadczeniem tego typu usług zawodowo i posiadające autoryzację producentów Routerów CE na prowadzenie instruktażu.

### Program samego instruktażu w części dotyczącej posiadanych Routerów CE musi być autoryzowany przez producenta posiadanych Routerów CE, a w części dotyczącej nowo dostarczonych Routerów CE innego producenta niż posiadane Routery CE autoryzowany przez producenta tych nowo dostarczanych Routerów CE.

### Przeprowadzenie instruktażu technicznego jest opcjonalne. Zamawiający może wymagać przeprowadzenia wszystkich zajęć, ich części, także dla mniejszej ilości osób, albo zrezygnować z całości.

### Zamawiający będzie rozliczał przeprowadzenie instruktażu osobno dla każdego uczestnika, dla każdego faktycznie przeprowadzonego instruktażu.

### Zamawiający oświadcza, że wymagany instruktaż techniczny będzie miał charakter usługi kształcenia zawodowego i w całości finansowany będzie ze środków publicznych zgodnie z art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2001 r. Nr 177, poz. 1054 ze zm.).

### Jeżeli w okresie obowiązywania Umowy zaproponowany przez Wykonawcę instruktaż zostanie wycofany przez producenta Routerów CE, Wykonawca zaproponuje jeden instruktaż, lub kilka, które swoim zakresem obejmą łączną wskazaną poniżej wymagana tematykę.

### Instruktaż techniczny ma na celu objaśnienie działania i obsługi Routerów CE wraz z komponentami dla maksymalnie 2 pracowników Zamawiającego w terminie bądź terminach uzgodnionych z Zamawiającym.

### Każdy z uczestników instruktażu otrzyma imienny certyfikat uczestnictwa w danym instruktażu.

### Wykonawca przeprowadzi instruktaż teoretyczny i praktyczny (w stosunku czasowym 1:1) w języku polskim. Zakres obejmuje zagadnienia konieczne do poprawnego administrowania dostarczonymi Routerami CE i kontrolowania Funkcjonalności transmisji danych w Sieci WAN oraz dostępu do Internetu, w tym wykrywania nieprawidłowości.

### W ramach instruktażu Wykonawca zapewni kompletną i szczegółową dokumentację instruktorską, w tym podręczniki, w języku polskim lub angielskim, w szczególności dokładnie objaśnione zagadnienia teoretyczne dla stosowanych rozwiązań technicznych, opis dla wykonywanych ćwiczeń oraz opis praktycznego administrowania Routerami CE.

### Wykonawca dostosuje testowe środowisko techniczne w taki sposób, żeby każdy uczestnik instruktażu mógł **samodzielnie** wykonać ćwiczenia, w szczególności konfigurację, analizę działania i diagnozowanie błędów.

### Zajęcia muszą trwać minimum 7 godzin licząc na każdy dzień bez wliczania przerw na posiłek (wymagany przynajmniej jeden posiłek dziennie).

### Kolejność zajęć zostanie zaproponowana przez Wykonawcę w taki sposób, żeby zachować logiczną ciągłość instruktażu.

### Przerwa pomiędzy cyklami tematycznymi zajęć nie może być krótsza niż 2 tygodnie.

### Instruktaż w całości musi być przeprowadzony w Warszawie.

### Instruktaż musi być przeprowadzony przez osoby posiadające przynajmniej certyfikaty inżynierskie producenta w zakresie koniecznym do przeprowadzenia danego zakresu instruktażu.

### Instruktaż musi zostać przeprowadzony w terminie uzgodnionym wcześniej z Zamawiającym, zgodnym z wymaganiami Harmonogramu wykonywania prac, przy czym rozliczany jest oddzielnie i termin realizacji poszczególnych etapów instruktażu nie warunkuje odbioru końcowego.

## Zakres i podział tematyczny instruktażu przewidzianego dla Routerów CE firmy CISCO

W związku z posiadaniem przez Zamawiającego Routerów CE firmy CISCO Wykonawca musi zapewnić przeprowadzenie instruktażu z naciskiem na obsługę i implementację niżej wymienionych Funkcjonalności w routerach firmy CISCO. Instruktaż należy przeprowadzić w podziale na podane niżej cykle tematyczne.

### Instruktaż: Konfiguracja routingu Sieci LAN i Sieci WAN

Certyfikowany instruktaż „Implementing Cisco IP Routing (ROUTE) v2.0” lub równoważny zakresem (instruktaże równoważne) musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### planowanie i dokumentowanie konfiguracji i weryfikacji protokołów routingu oraz optymalizacji ich pracy w sieciach przedsiębiorstw;

#### identyfikacja technologii, komponentów i metryki użytej w protokole routingu dynamicznego w oparciu o wymagania różnych technologii sieciowych, w tym posiadanej przez Zamawiającego technologii EIGRP zaimplementowanej w Routerach CE i sieci komputerowej w siedzibie w Warszawie;

#### identyfikacja i analiza funkcji routingu protokołu OSPF działającego w ramach wielu obszarów (multiarea OSPF), analiza efektywności wykorzystania OSPF w złożonych instalacjach sieciowych;

#### implementacja i weryfikacji redystrybucji tras w złożonym środowisku sieciowym, wykorzystującym kilka protokołów routingu dynamicznego. Implementacja funkcji systemu IOS wspomagających optymalny wybór ścieżki dla pakietów, metody eliminacji pętli routingu;

#### ocena wydajności sieci i dobór narzędzi wymaganych dla dostarczenia mechanizmów kontroli ścieżki dla ruchu pakietów;

#### implementacja i weryfikacja rozwiązań warstwy 3, wykorzystujących protokół BGP w celu podłączenia sieci przedsiębiorstwa do sieci dostawcy Internetu (ISP).

### Instruktaż: Implementacja Multicast w sieciach LAN i WAN

Certyfikowany instruktaż „CISCO Multicast (MCAST) v2” lub równoważny zakresem (instruktaże równoważne) musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### koncepcje i technologie ruchu typu IP Multicast;

#### omówienie praktycznej implementacji ruchu multicast w Sieci LAN;

#### omówienie protokołu PIM sparse mode;

#### omówienie inżynierii RP (Randezvous Point) -Auto-RP, PIMv2 BSR, Anycast RP, MSDP;

#### omówienie rozszerzenia protokołu PIM Sparse Mode – SSM, SSM z IGMPv3, Bidirectional PIM;

#### omówienie rozszerzenia protokołu BGP (MP-BGP) – SSM, MSDP;

#### omówienie i praktyczna implementacja ruchu multicastowego pomiędzy domenami;

#### omówienie i praktyczna implementracja mechanizmów bezpieczeństwa ruchu IP Multicast;

#### optymalizacja multicastów i cechy wysokiej dostępności;

#### przegląd aplikacji multicastowych.

### Instruktaż: Implementacja QoS w Sieci WAN

Certyfikowany instruktaż „Implementing CISCO Quality of Service (QoS)” lub równoważny zakresem (instruktaże równoważne) musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### omówienie modeli Implementacyjnych QoS;

#### przegląd technik i metod QoS;

#### omówienie metod AutoQoS i AutoQoS Enterprise;

#### omówienie klasyfikacji i oznaczania ruchu w sieciach IP;

#### zarządzanie spiętrzeniami (kolejkowanie ruchu);

#### zapobieganie zatorom;

#### ograniczanie (policing) i kształtowanie (shaping) ruchu;

#### optymalizacja wykorzystania łączy;

#### przykłady implementacji (best Practices).

### Instruktaż: Konfiguracja MPLS w Sieci LAN i Sieci WAN

Certyfikowany instruktaż „Implementing CISCO MPLS (MPLS) v3.0” lub równoważny zakresem (instruktaże równoważne) musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### koncepcje MPLS

##### wprowadzenie do podstawowych koncepcji MPLS;

##### etykieta MPLS i stos etykiet;

##### aplikacje MPLS.

#### przydział i dystrybucja etykiet

##### dystrybucja etykiet dla tryby pracy typu frame-mode MPLS;

##### konwergencja w trybie pracy typu frame-mode MPLS;

##### modele alokacji, dystrybucji i zachowania etykiet;

##### odkrywanie sąsiadów za pomocą LDP.

#### implementacja typu frame-mode MPLS

##### wprowadzenie do przełączania typu CEF switching;

##### konfigurowanie typu frame-mode MPLS;

##### monitorowanie trybu pracy typu frame-mode MPLS;

##### diagnozowanie trybu pracy typu frame-mode MPLS.

#### technologia sieci typu MPLS VPN

##### wprowadzenie do sieci VPN;

##### modele sieci typu overlay and peer-to-peer;

##### kategorie sieci VPN;

##### wprowadzenie do architektury MPLS VPN;

##### wprowadzenie do modelu routingu w MPLS VPN;

##### przesyłanie pakietów w MPLS VPN.

#### wdrażanie MPLS VPN

##### wykorzystanie mechanizmów MPLS VPN;

##### konfigurowanie tablicy VFR;

##### konfigurowanie sesji MP-BGP pomiędzy routerami PE;

##### konfigurowanie protokołów routingu (ścieżki statyczne, RIP, EIGRP) pomiędzy urządzeniami PE i CE;

##### monitorowanie pracy MPLS VPN;

##### konfigurowanie protokołu OSPF pomiędzy urządzeniami PE i CE;

##### konfigurowanie protokołu BGP pomiędzy urządzeniami PE i CE;

##### diagnozowanie MPLS VPN.

#### złożone MPLS VPN

##### VPN typu overlapping;

##### centralne usługi w VPN;

##### usługi typu managed CE routers services;

##### usługi typu MPLS Managed Services.

#### dostęp do Internetu poprzez MPLS VPN

##### topologie dostępu do sieci Internet z sieci MPLS VPN;

##### metody dostępu do Internetu z MPLS VPN;

##### oddzielenie dostępu do Internetu od usług VPN;

##### dostęp do sieci Internet za pomocą oddzielnego VPN;

##### omówienie MPLS TE;

##### wprowadzenie do koncepcji zarządzania ruchem (TE);

##### składowe MPLS TE;

##### konfigurowanie MPLS TE;

##### monitorowanie MPLS TE.

### Zaawansowany instruktaż typu bootcamp, który musi zostać przeprowadzony jako ostatni, po wcześniejszym przeprowadzeniu pozostałych instruktaży: Praktyczne zarządzanie sieciami LAN i WAN

Certyfikowany instruktaż „Advanced Routing & Switching Bootcamp (ADVRSBC)” lub równoważny zakresem (instruktaże równoważne) musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### podstawy sieci i urządzeń sieciowych

##### transmisja sieciowe, dane pakietowe, unicast, multicast, broadcast, usługi połączeniowe i bezpołączeniowe, topologie;

##### modele ISO/OSI/Internet/warstwowe, enkapsulacja, PDU, SDU;

##### używanie poprawnej terminologii: bity, pakiety, ramki, datagramy, segmenty;

##### organizacje standaryzacyjne i inne: IETF, IEEE, IANA, RIPE, dokumenty RFC;

##### stosy IP Windows i Linux;

##### wgląd w pakiety: sniffery, analizatory, tcpdump, Wireshark;

##### dostęp do urządzeń Cisco poprzez IPv4 oraz IPv6;

##### podstawy protokołów IPv4/IPv6. Wymiana informacji, routing, przełączanie;

##### protokoły TCP/UDP/inne;

##### metody dostępu do urządzeń Cisco, CLI/GUI/inne;

##### kontrola lokalna i zdalna dostępu Telnet/SSH, linie terminalowe i ich parametry;

##### zarządzanie użytkownikami lokalnymi, no aaa new-model, lokalne AAA;

##### protokoły AAA: RADIUS i Tacacs;

##### efektywne CLI: filtry, aliasy, ranges, itp.;

##### systemy plików IOS, protokoły wymiany TFTP/FTP/SCP. Zarządzanie oprogramowaniem;

##### zarządzanie konfiguracjami, config replace, funkcjonalność archive;

##### podstawy kryptografii: hashe MD5/SHA, szyfrowanie, klucze symetryczne i asymetryczne;

##### bezpieczeństwo konfiguracji, plain text, ochrona haseł;

##### opisywanie interfejsów;

##### właściwe logowanie: ustawienia syslog, NTP, Embedded Syslog Manager (ESM);

##### bezpieczniki errdisable;

##### wprowadzenie do architektur urządzeń sieciowych;

##### Control / Data / Management plane, dane tranzytowe i lokalne.

#### podstawowa praca sieci Ethernet / IP

##### Ethernet i jego standardy: miedziane i optyczne, 10/100G, monitorowanie i diagnostyka, TDR;

##### struktura i adresacja ramek, unicast i multicast, bit U/L;

##### Internet Protocol, adresy IPv4, IPv6, planowanie adresacji;

##### multicasty w L3, IPv4 i IPv6;

##### IPv4 ARP kontra IPv6 Neighbor Discovery, funkcje ICMPv4 oraz ICMPv6;

##### DHCP w IPv4 oraz IPv6;

##### opcje IPv4, nagłówki rozszerzeń IPv6;

##### praca protokołów TCP oraz UDP;

##### praca hosta w sieci IP, wiele interfejsów, interfejs źródłowy ruchu;

##### brama domyślna, redundancja bramy domyślnej, potrzeba FHRP (HSRP/GLBP/VRRP) w IPv4 and IPv6;

##### wpływ MTU na ruch, fragmentacja w IPv4 i IPv6, PMTUD;

##### znaczniki QoS w ramkach i pakietach;

##### podstawy troubleshootingu i diagnostyki, metodologia;

##### narzędzia diagnostyczne IOS oraz Open Source;

##### przełączanie L2 i L3;

##### praca przełącznika Ethernet, tablica przełączania, implementacja, skalowalność;

##### praca routera, tablica routingu, metryka, admin distance, przełączanie L3;

##### wiele podsieci IP: IPv4 secondary, kilka podsieci IPv6;

##### tablica przełączania: podział na RIB i FIB, przełączanie CEF (Cisco Express Forwarding);

##### wirtualizacja przełączania L2 i L3, co to jest VPN, taksonomia VPN;

##### wirtualizacja przełączania L2 (VLANy, VLAN database, zarządzanie VLANami, VTP);

##### wirtualizacja przełączania L3, VRF;

##### łączenie L2 i L3, trunki 802.1q;

##### praca współczesnych przełączników: multilayer i L3, porty switched, routed, subinterfejsy;

##### najprostsza wymiana informacji między tablicami urządzeń, VRF-Lite;

##### klasyczne brydżowanie na routerze;

##### dokumentacja sieci;

##### brama domyślna kontra trasa domyślna;

##### powiązanie między L2 i L3, timery ARP / ND / MAC;

##### interfejsy wirtualne: null, loopback, tunnel, SVI, virtual-template, NVI;

##### zarządzania VRF, VRF i interfejs źródłowy ruchu wysyłanego przez urządzenie;

##### przeskakiwanie między urządzeniami

##### podstawy IP multicast;

##### filozofia przełączania multicast;

##### kontrola dołączania do sieci multicast: IGMP/MLD. IGMP snooping;

##### routing PIM.

#### topologie sieciowe

##### zarządzanie topologiami Ethernet/IP;

##### topologie L1, L2, L3, inne;

##### zarządzanie topolgią L2 poprzez STP: PVSTP, PVRSTP, MST, narzędzia STP;

##### architektura sieci kampusowej;

##### interakcja między L2 i L3 oraz FHRP;

##### topologie wirtualne L2, połączenia fizyczne, logiczne, kanały (PVC, SVC), NBMA;

##### technologie starożytne: Frame Relay, ATM;

##### NBMA w Ethernet: private VLANs;

##### ścieżki równoległe: ECMP (Equal-Cost MultiPath), ECMP CEF load-sharing;

##### ścieżki równoległe: L2/L3 portchannel, 802.3ad/PAgP/LACP;

##### wykrywanie topologii poprzez MAC/ARP/CDP/LLDP, ping, traceroute, STP, itp.

#### wirtualizacja i tunelowanie

##### tunelowanie L2: ukrywanie tagów, QinQ, 802.1ad;

##### globalna i lokalna pula VLANów;

##### tunelowanie MAC: Provider Backbone Bridging, 802.1ah;

##### infrastruktura Carrier Etherhet;

##### tunelowanie L3: GRE, non-IP, multipoint GRE, konieczność NHRP, tunele IPv6;

##### ukrywanie adresacji poprzez NATv4, NATv6, ALG, kontrola routingu poprzez NAT;

##### generyczny mechanizm tunelowania: labelki, wprowadzenie do filozofii i aplikacji MPLS;

##### wirtualizacja urządzeń, urządzenia logiczne, VDC, stakowanie, VSS, extenders, moduły wyniesione;

##### wpływ wirtualizacji na zagadnienia projektowe.

#### kontrola ruchu typu data plane

##### walidacja ruchu wchodzącego: statyczna, anti-spoofing;

##### ACL na przełączniku L3: PACL, RACL, VACL, implementacja storm control;

##### prosta kontrola MAC: ACLki MAC, port-security;

##### dynamiczna kontrola, anti-spoofing, DHCP snooping, uRPF, source guard;

##### walidacja ARP;

##### zaawansowana kontrola: 802.1x / EAP / MAB;

##### podstawy QoS: klasyfikacja, oznaczanie, policing, wygładzanie, WRED, QoS na routerze i przełączniku;

##### monitorowanie ruchu tranzytowego;

##### statystyki, liczniki, NetFlow;

##### przechwytywanie ruchu, SPAN/RSPAN/ERSPAN, VLAN filters, Embedded Packet Capture;

##### budowa konfiguracji Data Plane, makra, wzorce, AutoConf;

##### tworzenie rekomendowanego wzorca konfiguracji Data Plane;

##### podstawy technologii szyfrowania, IPSec (S2S, RA), GETVPN, SSL, Flex, MACSec, 802.3ae;

##### funkcje firewalli, IOS firewall;

##### PoE i wsparcie dla telefonii IP, Voice VLAN;

##### EEM (Embedded Event Manager).

#### zaawansowane zarządzanie siecią

##### narzędzia dynamiki: IP SLA, Enhanced Object Tracking (EOT);

##### omijanie tablicy routingu poprzez Policy-Based Routing (PBR);

##### routing statyczny nie taki statyczny: opcje ‚ip route’ + EOT + IP SLA + EEM;

##### podstawy routingu dynamicznego, źródła informacji routingowej;

##### osiągalność (reachability) kontra topologia (topology);

##### klasy protokołów routingu: Distance-Vector / Link State / Path Vector;

##### system Autonomiczny (AS), routing wewnątrz i pomiędzy AS;

##### uruchamianie routingu EIGRP, OSPF, IS-IS, BGP;

##### komenda ‚network’ i jej dwie funkcje, konfiguracje AF w OSPF i EIGRP;

##### uwierzytelnianie sąsiadów i informacji routingowej;

##### rozgłaszanie sieci, natywne i redystrybucja;

##### równoległe procesy routingu, ships in the night, IPv4/IPv6 dual stack, tablice protokołów;

##### kontrolowanie metryki, mechanizmy unikania pętli w protokołach routingu;

##### rozgłaszanie trasy domyślnej;

##### kontrolowanie topologii – segmentacja sieci, podział na regiony, obszary i systemy autonomiczne;

##### znakowanie informacji routingowej, tagi, community;

##### narzędzia kontroli routingu: prefix-listy, route-mapy, RPL (Route Policy Language);

##### redystrybucja informacji między protokołami;

##### redukcja prefiksów: sumaryzacja, agregacja, filtrowanie, routing stub (EIGRP, OSPF).

#### kontrola ścieżki i topologii

##### proces konwergencji: składowe, analiza procesu;

##### przyśpieszanie konwergencji, tuning protokołów, BFD (Bidirectional Forwarding Detection);

##### zarządzanie FIB: priorytetyzacja prefiksów, Prefix Independent Convergence (PIC);

##### stabilizacja informacji: dampening;

##### budowa rekomendowanej konfiguracji routingu;

##### fałszywe ścieżki: blackholing;

##### pułapki FHRP: suboptymalny routing, pułapki agregacji prefiksów;

##### celowy blackholing: RTBH (Remote Triggered BlackHoling);

##### pętle w sieci: informacji, danych, mikropętle, pętle sąsiedztwa, nieskończona rekurencja;

##### budowa ścieżek z wykorzystaniem MPLS: L2VPN, L3VPN, MPLS over GRE;

##### ścieżki zapasowe: EIGRP feasible successor, IP LFA, BGP AddPath;

##### dodatkowe narzędzia do kontroli ścieżki w BGP: AS\_PATH ACL, community lists;

##### kontrola ruchu wchodzącego i wychodzącego;

##### asymetria routingu, routing nieoptymalny;

##### wzajemna redystrybucja, migracja protokołów routingu;

##### automatyczna kontrola ścieżki z wykorzystaniem PfR (Performance Routing);

##### topologie zaawansowane i sieci nakładkowe;

##### VRF a VPN, złożone VPN, wymiana informacji między VPN;

##### proste sieci nakładkowe, L2TPv3, MPLS AToM;

##### sieci nakładkowe NVGRE, OTV, VxLAN;

##### podstawy routingu dynamicznego, trzy źródła informacji routingowej;

##### osiągalność (reachability) kontra topologia (topology);

##### klasy protokołów routingu: Distance-Vector / Link State / Path Vector;

##### system Autonomiczny (AS), routing wewnątrz i pomiędzy AS;

##### uruchamianie routingu EIGRP, OSPF, IS-IS, BGP;

##### komenda ‚network’ i jej dwie funkcje, konfiguracje AF w OSPF i EIGRP;

##### uwierzytelnianie sąsiadów i informacji routingowej;

##### rozgłaszanie sieci, natywne i redystrybucja;

##### równoległe procesy routingu, ships in the night, IPv4/IPv6 dual stack, tablice protokołów;

##### kontrolowanie metryki, mechanizmy unikania pętli w protokołach routingu;

##### rozgłaszanie trasy domyślnej;

##### kontrolowanie topologii – segmentacja sieci, podział na regiony, obszary i systemy autonomiczne;

##### znakowanie informacji routingowej, tagi, community;

##### narzędzia kontroli routingu: prefix-listy, route-mapy, RPL (Route Policy Language);

##### redystrybucja informacji między protokołami;

##### redukcja prefiksów: sumaryzacja, agregacja, filtrowanie, routing stub (EIGRP, OSPF).

## Zakres i podział tematyczny instruktażu przewidzianego dla Routerów CE innej firmy niż CISCO

W przypadku dostarczenia Routerów CE innej firmy niż CISCO Wykonawca musi zapewnić **dodatkowo** przeprowadzenie instruktażu z naciskiem na obsługę i implementację niżej wymienionych Funkcjonalności w Routerach CE danej firmy. Oznacza to, że w przypadku przeprowadzenia danego instruktażu dla urządzeń firmy CISCO Wykonawca jest zobowiązany jednocześnie zapewnić przeprowadzenie dodatkowego analogicznego instruktażu certyfikowanego przez producenta dostarczonych Routerów CE w podziale na podane niżej cykle tematyczne.

### Instruktaż: Konfiguracja routingu Sieci LAN i Sieci WAN

Certyfikowany instruktaż musi trwać minimum 5 Dni Roboczych i obejmować zakresem minimum następującą tematykę:

#### planowanie i dokumentowanie konfiguracji i weryfikacji protokołów routingu oraz optymalizacji ich pracy w sieciach przedsiębiorstw;

#### identyfikacja technologii, komponentów i metryki użytej w protokole routingu dynamicznego w oparciu o wymagania różnych technologii sieciowych, w tym posiadanej przez Zamawiającego technologii EIGRP zaimplementowanej w Routerach CE i sieci komputerowej w siedzibie w Warszawie;

#### identyfikacja i analiza funkcji routingu protokołu OSPF działającego w ramach wielu obszarów (multiarea OSPF), analiza efektywności wykorzystania OSPF w złożonych instalacjach sieciowych;

#### implementacja i weryfikacji redystrybucji tras w złożonym środowisku sieciowym, wykorzystującym kilka protokołów routingu dynamicznego. Implementacja funkcji systemu IOS wspomagających optymalny wybór ścieżki dla pakietów, metody eliminacji pętli routingu;

#### ocena wydajności sieci i dobór narzędzi wymaganych dla dostarczenia mechanizmów kontroli ścieżki dla ruchu pakietów;

#### implementacja i weryfikacja rozwiązań warstwy 3, wykorzystujących protokół BGP w celu podłączenia sieci przedsiębiorstwa do sieci dostawcy Internetu (ISP).

### Instruktaż: Implementacja Multicast w sieciach LAN i WAN

Certyfikowany instruktaż musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### koncepcje i technologie ruchu typu IP Multicast;

#### omówienie praktycznej implementacji ruchu multicast w Sieci LAN;

#### omówienie protokołu PIM sparse mode;

#### omówienie inżynierii RP (Randezvous Point) -Auto-RP, PIMv2 BSR, Anycast RP, MSDP;

#### omówienie rozszerzenia protokołu PIM Sparse Mode – SSM, SSM z IGMPv3, Bidirectional PIM;

#### omówienie rozszerzenia protokołu BGP (MP-BGP) – SSM, MSDP;

#### omówienie i praktyczna implementacja ruchu multicastowego pomiędzy domenami;

#### omówienie i praktyczna implementracja mechanizmów bezpieczeństwa ruchu IP Multicast;

#### optymalizacja multicastów i cechy wysokiej dostępności;

#### przegląd aplikacji multicastowych.

### Instruktaż obejmujący zakres: Implementacja QoS w Sieci WAN

Certyfikowany instruktaż musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### omówienie modeli Implementacyjnych QoS;

#### przegląd technik i metod QoS;

#### omówienie metod AutoQoS i AutoQoS Enterprise;

#### omówienie klasyfikacji i oznaczania ruchu w sieciach IP;

#### zarządzanie spiętrzeniami (kolejkowanie ruchu);

#### zapobieganie zatorom;

#### ograniczanie (policing) i kształtowanie (shaping) ruchu;

#### optymalizacja wykorzystania łączy;

#### przykłady implementacji (best Practices).

### Instruktaż obejmujący zakres: Konfiguracja MPLS w Sieci LAN i Sieci WAN

Certyfikowany instruktaż musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### koncepcje MPLS

##### wprowadzenie do podstawowych koncepcji MPLS;

##### etykieta MPLS i stos etykiet;

##### aplikacje MPLS.

#### przydział i dystrybucja etykiet

##### dystrybucja etykiet dla tryby pracy typu frame-mode MPLS;

##### konwergencja w trybie pracy typu frame-mode MPLS;

##### modele alokacji, dystrybucji i zachowania etykiet;

##### odkrywanie sąsiadów za pomocą LDP.

#### implementacja typu frame-mode MPLS

##### wprowadzenie do przełączania typu CEF switching;

##### konfigurowanie typu frame-mode MPLS;

##### monitorowanie trybu pracy typu frame-mode MPLS;

##### diagnozowanie trybu pracy typu frame-mode MPLS.

#### technologia sieci typu MPLS VPN

##### wprowadzenie do sieci VPN;

##### modele sieci typu overlay and peer-to-peer;

##### kategorie sieci VPN;

##### wprowadzenie do architektury MPLS VPN;

##### wprowadzenie do modelu routingu w MPLS VPN;

##### przesyłanie pakietów w MPLS VPN.

#### wdrażanie MPLS VPN

##### wykorzystanie mechanizmów MPLS VPN;

##### konfigurowanie tablicy VFR;

##### konfigurowanie sesji MP-BGP pomiędzy routerami PE;

##### konfigurowanie protokołów routingu (ścieżki statyczne, RIP, inne) pomiędzy urządzeniami PE i CE;

##### monitorowanie pracy MPLS VPN;

##### konfigurowanie protokołu OSPF pomiędzy urządzeniami PE i CE;

##### konfigurowanie protokołu BGP pomiędzy urządzeniami PE i CE;

##### diagnozowanie MPLS VPN.

#### złożone MPLS VPN

##### VPN typu overlapping;

##### centralne usługi w VPN;

##### usługi typu managed CE routers services;

##### usługi typu MPLS Managed Services.

#### dostęp do Internetu poprzez MPLS VPN

##### topologie dostępu do sieci Internet z sieci MPLS VPN;

##### metody dostępu do Internetu z MPLS VPN;

##### oddzielenie dostępu do Internetu od usług VPN;

##### dostęp do sieci Internet za pomocą oddzielnego VPN;

##### omówienie MPLS TE;

##### wprowadzenie do koncepcji zarządzania ruchem (TE);

##### składowe MPLS TE;

##### konfigurowanie MPLS TE;

##### monitorowanie MPLS TE.

### Zaawansowany instruktaż typu bootcamp, który musi zostać przeprowadzony jako ostatni, po wcześniejszym przeprowadzeniu pozostałych instruktaży: Praktyczne zarządzanie sieciami LAN i WAN

Certyfikowany instruktaż musi trwać minimum 5 Dni Roboczych i obejmować minimum następującą tematykę:

#### podstawy sieci i urządzeń sieciowych

##### transmisja sieciowe, dane pakietowe, unicast, multicast, broadcast, usługi połączeniowe i bezpołączeniowe, topologie;

##### modele ISO/OSI/Internet/warstwowe, enkapsulacja, PDU, SDU;

##### używanie poprawnej terminologii: bity, pakiety, ramki, datagramy, segmenty;

##### organizacje standaryzacyjne i inne: IETF, IEEE, IANA, RIPE, dokumenty RFC;

##### stosy IP Windows i Linux;

##### wgląd w pakiety: sniffery, analizatory, tcpdump, Wireshark;

##### dostęp do urządzeń poprzez IPv4 oraz IPv6;

##### podstawy protokołów IPv4/IPv6. Wymiana informacji, routing, przełączanie;

##### protokoły TCP/UDP/inne;

##### metody dostępu do urządzeń, CLI/GUI/inne;

##### kontrola lokalna i zdalna dostępu Telnet/SSH, linie terminalowe i ich parametry;

##### zarządzanie użytkownikami lokalnymi, lokalne AAA;

##### protokoły AAA: RADIUS i TACACS;

##### system plików, protokoły wymiany TFTP/FTP/SCP. Zarządzanie oprogramowaniem;

##### zarządzanie konfiguracjami, funkcjonalność archiwizacji;

##### podstawy kryptografii: hashe MD5/SHA, szyfrowanie, klucze symetryczne i asymetryczne;

##### bezpieczeństwo konfiguracji, ochrona haseł;

##### opisywanie interfejsów;

##### właściwe logowanie: ustawienia syslog, NTP.

#### podstawowa praca sieci Ethernet / IP

##### Ethernet i jego standardy: miedziane i optyczne, 10/100G, monitorowanie i diagnostyka;

##### multicasty w L3, IPv4 i IPv6;

##### IPv4 ARP kontra IPv6 Neighbor Discovery, funkcje ICMPv4 oraz ICMPv6;

##### DHCP w IPv4 oraz IPv6;

##### opcje IPv4, nagłówki rozszerzeń IPv6;

##### praca protokołów TCP oraz UDP;

##### praca hosta w sieci IP, wiele interfejsów, interfejs źródłowy ruchu;

##### brama domyślna, redundancja bramy domyślnej, potrzeba FHRP (GLBP/VRRP) w IPv4 and IPv6;

##### znaczniki QoS w ramkach i pakietach;

##### podstawy troubleshootingu i diagnostyki, metodologia;

##### narzędzia diagnostyczne;

##### przełączanie L2 i L3;

##### praca przełącznika Ethernet, tablica przełączania, implementacja, skalowalność;

##### praca routera, tablica routingu, metryka, admin distance, przełączanie L3;

##### wiele podsieci IP: IPv4 secondary, kilka podsieci IPv6;

##### tablica przełączania;

##### wirtualizacja przełączania L2 i L3, VPN, taksonomia VPN;

##### wirtualizacja przełączania L2 (VLANy, VLAN database, zarządzanie VLANami, VTP);

##### wirtualizacja przełączania L3, VRF;

##### łączenie L2 i L3, trunki 802.1q;

##### praca współczesnych przełączników: multilayer i L3, porty switched, routed, subinterfejsy;

##### wymiana informacji między tablicami urządzeń, VRF-Lite;

##### klasyczne brydżowanie na routerze;

##### brama domyślna, trasa domyślna;

##### powiązanie między L2 i L3, timery ARP / ND / MAC;

##### interfejsy wirtualne;

##### zarządzania VRF, VRF i interfejs źródłowy ruchu wysyłanego przez urządzenie;

##### przeskakiwanie między urządzeniami;

##### podstawy IP multicast;

##### filozofia przełączania multicast;

##### kontrola dołączania do sieci multicast;

##### routing PIM.

#### topologie sieciowe

##### zarządzanie topologiami Ethernet/IP;

##### topologie L1, L2, L3, inne;

##### zarządzanie topolgią L2 poprzez STP: PVSTP, PVRSTP, MST, narzędzia STP;

##### architektura sieci kampusowej;

##### interakcja między L2 i L3 oraz FHRP;

##### topologie wirtualne L2, połączenia fizyczne, logiczne, kanały (PVC, SVC), NBMA;

##### NBMA w Ethernet: private VLANs;

##### ścieżki równoległe: L2/L3 portchannel, 802.3ad/PAgP/LACP;

##### wykrywanie topologii poprzez MAC/ARP/LLDP, ping, traceroute, STP, itp.

#### wirtualizacja i tunelowanie

##### tunelowanie L2: ukrywanie tagów, QinQ, 802.1ad;

##### globalna i lokalna pula VLANów;

##### tunelowanie MAC: Provider Backbone Bridging, 802.1ah;

##### tunelowanie L3: GRE, non-IP, multipoint GRE, konieczność NHRP, tunele IPv6;

##### ukrywanie adresacji poprzez NATv4, NATv6, ALG, kontrola routingu poprzez NAT;

##### generyczny mechanizm tunelowania: labelki, wprowadzenie do filozofii i aplikacji MPLS.

#### kontrola ruchu typu data plane

##### walidacja ruchu wchodzącego: statyczna, anti-spoofing;

##### ACL na przełączniku L3: PACL, RACL, VACL, implementacja storm control;

##### prosta kontrola MAC: ACLki MAC, port-security;

##### dynamiczna kontrola, anti-spoofing, DHCP snooping, uRPF, source guard;

##### walidacja ARP;

##### zaawansowana kontrola: 802.1x / EAP / MAB;

##### podstawy QoS: klasyfikacja, oznaczanie, policing, wygładzanie, WRED, QoS na routerze i przełączniku;

##### monitorowanie ruchu tranzytowego;

##### statystyki, liczniki, NetFlow;

##### przechwytywanie ruchu;

##### tworzenie rekomendowanego wzorca konfiguracji;

##### podstawy technologii szyfrowania, IPSec (S2S, RA), , SSL, 802.3ae;

##### funkcje firewalli;

##### PoE i wsparcie dla telefonii IP, Voice VLAN.

#### zaawansowane zarządzanie siecią

##### narzędzia dynamiki: SLA, inne;

##### omijanie tablicy routingu poprzez Policy-Based Routing (PBR);

##### automatyczne zmiany routingu statycznego w zależności od zdarzeń w sieci;

##### podstawy routingu dynamicznego, trzy źródła informacji routingowej;

##### osiągalność (reachability) kontra topologia (topology);

##### klasy protokołów routingu: Distance-Vector / Link State / Path Vector;

##### system Autonomiczny (AS), routing wewnątrz i pomiędzy AS;

##### uruchamianie routingu IGRP, OSPF, IS-IS, BGP;

##### uwierzytelnianie sąsiadów i informacji routingowej;

##### rozgłaszanie sieci, natywne i redystrybucja;

##### kontrolowanie metryki, mechanizmy unikania pętli w protokołach routingu;

##### rozgłaszanie trasy domyślnej;

##### kontrolowanie topologii – segmentacja sieci, podział na regiony, obszary i systemy autonomiczne;

##### znakowanie informacji routingowej, tagi, community;

##### narzędzia kontroli routingu: prefix-listy, route-mapy, RPL (Route Policy Language);

##### redystrybucja informacji między protokołami;

##### redukcja prefiksów: sumaryzacja, agregacja, filtrowanie, routing stub (IGRP, OSPF).

#### kontrola ścieżki i topologii

##### proces konwergencji: składowe, analiza procesu;

##### przyspieszanie konwergencji, tuning protokołów;

##### zarządzanie FIB: priorytetyzacja prefiksów, Prefix Independent Convergence (PIC);

##### stabilizacja informacji: dampening;

##### budowa rekomendowanej konfiguracji routingu;

##### fałszywe ścieżki: blackholing;

##### pułapki FHRP: suboptymalny routing, pułapki agregacji prefiksów;

##### celowy blackholing: RTBH (Remote Triggered BlackHoling);

##### pętle w sieci: informacji, danych, mikropętle, pętle sąsiedztwa, nieskończona rekurencja;

##### budowa ścieżek z wykorzystaniem MPLS: L2VPN, L3VPN, MPLS over GRE;

##### dodatkowe narzędzia do kontroli ścieżki w BGP: AS\_PATH ACL, community lists;

##### kontrola ruchu wchodzącego i wychodzącego;

##### asymetria routingu, routing nieoptymalny;

##### wzajemna redystrybucja, migracja protokołów routingu;

##### automatyczna kontrola ścieżki z wykorzystaniem PfR (Performance Routing);

##### topologie zaawansowane i sieci nakładkowe;

##### VRF a VPN, złożone VPN, wymiana informacji między VPN;

##### proste sieci nakładkowe, L2TPv3, MPLS AToM;

##### sieci nakładkowe NVGRE, OTV, VxLAN;

##### matryce L2; FabricPath, TRILL;

##### podstawy routingu dynamicznego, trzy źródła informacji routingowej;

##### osiągalność (reachability) kontra topologia (topology);

##### klasy protokołów routingu: Distance-Vector / Link State / Path Vector;

##### system Autonomiczny (AS), routing wewnątrz i pomiędzy AS;

##### uruchamianie routingu IGRP, OSPF, IS-IS, BGP;

##### uwierzytelnianie sąsiadów i informacji routingowej;

##### rozgłaszanie sieci, natywne i redystrybucja;

##### równoległe procesy routingu, ships in the night, IPv4/IPv6 dual stack, tablice protokołów;

##### kontrolowanie metryki, mechanizmy unikania pętli w protokołach routingu;

##### rozgłaszanie trasy domyślnej;

##### kontrolowanie topologii – segmentacja sieci, podział na regiony, obszary i systemy autonomiczne;

##### znakowanie informacji routingowej, tagi, community;

##### narzędzia kontroli routingu: prefix-listy, route-mapy, RPL (Route Policy Language);

##### redystrybucja informacji między protokołami;

##### redukcja prefiksów: sumaryzacja, agregacja, filtrowanie, routing stub.

# Dokumentacja powykonawcza

## Informacje wstępne

### Wszystkie kopie dokumentów dołączane do dokumentacji powykonawczej muszą mieć pieczęć i podpis 'za zgodność z oryginałem' osoby uprawnionej do weryfikacji dokumentów.

### Zamawiający wymaga dostarczenia przynajmniej jednego egzemplarza całej dokumentacji w formie drukowanej i dwóch egzemplarzy na płycie CD lub DVD, przy czym Wykonawca dostarczy dokumentację powykonawczą w formie elektronicznej w formatach PDF (tj. skan **podpisanej** dokumentacji papierowej) oraz dodatkowo w formacie specjalistycznym edytowalnym, tj.: dla rysunków projektowych w formacie DWG, a dla dokumentów tekstowych w formacie DOC(X), XLS(X).

## Dokumentacja robót budowlanych

### Dokumentację powykonawczą dotyczącą robót budowlanych Wykonawca opracuje zgodnie z obowiązującymi przepisami prawa. W ramach dokumentacji dotyczącej robót budowlanych dla każdej Lokalizacji w obrębie budynków, na, i w budynkach Zamawiającego muszą znajdować się przynajmniej:

#### mapy projektowe z naniesionymi trasami przyłączy i studzienek rewizyjnych - jeżeli wykonano lub użyto istniejących;

#### projekty wykonawcze instalacji;

#### projekty wykonawcze budowlano-konstrukcyjne;

#### wszelkie zgody i decyzje wynikające z przepisów Prawo budowlane i pokrewnych uzyskane przez Wykonawcę w imieniu Zamawiającego;

#### wszelką korespondencję i decyzje konserwatora zabytków uzyskane przez Wykonawcę w imieniu Zamawiającego, jeżeli wymagane;

#### zgoda na użytkowanie pasma koncesjonowanego, zgodnie z wymaganiami przepisów prawa - dla każdego zamontowanego bezprzewodowego łącza telekomunikacyjnego;

#### dokumenty stwierdzające dopuszczenie użytych materiałów do stosowania w budownictwie;

#### oświadczenie Wykonawcy o wykonaniu robót budowlanych w Lokalizacjach zgodnie z aktualnymi przepisami;

#### dokumenty potwierdzające utylizację odpadów powstałych w toku wykonywanych w Lokalizacjach robót.

### Dokumentacja dotycząca robót budowlanych złożona u Zamawiającego musi zawierać wymagane pieczęcie i podpisy osób uprawnionych do przygotowania tej dokumentacji, w szczególności oświadczenie, podpis i pieczęć osoby uprawnionej **stwierdzające wykonanie robót zgodnie z projektem**.

### Jeden egzemplarz dokumentacji dotyczącej robót budowlanych musi pozostać w Lokalizacji, której dotyczy ta dokumentacja, a drugi Wykonawca dostarczy do siedziby Zamawiającego w Warszawie i dołączy do protokołu odbioru końcowego.

## Pozostała dokumentacja

### W ramach pozostałej dokumentacji Zamawiający wymaga:

#### podania typu i parametrów katalogowych producenta oferowanych Routerów CPE oddzielnie dla każdego rodzaju routera;

#### podania rzeczywistych parametrów łączy Wykonawcy i fizycznego rodzaju każdego z Łączy IP VPN MPLS dla każdej Lokalizacji;

#### podania parametrów łączy dla dostępu do Internetu (tj. rzeczywistych parametrów łączy Wykonawcy) w siedzibie Zamawiającego w Warszawie;

#### podania spisu oraz wartości księgowej brutto na dzień instalacji zainstalowanych w każdej Lokalizacji urządzeń Wykonawcy podlegających zwrotowi po zakończeniu Umowy, w szczególności Routerów CPE;

#### dołączenia kopii licencji na oprogramowanie - jeżeli zostanie takowe wykorzystane w urządzeniach Wykonawcy, w szczególności w systemie monitoringu;

#### dokumentacji (wraz z wynikami pomiarów) pierwszej i drugiej części wykonanych testów akceptacyjnych;

#### dołączenia szczegółowej dokumentacji technicznej producenta dla dostarczanych Routerów CE wraz z zaznaczeniem w tej dokumentacji miejsc potwierdzających spełnianie przez routery wymaganych parametrów;

#### dołączenia certyfikatów, instrukcji obsługi i eksploatacji, haseł, kart gwarancyjnych i innych koniecznych;

#### podania dokładnego opisu, z uzasadnieniem (dla każdej linijki kodu), plików konfiguracyjnych Routera CE lub, jeśli zainstalowano więcej, wszystkich Routerów CE dla Jednostki Terenowej w Gdańsku, Goławicach oraz w siedzibie Zamawiającego w Warszawie, a także wykonaniu kopii zapasowej plików konfiguracyjnych i oprogramowania (IOS) Routerów CE we wszystkich Lokalizacjach;

#### podania dostępu do baz wiedzy dotyczących obsługi i konfiguracji dostarczonych Routerów CE oraz informacji producenta na temat bezpieczeństwa oprogramowania i aktualizacji oprogramowania routerów;

#### podania dokładnego opisu i rysunku topologii dla Sieci WAN;

#### podania dokładnego opisu, tj. procedury dodawania kolejnego oraz usuwania VRF;

#### podania dokładnego opisu i rysunku topologii dla wdrożonego IP Multicast;

#### podania dokładnego opisu, tj. procedury dodawania kolejnego oraz usuwania kanału IP Multicast;

#### podania dokładnego opisu systemu monitoringu, w szczególności instrukcji jego użytkowania w zakresie historycznych danych oraz komunikatów wysyłanych przez ten system;

#### dołączenia oświadczenia Wykonawcy o wykonaniu Łączy IP VPN MPLS i łączy dla dostępu do Internetu, a także systemu monitoringu i Funkcjonalności zgodnie z warunkami technicznymi wymaganymi niniejszym dokumentem;

#### podania danych kontaktowych serwisu Wykonawcy;

#### podania innych danych nie wymienionych powyżej, a koniecznych do kompletacji dokumentacji powykonawczej.

# Współpraca Stron Umowy

## Plan komunikacji Wykonawcy z Zamawiającym

### Możliwe kanały komunikacji to:

#### wideokonferencja (obsługę zapewnia Zamawiający);

#### telefon;

#### e-mail;

#### spotkanie w siedzibie NIK.

## Zasady współpracy

### Wszystkie prace będą realizowane przy udziale lub w konsultacji z pracownikami Zamawiającego.

### Wykonawca będzie konsultował z Zamawiającym wszystkie przyjmowane założenia poczynione w związku z realizacją Umowy. W związku z tym, w razie potrzeby dostarczy wszelkich niezbędnych wyjaśnień i materiałów dodatkowych (opisów, dokumentacji itp.) pracownikom Zamawiającego tak, aby możliwe było jednoznaczne zrozumienie proponowanych przez niego założeń.

### Wszystkie ustalenia poczynione za pośrednictwem wideokonferencji, telefonicznie lub w trakcie spotkania muszą zostać niezwłocznie potwierdzone za pośrednictwem wiadomości e-mail. Mogą zostać z nich także sporządzone notatki zgodnie ze wzorem dostarczonym przez Zamawiającego.

### Wykonawca zobowiązany jest poinformować Zamawiającego o wszystkich zdarzeniach lub przeszkodach mogących spowodować opóźnienie w wykonaniu Umowy w stosunku do terminów przewidzianych w umowie.

### W trakcie realizacji Przedmiotu Umowy Wykonawca jest zobowiązany na bieżąco prowadzić z Zamawiającym ustalenia w sprawie szczegółowych Funkcjonalności oraz w sprawie minimalnych wymogów dla Sieci WAN i dostępu do Internetu, a także instalacji, oprogramowania i urządzeń towarzyszących. W przypadku wdrożenia rozwiązań lub wykonania zmian bez wcześniejszego uzgodnienia i zaakceptowania przez Zamawiającego, na żądanie Zamawiającego Wykonawca będzie zobowiązany dokonać stosownych zmian wdrożeniowych bez naliczania dodatkowych opłat.

### W celu możliwości konsultacji, kontroli wykonywanych prac prowadzonych przez Wykonawcę, Zamawiający zastrzega sobie możliwość powołania komisji, w skład której wejdą przynajmniej dwie osoby opiniujące w zakresie ochrony bezpieczeństwa systemów teleinformatycznych Zamawiającego oraz kierownik projektu Zamawiającego.

### Zamawiający zastrzega sobie prawo do przeprowadzenia, po poinformowaniu Wykonawcy, zewnętrznego audytu bezpieczeństwa wykonanej infrastruktury, jednak nie częściej niż co 6 miesięcy. W przypadku uwag audytora zewnętrznego Wykonawca jest zobowiązany do odpowiedniego dostosowania konfiguracji w ramach świadczonego serwisu, zgodnie z zaleceniami z wniosków pokontrolnych, w terminie do **10 Dni Roboczych** od ich przekazania przez Zamawiającego i bez naliczania dodatkowych opłat.

### Wykonawca jest zobowiązany prowadzić na bieżąco i chronologicznie pełną dokumentację robót, w szczególności robót budowlanych.

### Wykonawca jest zobowiązany do utrzymania ciągłości pracy modernizowanych i serwisowanych systemów i instalacji przynajmniej w godzinach pracy Zamawiającego.

### W ramach obowiązków wynikających z wykonywania zapisów Umowy wiążące są wyłącznie ustalenia poczynione w formie pisemnej i podpisane przez Kierowników projektu obu Stron Umowy, przy czym ustalenia dotyczące robót budowlanych będą wiążące dopiero po ich podpisaniu także przez odpowiedniego inspektora nadzoru inwestorskiego, a w przypadku ustalenia wiążącego branże - inspektorów nadzoru inwestorskiego wszystkich branż.

## Sposób realizacji zdalnego dostępu spoza siedziby Zamawiającego

### Jeżeli Wykonawca będzie zainteresowany skorzystaniem na potrzeby Umowy ze zdalnego dostępu, przekaże Zamawiającemu listę pracowników wraz z niezbędnymi danymi określonymi każdorazowo przez Zamawiającego (w szczególności: imię, nazwisko, adres e-mail, nr telefonu komórkowego oraz dane jednoznacznie identyfikujące komputer z którego będzie uzyskiwany dostęp) do konfiguracji zdalnego dostępu. Wskazane osoby muszą znajdować się na aktualnej liście osób odpowiedzialnych za realizację Przedmiotu Umowy będącej załącznikiem do Umowy.

### Zdalny dostęp będzie realizowany za pośrednictwem rozwiązania udostępnianego przez Zamawiającego, na zasadach przez niego określonych i tylko do wybranych elementów.

### Zdalny dostęp będzie przyznany uznaniowo wyłącznie w celu wykonywania prac wynikających z Umowy.

### Zamawiający przekaże Wykonawcy warunki techniczne jakie muszą spełniać komputery Wykonawcy wykorzystywane do zdalnego dostępu. Warunki te mogą być przez Zamawiającego modyfikowane w trakcie realizacji Umowy po uprzednim powiadomieniu Wykonawcy.

### Zamawiający zastrzega sobie możliwość ograniczenia ilości osób, którym przyznany zostanie zdalny dostęp.

### Pracownicy Wykonawcy, którym przyznany został zdalny dostęp zobowiązani są do nie przekazywania danych umożliwiających jego uzyskanie osobom trzecim (w szczególności są to: adres systemu, login, hasło, kody jednorazowe).

### Zamawiający zastrzega sobie możliwość nagrywania wszystkich czynności realizowanych przez pracowników Wykonawcy za pośrednictwem zdalnego dostępu.

### W przypadku czasowej niedostępności zdalnego dostępu z przyczyn niezależnych od Wykonawcy lub Zamawiającego prace wynikające z Umowy będą realizowane przez pracowników Wykonawcy w odpowiedniej Lokalizacji.

### Brak zdalnego dostępu z dowolnych przyczyn nie zwalnia Wykonawcy z wykonania prac serwisowych i usunięcia Awarii w wymaganym czasie.

### Wykonawca zobowiązany jest każdorazowo do wcześniejszego uzgodnienia z upoważnionymi pracownikami Zamawiającego zakresu prac realizowanych za pośrednictwem zdalnego dostępu.

### Wykonawca zobowiązuje się do podjęcia wszelkich niezbędnych działań, w tym organizacyjnych i technicznych, mających na celu zabezpieczenie sprzętu, za pomocą którego pracownicy Wykonawcy będą realizowali prace za pośrednictwem zdalnego dostępu.

## Lista upoważnionych w Lokalizacjach pracowników Zamawiającego

### Lista pracowników Zamawiającego w każdej Lokalizacji upoważnionych do współpracy w zakresie prac wdrożeniowych oraz w trakcie realizacji Umowy do zgłaszania Awarii i obsługi Awarii zostanie przekazana Wykonawcy przed podpisaniem Umowy.

## Harmonogram wykonywania prac

### Wykonawca jest zobowiązany prowadzić prace zgodnie z ogólnym harmonogramem prac przedstawionym w *Tabeli nr 12*. Szczegółowy harmonogram prac opracowany na podstawie ogólnego harmonogramu prac i zawierający faktyczne daty wykonania poszczególnych zadań Wykonawca ustali z kierownikiem projektu Zamawiającego na etapie wdrożenia.

Tabela nr 12

| **Lp.** | **Zadanie** | **Termin wykonania** | **Uwagi** |
| --- | --- | --- | --- |
| 1. | podpisanie Umowy | -------------- | --------------- |
| 2. | przygotowanie i uzgodnienie z kierownikiem projektu Zamawiającego szczegółowego harmonogramu prac | do 21 dni od dnia podpisania Umowy | Szczegółowy harmonogram prac przygotować przy uwzględnieniu rozpoczęcia świadczenia usług w dniu **23 czerwca 2020** r, chyba, że w Umowie zostanie wskazany inny termin, nie późniejszy jednak niż 6 miesięcy od dnia podpisania Umowy |
| 3. | przygotowanie projektów i uzyskanie wymaganych pozwoleń i zezwoleń zgodnie z wymaganiami ustawy Prawo budowlane i pokrewnych | po odbiorze bez uwag zadania 2 | dokumentacja przed wysłaniem do organów zewnętrznych musi zostać uzgodniona i zatwierdzona przez inspektora nadzoru inwestorskiego |
| 4. | przygotowanie projektu transmisji strumieniowej w technologii IP Multicast | do 8 maja 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 45 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadania 2 | przy założeniu 5 Dni Roboczych na ocenę przez Zamawiającego oraz 5 Dni Roboczych na poprawki i ich odbiór |
| 5. | przekazanie do oceny pierwszej części testów akceptacyjnych | do 22 maja 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 31 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadania 2 | przy założeniu 5 Dni Roboczych na ocenę przez Zamawiającego oraz 5 Dni Roboczych na poprawki i ich odbiór |
| 6. | przekazanie do oceny drugiej części testów akceptacyjnych | do 29 maja 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 24 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadań 2,4 | przy założeniu 5 Dni Roboczych na ocenę przez Zamawiającego oraz 5 Dni Roboczych na poprawki i ich odbiór |
| 7. | wykonanie, instalacja, konfiguracja i uruchomienie Łączy IP VPN MPLS oraz łączy dla usługi dostępu do Internetu, a także dostawa, instalacja, konfiguracja i uruchomienie Routerów CPE | do 5 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 17 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadania 3 | --------------- |
| 8. | wykonanie pierwszej części testów akceptacyjnych | do 9 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 13 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadań 5,7 | założyć minimum 3 Dni Robocze na wykonanie testów |
| 9. | dostawa, instalacja, konfiguracja i uruchomienie Routerów CE oraz uruchomienie testowej usługi transmisji danych w Sieci WAN oraz testowej usługi dostępu do Internetu w siedzibie Zamawiającego w Warszawie | do 9 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 13 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadania 8 | uruchomienie testowej transmisji danych w Sieci WAN oraz testowej usługi dostępu do Internetu możliwe do wykonania po godz. 17:00 wyłącznie wtedy kiedy **dostępni jednocześnie** będą wszyscy upoważnieni w Lokalizacjach pracownicy Zamawiającego |
| 10. | dostawa, instalacja, konfiguracja i uruchomienie *systemu monitoringu* | do 12 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 10 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadania 2 | --------------- |
| 11. | przeprowadzenie instruktażu powdrożeniowego | do 12 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 10 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadania 2 | Wykonawca przeprowadzi instruktaż w sposób nie kolidujący z wykonaniem innych zadań dla siedziby Zamawiającego w Warszawie |
| 12. | wykonanie drugiej części testów akceptacyjnych | do 15 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż na 7 dni przed planowanym wykonaniem zadania 15, po odbiorze bez uwag zadań 4, 6, 9 | założyć minimum 3 Dni Robocze na wykonanie testów |
| 13. | odbiór dokumentacji powykonawczej | do 22 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż w dniu wykonania zadania 15, po odbiorze bez uwag zadania 2 | dokumentacja w części roboty budowlane musi zostać w pierwszej kolejności zatwierdzona przez inspektora nadzoru inwestorskiego |
| 14. | odbiór aktywacji Serwisu Producenta dla Routerów CE | do 22 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - nie później niż w dniu wykonania zadania 15, po odbiorze bez uwag zadania 2 | --------------- |
| 15. | podpisanie protokołu odbioru końcowego potwierdzającego produkcyjne rozpoczęcie świadczenia usług transmisji danych w Sieci WAN oraz dostępu do Internetu zgodnie z Umową | do 22 czerwca 2020 r. - a w przypadku podpisania Umowy w terminie uniemożliwiającym rozpoczęcie świadczenia usług - po odbiorze bez uwag zadań 2-14 | odbiór końcowy muszą podpisać przynajmniej:   1. Ze strony Wykonawcy – Kierownik projektu oraz Kierownik robót w branży elektrycznej 2. Ze strony Zamawiającego – Kierownik projektu oraz inspektorzy nadzoru inwestorskiego w branżach |
| 16. | opcjonalnie - przeprowadzenie instruktażu technicznego | po odbiorze bez uwag zadania 15 - w terminie do 36 miesięcy | wymaga protokolarnego odbioru i dołączenia do protokołu oryginału listy uczestników wraz z ich podpisami  każdy przeprowadzony instruktaż odbierany będzie osobno dla każdego uczestnika |
| 17. | demontaż i zwrot urządzeń Wykonawcy po zakończeniu świadczenia usług transmisji danych w Sieci WAN oraz dostępu do Internetu | po zakończeniu świadczenia usług transmisji danych w sieci WAN oraz dostępu do Internetu wymaganych Umową, w terminie do 48 miesięcy od dnia podpisania Umowy | wykonanie demontażu i odbiór urządzeń Wykonawcy jest warunkiem koniecznym do uznania przez Zamawiającego, że Przedmiot Zamówienia został należycie wykonany  prace możliwe do wykonania po uzgodnieniu z upoważnionymi w Lokalizacjach pracownikami Zamawiającego |

## Zasady postępowania Wykonawcy na placu budowy

Wykonawca zobowiązany jest wykonywać wszystkie prace w Lokalizacjach Zamawiającego zgodnie z zasadami wymienionymi poniżej.

### Zasady ogólne

#### pracownicy Wykonawcy mają prawo korzystać z pomieszczeń socjalnych zgodnie z ich przeznaczeniem, w szczególności z łazienek i toalet położonych najbliżej miejsca prowadzenia robót.

#### na co najmniej **2 Dni Robocze** przed przystąpieniem do wykonywania prac w danej Lokalizacji Wykonawca zgłosi listę pracowników, dla których upoważniony w danej Lokalizacji pracownik Zamawiającego wystawi przepustki imienne umożliwiające poruszanie się po budynkach Zamawiającego w tej Lokalizacji.

#### pracownicy Wykonawcy nie posiadający przepustek lub mający nieważne przepustki nie będą wpuszczani na teren budynków Zamawiającego.

#### jeżeli zajdzie konieczność wprowadzenia innego pracownika, Wykonawca poinformuje o tym upoważnionego w danej Lokalizacji pracownika Zamawiającego nie później niż na **2 Dni Robocze** przed planowanym wprowadzeniem tego pracownika na teren budynków Zamawiającego celem przygotowania przepustki.

#### pracownik Wykonawcy poza przepustką musi posiadać dokument stwierdzający tożsamość i okazywać go na żądanie ochrony Zamawiającego.

#### w przypadku wykonywania prac mogących prowadzić do uszkodzenia instalacji wodno-kanalizacyjnych Wykonawca zobowiązany jest do posiadania wyposażenia, które zminimalizuje skutki zalewania do czasu usunięcia awarii.

#### Wykonawca musi zabezpieczyć istniejące instalacje ppoż. w taki sposób, żeby nie uległy awarii podczas prowadzonych prac i jednocześnie nie zostały aktywowane.

#### w przypadku wykonywania prac mogących wywołać działanie zabezpieczeń ppoż., Wykonawca musi z wyprzedzeniem powiadomić upoważnionego w danej Lokalizacji pracownika Zamawiającego, że może wystąpić alarm. W przeciwnym wypadku ewentualne koszty interwencji straży pożarnej lub serwisu systemu ppoż. ponosi Wykonawca.

#### Wykonawca jest zobowiązany do zabezpieczenia i utrzymania czystości w miejscu prowadzenia prac i na terenie dróg transportowych wewnątrz budynków Zamawiającego.

#### przebywanie pracowników Wykonawcy w serwerowniach i centrali telefonicznej jak i wszelkie prace tam prowadzone muszą być wykonywane pod czynnym nadzorem upoważnionego w danej Lokalizacji pracownika Zamawiającego i za jego zgodą.

#### zabrania się palenia tytoniu w miejscach do tego nie przeznaczonych, spożywania alkoholu i przebywania pod wpływem środków odurzających na terenie budynków Zamawiającego, pod rygorem unieważnienia przepustki imiennej i zakazu wstępu do budynków Zamawiającego.

### Przystąpienie pracowników Wykonawcy do prac

#### pracownicy Wykonawcy muszą się kontaktować przed przystąpieniem do prac z upoważnionym w danej Lokalizacji pracownikiem Zamawiającego w celu określenia zakresu prac.

#### dostęp do pomieszczeń jest możliwy za zgodą upoważnionego w danej Lokalizacji pracownika Zamawiającego.

#### klucze do pomieszczeń pobiera upoważniony w danej Lokalizacji pracownik Zamawiającego na wniosek pracowników Wykonawcy.

#### przed przekazaniem pomieszczenia upoważniony w danej Lokalizacji pracownik Zamawiającego sprawdza stan pomieszczenia i przekazuje Wykonawcy.

#### od momentu przekazania za pomieszczenie wraz z wyposażeniem odpowiada Wykonawca.

#### przed przystąpieniem do prac, jeśli to konieczne, Wykonawca zabezpieczy pomieszczenie i jego wyposażenie przed zniszczeniem i zabrudzeniem. W szczególności Wykonawca zabezpieczy serwery i inne urządzenia przez zapyleniem.

#### pracownicy Wykonawcy zobowiązani są do przebywania tylko w obrębie pomieszczeń placu budowy.

#### za nadzór nad pracownikami Wykonawcy oraz wszelkie działania na terenie budynków Zamawiającego odpowiada Wykonawca.

### Wykonywanie prac

#### prace głośne, roboty uciążliwe oraz wywóz gruzu i odpadów mogą być wykonywane:

##### w Dni Robocze w godzinach od 8:00-16:00 tylko po uzgodnieniu z upoważnionym w danej Lokalizacji pracownikiem Zamawiającego;

##### w Dni Robocze w godzinach od 16:00-21:00 bez ograniczeń, chyba że Wykonawca ustali inaczej z upoważnionym w danej Lokalizacji pracownikiem Zamawiającego.

#### w przypadku wystąpienia okoliczności nieprzewidzianych (wwiercenie w instalację CO, wod-kan, elektryczną, sieci komputerowej, światłowodową, telewizyjną, ppoż., itp.) upoważniony w danej Lokalizacji pracownik Zamawiającego natychmiast zostanie powiadomiony, a prace zostaną przerwane na czas wyjaśnienia zdarzenia z przedstawicielem Wykonawcy. Wykonawca jest zobowiązany do niezwłocznego podjęcia działań mających na celu zapobieżenie skutkom, ograniczenia rozmiarów szkody i naprawienia tej szkody w taki sposób, żeby odtworzyć stan sprzed wystąpienia szkody.

### Zakończenie prac

#### zakończenie prac w danym dniu pracownicy Wykonawcy każdorazowo zgłaszają upoważnionemu w danej Lokalizacji pracownikowi Zamawiającego.

#### upoważniony w danej Lokalizacji pracownik Zamawiającego dokonuje odbioru przekazywanych pomieszczeń.

#### klucze do pomieszczeń Wykonawca zdaje upoważnionemu w danej Lokalizacji pracownikowi Zamawiającego.

#### po zakończeniu robót budowlanych na dany dzień Wykonawca musi obowiązkowo dokonać odkurzenia rejonu, który uległ zapyleniu lub zabrudzeniu, a jeżeli zajdzie konieczność zmyć na mokro.

#### plac budowy musi być zostawiony w takim stanie, żeby umożliwić Zamawiającemu bieżącą pracę (czynny zakład pracy).

#### wszelkie zauważone usterki i zniszczenia muszą być usunięte przez Wykonawcę natychmiast.

#### pracownicy Wykonawcy mogą opuścić plac budowy dopiero po uzyskaniu zgody upoważnionego w danej Lokalizacji pracownika Zamawiającego.

## Odbiory prac

### Kierownik projektu Wykonawcy zobowiązany jest powiadomić bez zbędnej zwłoki, w sposób pisemny lub emailem, kierownika projektu Zamawiającego o fakcie wykonania danych robót i przedstawieniu ich do odbioru.

### Każdy odbiór robót budowlanych lub odbiór dokumentacji powykonawczej robót budowlanych, musi zostać protokolarnie potwierdzony przez inspektora nadzoru inwestorskiego oraz kierownika projektu Zamawiającego lub upoważnionego w danej Lokalizacji pracownika Zamawiającego, a także upoważnionego pracownika Wykonawcy, pod rygorem nieważności tego protokołu i odbioru.

### Zamawiający wymaga następujących odbiorów:

#### w przypadku konieczności wykonania robót budowlanych - w każdej Lokalizacji Zamawiającego;

#### propozycji pierwszej części testów akceptacyjnych;

#### dostawy urządzeń Wykonawcy w każdej Lokalizacji (odbiór ilościowy);

#### wykonania usług instalacyjno-konfiguracyjnych dla Łączy IP VPN MPLS w każdej Lokalizacji i łączy dla dostępu do Internetu w siedzibie Zamawiającego w Warszawie;

#### wykonania pierwszej części testów akceptacyjnych;

#### propozycji drugiej części testów akceptacyjnych;

#### dostawy Routerów CE (odbiór ilościowy) oraz odbioru technicznego Routerów CE w siedzibie w Warszawie;

#### wykonania prac instalacyjno-konfiguracyjnych dla usług transmisji danych w Sieci WAN w każdej Lokalizacji i dostępu do Internetu w siedzibie Zamawiającego w Warszawie;

#### wykonania drugiej części testów akceptacyjnych;

#### dokumentacji powykonawczej, w tym wymaganej dokumentacji robót budowlanych, w szczególności: projektów wykonawczych, dokumentacji powykonawczej, potwierdzonej za zgodność z oryginałem kopii zezwoleń, uzgodnień i dzienników budowy dla każdej Lokalizacji;

#### odbiór aktywacji Serwisu Producenta dla Routerów CE;

#### przeprowadzenia instruktażu powdrożeniowego;

#### końcowego, potwierdzającego możliwość produkcyjnego świadczenia przez Wykonawcę usług transmisji danych w Sieci WAN i dostępu do Internetu oraz możliwość świadczenia gwarancji i usług serwisu od dnia odbioru końcowego bez uwag;

#### przeprowadzenia instruktażu technicznego (w zależności od sytuacji dla pojedynczych instruktaży, bądź grupy instruktaży);

#### odbioru urządzeń Wykonawcy przez serwis Wykonawcy w każdej Lokalizacji Zamawiającego po zakończeniu świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu.

### Kierownik projektu Zamawiającego lub pracownik upoważniony w danej Lokalizacji uprawnieni są do podpisywania protokołów odbioru powstałych w wyniku realizacji Umowy, z zastrzeżeniem wymaganych potwierdzeń inspektora nadzoru inwestorskiego.

### Za przygotowanie stosownego protokołu i przedstawienie do podpisu odpowiedzialny jest kierownik projektu Wykonawcy.

### Odbioru dokonuje się w terminie do **5 Dni Roboczych**, chyba, że w sposób szczególny wskazano inaczej, od dnia pisemnego przekazania do odbioru przez kierownika projektu Wykonawcy informacji o gotowości do odbioru wraz ze wskazaniem miejsca wykonania prac, rodzaju i zakresu odbioru.

### Jeżeli w trakcie przeprowadzania odbioru Zamawiający zgłosi zastrzeżenia na piśmie lub emailem do przedmiotu odbioru, obie strony Umowy ustalą protokolarnie zakres i termin bezpłatnego dokonania przez Wykonawcę niezbędnych zmian i uzupełnień. Wykonawca dokona zmian lub uzupełnień w wyznaczonym terminie.

### Odbiór przedmiotu odbioru po naniesieniu poprawek nastąpi w terminie do **3 Dni Roboczych** od dnia ich protokolarnego przekazania przez kierownika projektu Wykonawcy.

### W przypadku braku wniesienia przez Zamawiającego zastrzeżeń do przekazanych do przedmiotu odbioru, przedmiot odbioru będzie uważany za zaakceptowany a protokół odbioru zostanie podpisany w terminie do **3 Dni Roboczych**.

### Wykonawca przystąpi do realizacji testów akceptacyjnych nie wcześniej niż po ich protokolarnym zatwierdzeniu przez kierownika projektu Zamawiającego, tj. po uzyskaniu przez Wykonawcę odpowiednich protokołów odbioru bez uwag.

### Potwierdzeniem prawidłowej realizacji przedmiotu odbioru jest protokół odbioru podpisany bez uwag.

### Testowe uruchomienie transmisji danych w Sieci WAN i dostępu do Internetu w Lokalizacjach Wykonawca rozpocznie najwcześniej po dokonaniu odbioru bez uwag wyników pierwszej części testów akceptacyjnych dla łączy we wszystkich Lokalizacjach Zamawiającego.

### Kierownik projektu Wykonawcy najpóźniej wraz ze zgłoszeniem gotowości do odbioru końcowego, tj. produkcyjnego uruchomienia transmisji danych w Sieci WAN i dostępu do Internetu, obowiązany jest dostarczyć kierownikowi projektu Zamawiającego do odbioru dokumentację powykonawczą.

### Potwierdzeniem realizacji produkcyjnego uruchomienia transmisji danych w Sieci WAN we wszystkich Lokalizacjach Zamawiającego, a także dostępu do Internetu w siedzibie w Warszawie będą wszystkie wymagane protokoły odbioru bez uwag.

## Protokoły odbioru oraz protokół odbioru końcowego

### Protokoły odbioru

#### Zamawiający wymaga sporządzenia przez Wykonawcę protokołów odbioru poświadczających wykonanie wymaganych Umową odbiorów.

#### W razie konieczności kierownicy projektu obu stron Umowy mogą sporządzić inne, nie wymienione powyżej protokoły odbioru lub przekazania.

#### Za przygotowanie protokołów odbioru odpowiada kierownik projektu Wykonawcy.

#### Protokoły odbioru muszą być zgodne ze wzorami zamieszczonymi poniżej.

#### Do protokołów wykonania usługi instruktażu powdrożeniowego Wykonawca musi dołączyć oryginały list obecności uczestników wskazanych przez Zamawiającego.

#### Usługa instruktażu powdrożeniowego nie zostanie odebrana przez Zamawiającego w przypadku, jeżeli Wykonawca nie dostarczy protokołu i wymaganych list obecności.

#### Wszystkie wymagane protokoły Wykonawca sporządzi w trzech egzemplarzach: jeden dla upoważnionego w danej Lokalizacji pracownika Zamawiającego, jeden dla siedziby Zamawiającego w Warszawie i jeden dla Wykonawcy.

#### Egzemplarz protokołu odbioru dostarczany do siedziby Zamawiającego w Warszawie będzie załącznikiem do końcowego protokołu odbioru.

#### Każdy protokół, w którym Zamawiający wskaże uwagi (wypełni pole uwagi), tzw. protokół z uwagami, jest protokołem opisującym błędy Wykonawcy stwierdzone podczas odbioru i nie stanowi protokołu potwierdzającego wykonanie w określonym terminie przedmiotu opisanego w protokole. Oznacza to, że taki protokół nie może być załącznikiem do protokołu odbioru końcowego oraz, że w takim przypadku mogą wystąpić opóźnienia w rozpoczęciu świadczenia usług transmisji danych w Sieci WAN oraz dostępu do Internetu z winy Wykonawcy.

### Protokół odbioru końcowego

#### Za przygotowanie protokołu odbioru końcowego odpowiada kierownik projektu Wykonawcy.

#### Protokół obioru końcowego bez uwag poświadcza wykonanie przez Wykonawcę wszystkich wymaganych Umową robót budowlanych, dostaw, usług, prac instalacyjno-konfiguracyjnych i instruktażu powdrożeniowego niezbędnych w celu umożliwienia produkcyjnego świadczenia usług transmisji danych w Sieci WAN oraz dostępu do Internetu.

#### Do protokołu odbioru końcowego bez uwag, jako załączniki, Wykonawca dołączy wszystkie oryginalne protokoły odbioru bez uwag powstałe w trakcie prowadzonych prac.

#### Protokół odbioru końcowego bez uwag musi być podpisany w Warszawie przez kierowników projektu obu stron Umowy.

#### W przypadku, jeżeli protokół odbioru końcowego zostanie spisany z opóźnieniem, tj. po dniu rozpoczęcia świadczenia usług wymaganym w Umowie, Wykonawca obniży opłatę miesięczną za wszystkie usługi wymagane w Umowie proporcjonalnie do ilości dni opóźnienia w danym miesiącu kalendarzowym, nawet w przypadku jeżeli część z tych usług działała poprawnie.

#### Obniżenie opłaty miesięcznej nie zwalnia Wykonawcy ze wskazanych w Umowie opłat dodatkowych wynikających z opóźnień.

#### Protokół odbioru końcowego, w którym Zamawiający wskaże uwagi (wypełni pole uwagi), tzw. protokół z uwagami, jest protokołem opisującym błędy Wykonawcy w wykonaniu odbioru końcowego i nie stanowi protokołu potwierdzającego wykonanie w określonym terminie przedmiotu opisanego w protokole. Oznacza to, że taki protokół nie stanowi wymaganego protokołu odbioru końcowego oraz, że w takim przypadku mogą wystąpić opóźnienia w rozpoczęciu świadczenia usług transmisji danych w Sieci WAN oraz dostępu do Internetu z winy Wykonawcy.

## Serwis Wykonawcy

### W celu świadczenia Przedmiotu Zamówienia Wykonawca musi posiadać funkcjonujący całodobowo serwis odpowiedzialny za przyjmowanie zgłoszeń, obsługę zdarzeń dla Awarii oraz odpowiedzialny za usuwanie Awarii.

### Wykonawca musi zapewnić pracowników z odpowiednimi uprawnieniami i certyfikatami. Weryfikacja zostanie przeprowadzona przez Zamawiającego na etapie prowadzenia postępowania przetargowego na podstawie dostarczonych kserokopii stosownych uprawnień i certyfikatów dla osób przewidzianych do realizacji Przedmiotu Zamówienia. Osoby wskazane podczas postępowania przetargowego zostaną wpisane do Umowy jako osoby odpowiedzialne za realizację Przedmiotu Zamówienia.

### Przyjmowanie zgłoszeń będzie następowało w sposób i na dane kontaktowe wskazane w Umowie.

### Wykonawca jest zobowiązany zapewnić obsługę Serwisu Producenta względem Zamawiającego, w tym zapewnić usługę serwisu gwarancyjnego na nowo dostarczone Routery CE.

### Wszystkie usługi serwisu Wykonawcy, w tym usługi serwisu gwarancyjnego na nowo dostarczone Routery CE i usługi serwisu pogwarancyjnego na istniejące Rutery CE, które w danym momencie są używane w celu świadczenia usług, są świadczone w ramach świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu bez naliczania dodatkowych opłat.

### Wykryte Awarie usług transmisji danych w Sieci WAN, usługi dostępu do Internetu, Routerów CE, a także systemu monitoringu serwis Wykonawcy będzie usuwał nawet, jeżeli nie zostaną one zgłoszone przez upoważnionego w danej Lokalizacji pracownika Zamawiającego.

### Serwis Wykonawcy jest zobowiązany udzielać telefonicznie upoważnionemu w siedzibie Zamawiającego w Warszawie pracownikowi konsultacji w zakresie obsługi, funkcjonowania, konfiguracji, parametrów, protokołów transmisji dla Routerów CE, multicastów, transmisji danych w Sieci WAN, dostępu do Internetu, w tym usługi AntyDDoS oraz systemu monitoringu, w godzinach od 8:00 do 16:00 w Dni Robocze, według potrzeb Zamawiającego w średnim miesięcznym wymiarze około 8 godzin.

### Dane kontaktowe na potrzeby konsultacji zostały wskazane w Umowie.

## Gwarancja i rękojmia Wykonawcy

### Gwarancja i rękojmia na Routery CE

#### Na dostarczone Routery CE Wykonawca udziela gwarancji na okres wskazany w Umowie.

#### Gwarancja obejmuje:

##### aktualizację/wymianę oprogramowania Routerów CE w przypadku zdiagnozowania przez Wykonawcę lub Zamawiającego błędu w oprogramowaniu lub udostępnienia przez producenta tego routera aktualizacji krytycznych oprogramowania;

##### dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej Routerów CE;

##### naprawę Routerów CE;

##### wymianę Routerów CE na nowe, nieużywane, nieregenerowane, nienaprawiane i nierefabrykowane, tego samego producenta, takie same lub o lepszych parametrach, w przypadku braku możliwości skutecznej naprawy (odbiór i dostawa nastąpi w miejscu aktualnego zainstalowania).

#### W przypadku trzykrotnej naprawy tego samego elementu składowego danego Routera CE, Zamawiającemu przysługuje prawo żądania wymiany tego Routera CE na nowy, wolny od wad.

#### Wykonawca przedłuża okres gwarancji udzielonej na dany Router CE o czas trwania jego naprawy gwarancyjnej. W przypadku dostarczenia nowego Routera CE w wyniku wymiany gwarancyjnej, okres gwarancji na to urządzenie liczony będzie od nowa.

#### Obowiązki wynikające z udzielonej gwarancji, tj. serwis gwarancyjny, świadczy serwis Wykonawcy.

#### Gwarancja będzie świadczona u Zamawiającego w miejscu instalacji danego Routera CE w obecności upoważnionego w Lokalizacji pracownika Zamawiającego.

#### Zamawiający zastrzega sobie prawo do przenoszenia danego Routera CE między Lokalizacjami. W takim wypadu Wykonawca będzie świadczył gwarancję w miejscu aktualnego zainstalowania tego Routera CE.

#### Gwarancja nie może ograniczać praw Zamawiającego do instalowania i wymiany w zakupionym Routerze CE standardowych kart i urządzeń, zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego i pod nadzorem serwisu Wykonawcy.

#### Uprawnienia z tytułu rękojmi za wady fizyczne wygasają po upływie okresu świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu, tj. w dniu zakończenia świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu.

### Gwarancja i rękojmia na prace projektowe, instalacyjne i konfiguracyjne Routerów CE

#### Na wykonane prace projektowe, instalacyjne i konfiguracyjne Routerów CE (w tym IP Multicast) Wykonawca udziela gwarancji na okres wskazany w Umowie.

#### Obowiązki wynikające z udzielonej gwarancji świadczy serwis Wykonawcy.

#### Gwarancja nie może ograniczać praw Zamawiającego do wykonywania prac konfiguracyjnych w Routerach CE zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego i pod nadzorem serwisu Wykonawcy.

#### Uprawnienia z tytułu rękojmi na wykonane prace instalacyjne i konfiguracyjne Routerów CE wygasają po upływie okresu świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu, tj. w dniu zakończenia świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu.

### Gwarancja i rękojmia na roboty budowlane

#### Na wykonane roboty budowlane Wykonawca udziela gwarancji na okres wskazany w Umowie.

#### Obowiązki wynikające z udzielonej gwarancji świadczy Wykonawca.

#### Gwarancja obejmuje:

##### roboty budowlane i elektroinstalacyjne wykonane w ramach Umowy;

##### materiały wbudowane podczas wykonywania robót budowlanych;

##### działanie wykonanych instalacji;

#### Zamawiający w razie stwierdzenia w okresie gwarancji:

##### wad wykonanych robót budowlanych i elektroinstalacyjnych;

##### wad materiałów wbudowanych podczas wykonywania robót budowlanych;

##### nieprawidłowego działania wykonanych instalacji;

##### innych stwierdzonych nieprawidłowości

przedłoży Wykonawcy, najpóźniej w ciągu **7 dni** od dnia ich ujawnienia, stosowne zgłoszenie gwarancyjne.

#### Uprawnienia z tytułu rękojmi na wykonane roboty budowlane wygasają po upływie okresu świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu, tj. w dniu zakończenia świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu.

#### Usunięcie wskazanych w reklamacji nieprawidłowości musi nastąpić w terminie do **28 dni** od zgłoszenia.

#### Jeżeli Wykonawca nie usunie wskazanych w reklamacji nieprawidłowości we wskazanym terminie, Zamawiający może powierzyć ich usunięcie osobie trzeciej na koszt i ryzyko Wykonawcy oraz bez utraty gwarancji udzielonej przez Wykonawcę.

#### W ramach świadczenia gwarancji Wykonawca:

##### pokrywa koszty robocizny oraz dojazdu serwisantów;

##### musi wziąć pod uwagę możliwą konieczność wykonywania czynności naprawczych w godzinach nocnych lub w dni ustawowo wolne od pracy. W takim przypadku wymagana jest każdorazowa zgoda Zamawiającego na takie prace;

##### zobowiązuje się do usuwania skutków nieprawidłowości w sposób jak najmniej zakłócający funkcjonowanie Zamawiającego.

### Gwarancja i rękojmia na dokumentacje powykonawczą

#### Na wykonaną dokumentację powykonawczą Wykonawca udziela gwarancji na okres wskazany w Umowie.

#### Obowiązki wynikające z udzielonej gwarancji będzie świadczył Wykonawca.

#### Gwarancja obejmuje całą wykonana w ramach Przedmiotu Zamówienia dokumentację powykonawczą, w szczególności wady ukryte tej dokumentacji.

#### Zamawiający w razie stwierdzenia w okresie gwarancji:

##### wad dokumentacji powykonawczej, w szczególności wad ukrytych tej dokumentacji;

##### innych stwierdzonych nieprawidłowości

przedłoży Wykonawcy, najpóźniej w ciągu **7 dni** od dnia ich ujawnienia, stosowne zgłoszenie gwarancyjne.

#### Usunięcie wad dokumentacji powykonawczej musi nastąpić w terminie do **28 dni** od zgłoszenia.

### Gwarancja i rękojmia na świadczone usługi

#### Wykonawca zobowiązany jest dochować jakości świadczonych usług, co Zamawiający rozumie jako zachowanie parametrów wszystkich świadczonych usług oraz usług składowych tych usług (np. usługi AntyDDoS w ramach świadczenia usługi dostępu do Internetu), a w przypadku wystąpienia Awarii tych usług lub usług składowych wykonanie napraw najszybciej jak to możliwe, również w przypadku, kiedy Zamawiający nie zgłosi Awarii w sposób formalny.

## Serwis pogwarancyjny Routerów CE świadczony przez Wykonawcę

### Wykonawca będzie świadczył serwis pogwarancyjny łącznie na 17 szt. Routerów CE, aktualnie używanych w celu świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu, przez okres wskazany w Umowie. Zestawienie 20 szt. Routerów CE aktualnie istniejących u Zamawiającego, z których w danym momencie 17 szt. będzie podlegało serwisowi pogwarancyjnemu, znajduje się w części *Specyfikacja istniejących u Zamawiającego Routerów CE*.

### W przypadku skorzystania przez Zamawiającego z prawa opcji dotyczącego przedłużenia świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu, Wykonawca będzie zobowiązany świadczyć serwis pogwarancyjny łącznie na 20 szt. Routerów CE, aktualnie używanych w celu świadczenia usług transmisji danych w Sieci WAN i dostępu do Internetu, przez okres na jaki zostało przedłużone świadczenie usług, przy czym 3 szt. Routerów CE będą to nowo dostarczone Routery CE, a pozostałe 17 szt. Routerów CE – aktualnie używane u Zamawiającego. Zestawienie 20 szt. Routerów CE aktualnie istniejących u Zamawiającego, z których w danym momencie 17 szt. będzie podlegało serwisowi pogwarancyjnemu, znajduje się w części *Specyfikacja istniejących u Zamawiającego Routerów CE*.

### Serwis pogwarancyjny Wykonawcy obejmuje:

#### aktualizację/wymianę oprogramowania dostarczonych nowych Routerów CE oraz Routera CE serii ASR1001, model: ASR1001X-SECK9 w przypadku zdiagnozowania przez Wykonawcę lub Zamawiającego błędu w oprogramowaniu lub udostępnienia przez producenta tego routera aktualizacji krytycznych oprogramowania;

#### dostęp do dokumentacji technicznej Routerów CE;

#### w ramach możliwości Wykonawcy - naprawę aktualnie używanych Routerów CE nie podlegających Serwisowi Producenta;

#### w przypadku pierwszej Awarii Routera CE serii 2900, model: CISCO2921-HSEC/K9 wykorzystanie Routera CE zdemontowanego wcześniej z Jednostki Terenowej w Goławicach, dostarczenie z siedziby Zamawiającego w Warszawie do miejsca Awarii, odtworzenie konfiguracji Routera CE i przywrócenie świadczenia usług (zepsuty Router CE zostaje w miejscu instalacji);

#### w przypadku kolejnych Awarii Routera CE serii 2900, model: CISCO2921-HSEC/K9 – wymianę Routera CE na nowy, nieużywany, nieregenerowany, nienaprawiany i nierefabrykowany, tego samego producenta taki sam lub o lepszych parametrach, w przypadku braku możliwości skutecznej naprawy (odbiór i dostawa nastąpi w miejscu aktualnego zainstalowania, zepsuty Router CE zostaje w miejscu instalacji);

#### w przypadku pierwszych dwóch Awarii Routera CE serii ASR1001, model: ASR1001-2.5G-SECK9 wykorzystanie Routera CE zdemontowanego wcześniej w siedzibie Zamawiającego w Warszawie, dostarczenie z siedziby Zamawiającego w Warszawie do miejsca Awarii, odtworzenie konfiguracji Routera CE i przywrócenie świadczenia usług (zepsuty Router CE zostaje w miejscu instalacji);

#### w przypadku trzeciej Awarii Routera CE serii ASR1001, model: ASR1001-2.5G-SECK9, Zamawiający dostarczy Wykonawcy inny nowy o nie mniejszej Funkcjonalności. W takim wypadku Wykonawca zobowiązany jest odtworzyć konfigurację Routera CE i przywrócić świadczenie usług.

### Usługę serwisu pogwarancyjnego świadczy serwis Wykonawcy.

### Usługa serwisu pogwarancyjnego będzie świadczona u Zamawiającego w miejscu instalacji Routerów CE w obecności upoważnionego w danej Lokalizacji pracownika Zamawiającego.

### Zamawiający zastrzega sobie prawo do przenoszenia danego Routera CE między Lokalizacjami. W takim wypadu Wykonawca będzie świadczył serwis pogwarancyjny w miejscu aktualnego zainstalowania tego Routera CE.

### Świadczenie usługi serwisu pogwarancyjnego nie może ograniczać praw Zamawiającego do instalowania i wymiany w danym Routerze CE standardowych kart i urządzeń, zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego i pod nadzorem serwisu Wykonawcy.

## Klasyfikacja Awarii

### Każda zgłoszona przez Zamawiającego Awaria musi zostać sklasyfikowana jako:

#### Awaria usługi transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IPVPN MPLS;

#### Awaria usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS;

#### Awaria usługi dostępu do Internetu;

#### Awaria Routera CE;

#### Awaria systemu monitoringu.

### W szczególności następujące przypadki Awarii będą klasyfikowane we wskazany poniżej sposób:

#### niedotrzymywanie parametrów technicznych dla usługi transmisji danych w Sieci WAN z wykorzystaniem głównych lub zapasowych Łączy IP VPN MPLS jest przez strony Umowy traktowane jako Awaria tej usługi pomimo możliwego faktycznego braku przerwy w transmisji danych;

#### wielokrotna, powtarzająca się w odstępach nie dłuższych niż 5 godzin utrata łączności lub wielokrotne powtarzające się w odstępach nie dłuższych niż 5 godzin niedotrzymanie parametrów technicznych usługi transmisji danych w Sieci WAN dla danej Lokalizacji jest traktowane jako ciągła Awaria usługi transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IPVPN MPLS i jednocześnie ciągła Awaria usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IPVPN MPLS, lub jako ciągła Awaria Routera CE – w zależności od rodzaju zgłoszonej Awarii;

#### brak łączności w ramach usługi transmisji danych w Sieci WAN z wykorzystaniem głównego Łącza IP VPN MPLS w danej Lokalizacji jest przez strony Umowy traktowany jako Awaria usługi transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS;

#### brak łączności w ramach usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowego Łącza IP VPN MPLS w danej Lokalizacji jest przez strony Umowy traktowany jako Awaria usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS;

#### całkowita utrata łączności w danej Lokalizacji jest przez strony Umowy traktowany jako jednoczesne wystąpienie dwóch Awarii: usługi transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS i jednocześnie usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS;

#### niedotrzymywanie parametrów technicznych dla usługi dostępu do Internetu poprzez główne lub zapasowe łącze dla usługi dostępu do Internetu jest przez strony Umowy traktowane jako Awaria tej usługi pomimo możliwego faktycznego braku przerwy w transmisji danych;

#### wielokrotna, powtarzająca się w odstępach nie dłuższych niż 5 godzin utrata łączności lub wielokrotne powtarzające się w odstępach nie dłuższych niż 5 godzin niedotrzymanie parametrów technicznych usługi dla dostępu do Internetu jest traktowane jako ciągła Awaria usługi dostępu do Internetu poprzez główne łącze dla dostępu do Internetu i jednocześnie ciągła Awaria usługi dostępu do Internetu poprzez zapasowe łącze dla dostępu do Internetu, lub jako ciągła Awaria jednego Routera CE lub dwóch Routerów CE – w zależności od rodzaju zgłoszonej/zgłoszonych Awarii;

#### brak łączności poprzez główne albo zapasowe łącze dla usługi dostępu do Internetu w siedzibie Zamawiającego w Warszawie jest przez strony Umowy traktowany jako Awaria usługi dostępu do Internetu;

#### całkowity brak dostępu do Internetu jest przez strony Umowy traktowany jako Awaria usługi dostępu do Internetu;

#### niedotrzymywanie Funkcjonalności dla Sieci WAN w danej Lokalizacji jest przez strony Umowy traktowane jako Awaria Routera CE w tej Lokalizacji;

#### niedotrzymywanie Funkcjonalności dla dostępu do Internetu jest przez strony Umowy traktowane jako jednoczesne wystąpienie dwóch Awarii obu Routerów CE terminujących te łącza;

#### brak działania lub nieprawidłowe działanie systemu monitoringu jest przez strony Umowy traktowane jako Awaria tego systemu.

### Klasyfikacje niektórych z możliwych Awarii ulegną zmianie w przypadku jeżeli:

#### upoważniony w danej Lokalizacji pracownik Zamawiającego zgłaszając Awarię sklasyfikuje ją inaczej;

#### podczas analizy zgłoszonej Awarii serwis Wykonawcy zdiagnozuje inną jej przyczynę i skutecznie zgłosi zmianę klasyfikacji Awarii, a upoważniony w danej Lokalizacji pracownik Zamawiającego nie będzie miał uwag co do faktycznie wykonanych czynności naprawczych po zmianie klasyfikacji, zgodnie z wymaganiami procedury *Zmiany klasyfikacji Awarii*.

### Jeżeli upoważniony w danej Lokalizacji pracownik Zamawiającego nie dokona klasyfikacji zgłaszanej Awarii dotyczącej usługi transmisji danych w Sieci WAN, strony Umowy przyjmują, że nastąpiła jednoczesna Awaria usługi transmisji danych w Sieci WAN z wykorzystaniem głównego i zapasowego łącza IP VPN MPLS i serwis Wykonawcy zarejestruje dwa odpowiadające tym Awariom zgłoszenia.

### Jeżeli upoważniony w siedzibie w Warszawie pracownik Zamawiającego nie dokona klasyfikacji zgłaszanej Awarii dotyczącej usługi dostępu do Internetu, strony Umowy przyjmują, że nastąpiła Awaria usługi dostępu do Internetu jednocześnie poprzez główne łącze dla usługi dostępu do Internetu i zapasowe łącze dla usługi dostępu do Internetu i serwis Wykonawcy zarejestruje jedno odpowiadające tej Awarii zgłoszenie.

### Każda zgłoszona Awaria jest przez strony Umowy traktowana i rozliczana jako osobne zdarzenie.

### Zgłoszenie Awarii dotyczące jednocześnie transmisji danych w Sieci WAN z wykorzystaniem głównych i zapasowych Łączy IP VPN MPLS jest przez Wykonawcę traktowane, a przez Zamawiającego rozliczane, jako dwie osobne Awarie odpowiednio dla usługi transmisji danych w Sieci WAN z wykorzystaniem głównych i dla usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS, przy czym jedna z nich może zostać usunięta wcześniej.

### Zgłoszenie Awarii dotyczące usługi dostępu do Internetu, niezależnie od faktu czy Awaria dotyczy całości usługi, czy tylko jej części, tj. świadczenia przez główne albo zapasowe łącze dla usługi dostępu do Internetu, jest przez Wykonawcę traktowane, a przez Zamawiającego rozliczane, jako jedna Awaria.

### Awaria usługi transmisji danych w Sieci WAN lub usługi dostępu do Internetu powstała w wyniku przerwy w zasilaniu elektrycznym w Lokalizacji Zamawiającego traktowana będzie tak, jakby nigdy nie wystąpiła jeżeli zostanie spełniony następujący warunek: wymagane jest zamknięcie tej Awarii przez serwis Wykonawcy zgodnie z wymaganiami Umowy (w szczególności w czasie przewidzianym na usunięcie tej Awarii) i wskazanie jako przyczyny Awarii przerwy w zasilaniu elektrycznym w Lokalizacji wraz ze wskazaniem imienia i nazwiska upoważnionego w danej Lokalizacji pracownika Zamawiającego, który przekazał taką informację.

### Jeżeli w wyniku prowadzenia przez Wykonawcę prac konserwacyjnych lub naprawczych, nie będących skutkiem usuwania zgłoszonej przez Zamawiającego Awarii, nastąpiła przerwa w dostępności danej usługi i w tym czasie upoważniony w danej Lokalizacji pracownik Zamawiającego zgłosił Awarię, to zdarzenie to przez strony Umowy traktowane jest jako Awaria tego łącza.

## Zmiana klasyfikacji Awarii

### W trakcie prowadzenia czynności naprawczych serwis Wykonawcy może stwierdzić inną rzeczywistą przyczynę Awarii niż zgłosił upoważniony w danej Lokalizacji pracownik Zamawiającego. W takim przypadku, jeżeli zgłoszenie dotyczyło Awarii usługi transmisji danych w Sieci WAN z wykorzystaniem głównych lub zapasowych Łączy IP VPN MPLS, albo Awarii usługi dostępu do Internetu poprzez główne lub zapasowe łącze dla usługi dostępu do Internetu, Zamawiający jednorazowo dopuszcza zmianę klasyfikacji Awarii na Awarię Routera CE lub Awarię systemu monitoringu.

### Informacja o zmianie klasyfikacji Awarii musi zostać skutecznie przesłana do Zamawiającego, zgodnie z wymaganiami określonymi w procedurze *Rejestracji Awarii i potwierdzania zdarzeń dla Awarii*, nie później niż w czasie przewidzianym na usunięcie Awarii zgłoszonej przez Zamawiającego, tj. usługi transmisji danych w Sieci WAN z wykorzystaniem głównych lub zapasowych Łączy IP VPN MPLS, albo Awarii usługi dostępu do Internetu poprzez główne lub zapasowe łącze dla usługi dostępu do Internetu. Brak skutecznego przesłania informacji w wymaganym czasie skutkuje brakiem ważności zmiany klasyfikacji Awarii.

### Skuteczna zmiana klasyfikacji Awarii jest przez strony Umowy traktowana tak, jakby upoważniony w danej Lokalizacji pracownik Zamawiającego zgłosił Awarię taką jak po zmianie klasyfikacji, w szczególności powoduje to zmianę dopuszczalnego czasu na usunięcie tej Awarii na zgodny z wymaganiami Umowy dla tego rodzaju Awarii, tj. Awarii Routera CE lub Awarii systemu monitoringu.

### Jeżeli w trakcie prowadzenia czynności naprawczych przez serwis Wykonawcy, a także czynności kontrolnych prowadzonych przez Zamawiającego, po zamknięciu tej Awarii okaże się, że nie było podstaw technicznych do zmiany klasyfikacji Awarii (w szczególności działań serwisu Wykonawcy niezbędnych do usunięcia tej Awarii po zmianie klasyfikacji), zostanie ona automatycznie anulowana i przez strony Umowy będzie traktowana jako niebyła.

## Bieg czasu trwania Awarii

### Bieg czasu trwania Awarii rozpoczyna się w momencie zgłoszenia Awarii przez upoważnionego w danej Lokalizacji pracownika Zamawiającego.

### Bieg czasu trwania Awarii może zostać zawieszony (wstrzymany) w razie spełnienia przez serwis Wykonawcy wymagań określonych w procedurze *Zawieszenia biegu czasu trwania Awarii*.

### Bieg czasu trwania Awarii kończy się w momencie otrzymania przez Zamawiającego informacji o zamknięciu tej Awarii przez serwis Wykonawcy, zgodnie z wymaganiami wskazanymi w procedurze *Rejestracji Awarii i potwierdzania zdarzeń dla Awarii*.

### W przypadku stwierdzenia przez upoważnionego w danej Lokalizacji pracownika Zamawiającego najpóźniej następnego Dnia Roboczego do godz. 12:00 licząc od dnia przysłania przez serwis Wykonawcy informacji kończącej bieg czasu trwania Awarii, nieskuteczności usunięcia tej Awarii, upoważniony w danej Lokalizacji pracownik Zamawiającego dokona powtórnego otwarcia, tj. wznowienia tej samej Awarii. W takim przypadku bieg czasu trwania Awarii liczy się od chwili pierwszego zgłoszenia.

### Prace konserwacyjne i naprawcze prowadzone przez Wykonawcę wewnątrz jego infrastruktury telekomunikacyjnej nie przerywają biegu czasu trwania Awarii.

## Zawieszenie biegu czasu trwania Awarii

### Zamawiający dopuszcza zawieszenie biegu czasu trwania Awarii na okres od chwili skutecznego zawieszenia przez serwis Wykonawcy do najbliższego Dnia Roboczego, do godz. 9:00, tylko po skutecznym uzgodnieniu z upoważnionym w danej Lokalizacji pracownikiem Zamawiającego w następujących przypadkach:

#### usunięcie Awarii wymaga wizyty serwisu Wykonawcy w Lokalizacji, a Awaria została zgłoszona po godz. 14:00 w ostatnim Dniu Roboczym przed dniem lub dniami ustawowo wolnymi od pracy;

#### usuwanie Awarii zgodnie z informacją przekazaną przez serwis Wykonawcy trwałoby dłużej niż od uzgodnionej godziny wizyty serwisowej do godz. 16:00. W takim przypadku naprawa musi zostać zakończona w kolejnym Dniu Roboczym bez możliwości zawieszania biegu, chyba, że upoważniony w danej Lokalizacji pracownik Zamawiającego, z przyczyn wewnętrznych Zamawiającego, w danym dniu nie może prowadzić asysty podczas usuwania Awarii.

### W przypadku braku zgody upoważnionego w danej Lokalizacji pracownika Zamawiającego na zawieszenie biegu czasu trwania Awarii serwis Wykonawcy zobowiązany jest usunąć Awarię bez zbędnej zwłoki, a bieg czasu trwania Awarii nie ulega zawieszeniu.

### Zawieszenie biegu czasu trwania Awarii Zamawiający będzie uznawał za dokonane od chwili skutecznego przesłania przez serwis Wykonawcy informacji o zdarzeniu, zgodnie z wymaganiami procedury *Zawieszenia biegu czasu trwania Awarii*, nie później niż w czasie przewidzianym na usunięcie zgłoszonej Awarii. Brak skutecznego przesłania potwierdzenia w wymaganym czasie skutkuje brakiem ważności zawieszenia biegu czasu trwania Awarii pomimo wcześniejszego uzgodnienia takiej możliwości z upoważnionym w danej Lokalizacji pracownikiem Zamawiającego.

## Rejestracja Awarii i potwierdzanie zdarzeń dla Awarii

### Upoważniony w danej Lokalizacji pracownik Zamawiającego zgłasza serwisowi Wykonawcy Awarię za pomocą faksu, emaila lub telefonu na numery lub adresy wskazane w Umowie.

### Każda Awaria otrzymuje unikalny numer identyfikacyjny nadawany przez serwis Wykonawcy w momencie jej zgłoszenia.

### Nie dopuszcza się sytuacji, w której informacje dotyczące tej samej zgłoszonej Awarii w korespondencji kierowanej do Zamawiającego posiadają inny numer identyfikacyjny nadany przez Wykonawcę oraz inny numer identyfikacyjny nadany przez ewentualnego podwykonawcę Wykonawcy odpowiedzialnego za obsługę rejestracji i potwierdzania zdarzeń dla Awarii.

### W celu potwierdzenia zgłoszenia Awarii serwis Wykonawcy jest zobowiązany, nie później niż w ciągu **15 minut** od chwili zgłoszenia Awarii, przesłać skutecznie potwierdzenie zdarzenia emailem na adres: wan\_internet@nik.gov.pl lub faksem na numer **22 4445410** zatytułowanym „Potwierdzenie zgłoszenia Awarii nr xxx”, gdzie „xxx” oznacza unikalny numer identyfikacyjny. W potwierdzeniu muszą się znaleźć przynajmniej następujące informacje: unikalny numer identyfikacyjny, data i godzina zgłoszenia, krótki opis zgłoszonej Awarii zawierający w szczególności informację o klasyfikacji Awarii, imię i nazwisko osoby zgłaszającej, imię i nazwisko osoby przyjmującej zgłoszenie.

### W celu potwierdzenia wznowienia Awarii serwis Wykonawcy jest zobowiązany, nie później niż w ciągu **15 minut** od chwili zgłoszenia Awarii, przesłać skutecznie potwierdzenie zdarzenia emailem na adres: wan\_internet@nik.gov.pl lub faksem na numer **22 4445410** zatytułowanym „Potwierdzenie ponownego otwarcia Awarii nr xxx”, gdzie „xxx” oznacza unikalny numer identyfikacyjny. W potwierdzeniu muszą się znaleźć przynajmniej następujące informacje: unikalny numer identyfikacyjny, data i godzina zgłoszenia, imię i nazwisko osoby zgłaszającej, imię i nazwisko osoby przyjmującej zgłoszenie.

### W celu potwierdzenia zmiany klasyfikacji Awarii serwis Wykonawcy zobowiązany jest skutecznie przekazać Zamawiającemu informację o zdarzeniu nie później niż w ciągu **15 minut** od stwierdzenia zmiany klasyfikacji emailem na adres: wan\_internet@nik.gov.pl lub faksem na numer **22 4445410** zatytułowanym „Zmiana klasyfikacji Awarii nr xxx”, gdzie „xxx” oznacza unikalny numer identyfikacyjny. W potwierdzeniu muszą się znaleźć przynajmniej następujące informacje: unikalny numer identyfikacyjny, data i godzina zmiany klasyfikacji, krótki opis podstawy zmiany klasyfikacji, imię i nazwisko osoby zmieniającej klasyfikację. Brak skutecznego przesłania wymaganego potwierdzenia lub brak załączenia wymaganych w potwierdzeniu informacji skutkuje brakiem ważności zmiany klasyfikacji Awarii.

### W celu potwierdzenia zawieszenia biegu czasu trwania Awarii serwis Wykonawcy zobowiązany jest skutecznie przekazać Zamawiającemu informację o zdarzeniu, nie później niż w ciągu **15 minut** od faktu zawieszenia lub przedłużenia zawieszenia, emailem na adres wan\_internet@nik.gov.pl lub faksem na numer **22 4445410** zatytułowanym "Zawieszenie zgłoszenia nr xxx”, gdzie „xxx” oznacza unikalny numer identyfikacyjny. W treści potwierdzenia muszą się znaleźć między innymi informacje na temat unikalnego numeru identyfikacyjnego, daty i godziny zawieszenia biegu czasu trwania Awarii, przyczyny zawieszenia biegu czasu trwania Awarii, imię i nazwisko osoby zawieszającej Awarię oraz imię i nazwisko upoważnionego w danej Lokalizacji pracownika Zamawiającego, z którym uzgodniono zawieszenie Awarii. Brak skutecznego przesłania wymaganego potwierdzenia lub brak załączenia wymaganych w potwierdzeniu informacji skutkuje brakiem ważności zawieszenia biegu czasu trwania Awarii.

### W celu potwierdzenia zakończenia biegu czasu trwania Awarii serwis Wykonawcy zobowiązany jest skutecznie przekazać Zamawiającemu informację o zdarzeniu za pomocą e-maila na adres wan\_internet@nik.gov.pl lub faksu na numer **22 4445410** zatytułowanego „Zamknięcie zgłoszenia nr xxx”, gdzie „xxx” oznacza unikalny numer identyfikacyjny. W treści powiadomienia muszą się znaleźć między innymi informacje na temat unikalnego numeru identyfikacyjnego, przyczyny wystąpienia Awarii, wykonanych działań koniecznych do usunięcia Awarii w szczególności po zmianie klasyfikacji oraz imię i nazwisko osoby zamykającej Awarię. Brak skutecznego przesłania wymaganego potwierdzenia lub brak załączenia wymaganych informacji w potwierdzeniu skutkuje brakiem ważności zakończenia biegu czasu trwania Awarii do czasu ponownego przesłania potwierdzenia z kompletem informacji.

### W przypadku Awarii usługi dostępu do Internetu w siedzibie Zamawiającego w Warszawie wymagane potwierdzenia, tj. potwierdzenie zgłoszenia Awarii, potwierdzenie wznowienia Awarii, potwierdzenie zmiany klasyfikacji Awarii, potwierdzenia zawieszenia biegu czasu trwania Awarii, potwierdzenie zakończenia biegu czasu trwania Awarii serwis Wykonawcy powinien skutecznie przesłać na faks Zamawiającego na numer **22 444 54 10**.

### W przypadku problemów technicznych leżących po stronie Wykonawcy, Zamawiający incydentalnie dopuszcza przekazanie stosownych potwierdzeń w formie pisemnej bezpośrednio do Biura Informatyki Zamawiającego w siedzibie w Warszawie, jednak nie później niż następnego Dnia Roboczego, do godziny 12:00.

## Zasady usuwania Awarii

### Awarię wymagającą wizyty serwisowej w Lokalizacji Zamawiającego Wykonawca może usuwać wyłącznie z asystą upoważnionego w danej Lokalizacji pracownika Zamawiającego w godz. od 8:00 do 16:00, po wcześniejszym telefonicznym (co najmniej na 1 godzinę przed planowaną wizytą) uzgodnieniu godziny wizyty z tym pracownikiem. Brak wymaganego uzgodnienia wizyty serwisowej przez Wykonawcę skutkować może nie wpuszczeniem serwisu Wykonawcy do siedziby Zamawiającego oraz skutkuje brakiem możliwości zawieszenia biegu czasu trwania Awarii.

### Wykonawca zobowiązany jest podczas uzgadniania wizyty serwisowej przekazać nazwę firmy serwisującej (w przypadku podwykonawcy) oraz dane personalne osoby lub osób, które będą uczestniczyły w danej wizycie serwisowej i będą jednocześnie osobami upoważnionymi do podpisywania protokołów w imieniu Wykonawcy. Brak podania tych danych skutkować może nie wpuszczeniem serwisu Wykonawcy do siedziby Zamawiającego oraz skutkuje brakiem możliwości zawieszenia biegu czasu trwania Awarii.

### Jeżeli Wykonawca przewiduje prowadzanie prac naprawczych na wysokości, w szczególności na dachu budynku Zamawiającego, osoby wykonujące te prace ze strony Wykonawcy muszą przedstawić upoważnionemu w danej Lokalizacji pracownikowi Zamawiającego stosowne aktualne świadectwa do pracy na wysokości i muszą posiadać właściwe zabezpieczenia umożliwiające pracę na wysokości, w szczególności na stromym dachu. W przypadku braku świadectw lub właściwego zabezpieczenia serwisanci Wykonawcy nie zostaną dopuszczeni do pracy na wysokości, a bieg czasu trwania Awarii nie zawiesza się.

### Usuwanie Awarii w Lokalizacji Zamawiającego nie może trwać jednorazowo dłużej niż 5 godzin od momentu przyjazdu serwisu Wykonawcy. Po upływie tego czasu upoważniony w danej Lokalizacji pracownik Zamawiającego ma prawo przerwać jej usuwanie, a bieg czasu trwania Awarii automatycznie nie zawiesza się.

### Jeżeli awarii uległy: Router CE lub Routery CE, lub system monitoringu, lub urządzenia telekomunikacyjne Wykonawcy (w szczególności Router CPE) i nie jest możliwe usunięcie Awarii w przewidzianym Umową czasie, serwis Wykonawcy w tym przewidzianym Umową czasie musi wstawić, skonfigurować i uruchomić urządzenie lub urządzenia zastępcze o nie gorszych parametrach niż te, które uległy awarii.

### Jeżeli wstawienie urządzenia lub urządzeń zastępczych doprowadziło do usunięcia Awarii i jednocześnie w zależności od przyczyny Awarii Funkcjonalność Sieci WAN albo dostępu do Internetu jest zgodna z wymaganiami Umowy, serwis Wykonawcy ma prawo i jednocześnie ma obowiązek przysłać Zamawiającemu informację o usunięciu Awarii, zgodnie z wymaganiami procedury *Rejestracji zdarzeń dla Awarii* w zakresie zamknięcia Awarii. W przeciwnym wypadku bieg czasu trwania Awarii nie kończy się.

### Serwis Wykonawcy wstawia i konfiguruje urządzenia zastępcze bez naliczania dodatkowych kosztów.

### Po wstawieniu urządzenia zastępczego serwis Wykonawcy dokona, w ramach gwarancji lub serwisu pogwarancyjnego naprawy Routera CE, lub systemu monitoringu w ciągu **50 dni** licząc od dnia protokolarnego przekazania do naprawy. Protokół przekazania do naprawy podpiszą upoważniony w danej Lokalizacji pracownik Zamawiającego oraz upoważniony pracownik Wykonawcy.

### Po usunięciu awarii Routera CE lub systemu monitoringu serwis Wykonawcy zobowiązany jest do ponownego jego montażu i uruchomienia w Lokalizacji Zamawiającego bez naliczania dodatkowych kosztów oraz demontażu i protokolarnego odbioru urządzenia zastępczego. Termin i godzinę montażu serwis Wykonawcy jest zobowiązany ustalić z upoważnionym w danej Lokalizacji pracownikiem Zamawiającego. W takim przypadku przerwa w świadczeniu usługi transmisji danych w Sieci WAN lub przerwa w świadczeniu usługi dostępu do Internetu będąca skutkiem montażu Routera CE w tej Lokalizacji nie jest traktowana jako Awaria i nie jest brana pod uwagę w rozliczeniu SLA.

## Czasy graniczne na usunięcie Awarii

Czasy graniczne na usunięcie Awarii Zamawiający wprowadził w celu kontroli czasu w jakim Wykonawca usuwa Awarie. W przypadku przekroczenia czasu granicznego Zamawiający naliczy Wykonawcy karę za nieprawidłowe świadczenie usługi usuwania Awarii. Zasady obliczenia kar wskazano w Umowie. Obciążenie Wykonawcy karą za brak usunięcia Awarii w wymaganym czasie nie jest równoważne naliczeniu przez Wykonawcę obniżenia opłat za brak świadczonych usług transmisji danych w Sieci WAN lub usługi dostępu do Internetu.

### Awaria usług transmisji danych w Sieci WAN:

#### Wykonawca gwarantuje skuteczne usunięcie Awarii transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS w siedzibie Zamawiającego w Warszawie w czasie wynoszącym **4 godziny** od momentu zgłoszenia Awarii;

#### Wykonawca gwarantuje skuteczne usunięcie Awarii transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS w siedzibie Zamawiającego w Warszawie w czasie wynoszącym **4 godziny** od momentu zgłoszenia Awarii;

#### Wykonawca gwarantuje skuteczne usunięcie Awarii transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS w Jednostkach Terenowych Zamawiającego w czasie wynoszącym **24 godziny** od momentu zgłoszenia Awarii;

#### Wykonawca gwarantuje skuteczne usunięcie Awarii transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS w Jednostkach Terenowych Zamawiającego w czasie wynoszącym **24 godziny** od momentu zgłoszenia Awarii.

### Awaria usługi dostępu do Internetu:

#### Wykonawca gwarantuje skuteczne usunięcie Awarii dostępu do Internetu poprzez główne łącze dla usługi dostępu do Internetu w czasie wynoszącym **4 godziny** od momentu zgłoszenia Awarii;

#### Wykonawca gwarantuje skuteczne usunięcie Awarii dostępu do Internetu poprzez zapasowe łącze dla usługi dostępu do Internetu w czasie wynoszącym **4 godziny** od momentu zgłoszenia Awarii;

### Awaria Routera CE:

#### usunięcie Awarii Routera CE przez Wykonawcę możliwe jest tylko lokalnie w danej Lokalizacji Zamawiającego i wymaga wizyty serwisu Wykonawcy w tej Lokalizacji, chyba że możliwe jest zdalne usunięcie tej Awarii z poziomu Routera CE w Warszawie;

#### Wykonawca gwarantuje skuteczne usunięcie Awarii Routera CE:

##### w przypadku gdy upoważniony pracownik Zamawiającego zgłosił Awarię w Dniu Roboczym przed godziną 14:00 - do godziny 15:00 następnego Dnia Roboczego;

##### w przypadku gdy upoważniony pracownik Zamawiającego zgłosił Awarię po godzinie 14:00 w Dniu Roboczym lub w dzień ustawowo wolny od pracy - do godziny 15:00 drugiego Dnia Roboczego liczonego od dnia zgłoszenia;

##### w przypadku zawieszenia biegu czasu trwania Awarii przez uprawnionego pracownika Zamawiającego - do godziny 15:00 następnego Dnia Roboczego.

### Awaria systemu monitoringu:

#### usunięcie Awarii systemu monitoringu przez Wykonawcę możliwe jest tylko lokalnie w danej Lokalizacji i wymaga wizyty serwisu Wykonawcy;

#### Wykonawca gwarantuje skuteczne usunięcie Awarii systemu monitoringu w danej Lokalizacji:

#### w przypadku gdy upoważniony pracownik Zamawiającego zgłosił Awarię do godziny 14:00 w Dzień Roboczy - do godziny 15:00 następnego Dnia Roboczego;

##### w przypadku gdy upoważniony pracownik Zamawiającego zgłosił Awarię po godzinie 14:00 w Dzień Roboczy lub w dzień ustawowo wolny od pracy – do godziny 15:00 drugiego Dnia Roboczego liczonego od dnia zgłoszenia;

##### w przypadku zawieszenia biegu czasu trwania Awarii przez uprawnionego pracownika Zamawiającego - do godziny 15:00 następnego Dnia Roboczego.

## SLA

SLA Zamawiający wprowadził w celu kontroli jakości i dostępności usług transmisji danych w Sieci WAN i dostępu do Internetu świadczonych przez Wykonawcę. W przypadku, w którym z dowolnych przyczyn usługa nie będzie świadczona poprawnie przez okres dłuższy od Miesięcznej Dostępności lub Rocznej Dostępności, Wykonawca jest zobowiązany do obniżenia opłaty naliczanej Zamawiającemu za tą usługę. Zasady obliczenia obniżenia opłaty wskazano w Umowie. Obniżenie przez Wykonawcę opłaty za brak świadczonych usług nie jest równoważne z naliczeniem przez Zamawiającego kary za nieprawidłowe świadczenie usługi usuwania Awarii, czyli brak usunięcia Awarii w wymaganym czasie.

### W celu definicji warunków SLA dla usług transmisji danych w Sieci WAN i dla usługi dostępu do Internetu Strony Umowy przyjmują, że miesiąc liczy **30 dni** kalendarzowych, tj. 720 godzin.

### Ze względów technicznych przyjmuje się, że usługa transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS traktowana jest jako komplet, tj. świadczona musi być jednocześnie we wszystkich Lokalizacjach Zamawiającego. Awaria choćby w jednej Lokalizacji oznacza przerwę w świadczeniu całej usługi.

### Ze względów technicznych przyjmuje się, że usługa transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS traktowana jest jako komplet, tj. świadczona musi być jednocześnie we wszystkich Lokalizacjach Zamawiającego. Awaria choćby w jednej Lokalizacji oznacza przerwę w świadczeniu całej usługi.

### Ze względów technicznych przyjmuje się, że usługa dostępu do Internetu musi być świadczona z wykorzystaniem jednocześnie głównego łącza dla dostępu do Internetu i zapasowego łącza dla dostępu do Internetu. W przypadku Awarii jednego łącza przyjmuje się, że usługa działa częściowo. Jednoczesna Awaria obu łączy oznacza przerwę w świadczeniu całej usługi.

### Czas trwania każdej zgłoszonej przez Zamawiającego Awarii:

#### usługi transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS w danej Lokalizacji Zamawiającego;

#### usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS w danej Lokalizacji Zamawiającego,

### w rozliczeniu SLA doliczany jest przez Strony Umowy do łącznego czasu trwania braku gwarantowanej dostępności tych usług odpowiednio jako całości w ramach Miesięcznej Dostępności i Rocznej Dostępności.

### Czas trwania każdej zgłoszonej przez Zamawiającego Awarii usługi dostępu do Internetu dotyczącej części tej usługi dostępnej wyłącznie poprzez:

#### główne łącze dla usługi dostępu do Internetu,

albo:

#### zapasowe łącze dla usługi dostępu do Internetu,

### w rozliczeniu SLA doliczany jest przez Strony Umowy do łącznego czasu trwania braku gwarantowanej dostępności usługi dostępu do Internetu jako całości w ramach Miesięcznej Dostępności i Rocznej Dostępności, przy czym z uwagi na to, że usługa działa częściowo, doliczana jest tylko **połowa** fatycznego czasu trwania Awarii.

### Czas trwania każdej zgłoszonej przez Zamawiającego Awarii usługi dostępu do Internetu dotyczącej całości tej usługi dostępnej poprzez:

#### główne łącze dla usługi dostępu do Internetu,

i jednocześnie:

#### zapasowe łącze dla usługi dostępu do Internetu,

### w rozliczeniu SLA doliczany jest przez Strony Umowy do łącznego czasu trwania braku gwarantowanej dostępności usługi dostępu do Internetu jako całości w ramach Miesięcznej Dostępności i Rocznej Dostępności.

### Wykonawca gwarantuje Miesięczną Dostępność usługi transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS na poziomie 99,4 %, co daje łącznie do **4 godzin** braku dostępności w ciągu jednego miesiąca.

### Wykonawca gwarantuje Miesięczną Dostępność usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS na poziomie 99,4 %, co daje łącznie do **4 godzin** braku dostępności w ciągu jednego miesiąca.

### Wykonawca gwarantuje Miesięczną Dostępność przynajmniej jednej z wymienionych usług:

#### transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS,

lub:

#### transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS,

na poziomie 99,8 %, co daje łącznie do **90 minut** całkowitej przerwy w transmisji danych w Sieci WAN w ciągu jednego miesiąca.

### Wykonawca gwarantuje Miesięczną Dostępność usługi dostępu do Internetu względem jednocześnie przynajmniej dwóch, ustalonych w czasie wdrożenia i wpisanych do dokumentacji powykonawczej referencyjnych, publicznych, nie umiejscowionych w infrastrukturze telekomunikacyjnej Wykonawcy lub kontrolowanych przez Wykonawcę i nie będących w sieci jednego operatora (właściciela) stałych adresów IP, na poziomie 99,8 % co daje łącznie do **90 minut** braku dostępności w ciągu miesiąca.

### Wykonawca gwarantuje Roczną Dostępność usługi transmisji danych w Sieci WAN z wykorzystaniem głównych Łączy IP VPN MPLS na poziomie 99,6 %, co daje łącznie do **36 godzin** braku dostępności w ciągu roku kalendarzowego.

### Wykonawca gwarantuje Roczną Dostępność usługi transmisji danych w Sieci WAN z wykorzystaniem zapasowych Łączy IP VPN MPLS na poziomie 99,6 %, co daje łącznie do **36 godzin** braku dostępności w ciągu roku kalendarzowego.

### Wykonawca gwarantuje Roczną Dostępność usługi dostępu do Internetu względem jednocześnie przynajmniej dwóch, ustalonych w czasie wdrożenia i wpisanych do dokumentacji powykonawczej referencyjnych, publicznych, nie umiejscowionych w infrastrukturze telekomunikacyjnej Wykonawcy lub kontrolowanych przez Wykonawcę i nie będących w sieci jednego operatora (właściciela) stałych adresów IP, na poziomie 99,8 % co daje łącznie do **18 godzin** braku dostępności w ciągu całego roku.

# Załącznik

„Zestawienie parametrów technicznych Routerów CE oraz serwera systemu monitoringu” znajduje się w Ofercie Wykonawcy będącej załącznikiem do Umowy i zawiera szczegółową specyfikację techniczną Funkcjonalności nowo dostarczanych Routerów CE oraz serwera na potrzeby systemu monitoringu.

# Wzory protokołów

|  |
| --- |
| **Protokół …………………………………………………….**\*) |

Na podstawie Umowy z dnia .......................20.…. r.

....................................................... zwan(y/a) dalej Wykonawcą

przekazuje **Najwyższej Izbie Kontroli** zwanej dalej Zamawiającym przedmiot pracu w postaci:

………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................

Zamawiający przyjmuje przedmiot odbioru **bez uwag / z uwagami \*\*)**:

………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................

Niniejszy protokół odbioru, sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron.

Warszawa dnia ................................................20…. r.

|  |  |
| --- | --- |
| Odbierający (NIK)  .............................................................  (czytelny podpis) | Przekazujący  .............................................................  (czytelny podpis) |

\*) wpisać rodzaj protokołu odbioru np. odbioru/odbioru końcowego/odbioru usługi, itp.

\*\*) niepotrzebne skreślić

|  |
| --- |
| **Protokół potwierdzający usunięcie Awarii** |

Na podstawie Umowy z dnia .......................20.…. r.

....................................................... zwan(y/a) dalej Wykonawcą

przekazuje **Najwyższej Izbie Kontroli** zwanej dalej Zamawiającym przedmiot odbioru w postaci:

………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................………………………………………………..................................................................................................................

Cel pobytu Wykonawcy:

………………………………………………..................................................................................................................………………………………………………..................................................................................................................

Opis wykonanych prac naprawczych:

………………………………………………..................................................................................................................………………………………………………..................................................................................................................

Awarię zgłoszono dnia: ........................................ o godzinie: .................................................

Awarię usunięto dnia: ........................................... o godzinie: .................................................

Niniejszy protokół odbioru, sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze Stron.

Warszawa dnia ................................................20…. r.

|  |  |
| --- | --- |
| Odbierający (NIK)  .............................................................  (czytelny podpis) | Przekazujący  .............................................................  (czytelny podpis) |