Załącznik nr 1 do SIWZ

„Świadczenie usług telekomunikacyjnych dla sieci WAN IMGW-PIB”

OPIS PRZEDMIOTU ZAMÓWIENIA

SPECYFIKACJA TECHNICZNA

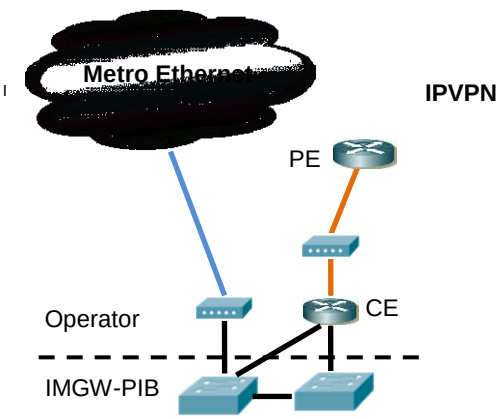
Spis treści

Załącznik nr 1 do SIWZ

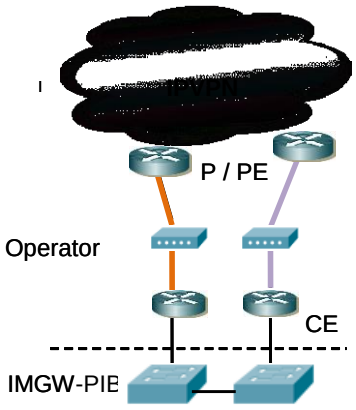
I. Podstawowe parametry usługi oraz Architektura WAN.

Ozn.	Opis
PU01	Usługa będzie świadczona od 8 marca 2018 r. do 30 czerwca 2018 r. albo do wyczerpania środków, jakie Zamawiający przeznaczył na realizację zamówienia, określonych w § 7 ust. 1 Umowy, w zależności od tego, co nastąpi wcześniej. Okres ten może zostać wydłużony maksymalnie do dnia 31 sierpnia 2018 r.
PU02	Usługa będzie tymczasowym rozwiązaniem technicznym, niezbędnym do przeprowadzenia procesu integracji usług transmisji danych i usług telefonicznych w planowanym rozwiązaniu technologicznym (realizowanym w przetargu publicznym).
PU03	Usługa będzie miała charakter kompleksowy i obejmie wszystkie lokalizacje Zamawiającego wymienione w załączniku nr 2 do SIWZ – Wykaz Lokalizacji.
PU04	Wykonawca będzie świadczył usługę transmisji danych na dwóch platformach sieciowych : IPVPN/MPLS i rozległego Ethernetu/VPLS - na bazie posiadanych (własnych lub pozyskanych) łączy dostępowych, zainstalowanych i skonfigurowanych urządzeń CE w szafach teletechnicznych wskazanych przez Zamawiającego oraz sieci szkieletowych Wykonawcy. Wykonawca udostępni wymagany sprzęt i łącza oraz będzie nimi zarządzał przez okres obowiązywania umowy.
PU05	W lokalizacjach kategorii 0 zgodnie ze Spisem Lokalizacji podstawowym systemem transmisji będzie sieć rozległego Ethernetu wykonana w technologii VPLS, opierająca się o połączenia w warstwie 2 (w odniesieniu do modelu OSI), za pomocą których zostaną podłączone urządzenia Zamawiającego. Maksymalne opóźnienie w połączeniach punkt-punkt nie może być większe niż 8 ms dla transmisji Warszawa-pozostałe lokalizacje, a maksymalny czas odpowiedzi nie może być większy niż 16 ms dla tych relacji. Pomiary powinny być wykonane w warstwie 3(L3) modelu OSI między interfejsami użytkownika na urządzeniach terminujących te połączenia. Łącze uważane jest za spełniające wymagania, jeżeli spośród 1000 wysłanych ramek o długości 1514 B (bajtów), co najmniej 900 zostanie odebranych w czasie krótszym niż 8 ms, przy utylizacji łącza na poziomie nie mniejszym niż 80%. Łącza zapasowe w lokalizacjach kategorii 0 i połączenia do pozostałych lokalizacji IMGW-PIB będą realizowane w ruchu IP (warstwa 3 modelu OSI) po sieci IPVPN/MPLS.
PU06	W ramach świadczenia usługi IPVPN, Wykonawca zainstaluje routery CE, przeprowadzi ich konfigurację oraz będzie odpowiadał za ich utrzymanie (zarządzanie, usuwanie awarii, wprowadzanie zmian konfiguracyjnych).
PU07	Wszystkie dostarczone łącza muszą być symetryczne - taka sama przepustowość dla kierunków „od” i „do” routera CE (lub urządzeń zakończenia sieci operatora).
PU08	Zamawiający wymaga, aby czas na routerach CE Wykonawcy był synchronizowany do wzorca czasu na poziomie Stratum3 Wykonawcy wg strefy czasowej UTC. Wykonawca dostarczy informacje na temat posiadanego systemu synchronizacji czasu.

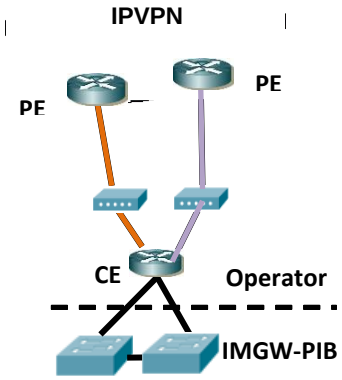
Załącznik nr 1 do SIWZ

Ozn.	Opis
PU09	Łącza podstawowe w sieci rozległego Ethernetu zostaną wykonane w technologii 1000base-T. Dla lokalizacji Warszawa w technologii 1000base-T lub 10Gbase-LRM.
PU10	Po stronie sieci lokalnej (LAN) dla usługi IPVPN, Wykonawca udostępni na routerze/routerach CE następujące interfejsy: • Lokalizacje kategorii 0 zgodnie ze Spisem Lokalizacji: 2 x 1000base-T (podstawowy i backup) z 802.1Q dla każdego VLAN na każdym routerze CE, • Lokalizacje kategorii 1 zgodnie ze Spisem Lokalizacji: 1 x FastEthernet z 802.1Q z HSRP/VVRP, • Lokalizacje kategorii 2 zgodnie ze Spisem Lokalizacji: 2 x FastEthernet z 802.1Q (podstawowy i backup), • Wszystkie pozostałe kategorie: 1 x FastEthernet z 802.1Q.
PU11	W sieci transmisji danych Zamawiającego, zbudowanej na bazie usług Wykonawcy, musi istnieć możliwość komunikacji w sieci w konfiguracji „każdy z każdym”, tak aby połączenia były nawiązywane bezpośrednio pomiędzy lokalizacjami Zamawiającego - dla obu platform transmisyjnych.
PU12	W lokalizacjach należących do ***kategorii „0”*** łącze dostępowe zostanie zrealizowane w konfiguracji: łącze podstawowe – Ethernet, łącze zapasowe – IPVPN (1PE+1CE), konfiguracja ta określa instalację pojedynczego routera dostępowego (CE), połączonego z jednym routerem szkieletowymi operatora (PE). Łącze Ethernet i łącze IPVPN mają przebiegać po dwóch rozłącznych trasach (patrz *Rysunek 2. Łącze dostępowe w konfiguracji „2CE + 2PE”*). Wymóg rozłączności tras nie dotyczy ostatniego odcinka kablowego (z wyjątkiem lokalizacji Warszawa, Kraków), stanowiącego dojście do budynku, w którym ma być świadczona usługa. ***Rysunek 1.*** *Łącze dostępowe w konfiguracji „Eth + IPVPN”* 

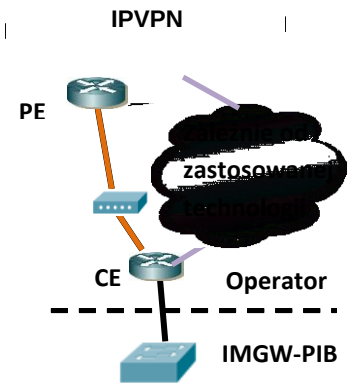
Załącznik nr 1 do SIWZ

Ozn.	Opis
PU13	W lokalizacjach należących do kategorii „1” łącze dostępowe zostanie zrealizowane w konfiguracji „2CE + 2PE”. Zakłada on instalację dwóch routerów dostępowych CE, które są połączone z dwoma różnymi routerami szkieletowymi operatora (P/PE) za pomocą dwóch łączy o rozłącznych trasach (patrz *Rysunek 2. Łącze dostępowe w konfiguracji „2CE + 2PE”*). Wymóg rozłączności tras nie dotyczy ostatniego odcinka kablowego, stanowiącego dojście do budynku, w którym ma być świadczona usługa. Wykonawca zainstaluje łącze zapasowe o takich samych parametrach, co łącze główne (niezawodność, opóźnienie, QoS, SLA). Łącza podstawowe i zapasowe będą realizowane za pomocą różnych usług podkładowych (np. DSL, Metro Ethernet, FR). ***Rysunek 2.*** *Łącze dostępowe w konfiguracji „2CE + 2PE”* 

Załącznik nr 1 do SIWZ

Ozn.	Opis
PU14	W lokalizacjach należących do kategorii „2” zostanie zrealizowane łącze dostępowe w konfiguracji „1 CE + 2 PE”, która zakłada podłączenie routera końcowego CE do dwóch różnych routerów szkieletowych operatora (P/PE) za pomocą dwóch łączy o rozłącznych trasach (patrz Rysunek *3. Łącze dostępowe w konfiguracji „1CE + 2PE”*3). Wymóg rozłączności tras nie dotyczy odcinka kablowego, od przyłącza telefonicznego w budynku gdzie będzie świadczona usługa do najbliższej studni telekomunikacyjnej, stanowiącego dojście do budynku, w którym ma być świadczona usługa. Wykonawca zainstaluje łącze zapasowe o takich samych parametrach, co łącze główne (niezawodność, opóźnienie, QoS, SLA). Łącza podstawowe i zapasowe będą realizowane za pomocą różnych usług podkładowych (np. DSL, Metro Ethernet, FR). ***Rysunek 3. Łącze dostępowe w konfiguracji „1CE + 2PE”*** 
PU15	W lokalizacjach należących do ***kategorii 3 i 4*** Wykonawca zainstaluje łącza dostępowe w konfiguracji „1 CE + 1 PE + Backup ” (jeden router CE podłączony łączem podstawowym do jednego routera P/PE Wykonawcy z dodatkowym łączem zapasowym w jednej z następujących technologii - ISDN/NAS, DSL, xDSL, Metro Ethernet, FR lub równoważnej (Rysunek4). Zamawiający wymaga, aby łącze zapasowe było uruchamiane niezwłocznie - nie dłużej niż w ciągu 30 sekund, po awarii łącza podstawowego. ***Rysunek 4.*** *Łącze dostępowe w konfiguracji „1 CE + 1 PE +Backup”*

Załącznik nr 1 do SIWZ

Ozn.	Opis
	

Załącznik nr 1 do SIWZ

<table>
<tr><th>Ozn.</th><th>Opis</th></tr>
<tr><td>PU16</td><td>W lokalizacjach należących do kategorii 5 (radary meteorologiczne), od routera CE powinny zostać poprowadzone dwa niezależne łącza do dwóch różnych routerów szkieletowych (P/PE) operatora. Wykonawca zainstaluje łącze zapasowe o takich samych parametrach, co łącze główne (niezawodność, opóźnienie, QoS, SLA). Łącza podstawowe i zapasowe będą realizowane za pomocą różnych usług podkładowych (np. DSL, Metro Ethernet, FR). Operator nie może stosować łączy radiowych (również w paśmie koncesjonowanym) jako jedynego medium dla łączy dostępowych do radarów, za wyjątkiem maksymalnie 2-miesięcznego okresu przejściowego.

Dodatkowo, łącza nie mogą powodować zakłóceń radarów meteorologicznych stosowanych przez Zamawiającego. Specyfikację radarów zawiera Tabela :

Tabela 2. Specyfikacja radarów meteorologicznych
<table>
<tr><th>l.p.</th><th>Typ radaru</th><th>Parametry</th><th>Lokalizacje</th></tr>
<tr><td>1</td><td>Meteor 1600 C
Producent: Selex Systems Integration (Gematronik), Niemcy</td><td>Typ: Dopplerowski, klistronowy
Rodzaj emisji - sygnał impulsowy
Częstotliwość pracy: 5620 MHz
Polaryzacja: pionowa, pozioma</td><td>Pastewnik, Ramża</td></tr>
<tr><td>2</td><td>Meteor 500 C:
Producent: Gematronik, Niemcy</td><td>Typ: Dopplerowski, magnetronowy
Rodzaj emisji - sygnał impulsowy
Częstotliwość pracy: 5660 MHz
Polaryzacja: pozioma</td><td>Brzuchania, Poznań, Świdwin</td></tr>
<tr><td>3</td><td>Meteor 1500C
Producent: Gematronik, Niemcy</td><td>Typ: Dopplerowski, klistronowy
Rodzaj emisji - sygnał impulsowy
Częstotliwość pracy: 5650 MHz
Polaryzacja: pozioma</td><td>Legionowo, Rzeszów, Gdańsk</td></tr>
<tr><td>4</td><td>Nieznany</td><td>Typ: Dopplerowski, magnetronowy
Rodzaj emisji - sygnał impulsowy
Częstotliwość pracy: 5650 MHz
Polaryzacja: pionowa, pozioma
Planowane oddanie do pracy operacyjnej – 2018 r.</td><td>Góra Św. Anny - w budowie</td></tr>
</table></td></tr>
<tr><td>PU17</td><td>Wykonawca może zestawić tymczasowe, ale spełniające kryteria jakościowe łącza oparte na dostępie radiowym punkt-punkt w paśmie koncesjonowanym w celu realizacji zamówienia w wymaganym terminie. Wykonawca ma obowiązek zastąpić łącza tymczasowe łączami docelowymi w terminie do 2 miesięcy od dnia uruchomienia łączy tymczasowych.</td></tr>
<tr><td>PU18</td><td>Ze względu na wymagania w zakresie bezpieczeństwa oraz potrzebę uniezależnienia transmisji WAN od warunków pogodowych, Zamawiający wyklucza możliwość (poza wyjątkiem określonym w punkcie następnym) zbudowania łączy dostępowych z wykorzystaniem:

• zasobów publicznej sieci Internet,
• łączy satelitarnych,
• łączy radiowych działających w paśmie niekoncesjonowanym,</td></tr>
</table>

Załącznik nr 1 do SIWZ

Ozn.	Opis
	• łączy radiowych typu punkt – wielopunkt, • technologii IEEE 801.11 (Wi-Fi), • łączy transmisji danych w sieciach operatorów komórkowych. Dopuszczalna jest realizacja łączy dostępowych w technologii radiowej – ale tylko punkt-punkt w paśmie koncesjonowanym, przy czym w lokalizacjach kategorii 5 łącza radiowe nie mogą stanowić jedynego medium dla łączy dostępowych, za wyjątkiem maksymalnie 2-miesięcznego okresu przejściowego.
PU19	Wyjątkiem dla zapisów w punktach PU16 i PU17 stanowi dopuszczenie linii radiowych punkt-punkt w paśmie koncesjonowanym w dwóch lokalizacjach na terenie parków narodowych: • Kasprowy Wierch, • Śnieżka, gdzie obiektywne warunki uniemożliwiają instalację sieci w oparciu o łącza kablowe. W zakresie tych lokalizacji w przypadku, gdy wykonawca zastosuje połączenie radiowe, przedstawi propozycje rozwiązań ograniczających ryzyko utraty łączności w przypadku złych warunków atmosferycznych.
PU20	Wykonawca, w ramach złożonej oferty cenowej (bez dodatkowych opłat) wykona następujące prace: • dostarczy łącza dostępowe, • zainstaluje, skonfiguruje i uruchomi wszystkie urządzenia do obsługi łącza dostępowego, w tym routery CE, • będzie zarządzał siecią IPVPN do portu LAN (FastEthernet, GigabitEthernet) w routerze CE włącznie, • będzie zarządzał siecią rozległego Ethernetu do urządzeń będących zakończeniem łącza Ethernetowego, • w wypadku wystąpienia awarii usunie ją z zachowaniem deklarowanych parametrów SLA.
PU21	Wykonawca, w ramach złożonej oferty cenowej (bez dodatkowych opłat), na żądanie Zamawiającego, wykona następujące prace: • przeniesie część łączy (jednak nie więcej, niż 10 łączy) do nowych lokalizacji z zastrzeżeniem, że instalacja łączy w nowych lokalizacjach nie będzie wymagała poniesienia przez Wykonawcę inwestycji w nowe łącza dostępowe, • zmieni przepustowość części łączy (w ramach sumarycznej wielkości użytkowanej przepływności dla każdej z sieci) z zastrzeżeniem, że zmiana parametrów nie pociągnie za sobą konieczności poniesienia inwestycji przez Wykonawcę w nowe łącze lub w nowy router CE, • wykona zlecone przez Zamawiającego zmiany w konfiguracji routerów CE, przy czym łączna liczba jednostkowych zmian w danym miesiącu będzie nie większa, niż łączna liczba użytkowanych routerów CE. Przez jednostkową zmianę rozumie się jednorazowe wykonanie kompletu zleconych zmian (routing, ACL, itd.) na pojedynczym routerze CE lub grupie routerów.
PU22	Wymagane jest, aby urządzenia końcowe CE wspierały protokół routingu OSPF, który jest

<table>
<tr><th>Ozn.</th><th>Opis</th></tr>
<tr><td></td><td>podstawowym protokołem routingu w sieci Zamawiającego.</td></tr>
<tr><td>PU23</td><td>Wykonawca dostarczy usługę IPVPN z trzema klasami ruchu (Class of service, CoS):
Klasa voice, dedykowana dla komunikacji głosowej – tylko wybrane lokalizacje przedstawione w Tabeli 3 dla wskazanych przez Zamawiającego adresów IP,
Klasa biznes, dedykowana dla aplikacji krytycznych (przekazywanie danych meteorologicznych, poczta elektroniczna itp.) – sieci prywatne oraz wskazane przez Zamawiającego adresy IP z sieci publicznej,
Klasa best effort, dedykowana dla pozostałych aplikacji (dostęp do Internetu) –sieci publiczne.</td></tr>
<tr><td>PU24</td><td>W wybranych lokalizacjach, przedstawionych w tabeli 3, sieć WAN będzie m.in. służyła do przekazywania głosu za pomocą VoIP, połączenia między centralami wymienionymi w tabeli 3 będą realizowane w klasie voice.
Tabela 1. Lokalizacje, w których WAN będzie służyła do komunikacji głosowej
<table>
<tr><th>Lokalizacja</th><th>Adres</th></tr>
<tr><td>Ośrodek Główny w Warszawie</td><td>ul. Podleśna 61, 00-967 WARSZAWA</td></tr>
<tr><td>Lokalizacja Legionowo</td><td>ul. Zegrzyńska 38, 05-119 Legionowo</td></tr>
<tr><td>Oddział we Wrocławiu</td><td>ul. Parkowa 30, 51-616 WROCŁAW</td></tr>
<tr><td>Oddział Morski w Gdyni</td><td>ul. Waszyngtona 42, 81-342 GDYNIA</td></tr>
<tr><td>Oddział w Krakowie</td><td>ul. Piotra Borowego 14, 30-215 KRAKÓW</td></tr>
<tr><td>Górnośląskie Centrum Hydrologiczno-Meteorologiczne</td><td>ul. Bratków 10, 40-045 KATOWICE</td></tr>
<tr><td>Lokalizacja Białystok</td><td>ul. Ciołkowskiego 2/3, 15-245 BIAŁYSTOK</td></tr>
<tr><td>Lokalizacja w Poznaniu</td><td>ul. Dąbrowskiego 174/176, 60-594 POZNAŃ</td></tr>
<tr><td>Lokalizacja Wrocław-Wyspa</td><td>ul. Parkowa 25, 51-616 Wrocław</td></tr>
</table></td></tr>
<tr><td>PU25</td><td>W lokalizacjach kategorii 2, 3, 4 i 5 pasmo zostanie przydzielone do klas biznes oraz best effort:
<table>
<tr><th>Klasa</th><th>Priorytet w wypadku awarii łącza głównego</th></tr>
<tr><td>Biznes</td><td>najwyższy priorytet</td></tr>
<tr><td>best ef fort</td><td>najniższy priorytet</td></tr>
</table>
W wypadku awarii łącza głównego, na łącze zapasowe zostanie przeniesiony wyłącznie ruch z klasy biznes.</td></tr>
</table>

Załącznik nr 1 do SIWZ

Ozn.	Opis
PU26	Zamawiający wymaga możliwości przypisywania pakietów IP do poszczególnych klas usług (CoS) na podstawie następujących parametrów: • adresy IP (źródłowy / docelowy), • nr portu protokołu warstwy 4 (źródłowy / docelowy), • DSCP, • etykieta VLAN (vlan tag) wg standardu IEEE 802.11q. Dokładny sposób markowania pakietów zostanie uzgodniony na etapie realizacji projektu pomiędzy przedstawicielami Wykonawcy oraz Zamawiającego. Sposób priorytetyzacji pakietów IP (przydziału do klas CoS) zostanie uzgodniony pomiędzy Wykonawcą a Zamawiającym na etapie realizacji wdrożenia.
PU27	Maksymalny czas usunięcia awarii zgodnie ze Spisem Lokalizacji.
PU28	Wszystkie łącza Wykonawca uruchomi w ciągu 7 dni roboczych od dnia podpisania umowy. Wymagany termin wynika z konieczności zapewnienia ciągłości transmisji danych w sieci WAN Zamawiającego. Obowiązek ten jest określony w zapisach ustawowych dotyczących roli i zadań Państwowej Służby Hydrologiczno – Meteorologicznej.
PU29	W terminie 2 dni roboczych od podpisania umowy Wykonawca dostarczy harmonogram wdrożenia wraz z opisem realizacji z uwzględnieniem zastosowanych technologii, informacją o parametrach i zastosowanych mediach transmisyjnych. Proces migracji poszczególnych lokalizacji będzie uzgadniany z wyprzedzeniem, pomiędzy przedstawicielami Wykonawcy oraz Zamawiającego. Proces migracji w danej lokalizacji ze starej do nowej sieci WAN powinien odbywać się z przerwami opisanymi niżej. Wykonawca przeprowadzi wdrożenia w dni powszednie, w godzinach od 8 do 16. Wykonawca przedstawi plan przełączenia z uwzględnieniem przerwy w ruchu nie dłuższej niż: • Kategoria 0 - zgodnie ze Spisem Lokalizacji: z przerwą niezbędną na przebudowanie tras routingu, nie dłuższą niż 8 minut, • Kategoria 1 – 4 zgodnie ze Spisem Lokalizacji: nie dłużej niż 2 godziny, • Kategoria 5 zgodnie ze Spisem Lokalizacji: z przerwą niezbędną na przebudowanie tras routingu, nie dłuższą niż 8 minut. W trakcie przełączania musi zostać zachowany ruch pomiędzy lokalizacjami obsługiwanymi przez łącza dostarczane dotychczasową umową i przez łącza wyłonionego w przetargu operatora o parametrach umożliwiających normalną pracę operacyjną Zamawiającego, w szczególności nie gorszych niż parametry sieci dla obecnie obowiązującej umowy. Wykonawca przedstawi do akceptacji Zamawiającego harmonogram migracji. Migracja od dnia rozpoczęcia do zakończenia nie będzie przekraczać 2 dni (w przypadku przekroczenia zostaną naliczane kary umowne). Przedmiot zamówienia będzie realizowany zgodnie z uznanymi międzynarodowymi metodykami w zakresie realizacji projektu i utrzymania.

II. Łącza do Internetu.

<table>
<tr><th>Ozn.</th><th>Opis</th></tr>
<tr><td>DI01</td><td>Wykonawca dostarczy łącza do Internetu, spełniające wymagania przedstawione w poniższej tabeli:
Tabela 2. Wymagania w zakresie łączy do Internetu
<table>
<tr><th>Lp</th><th>Lokalizacja</th><th>Konfiguracja węzła</th><th>Łącze główne</th><th>Łącze zapasowe</th><th>Max. czas usunięcia awarii [h]</th><th>Dostępność sieci [%]</th></tr>
<tr><td>1.</td><td>Warszawa</td><td>2PE+2CE</td><td>300 Mb/s</td><td>300 Mb/s</td><td>4</td><td>99.9%</td></tr>
<tr><td>2.</td><td>Kraków</td><td>1PE+1CE</td><td>100 Mb/s</td><td>-</td><td>4</td><td>99.9%</td></tr>
</table></td></tr>
<tr><td>DI02</td><td>Wykonawca wspólnie z Zamawiającym uzgodnią w jaki sposób łącza internetowe będą się wzajemnie zastępowały.</td></tr>
<tr><td>DI03</td><td>Do adresacji łączy internetowych Wykonawca wykorzysta udostępnioną przez IMGW-PIB pulę 254 publicznych adresów IP. Pula adresowa należy do klasy Provider Independent (PI) przydzielonej przez RIPE NCC dla potrzeb IMGW-PIB. Jeżeli podczas uruchamiania sieci pojawi się potrzeba przydzielenia dla któregoś z łączy internetowych dodatkowych adresów, Wykonawca przekaże do dyspozycji Zamawiającego odpowiednią dodatkową pulę adresów.</td></tr>
<tr><td>DI04</td><td>Od Wykonawcy jest wymagane, by był stroną umowy o Usługach Standardowych (Standard Service Agreement) zawartej z RIPE NCC i występował w niej jako LIR. Wykonawca będzie reprezentował Zamawiającego jako Użytkownika Końcowego przed RIPE NCC w celu przydzielenia dla Użytkownika Końcowego i utrzymania na jego rzecz Niezależnych Numerów Internetowych - zakres reprezentacji i obowiązki stron zostaną określone w osobnej umowie.</td></tr>
<tr><td>DI05</td><td>Łącza do Internetu zostaną zrealizowane jako wydzielone fizyczne łącza, zakończone stykiem w technologii FE/GE (nie jest dopuszczalne dostarczenie usługi dostępu do Internetu w ramach tego samego portu, co sieć WAN).</td></tr>
<tr><td>DI06</td><td>W lokalizacji „Warszawa” zostaną zainstalowane dwa łącza do Internetu o niezależnym przebiegu, do różnych punktów dostępowych (routerów szkieletowych) sieci Wykonawcy, zakończone routerami operatora wyposażonymi w funkcję przełączania między urządzeniem podstawowym a zapasowym (protokoły HSRP, VRRP). Węzły pracujące na styku sieci należy przystosować do funkcjonowania w oparciu o protokół BGP w celu zapewnia redundancji łączy w sposób automatyczny. Zainstalowane przez operatora routery powinny obsługiwać protokół OSPF. Lokalizacja „Gdynia” podłączona jest do operatora internetowego TASK, Zamawiający wymaga, aby połączenie z Internetem w tej lokalizacji było połączeniem zapasowym dla pozostałych połączeń do Internetu. Zamawiający wymaga dodatkowo aby dla sieci IPVPN podstawowym wyjściem do Internetu była lokalizacja Kraków lub Gdynia, w przypadku ich awarii Warszawa.</td></tr>
<tr><td>DI07</td><td>Routery dostarczone przez Wykonawcę do obsługi Internetu w Krakowie i Warszawie będą</td></tr>
</table>

	zarządzane przez Zamawiającego od złącza liniowego dostawcy. W lokalizacji „Gdynia” dla połączenia z Internetem Zamawiający posiada własny router Cisco 2821.
DI08	Internetowe rozwiązanie sieciowe zostanie doposażone o systemy bezpieczeństwa w celu ochrony przed różnego rodzaju zagrożeniami informatycznymi i atakami na sieć IMGW-PIB. Zamawiający wymaga dostarczenia i uruchomienia systemu zabezpieczeń dla wszystkich punktów dostępowych do Internetu (Warszawa, Kraków, Gdynia).
DI09	System zabezpieczeń musi być dostarczony jako dedykowane urządzenia zabezpieczeń sieciowych (appliance). W zaproponowanym systemie musi występować separacja modułu zarządzania i modułów przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta. Dla połączeń Internetowych w Gdyni i Krakowie dostarczy po jednym urządzaniu firewall, dla połączeń w Warszawie dwa urządzenia pracujące w klastrze niezawodnościowym. System udostępni jedną konsolę do konfiguracji wszystkich urządzeń firewall, Zamawijący może udostępnić na ten cel serwer wirtualny.
DI10	System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów i użytkowników w sieci wewnętrznej.
DI11	Każdy z dostarczonych firewalli musi posiadać przepływność nie mniej niż 2 Gb/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 1 Gb/s dla kontroli zawartości (w tym kontrola AV, AS, IPS i WF) i obsługiwać nie mniej niż 100 000 jednoczesnych połączeń i zapewniać ochronę dla wszystkich urządzeń wewnętrznych IMGW nie będąc wąskim gardłem dla połączeń Internetowych.
DI12	Każde z urządzeń systemu zabezpieczeń musi być wyposażone w co najmniej 6 portów Ethernet 10/100/1000.
DI13	System zabezpieczeń musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. Musi istnieć możliwość jednoczesnej konfiguracji i pracy poszczególnych interfejsów sieciowych w różnych trybach.
DI14	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1Q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi umożliwiać agregowanie linków.
DI15	Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
DI16	W ramach rozwiązania muszą zostać dostarczone kompletne, gotowe do pracy urządzenia. Wraz z produktem wymagane jest dostarczenie opieki technicznej ważnej przez okres 4 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów oraz bazy kategorii stron WWW, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

Załącznik nr 1 do SIWZ

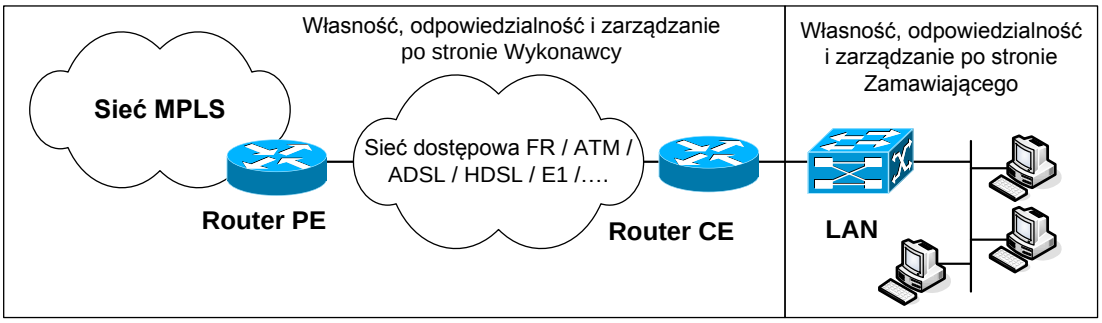
DI17	Zamawiający będzie zarządzał samodzielnie dostarczonymi routerami dla połączeń do Internetu oraz systemem zabezpieczeń, jednak oczekuje od Wykonawcy, że w ramach usługi internetowej zapewni: • instalację i wstępną konfigurację urządzeń (routerów, firewalli), • wsparcie certyfikowanego inżyniera przy konfiguracji urządzeń (routerów, firewalli), • wstępne przygotowanie reguł polityk bezpieczeństwa na podstawie dostarczonych informacji, • wsparcie w analizie zdarzeń pozwalająca na efektywną i szybką identyfikację obszarów zagrożeń bezpieczeństwa oraz odpowiednio szybką reakcję na nie, • natychmiastowe informowanie osób odpowiedzialnych po stronie Klienta za zarządzanie systemami informatycznymi, o zaobserwowanych w środowisku Wykonawcy potencjalnie groźnych dla Zamawiającego zagorżeniachpowstałych zagrożeniach oraz przypadkach naruszenia bezpieczeństwa, • podjęcie uzgodnionych z Klientem dodatkowych działań minimalizujących zidentyfikowane ryzyka.
DI18	Dostarczone system zabezpieczeń powinien realizować następujące założenia: • System zabezpieczeń musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji, • System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa, • Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ), • System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona AntiVirus i AntiSpyware), filtracja plików, danych i URL, • System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną, • System zabezpieczeń musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH, • System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które

	w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama, • System zabezpieczeń musi identyfikować co najmniej 1700 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS, nie mniej niż: Skype, Gada-Gadu, Tor, BitTorrent, eMule. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM), • System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta, • System zabezpieczeń musi umożliwiać zarządzanie, kontrolę i wgląd w ruch nierozpoznany przez urządzenie, • System zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji, • System zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego, • System zabezpieczeń musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, • System zabezpieczeń pozwoli na identyfikację zagrożeń oraz tworzenie reguł bezpieczeństwa dodatkowo dla użytkowników przechowywanych w usłudze katalogowej Zamawiającego (Active Directory).
DI19	**<u>Ochrona przed atakami DDoS:</u>** Zamawiający wymaga uruchomienia usługi ochrony przed atakami DDOS dla łączy internetowych w Warszawie (w szczególności serwerów WWW, pocztowych i DNS) w postaci: • TCP SYN flood, • UDP flood (w tym DNS reflection), • HTTP GET flood, • HTTP POST flood, • ICMP flood, • IGMP flood, • invalid packets, • IP fragments, • IP NULL

	• DNS flood • SIP request flood, • SSL negotiation
DI20	System musi zapewniać możliwość filtrowania ataków o wielkości przynajmniej 10Gbps i ochronę w warstwach ISO/OSI: od 3 do 7, przez 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Czas reakcji na zaistniałe zdarzenie lub zgłoszenie Zamawiającego maksymalnie 15 minut (SLA). Wymagany jest raport po każdej mityzacji/obronie i zbiorczy raport miesięczny dostarczany Zamawiającemu.

Załącznik nr 1 do SIWZ

III. Zarządzanie i monitorowanie sieci WAN.

Ozn.	Opis
ZM01	Wykonawca będzie zarządzał siecią IPVPN aż do portu LAN (włącznie) na urządzeniach CE znajdujących się w lokalizacjach Zamawiającego. ***Rysunek 5.*** *Podział odpowiedzialności między Zamawiającym a Wykonawcą* 
ZM02	Zamawiający oświadcza, że po jego stronie urządzeniem połączonym z routerem CE operatora może być: • przełącznik warstwy 2 i/lub 3 modelu ISO-OSI z możliwością znakowania pakietów zgodnie z IEEE 802.1Q, • przełącznik warstwy 2 i/lub 3 bez wsparcia dla IEEE 802.1Q, • router.

ZM03	Wykonawca, dla każdego łącza WAN, udostępni Zamawiającemu następujące statystyki w formie graficznej z dostępem przez www (odświeżanie danych maksymalnie co 5 minut):
	• Przepustowości na interfejsach LAN i WAN,
	• Informacje o awarii sprzętu CE oraz przełączeniu między łączem podstawowym a zapasowym,
	• Bieżące wartości parametrów QoS:
	  ○ opóźnienie pakietów (*delay*) - min, max, średnie opóźnienie w zadanym przedziale czasu,
	  ○ wariancja opóźnień (*jitter*),
	  ○ straty pakietów (*packet loss*),
	• Dostępność łącza (podstawowego i zapasowego).

ZM04	Wykonawca umożliwi generowanie komunikatów w wyniku zdarzeń lub awarii poprzez wysłanie komunikatów typu „SNMP trap”. Zamawiający posiada kolektor NNMI firmy HP i wymaga aby zdarzenia i awarie urządzeń CE dostarczonych w ramach zamówienia były rejestrowane w tym kolektorze. Zamawiający wymaga również możliwości odpytywania routerów CE przez protokół SNMP. Parametry przekazywane przez SNMP do kolektora będą uzgodnione z Zamawiającym.
ZM05	Wykonawca zapewni wysyłanie datagramów NetFlow lub Sflow ze wszystkich urządzeń CE i wszystkich ich interfejsów oraz sieci rozległego Ethernetu do wskazanej stacji monitorującej Zamawiającego.

Załącznik nr 1 do SIWZ

Ozn.	Opis
ZM06	Wykonawca zapewni Zamawiającemu dostęp do routerów końcowych (CE) przez protokół telnet lub SSH i umożliwi wykonanie następujących funkcji diagnostycznych: • *ping / extended ping z podaniem adresu lub interfejsu źródłowego, ilości powtórzeń, rozmiaru pakietu i upływu czasu* • *traceroute / extended traceroute* • *sh ip route* • *show snmp* • *show ntp status* • *sh ntp associations* • *sh clock* • *show standby* • *sh ip int brief* • *sh ip int* • *sh version* • *sh diag* • *sh controller* • *sh int* • *sh arp* • *show interfaces status* • *show interfaces switchport* • *show ip eigrp* • *show vlans* • *show vlan-switch* • *show dialer* • *show isdn active* • *show isdn history* • *show isdn status* W przypadku braku obsługi poniższych komend wymagana jest obsługa komend równoważnych dostarczających ten sam zasób informacyjny na bazie udokumentowanego języka zapytań.
ZM07	Wykonawca w okresie obowiązywania umowy będzie świadczył usługi zarządzania i administrowania urządzeniami CE w zakresie: • zdalnego zarządzania konfiguracją logiczną sieci oraz utrzymania urządzeń CE, • zmiany konfiguracji urządzeń CE na wniosek Zamawiającego, • konfigurację adresacji IP zgodnie z ustaleniami z Zamawiającym, • dokonywanie zmian w konfiguracji interfejsów w celu dołączenia sieci LAN Zamawiającego, w szczególności z zakresu routingu między wirtualnymi sieciami LAN (*Inter-VLAN routing*) oraz list dostępu (*Access List, ACL*), • naprawy lub wymiany uszkodzonego urządzenia CE, • wykrywanie awarii i naprawa łączy dostępowych, • zarządzanie siecią i monitorowanie stanu technicznego infrastruktury udostępnionej Zamawiającemu, • rozwiązywania problemów eksploatacyjnych przy pomocy Help Desk, • zapewnienia Zamawiającemu zdalnego przeglądania konfiguracji urządzeń CE

Załącznik nr 1 do SIWZ

Ozn.	Opis
	zainstalowanych we wszystkich lokalizacjach Zamawiającego w zakresie niezbędnym do monitorowania parametrów sieci, • zarządzanie CoS zgodnie z bieżącymi wymaganiami Zamawiającego, • utrzymania listy inwentaryzacyjnej wraz z informacją z dokumentacją eksploatacyjną każdego urządzenia.
ZM08	Zlecone przez Zamawiającego zmiany w konfiguracji routerów CE Wykonawca wprowadzi w ciągu 24 godzin od uzgodnienia zmian pomiędzy osobami technicznymi, wyznaczonymi przez Wykonawcę i Zamawiającego lub w terminie uzgodnionym przez Strony. Wykonanie zmiany konfiguracji przez Wykonawcę uważa się za zakończone po potwierdzeniu prawidłowego działania przez Zamawiającego.
ZM09	Wykonawca udostępni Zamawiającemu możliwość zgłaszania problemów i awarii WAN a za pomocą infolinii, faksu oraz poczty elektronicznej (e-mail). Wykonawca zapewni dedykowaną osobę (opiekuna technicznego) do kontaktu z Zamawiającym. Do jej obowiązków będzie należało przesyłanie co miesiąc raportu zawierającego: • wykonane zmiany w konfiguracji sieci; • aktualny stan inwentaryzacji i konfiguracji urządzeń, • dane odnośnie wywiązywania się Wykonawcy z deklarowanych parametrów jakości i niezawodności usług (SLA).
ZM10	Przy zgłoszeniu awarii, Wykonawca otworzy tzw. bilet problemowy, zawierający opis problemu oraz godzinę otwarcia biletu. Po rozwiązaniu problemu po stronie sieci Wykonawcy, przedstawiciel Wykonawcy skontaktuje się z przedstawicielem Zamawiającego w celu potwierdzenia usunięcia awarii. Bilet problemowy zostanie zamknięty po potwierdzeniu usunięcia awarii przez przedstawiciela Zamawiającego. Dodatkowo: • Bilet powinien zawierać tzw. numer zgłoszenia na który Zamawiający będzie się powoływał, • Treść biletu powinna być systematycznie uzupełniana przez Wykonawcę w trakcie postępu prac nad usunięciem problemu, • Otwarcie, zmiana treści i zamknięcie biletu problemowego będzie przesyłane przez Wykonawcę na adres e-mail „kontaktów technicznych” Zamawiającego. Dodatkowo każdy bilet problemowy będzie umieszczany w comiesięcznym raporcie przesyłanym przez opiekuna technicznego.

Załącznik nr 1 do SIWZ

IV. Poziom świadczenia usług i kary umowne.

Ozn.	Opis

SL01	Usługa IPVPN świadczona przez Wykonawcę będzie spełniała następujące parametry jakościowe (QoS):
	• Dla klasy voice:
	  ○ Opóźnienie w jedną stronę (*delay*) < 75 ms;
	  ○ Wariancja opóźnienia (*jitter*) < 20 ms;
	  ○ Straty pakietów w sieci operatora <0,5%;
	• Dla pozostałych klas:
	  ○ Opóźnienie w jedną stronę (*delay*) < 75 ms;
	  ○ Straty pakietów w sieci operatora <0,5%.
	Podane wyżej wymagania w zakresie opóźnienia nie dotyczą łączy dostępowych o przepustowościach 512 kb/s lub mniejszych. Dla tych łączy wymagane jest, aby opóźnienie w jedną stronę nie przekraczało 150 ms.
	W celu weryfikacji poprawności wykonania instalacji przez Wykonawcę, Zamawiający wymaga wykonania pomiarów następującą metodą:
	• 10 pakietów o długości 128B w odstępach 20ms, próbki wysyłane są co 5 mint pomiędzy elementami sieci zarządzanymi przez operatora (dla kasy D1, D2),
	• 10 pakietów o długości 64B w odstępach 20ms, próbki wysyłane są co 5 minut pomiędzy elementami sieci zarządzanymi przez operatora (dla kasy V1 i V2).
	Dla każdej z klas pomiar dokonywany oddzielnie. Do statystyk będą brane pomiary wykonane w warunkach obciążenia danej klasy usługi nieprzekraczającego wartości 75% dostępnego dla niej pasma. W przypadku, gdy warunki obciążenia nie sa respektowane, pomiar będzie odrzucany.

SL02	Wykonawca zapewnieni następujące parametry niezawodnościowe (SLA) usługi IPVPN we wszystkich relacjach koniec-koniec: • gwarancja przepustowości na poziomie 100% dostarczonego pasma, • dostępność usługi oraz czas usunięcia awarii dowolnego łącza zgodnie ze Spisem Lokalizacji, • czas reakcji na awarię (rozumianej jako przesłanie potwierdzenia przyjęcia zgłoszenia awarii oraz określenie trybu naprawy) - nie dłużej niż 1 godzina, liczona od zgłoszenia awarii przez Zamawiającego.
SL03	Usługa serwisu technicznego będzie obejmowała usuwanie problemów pracy z siecią po ich zgłoszeniu przez Zamawiającego na specjalnie do tego celu wydzielony numer telefoniczny do Centrum Kontaktu operatora (Biura Obsługi Klienta), dostępny bez przerwy - 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku. Powyższy numer telefoniczny powinien być dostępny wg standardowych stawek operatora lub bezpłatnie, niedopuszczalne jest zastosowanie numeru o podwyższonej płatności (np. 0-700).
SL04	Wykonawca dołoży wszelkich starań, aby prace serwisowe, wymagające dostępu do routerów i modemów, były dokonywane przez Wykonawcę zdalnie. W przypadkach, gdy zdalny dostęp z przyczyn technicznych nie będzie możliwy, odpowiednie działania mające na

Załącznik nr 1 do SIWZ

Ozn.	Opis
	celu przywrócenie poprawnej pracy urządzeń i łącza powinny być wykonywane w lokalizacji Zamawiającego po wcześniejszym uzgodnieniu terminu i zakresu prac z Zamawiającym. Wykonawca powiadomi o prowadzonych zdalnie pracach serwisowych przesyłając powiadomienie na adresy e-mail „kontaktów technicznych” Zamawiającego.
SL05	Wszelkie prace modernizacyjne w sieci WAN – poza tzw. oknem serwisowym operatora – muszą być zgłaszane i uzgadniane z Zamawiającym na minimum 7 dni roboczych przed rozpoczęciem prac.
SL06	Wykonawca zapłaci kary umowne z tytułu niedotrzymania parametrów SLA: a) Bonifikatę z tytułu niedotrzymania Gwarantowanego Czasu Usunięcia Awarii ustala się na podstawie poniższego wzoru: **Bonifikata za Awarię = (tA-TG)*KA**, gdzie: • Ta – Czas usunięcia Awarii [h], zaokrąglony wzwyż do pełnej godziny • TG – Gwarantowany czas usunięcia Awarii [h] • KA – bonifikata w wysokości 4 % miesięcznego abonamentu za łącze b) Bonifikatę z tytułu niedotrzymania Gwarantowanej dostępności usług transmisji danych ustala się na podstawie poniższego wzoru: **Całkowita bonifikata = [TA – MA*(Tusługi/T)]*KD**, gdzie: • MA – maksymalna liczba godzin Awarii dopuszczalna dla danego Poziomu Usługi [h] • TA – suma czasów trwania wszystkich Awarii w danym roku kalendarzowym [h] • Tusługi – czas korzystania z Usługi Podstawowej w danym roku kalendarzowym [h] • T – liczba godzin w danym roku kalendarzowym [h] • KD – bonifikata w wysokości 4 % miesięcznego abonamentu za łącze. • Wynik działania [TA – MA*(Tusługi/T)] – zaokrągla się wzwyż do pełnej godziny.
SL07	Wykonawca zapłaci kary umowne z tytułu opóźnienia w uruchomieniu łączy w stosunku do terminów zawartych w umowie na poziomie 300% miesięcznego abonamentu za łącze, za każdy kolejny rozpoczęty tydzień po terminie zawartym w umowie.
SL08	W ramach oferowanej ceny za łącza (bez dodatkowych opłat): a) Wykonawca przeprowadzi szkolenia z obsługi sieci dla pracowników Zamawiającego: • Zakres szkoleń: o Poziom Podstawowy: ▪ Informacje ogólne o systemie i technologii MPLS i VPLS, ▪ procedury zgłaszania awarii, ▪ podstawowe narzędzia monitorowania sieci;

Załącznik nr 1 do SIWZ

Ozn.	Opis
	○ Poziom Zaawansowany: ▪ Informacje ogólne o systemie i technologii MPLS i VPLS, ▪ procedury zgłaszania awarii i modyfikacji sieci, ▪ narzędzia monitorowania i administrowania siecią, ▪ narzędzia diagnozowania błędów; • Liczba uczestników szkoleń: ○ Poziom podstawowy – 2 ○ Poziom zaawansowany – 2 • Termin szkolenia zostanie ustalony z Wykonawcą w trakcie realizacji Umowy. b) Wykonawca przeprowadzi dla pracowników Zamawiającego szkolenia w języku polskim z dostarczonego systemu zabezpieczeń. Szkolenia będą posiadały autoryzację producenta dostarczonego systemu zabezpieczeń: • Zakres szkolenia - Konfiguracja i zarządzanie zaproponowanym systemem zabezpieczeń. • Liczba uczestników szkoleń: 2 osoby • Termin szkolenia zostanie ustalony z Wykonawcą w trakcie realizacji Umowy. c) Wykonawca przeprowadzi dla pracowników Zamawiającego zaawansowane szkolenia z zakresu konfiguracji oraz optymalizacji protokołu routingu BGP na poziomie zaawansowanym. Szkolenie będzie posiadało autoryzację producenta dostarczonych routerów internetowych: • Zakres szkolenia: ○ Wprowadzenie do protokołu BGP ○ Tranzytowe systemy autonomiczne ○ Atrybuty BGP (mechanizmy wyboru drogi) ○ Filtrowanie routingu i dobór tras w BGP ○ Rozwiązania typu BGP route reflector ○ Rozwiązania typu BGP confederations ○ Rozwiązania bazujące na Multi-Exit Discriminator ○ Rozwiązania bazujące na AS-path prepending ○ Rozwiązania bazujące na BGP communities ○ Tłumienie niestabilnych ścieżek w BGP (route flap dampening) ○ Łączenie sieci klienckich do sieci Internet Service Provider za pomocą BGP ○ Optymalizacja pracy BGP • Liczba uczestników szkoleń: 2 osoby • Termin szkolenia zostanie ustalony z Wykonawcą w trakcie realizacji Umowy.