OPIS PRZEDMIOTU ZAMÓWIENIA

Usługa dostępu do Internetu z łączem podstawowym i zapasowym, mechanizmem automatycznego przełączania (failover), ochroną AntyDDoS, usługami DNS oraz redundancją urządzeń brzegowych

1 Cel i zakres zamówienia

Celem zamówienia jest zapewnienie Urzędowi Zamówień Publicznych (UZP) w lokalizacji Warszawa, ul. Postępu 17A, 02-676, ciągłego, bezpiecznego i wysokodostępnego dostępu do Internetu poprzez dwa niezależne łącza transmisyjne, przy zachowaniu niezależności infrastrukturalnej. Zamówienie ma na celu minimalizację ryzyka utraty dostępu do Internetu w wyniku awarii infrastruktury lub usług jednego operatora, poprzez zapewnienie alternatywnej ścieżki transmisji danych, niezależnej pod względem technicznym i fizycznym.

1.1 Zakres rzeczowy

Przedmiotem zamówienia jest świadczenie usługi dostępu do Internetu obejmującej:

1. Dostarczenie dwóch niezależnych łączy transmisyjnych do punktu adresowego Warszawa, ul. Postępu 17A, 02-676, spełniających następujące warunki:
    - Łącze podstawowe: światłowodowe, spełniające wymagania opisane w 7.1 Parametry łącza podstawowego (światłowodowego).
    - Łącze zapasowe: światłowodowe lub radiowe spełniające wymagania opisane w 7.2 Parametry łącza zapasowego – dwa warianty (równoważne).
2. Zapewnienie niezależności infrastrukturalnej obu łączy, zgodnie z definicją w rozdziale 6 Warunki niezależności tras i punktów zakończenia infrastruktury.
3. Dostawę, instalację i konfigurację redundantnych urządzeń brzegowych (CPE) oraz wdrożenie i utrzymanie mechanizmu automatycznego, bezobsługowego przełączania (failover) pomiędzy łączami, gwarantującego nieprzerwaną dostępność usług.

4. Świadczenie usług wsparcia technicznego, monitoringu, raportowania operacyjnego oraz serwisu, obejmujących:
    - Ciągły (24/7/365) monitoring parametrów technicznych obu łączy transmisyjnych, urządzeń brzegowych (CPE), usług DNS oraz ochrony AntyDDoS.
    - Powiadamianie Zamawiającego o wykrytych awariach i incydentach zgodnie z wymaganiami SLA.
5. Świadczenie usług ochrony AntyDDoS, usług DNS (Secondary DNS i revDNS z możliwością samodzielnego zarządzania rekordami przez UZP) oraz zapewnienie ciągłości działania tych usług na obu łączach.
6. Przeprowadzenie testów odbiorczych, okresowych oraz przekazanie dokumentacji powykonawczej i przeprowadzenie szkolenia personelu UZP w zakresie obsługi urządzeń brzegowych, procedur awaryjnych, panelu AntyDDoS i DNS.
7. Przeprowadzenie testów odbiorczych, okresowych oraz przekazanie dokumentacji powykonawczej i przeprowadzenie szkolenia personelu UZP.

1.2 Okres i terminy

- Okres świadczenia: 24 miesiące + opcjonalne wznowienie 2 x 12 miesięcy.
- Uruchomienie:
    - łącze podstawowe do 20 dni kalendarzowych od zawarcia umowy;
    - łącze zapasowe do 90 dni kalendarzowych od zawarcia umowy.

2 Klasyfikacja CPV

- 72400000-4 Usługi internetowe
- 72411000-4 Dostawcy usług internetowych

3 Warunki udziału

1. Wykonawca musi posiadać aktualny wpis do Rejestru Przedsiębiorców Telekomunikacyjnych prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej (UKE).
2. Weryfikacja wpisu będzie dokonywana na podstawie publicznie dostępnego rejestru RPT, dostępnego pod adresem: https://rejestry.uke.gov.pl/rejestr_rpt.

4 Uzasadnienie braku kryteriów jakościowych w ocenie ofert

Wszystkie istotne wymagania jakościowe, funkcjonalne, techniczne oraz organizacyjne zostały szczegółowo określone w Opisie Przedmiotu Zamówienia (OPZ). Dotyczy to w szczególności:

- Parametrów technicznych łączy transmisyjnych (przepustowość, opóźnienia, utrata pakietów, niezależność tras, redundancja urządzeń brzegowych),
- Poziomów dostępności usług (SLA) oraz czasów reakcji i naprawy,
- Wymagań dotyczących ochrony AntyDDoS, usług DNS, monitoringu i raportowania,
- Wymagań dotyczących doświadczenia, kompetencji personelu oraz infrastruktury technicznej,
- Szczegółowych procedur odbioru, testów, dokumentacji oraz szkoleń,
- Warunków serwisu, wsparcia technicznego i obsługi incydentów bezpieczeństwa,
- Wymagań formalnych (wpis do rejestru UKE).

Wszystkie powyższe wymagania mają charakter minimalny i są obligatoryjne dla wszystkich Wykonawców. Oznacza to, że jakość usługi została w całości opisana w OPZ.

5 Definicje i skróty

- **Awaria zwykła** – za awarię zwykłą uznaje się sytuację, w której
    - nastąpi całkowita utrata dostępności jednego z łączy transmisyjnych (podstawowego lub zapasowego), przy zachowanej dostępności drugiego łącza,
    - nastąpi degradacja parametrów technicznych jednego z łączy (przepustowość, opóźnienia, utrata pakietów) o więcej niż 30% wartości gwarantowanej w OPZ przez okres dłuższy niż 10 minut, skutkująca istotnym ograniczeniem jakości lub dostępności usług, ale bez całkowitej utraty funkcjonalności,
    - wystąpią inne zdarzenia skutkujące ograniczeniem funkcjonalności usług (np. częściowa utrata adresacji IP, ograniczona funkcjonalność usług DNS lub AntyDDoS), które nie uniemożliwiają realizacji usług kluczowych, lecz wpływają na ich jakość lub dostępność.

- **Awaria krytyczna** - za awarię krytyczną uznaje się sytuację, w której:
    - nastąpi całkowita utrata dostępności obu łącz transmisyjnych,
    - nastąpi degradacja parametrów łącza podstawowego (przepustowości, opóźnienia, utraty pakietów) do poziomu mniejszego niż 30% przy jednoczesnej degradacji parametrów łącza zapasowego o więcej niż 80% wartości gwarantowanej w OPZ przez okres dłuższy niż 5 minut,
    - wystąpią inne zdarzenia skutkujące brakiem możliwości realizacji usług kluczowych (np. utrata adresacji IP, brak działania mechanizmu failover, brak ochrony AntyDDoS).
- **Incydent bezpieczeństwa** - każde zdarzenie, które powoduje lub może spowodować naruszenie poufności, integralności, dostępności lub autentyczności usług telekomunikacyjnych świadczonych na rzecz Zamawiającego:
    - Atak zewnętrzny lub wewnętrzny na infrastrukturę telekomunikacyjną, urządzenia brzegowe (CPE), systemy DNS lub mechanizmy ochrony AntyDDoS, skutkujący:
        - niedostępnością usług (całkowitą lub częściową),
        - nieautoryzowanym dostępem do zasobów lub danych,
        - przejęciem kontroli nad urządzeniami lub usługami,
        - modyfikacją lub usunięciem danych konfiguracyjnych.
    - Wykrycie prób lub realizacji ataków typu DDoS, DoS, spoofing, phishing, malware, ransomware, brute force, skanowanie podatności, włamanie do systemów telekomunikacyjnych lub usług DNS.
    - Nieautoryzowane zmiany konfiguracji urządzeń sieciowych, usług DNS, mechanizmów failover lub ochrony AntyDDoS, niezależnie od tego, czy skutkują one natychmiastową niedostępnością usług.
    - Wykrycie podatności lub luk bezpieczeństwa w infrastrukturze telekomunikacyjnej, które mogą zostać wykorzystane do naruszenia bezpieczeństwa usług.
- **Czas reakcji** – czas liczony od momentu wystąpienia jednego z poniższych zdarzeń (w zależności od tego, które nastąpi wcześniej):
    - zgłoszenia awarii lub incydentu bezpieczeństwa przez Zamawiającego za pośrednictwem systemu zgłoszeń, telefonu lub e-mail,

    - automatycznego wykrycia awarii lub incydentu przez system monitoringu Wykonawcy,
    - do momentu podjęcia przez Wykonawcę działań naprawczych oraz powiadomienia Zamawiającego o przyjęciu zgłoszenia i rozpoczęciu działań.
- **Czas naprawy** – czas liczony od momentu wystąpienia jednego z poniższych zdarzeń (w zależności od tego, które nastąpi wcześniej):
    - zgłoszenia awarii lub incydentu bezpieczeństwa przez Zamawiającego,
    - automatycznego wykrycia awarii lub incydentu przez system monitoringu Wykonawcy,
    - do momentu pełnego przywrócenia funkcjonalności usług zgodnie z wymaganiami OPZ.
- **Dostępność parametru usługi** - procentowy udział czasu, w którym parametr usługi spełniał SLA, w stosunku do całkowitego czasu w danym okresie rozliczeniowym.
- **CPE** – urządzenie brzegowe (Customer Premises Equipment).
- **CIR/EIR** – Committed/Excess Information Rate.
- **BGP** – Border Gateway Protocol; BFD – Bidirectional Forwarding Detection.
- **VRRP** – Virtual Router Redundancy Protocol (lub równoważny mechanizm brzegowy).
- **RTBH/Flowspec** – mechanizmy mitygacji DDoS w warstwie routingu.
- **L3/L4/L7** – warstwy modelu OSI (sieciowa/transportowa/aplikacyjna).
- **DNS** (Secondary, revDNS) – odpowiednio serwer zapasowy i odwrotne mapowanie nazw.
- **SLA** – poziomy świadczenia usług;
- **KPI** – wskaźniki efektywności.

6 Warunki niezależności tras i punktów zakończenia infrastruktury

6.1 Definicja niezależności tras i punktów zakończenia

Za niezależne usługi internetowe uznaje się łącza internetowe, które spełniają łącznie następujące warunki:

1. **Niezależność fizyczna tras**: Trasy przesyłowe obu łączy muszą być całkowicie niezależne na odcinku od punktu wejścia do budynku Zamawiającego do najbliższego węzła dystrybucyjnego/operatora (POP), z dopuszczeniem wspólnego przebiegu na odcinku nie dłuższym niż 200 metrów liczonym w promieniu od punktu adresowego Warszawa, ul. Postępu 17A. Poza tym odcinkiem trasy muszą być w pełni odseparowane.
2. **Niezależność węzła dystrybucyjnego (POP)**: Każde z łączy transmisyjnych (podstawowe i zapasowe) musi być zakończone w odrębnym węźle dystrybucyjnym/operatora (POP), zlokalizowanym w innym budynku niż węzeł dystrybucyjny drugiego łącza. Za odrębne węzły dystrybucyjne uznaje się wyłącznie takie, które są fizycznie zlokalizowane w różnych budynkach, posiadają niezależne przyłącza do sieci szkieletowej oraz nie współdzielą infrastruktury pasywnej (np. zasilania, klimatyzacji, systemów bezpieczeństwa) w ramach tego samego obiektu.
3. **Niezależność systemów i urządzeń**: Każde z łączy musi być zakończone na odrębnym, niezależnym urządzeniu brzegowym (CPE).
4. **Brak współdzielenia infrastruktury pasywnej**: Brak współdzielenia kanalizacji teletechnicznej, studzienek, przepustów, masztów radiowych na odcinku poza dopuszczonym fragmentem.
5. **Niezależność usługowa**: Każde z łączy musi zapewniać pełną funkcjonalność usługową (adresacja IP, ochrona AntyDDoS, DNS, monitoring, SLA, wsparcie serwisowe) niezależnie od drugiego łącza.

6.2 Weryfikacja spełnienia warunków niezależności

1. Wykonawca zobowiązany jest do przedstawienia na etapie składania oferty:
    a. Oświadczenia o spełnieniu warunków niezależności tras i punktów zakończenia infrastruktury.
    b. Map przebiegu tras obu łączy, od punktu wejścia do budynku Zamawiającego do najbliższego węzła dystrybucyjnego/operatora (POP).
2. Wykonawca zobowiązany jest na etapie odbioru usługi łącza podstawowego lub zapasowego do przedstawienia:

    a. Kopii umów SLA lub oświadczeń operatorów potwierdzających poziomy SLA nie gorsze niż wymagane w OPZ – jeśli wybrane łącze jest świadczone przez podwykonawcę,
    b. Wskazania punktów wejścia do budynku.
3. W przypadku wykrycia naruszenia warunków niezależności tras i punktów zakończenia infrastruktury w trakcie trwania umowy, Zamawiający może:
    a. żądać wymiany łącza na spełniające wymagania, bez dodatkowych kosztów,
    b. rozwiązać umowę.

7 Wymagania funkcjonalne i wydajnościowe

7.1 Parametry łącza podstawowego (światłowodowego)

- Przepustowość dostępowa: ≥ 1 Gbps symetrycznie; CIR=EIR; brak limitów transferu i blokad protokołów/portów.
- Medium: światłowód (zakończenie w szafie rack UZP, poziom −1).
- Adresacja: minimum 32 publiczne adresy IPv4 w jednej puli PA (własność operatora), dedykowane dla UZP.
- DNS: Secondary DNS i revDNS; zarządzanie rekordami przez UZP.
- Ochrona AntyDDoS: zgodnie z rozdz. 8.

7.2 Parametry łącza zapasowego – dwa warianty (równoważne)

Zamawiający oczekuje realizacji łącza zapasowego w jednym z dwóch poniższych wariantów A lub B.

7.2.1 A) Światłowodowe (osobna trasa):

- Przepustowość dostępowa: ≥ 300 Mbps symetrycznie; CIR=EIR; brak limitów transferu i blokad protokołów/portów.
- Pozostałe wymagania jak dla łącza podstawowego.

7.2.2 B) Radiowe (punkt–punkt, wyłącznie pasmo licencjonowane):

- Przepustowość dostępowa: ≥ 300 Mbps symetrycznie; CIR=EIR.
- Stały monitoring parametrów radiowych (co najmniej RSSI, MSE/BER, modulacja, spektrum).
- DNS i AntyDDoS jak dla łącza podstawowego.

7.3 Redundancja i separacja

- Zamawiający wymaga, aby trasy światłowodowe (lub radiowe) łączy podstawowego i zapasowego spełniały kryteria niezależności opisanej w **Błąd! Nie można odnaleźć źródła odwołania.**.
- Dopuszcza się cross-connect w siedzibie UZP do innych operatorów.
- Wykonawca zapewnia redundancję urządzeń brzegowych (CPE). Oznacza to, że łącze podstawowe i zapasowe docelowo mają być zakończone na dwóch niezależnych, redundantnych urządzeniach CPE, zapewniających pełną ciągłość działania w przypadku awarii jednego z nich. Wymagane jest, aby po wdrożeniu redundancji:
    - każde z łączy było fizycznie zakończone na oddzielnym urządzeniu CPE,
    - urządzenia te współpracowały w trybie wysokiej dostępności (np. VRRP lub równoważny mechanizm),
    - awaria jednego urządzenia nie powodowała utraty dostępności usług.
- Dopuszcza się, aby w okresie dostępności wyłącznie łącza podstawowego, usługa była świadczona na jednym urządzeniu CPE. Uruchomienie łącza zapasowego musi zostać wykonane razem z konfiguracją redundancji (tj. uruchomienie drugiego, niezależnego urządzenia CPE oraz wdrożeniem mechanizmu 7.4 Failover i ciągłość adresacji).

7.4 Failover i ciągłość adresacji

- UZP nie posiada własnej puli PI ani numeru AS. Dopuszcza się adresację PA (własność operatora). UZP przewiduje pozyskanie własnej adresacji w trakcie umowy; po pisemnym zgłoszeniu nowej puli Wykonawca przeprowadzi rekonfigurację w terminie do 10 dni roboczych (bez dodatkowych opłat za zmianę konfiguracji).
- W przypadku braku własnej puli adresowej PI oraz numeru AS po stronie Zamawiającego, dopuszcza się realizację mechanizmu failover poprzez szybkie przełączenie obsługi DNS (DNS failover) z czasem propagacji (TTL) nie dłuższym niż 60 sekund.
- Wykonawca zobowiązany jest do wdrożenia i utrzymania rozwiązania umożliwiającego automatyczne wykrycie awarii łącza podstawowego i automatyczną zmianę wpisów DNS na adresację łącza zapasowego, bez konieczności ręcznej ingerencji Zamawiającego.

- W przypadku pozyskania przez Zamawiającego własnej puli PI/AS w trakcie trwania umowy, Wykonawca zobowiązany jest do rekonfiguracji usługi zgodnie z nowymi danymi, bez dodatkowych opłat.

7.5 DNS

- Secondary DNS i revDNS dla puli operatora; samodzielne zarządzanie rekordami przez UZP (panel www).

8 Ochrona AntyDDoS (wymagana na obu łączach)

8.1 Zakres i funkcjonalności minimalne

- Ochrona w warstwie 3 oraz 4 modelu OSI: ochrona wolumetryczna, co najmniej przed: SYN/UDP/ICMP Flood, HTTP GET/POST Flood, SSL/TLS (nieprawidłowe/niekompletne sesje), spoofing źródeł, źródła botnetowe.
- Niezależne ustawianie reguł i poziomów reakcji usługi dla każdego publicznego adresu IP: 10 serwisów www, VPN, końcówka usługi wideokonferencyjnej (rozprawy zdalne).
- Mechanizmy: automatyczna i ręczna mitygacja, BGP Flowspec/RTBH po stronie operatora, filtracja oparta na nagłówkach i wyrażeniach regularnych dla TCP/UDP/HTTP/DNS, limity RPS/QPS.
- Gwarantowany wolumen ochrony: ≥ 5 Gbps.
- Panel klienta (PL lub EN) z dostępem dla UZP.
- Powiadomienia e-mail o incydentach spełniających progi uzgodnione w dokumentacji operacyjnej.
- Możliwość przerwania mitygacji na żądanie UZP (czas realizacji ≤ 15 min) lub jako opcja do samodzielnego przerwania mitygacji w panelu klienta.

9 Monitoring, SLA, wsparcie

9.1 Monitoring usług

1. Wykonawca zobowiązany jest do zapewnienia ciągłego (24/7/365) monitoringu parametrów technicznych obu łączy transmisyjnych (podstawowego i zapasowego), urządzeń brzegowych (CPE), usług DNS oraz ochrony AntyDDoS.
2. Monitoring obejmuje co najmniej: przepustowość, opóźnienia, utratę pakietów, dostępność łącza, status urządzeń CPE, status usług DNS i AntyDDoS.

3. Zamawiający otrzymuje dostęp do panelu monitoringu online (PL lub EN), umożliwiającego bieżący podgląd parametrów, historię zdarzeń oraz generowanie raportów.
4. W przypadku wykrycia awarii zwykłej, awarii krytycznej lub incydentu bezpieczeństwa, system monitoringu automatycznie generuje powiadomienie e-mail do wskazanych osób po stronie Zamawiającego.
5. Powiadomienia muszą być generowane nie później niż 15 minut od wykrycia zdarzenia.
6. Zamawiający ma prawo do przeprowadzenia niezależnych pomiarów kontrolnych będących podstawą do weryfikacji dostępności usługi i jej parametrów:
    a. Zamawiający bada przepustowość z użyciem serwisu https://www.speedtest.pl/. Pomiary wykonywane w ten sposób są podstawą do określenia poziomu przepustowości łącza w trakcie trwania umowy.
    b. Opóźnienie (RTT) oraz utratę pakietów Zamawiający bada przez wykonanie polecenia ping: czas trwania ponad 5 minut na trzy adresy: biznes.gov.pl, polskacyfrowa.gov.pl, punktu wymiany ruchu IP podanego przez Wykonawcę. Wynik jest uśredniany.
    c. Status usług DNS Zamawiający bada poprzez zapytania DNS.
    d. Status usług AntyDDoS Zamawiający bada poprzez symulacje obciążenia lub testy penetracyjne.

9.2 Czas reakcji i naprawy

1. Maksymalne czasy reakcji i naprawy:
    a. Awaria krytyczna lub incydent bezpieczeństwa:
        i. czas reakcji: do 15 minut,
        ii. czas naprawy: do 4 godzin.
    b. Awaria zwykła:
        i. czas reakcji: do 1 godziny,
        ii. czas naprawy: do 24 godzin.
2. Wymagane czasy reakcji i naprawy dotyczą wszystkich elementów infrastruktury i usług objętych zamówieniem, niezależnie od tego, czy awaria lub incydent wystąpił w infrastrukturze własnej Wykonawcy, czy u podwykonawców/operatorów trzecich, z wyłączeniem przypadków siły wyższej oraz przerw serwisowych uprzednio uzgodnionych z Zamawiającym.
3. Czas reakcji i naprawy liczony jest w trybie ciągłym (24/7/365), niezależnie od pory dnia i dnia tygodnia.
4. Wykonawca zobowiązany jest do prowadzenia rejestru wszystkich zgłoszeń, awarii i incydentów bezpieczeństwa w systemie zgłoszeń (ticketowym) oraz do przekazywania Zamawiającemu raportu po każdej awarii lub incydencie, zawierającego:

a. datę i godzinę wykrycia lub zgłoszenia,
b. datę i godzinę podjęcia działań,
c. datę i godzinę usunięcia awarii/incydentu,
d. opis przyczyny i podjętych działań,
e. informację o dotrzymaniu lub przekroczeniu czasów reakcji i naprawy.

9.3 Obowiązek powiadomienia telefonicznego

1. W przypadku wystąpienia awarii krytycznej, Wykonawca zobowiązany jest do niezwłocznego, bezpośredniego powiadomienia Zamawiającego telefonicznie na wskazany numer alarmowy, nie później niż w ciągu 15 minut od wykrycia awarii przez system monitoringu lub otrzymania zgłoszenia od Zamawiającego. Powiadomienie musi być równolegle przekazane e-mailem oraz przez system zgłoszeniowy.
2. Powiadomienie telefoniczne musi zawierać: identyfikację usługi, opis awarii, przewidywany czas podjęcia działań naprawczych oraz dane kontaktowe osoby prowadzącej sprawę po stronie Wykonawcy.
3. W przypadku, gdy Zamawiający wejdzie w posiadanie informacji o wystąpieniu awarii krytycznej, a w ciągu 15 minut nie otrzyma powiadomienia telefonicznego od Wykonawcy, Zamawiający ma prawo naliczyć karę umowną w wysokości kosztu jednego miesiąca za łącze, które uległo awarii.

9.4 Poziomy SLA dla usług transmisyjnych

1. Dostępność miesięczna usług, rozumiana jako czas bez awarii krytycznej oraz zwykłej:
   a. Łącze podstawowe (światłowód): ≥ 99,5% w skali miesiąca.
   b. Łącze zapasowe: światłowód ≥ 99,5% w skali miesiąca; radiolinia ≥ 99,0% w skali miesiąca.
2. Planowane prace serwisowe mogą być prowadzone wyłącznie po uprzednim zgłoszeniu Zamawiającemu z co najmniej 7-dniowym wyprzedzeniem.
3. Prace serwisowe nie mogą powodować niedostępności usług w godzinach 8:00–16:00 w dni robocze, z wyjątkiem sytuacji awaryjnych.
4. Maksymalne średnie opóźnienie (RTT) do punktu wymiany ruchu IP: ≤ 10 ms, mierzone w godzinach szczytu (8:00–18:00) jako średnia z 10 pomiarów w ciągu godziny.
5. Maksymalne średnie opóźnienie (RTT) do trzech serwisów: biznes.gov.pl, polskacyfrowa.gov.pl, punktu wymiany ruchu IP podanego przez Wykonawcę ≤ 20 ms, mierzone w godzinach szczytu (8:00–18:00) jako średnia z 10 pomiarów w ciągu godziny.
6. Maksymalny poziom utraty pakietów ≤ 0,1% w dowolnym 10-minutowym oknie pomiarowym do punktu wymiany ruchu IP podanego przez Wykonawcę.

7. Maksymalny poziom utraty pakietów ≤ 1% (średnio) w dowolnym 5-minutowym oknie pomiarowym dla każdego z trzech serwisów: biznes.gov.pl, polskacyfrowa.gov.pl, punktu wymiany ruchu IP podanego przez Wykonawcę.

9.5 SLA dla DNS

1. Dostępność usług DNS (Secondary DNS, revDNS, panel zarządzania rekordami): ≥ 99,9% w skali miesiąca.
2. Czas reakcji na zgłoszenie awarii DNS maksymalnie 1 godzina od zgłoszenia lub wykrycia przez system monitoringu.

9.6 SLA dla AntyDDoS

1. Maksymalnie 15 minut od wykrycia ataku przez system ochrony.
2. Maksymalnie 5 minut od przekroczenia progów detekcyjnych.
3. Maksymalnie 72 godziny od zakończenia ataku.
4. Wykonawca zapewnia dostęp do panelu online z historią incydentów, zawierający informacje o rozmiarze, typie, źródle/ASN, czasie trwania, zastosowanych środkach mitygacji.

9.7 Wsparcie techniczne i obsługa zgłoszeń

1. Zgłoszenia awarii, incydentów i zapytań serwisowych przyjmowane są całodobowo (24/7/365) przez telefon oraz portal klienta.
2. Na żądanie Zamawiającego, Wykonawca sporządza raport kwartalny (w formacie PDF/XLSX), obejmujący: dostępność usług, zgłoszenia i awarie, czasy reakcji i napraw, testy failover, incydenty bezpieczeństwa, rekomendacje dotyczące poprawy jakości usług.

10 Instalacja, dostęp do budynku, BHP

1. Prace instalacyjne powinny być realizowane w uzgodnieniu z zarządcą budynku (Adgar).
2. Wykonawca odpowiada za uzyskanie wymaganych zgód i pokrycie opłat związanych z pracami instalacyjnymi i eksploatacyjnymi.

11 Odbiory, testy i dokumentacja

11.1 Testy odbiorcze (w obecności UZP)

- Testy przepustowości:
    - Rzeczywista prędkość nie może być niższa niż 90% prędkości dostępowej.

    - Metody: średnia z dwóch niezależnych pomiarów – narzędzie Wykonawcy oraz speedtest.pl; dopuszcza się badania usługowe wg ITU-T Y.1564 i/lub procedury RFC 2544 (dla warstwy 2/3).

- Testy opóźnień:
    - Maksymalne średnie opóźnienie (RTT) do punktu wymiany ruchu IP: ≤ 10 ms, jako średnia z 10 pomiarów.
    - Maksymalne średnie opóźnienie (RTT) do trzech serwisów: biznes.gov.pl, polskacyfrowa.gov.pl, punktu wymiany ruchu IP podanego przez Wykonawcę ≤ 20 ms, jako średnia z 10 pomiarów.
    - Maksymalny poziom utraty pakietów ≤ 0,1% w 10-minutowym oknie pomiarowym do punktu wymiany ruchu IP podanego przez Wykonawcę.
    - Maksymalny poziom utraty pakietów ≤ 1% (średnio) w 5-minutowym oknie pomiarowym dla każdego z trzech serwisów: biznes.gov.pl, polskacyfrowa.gov.pl, punktu wymiany ruchu IP podanego przez Wykonawcę.
    - Metoda: ICMP Ping.
- Test failover:
    - Symulacja awarii łącza podstawowego; automatyczne przełączenie ≤ 60 s.
    - Weryfikacja parametrów ruchowych na łączu zapasowym (jak wyżej). Powrót do pracy na łączu podstawowym; brak utraty sesji krytycznych (VPN, VoIP, usługi biznesowe) – dopuszczalne ponowne zestawienie w ramach protokołów, jeśli aplikacja na to pozwala.

11.2 Testy okresowe

- Raz na rok Wykonawca zrealizuje testy failover i raport pokontrolny (zestawienie czasu przełączenia, obserwowane parametry).
- Zamawiający ma prawo do przeprowadzenia niezależnych pomiarów kontrolnych w dowolnym momencie trwania umowy.

11.3 Dokumentacja i szkolenia

- Na dokumentacje powykonawczą składają się: schematy połączeń, trasy światłowodów/radiolinii (mapy), zdjęcia instalacji, protokoły pomiarowe, dokumentacja użytkownika AntyDDoS (progi, polityki, kontakty i eskalacja).
- Szkolenie: administracja CPE, procedury awaryjne, panel AntyDDoS/DNS (min. 4 h dla 4 osób).

12Zgłoszenia, serwis, podwykonawcy

- Kanały: telefon lub portal 24/7/365; potwierdzenie przyjęcia zgłoszenia ≤ 15 min (powiadomienie email); dostęp do statusu zgłoszenia w portalu klienta.

13Prawo opcji

1. Zamawiający zgłosi Wykonawcy zamiar skorzystania z prawa opcji w formie pisemnej (w tym e-mail), z wyprzedzeniem co najmniej 30 dni przed planowaną datą rozpoczęcia świadczenia usługi w ramach opcji.
2. W zgłoszeniu Zamawiający wskaże:
    a. zakres prawa opcji (np. liczba dodatkowych adresów IPv4, rozszerzenie przepustowości, wydłużenie okresu umowy),
    b. okres, na jaki dana opcja ma zostać uruchomiona.
3. Usługa w ramach prawa opcji będzie świadczona przez okres wskazany w zgłoszeniu Zamawiającego, nie dłuższy niż okres obowiązywania umowy (w tym okres opcji).
4. Cena za realizację prawa opcji zostanie ustalona zgodnie z ofertą Wykonawcy.

13.1 Wydłużenie obowiązywania umowy do dwóch razy o kolejne 12 miesięcy.

1. Zamawiający zastrzega sobie prawo do jednokrotnego lub dwukrotnego wydłużenia okresu obowiązywania umowy o kolejne 12 miesięcy każdorazowo, na warunkach identycznych jak w okresie podstawowym, w szczególności w zakresie:
    a. parametrów SLA,
    b. cen jednostkowych i zasad rozliczeń,
    c. zakresu usług,
    d. kar umownych,
    e. zasad waloryzacji (zgodnie z postanowieniami umowy).
2. Decyzja o skorzystaniu z prawa opcji na każdy kolejny okres 12 miesięcy jest niezależna i podejmowana odrębnie.
3. O zamiarze skorzystania z prawa opcji Zamawiający poinformuje Wykonawcę w formie pisemnej, z co najmniej 30-dniowym wyprzedzeniem przed upływem okresu podstawowego lub poprzedniego okresu opcji.
4. W okresie opcji mogą być realizowane również pozostałe elementy prawa opcji, o ile Zamawiający zgłosi taką potrzebę.

13.2 Zakup dodatkowego, stałego adresu ipv4 (1 adres) do 12 adresów maksymalnie

1. Zamawiający może w trakcie obowiązywania umowy (w tym w okresie opcji) zgłosić zapotrzebowanie na przydzielenie dodatkowych, stałych adresów IPv4, w liczbie od 1 do 12 adresów łącznie.
2. Adresy IPv4 muszą być publiczne i przydzielone z regionu geograficznego Polska/Europa.
3. Dopuszcza się przydział adresów z innych pul niż pula adresów podstawowych.
4. Dodatkowe adresy IPv4 muszą być dostępne na obu łączach (podstawowym i zapasowym) z zachowaniem mechanizmu failover.
5. Zamawiający może zgłosić zapotrzebowanie na jeden lub kilka adresów jednocześnie, w jednym zgłoszeniu.
6. Dla dodatkowych adresów IPv4 obowiązują standardowe ustawienia DNS (w tym revDNS) oraz ochrona AntyDDoS na zasadach identycznych jak dla adresów podstawowych.
7. Dodatkowe adresy IPv4 muszą być stale aktywne przez cały okres umowy, bez możliwości czasowego wyłączenia.
8. Cena jednostkowa za każdy dodatkowy adres IPv4 jest stała przez cały okres obowiązywania umowy.
9. Nie przewiduje się możliwości zwrotu lub rezygnacji z przydzielonych adresów IPv4 w trakcie trwania umowy.

13.3 Rozszerzenie przepustowości łącza podstawowego do 2 Gbps razem z modyfikacją ochrony AntyDDoS do parametrów nowego łącza.

1. Zamawiający może w trakcie obowiązywania umowy (w tym w okresie opcji) zgłosić jednorazowe rozszerzenie przepustowości łącza podstawowego z 1 Gbps do 2 Gbps prędkości dostępowej.
2. Rozszerzenie przepustowości jest nieodwracalne i nie przewiduje się możliwości powrotu do niższej przepustowości ani dalszego zwiększenia powyżej 2 Gbps.
3. Po rozszerzeniu przepustowości muszą zostać zachowane wszystkie dotychczasowe parametry SLA (czas reakcji, dostępność, czas naprawy).
4. Wszelkie prace związane z rozszerzeniem przepustowości muszą być realizowane poza godzinami pracy Zamawiającego (tj. poza 8:00–16:00 w dni robocze) lub w terminie uzgodnionym z Zamawiającym, a ewentualna niedostępność usługi musi być uprzednio uzgodniona i zaakceptowana przez Zamawiającego.
5. Po rozszerzeniu przepustowości Zamawiający musi mieć możliwość dalszego korzystania z dotychczasowych adresów IPv4 bez konieczności rekonfiguracji po stronie UZP.

6. Po zakończeniu prac Wykonawca przeprowadzi testy odbiorcze w obecności przedstawiciela Zamawiającego, obejmujące co najmniej:
    a. testy przepustowości (potwierdzenie osiągnięcia minimum 1,8 Gbps w obu kierunkach),
    b. testy failover,
    c. testy skuteczności ochrony AntyDDoS.
7. Cena miesięczna za usługę po rozszerzeniu przepustowości jest ustalana, zgodnie z cennikiem przedstawionym na etapie składania ofert.

14 Warunki rozliczeń i podstawy do naliczenia kar umownych

1. Wynagrodzenie Wykonawcy obejmuje miesięczny abonament za świadczenie usług dostępu do Internetu, adresacji IP, DNS, usług AntyDDoS, serwisu, monitoringu, raportowania oraz opłat dla zarządcy, obejmujących łącze podstawowe oraz łącze zapasowe, zgodnie z ofertą Wykonawcy.
2. Rozliczenia dokonywane są w okresach miesięcznych, z zastrzeżeniem postanowień poniżej dotyczących momentu uruchomienia poszczególnych łączy.
3. Opłata abonamentowa za łącze podstawowe naliczana jest od dnia podpisania protokołu odbioru potwierdzającego uruchomienie i prawidłowe działanie łącza podstawowego razem z kosztami usług adresacji IP, DNS, AntyDDoS, serwisu, monitoringu, raportowania oraz opłat dla zarządcy.
4. Opłata abonamentowa za łącze zapasowe naliczana jest od dnia podpisania protokołu odbioru potwierdzającego uruchomienie i prawidłowe działanie łącza zapasowego razem z kosztami adresacji IP, usługi DNS, AntyDDoS, serwisu, monitoringu, raportowania oraz opłat dla zarządcy.
5. Do momentu uruchomienia łącza zapasowego Zamawiający ponosi opłaty wyłącznie za łącze podstawowe.
6. W przypadku uruchomienia łącza zapasowego w trakcie trwającego okresu rozliczeniowego (roku), opłata za łącze zapasowe za pierwszy okres rozliczeniowy zostanie naliczona proporcjonalnie do liczby dni pozostałych do końca tego okresu.
7. Analogicznie, w przypadku uruchomienia innych elementów opcji (np. dodatkowych adresów IPv4, rozszerzenia przepustowości), opłata za te elementy naliczana jest od dnia ich odbioru, proporcjonalnie do okresu świadczenia usługi w danym okresie rozliczeniowym.
8. W przypadku niedostępności któregokolwiek z łączy z przyczyn leżących po stronie Wykonawcy, Zamawiającemu naliczy kary umowne określone w umowie, proporcjonalnie do czasu i zakresu niedostępności, zgodnie z zapisami dotyczącymi SLA i kar umownych.

9. W przypadku całkowitej niedostępności łącza zapasowego przez okres dłuższy niż 7 dni kalendarzowych, Zamawiający ma prawo do proporcjonalnego obniżenia opłaty abonamentowej za to łącze o wartość dwukrotności opłaty za okres niedostępności.
10. Kary umowne:
    a. Za opóźnienie w uruchomieniu łącza podstawowego lub zapasowego w stosunku do terminów określonych w umowie, Zamawiający naliczy karę umowną w wysokości 0,5% wynagrodzenia miesięcznego brutto za każde rozpoczęte 24 godziny opóźnienia, nie więcej jednak niż 10% łącznego wynagrodzenia miesięcznego brutto za dany element.
    b. Za niespełnienie wymaganego poziomu dostępności miesięcznej dla łącza podstawowego lub zapasowego, Zamawiający naliczy karę umowną w wysokości 10% opłaty miesięcznej brutto za każde rozpoczęte 0,5 punktu procentowego poniżej progu SLA, maksymalnie do 50% opłaty miesięcznej brutto za dane łącze.
    c. W przypadku gdy Zamawiający samodzielnie zidentyfikuje awarię lub incydent, który trwał dłużej niż maksymalny czas przewidziany na powiadomienie Zamawiającego przez Wykonawcę, Zamawiający naliczy karę umowną w wysokości 30% miesięcznego wynagrodzenia brutto za każde takie zdarzenie.
    d. W przypadku całkowitej niedostępności łącza zapasowego przez okres dłuższy niż 2 dni kalendarzowe, Zamawiający ma prawo do proporcjonalnego obniżenia opłaty abonamentowej za to łącze o wartość trzykrotności opłaty za okres niedostępności.
    e. Łączna wysokość kar umownych i obniżeń naliczonych w danym okresie rozliczeniowym nie może przekroczyć 80% wynagrodzenia należnego za ten okres.
    f. Łączna wysokość kar umownych i obniżeń naliczonych za cały okres obowiązywania umowy nie może przekroczyć 30% łącznego wynagrodzenia brutto.
    g. W przypadku powtarzających się naruszeń obowiązków Wykonawcy przejawiających się naliczeniem kar za 3 lub więcej miesięcy w okresie 12-miesięcy, Zamawiający zastrzega sobie prawo do rozwiązania umowy ze skutkiem natychmiastowym z winy Wykonawcy.
11. Kary nie są naliczane w przypadkach, gdy przyczyna awarii lub incydentu leży poza wpływem Wykonawcy (siła wyższa).

14.1 Waloryzacja

1. Ceny określone w ofercie Wykonawcy są stałe przez pierwsze 12 miesięcy obowiązywania umowy. Po upływie tego okresu, Wykonawca może wystąpić z wnioskiem o waloryzację ceny (łącza lub opcji), jeżeli spełnione zostaną warunki

określone poniżej. Waloryzacja może być dokonywana nie częściej niż raz na 12 miesięcy, a maksymalna zmiana ceny nie może przekroczyć 10% w stosunku do ceny pierwotnej.

2. Wniosek o waloryzację ceny opcji powinien zostać złożony w formie pisemnej wraz z uzasadnieniem i dokumentacją potwierdzającą spełnienie warunków waloryzacji. Zmiana ceny obowiązuje od pierwszego dnia miesiąca następującego po miesiącu, w którym wniosek został skutecznie złożony i zaakceptowany przez Zamawiającego.
3. Waloryzacja ceny jednostkowej za dodatkowy, stały adres IPv4 (opcja) może nastąpić, jeżeli średnia cena rynkowa adresów IPv4 w regionie Polska/Europa, publikowana przez co najmniej dwa niezależne źródła branżowe (np. RIPE, IPv4.Global, IPXO), wzrośnie o co najmniej 10% w stosunku do ceny z okresu sprzed 12 miesięcy. Wniosek o waloryzację musi zawierać dokumentację potwierdzającą zmianę cen rynkowych.
4. Waloryzacja wynagrodzenia Wykonawcy z tytułu świadczenia usług dostępu do Internetu (łączy podstawowego i zapasowego, lub łącza zwiększonego w wyniku opcji do 2 gbps), obejmujące abonament miesięczny za dostęp do Internetu, adresację IP, DNS, usługi AntyDDoS, serwis, monitoring, raportowanie oraz opłaty dla zarządcy, może nastąpić, jeżeli zmiana r/r średniego miesięcznego kosztu usługi w PL wynikającego z publikacji OECD „fixed broadband basket, high user”[1], będzie wynosić więcej niż 10%. Wniosek o waloryzację musi zawierać dokumentację potwierdzającą zmianę cen rynkowych.

15 Wymagania formalne i zgodność

- Wykonawca posiada wpis do rejestru przedsiębiorców telekomunikacyjnych UKE właściwy dla usług światłowodowych lub radiowych.
- Wykonawca posiada certyfikat ISO/IEC 27001 lub równoważny potwierdzający wdrożenie systemu zarządzania bezpieczeństwem informacji, wydany przez niezależną jednostkę certyfikującą, lub udokumentowane procedury bezpieczeństwa obejmujące:
    - politykę bezpieczeństwa informacji,
    - zarządzanie incydentami,
    - zarządzanie dostępem,
    - zarządzanie ciągłością działania,
    - regularne audyty bezpieczeństwa.

[1] https://www.oecd.org/en/topics/broadband-statistics.html

- Język dokumentacji i instrukcji: polski.
- W ramach realizacji nie przewiduje się przetwarzania danych osobowych będących w posiadaniu UZP.

16 Załączniki (wzory)

- Załącznik 1: Protokół odbioru instalacji i uruchomienia (testy przepustowości, failover, DNS).
- Załącznik 1a: Protokół odbioru uruchomienia usługi AntyDDoS
- Załącznik 2: Protokół testów okresowych (failover, parametry).
- Załącznik 3: Wzór raportu kwartalnego (na żądanie).
- Załącznik 5: Wytyczne Adgar Plaza do wykonywania prac w kompleksie.
- Załącznik 6: Wzór formularza ofertowego

Załącznik nr 1 do Umowy

Protokół odbioru instalacji i uruchomienia usługi dostępu do Internetu

Urząd Zamówień Publicznych, Warszawa, ul. Postępu 17A

1. Dane podstawowe

- Data odbioru: .....
- Wykonawca: .....
- Przedstawiciel Wykonawcy: .....
- Przedstawiciel Zamawiającego: .....

2. Zakres odbioru

Protokół dotyczy:

☐ Instalacja i uruchomienie łącza podstawowego
☐ Instalacja i uruchomienie łącza zapasowego

Usługi towarzyszące:

☐ Instalacja i konfiguracja urządzeń brzegowych (CPE)
☐ Konfiguracja usług DNS
☐ Przydzielenie adresów IP
☐ Testy failover (jeśli dotyczy łącza zapasowego)

---

3. Wyniki testów odbiorczych

3.1 Testy przepustowości

Łącze	Przepustowość wymagana	Wynik testu 1 (Mbps)	Wynik testu 2 (Mbps)	Średnia (Mbps)	Spełnienie wymagań (TAK/NIE)
Podstawowe	≥ 900 (dla 1 Gbps)				
Zapasowe	≥ 270 (dla 300 Mbps)				

Metoda testu: ☐ narzędzie Wykonawcy ☐ speedtest.pl ☐ ITU-T Y.1564 ☐ RFC 2544

Uwagi do testów: .....

3.2 Test failover

- Symulacja awarii łącza podstawowego: Czas przełączenia (w sekundach): ..... (wymagane ≤ 60 s)
- Utrata sesji krytycznych (VPN, VoIP, usługi biznesowe): ☐ NIE ☐ TAK (szczegóły: .....)
- Powrót do pracy na łączu podstawowym: ☐ TAK ☐ NIE
- Spełnienie wymagań failover: ☐ TAK ☐ NIE

Uwagi: .....

3.3 Testy parametrów jakościowych

Parametr	Wymaganie OPZ	Wynik testu	Spełnienie wymagań (TAK/NIE)
Opóźnienie RTT (do punktu wymiany ruchu IP)	≤ 10 ms (średnia z 10 pomiarów)		
Opóźnienie RTT (do 3 serwisów)	≤ 20 ms (średnia z 10 pomiarów)		
Utrata pakietów (do punktu wymiany ruchu IP)	≤ 0,1% (10-min. okno)		
Utrata pakietów (do 3 serwisów)	≤ 1% (5-min. okno)		

Metoda: ICMP Ping

3.4 Testy DNS

- Secondary DNS: ☐ działa poprawnie ☐ nie działa
- revDNS: ☐ działa poprawnie ☐ nie działa
- Panel zarządzania rekordami: ☐ dostępny ☐ niedostępny

Spełnienie wymagań DNS: ☐ TAK ☐ NIE

Uwagi: .....

3. Dokumentacja powykonawcza

- Schematy połączeń: ☐ przekazano ☐ nie przekazano
- Mapy tras światłowodów/radiolinii: ☐ przekazano ☐ nie przekazano

- Zdjęcia instalacji: ☐ przekazano ☐ nie przekazano
- Protokoły pomiarowe: ☐ przekazano ☐ nie przekazano

4. Szkolenie personelu

- Data szkolenia: .....
- Liczba przeszkolonych osób: .....
- Tematyka: ☐ administracja CPE ☐ procedury awaryjne ☐ panel DNS ☐ panel AntyDDoS

Potwierdzenie przeprowadzenia szkolenia: ☐ TAK ☐ NIE

5. Uwagi końcowe

.....

6. Oświadczenia

Oświadczam, że wszystkie wymagania określone w OPZ i umowie zostały spełnione w zakresie instalacji i uruchomienia usługi dostępu do Internetu. Oświadczam, że przekazano kompletną dokumentację powykonawczą.

..... Przedstawiciel Wykonawcy (data, podpis)

..... Przedstawiciel Zamawiającego (data, podpis)

Załączniki do protokołu:

- Dokumentacja powykonawcza

Załącznik nr 1a do Umowy

Protokół odbioru uruchomienia usługi AntyDDoS

Urząd Zamówień Publicznych, Warszawa, ul. Postępu 17A

1. Dane podstawowe

Data odbioru: .....

Wykonawca: .....

Przedstawiciel Wykonawcy: .....

Zamawiający: Urząd Zamówień Publicznych

Przedstawiciel Zamawiającego: .....

2. Zakres odbioru

2.1 Protokół dotyczy: ☐ Uruchomienie i konfiguracja usługi AntyDDoS na łączu podstawowym ☐ Uruchomienie i konfiguracja usługi AntyDDoS na łączu zapasowym

2.2 Usługi towarzyszące:

- Konfiguracja panelu klienta
- Ustawienie reguł ochrony dla wskazanych usług
- Przekazanie dokumentacji użytkownika AntyDDoS

3. Wyniki testów odbiorczych

3.1 Testy funkcjonalności

Panel klienta: ☐ dostępny ☐ niedostępny

Możliwość samodzielnego zarządzania regułami: ☐ TAK ☐ NIE

Powiadomienia e-mail: ☐ działają ☐ nie działają

Możliwość przerwania mitygacji: ☐ TAK ☐ NIE

3.2 Testy penetracyjne (organizowane przez Zamawiającego)

Data testu: .....

Rodzaj testu: ☐ SYN Flood ☐ UDP Flood ☐ HTTP Flood ☐ inne: .....

Wynik testu:

- Skuteczność blokady ataku: ☐ TAK ☐ NIE
- Czas reakcji systemu: ..... min (wymagane ≤ 15 min)

- Raport z incydentu wygenerowany: ☐ TAK ☐ NIE Uwagi: .....

4. Dokumentacja powykonawcza

Dokumentacja użytkownika AntyDDoS: ☐ przekazano ☐ nie przekazano

Polityki i progi ochrony: ☐ przekazano ☐ nie przekazano

Dane kontaktowe i ścieżka eskalacji: ☐ przekazano ☐ nie przekazano

5. Szkolenie personelu

Data szkolenia: .....

Liczba przeszkolonych osób: .....

Tematyka: ☐ panel AntyDDoS ☐ procedury awaryjne

Potwierdzenie przeprowadzenia szkolenia: ☐ TAK ☐ NIE

6. Uwagi końcowe

.....

7. Oświadczenia

Oświadczam, że wszystkie wymagania określone w OPZ i umowie zostały spełnione w zakresie uruchomienia i konfiguracji usługi AntyDDoS. Oświadczam, że przekazano kompletną dokumentację powykonawczą.

8. Podpisy stron

..... Przedstawiciel Wykonawcy (data, podpis)

..... Przedstawiciel Zamawiającego (data, podpis)

Załączniki do protokołu:

- Raporty z testów penetracyjnych
- Dokumentacja powykonawcza
- Lista obecności ze szkolenia

Protokół testów okresowych (failover, parametry)

Urząd Zamówień Publicznych, Warszawa, ul. Postępu 17A

1. Dane podstawowe

Data testu: .....

Wykonawca: .....
Przedstawiciel Wykonawcy: .....
Zamawiający: Urząd Zamówień Publicznych Przedstawiciel

Zamawiającego: .....

2. Zakres testów okresowych

☐ Test failover ☐ Testy przepustowości ☐ Testy parametrów jakościowych (opóźnienia, utrata pakietów) ☐ Testy DNS ☐ Testy AntyDDoS (jeśli dotyczy)

3. Wyniki testów

3.1 Test failover Data i godzina testu: .....

Czas przełączenia (w sekundach): .....

Utrata sesji krytycznych: ☐ NIE ☐ TAK (szczegóły: .....)

Powrót do pracy na łączu podstawowym: ☐ TAK ☐ NIE Uwagi:
.....

3.2 Testy przepustowości

Łącze	**Przepustowość wymagana**	**Wynik testu 1 (Mbps)**	**Wynik testu 2 (Mbps)**	**Średnia (Mbps)**	**Spełnienie wymagań (TAK/NIE)**
Podstawowe	≥ 900 (dla 1 Gbps)				
Zapasowe	≥ 270 (dla 300 Mbps)				

Metoda testu: ☐ narzędzie Wykonawcy ☐ speedtest.pl ☐ ITU-T Y.1564 ☐ RFC 2544
Uwagi: .....

3.3 Testy parametrów jakościowych

Opóźnienie RTT: ..... ms

Utrata pakietów: ..... %

Uwagi: .....

3.4 Testy DNS

Secondary DNS: ☐ działa poprawnie ☐ nie działa revDNS: ☐ działa poprawnie ☐ nie działa Panel zarządzania rekordami: ☐ dostępny ☐ niedostępny

Uwagi: .....

3.5 Testy AntyDDoS (jeśli dotyczy)

Data testu: .....

Rodzaj testu: ☐ SYN Flood ☐ UDP Flood ☐ HTTP Flood ☐ inne: .....

Wynik testu:

- Skuteczność blokady ataku: ☐ TAK ☐ NIE
- Czas reakcji systemu: ..... min

Uwagi: .....

4. Uwagi końcowe

.....

5. Podpisy stron

..... Przedstawiciel Wykonawcy (data, podpis)

..... Przedstawiciel Zamawiającego (data, podpis)

Załączniki do protokołu:

- Wyniki testów (wydruki, screeny)

Załącznik nr 3 do Umowy - Wzór raportu kwartalnego (na żądanie)

Urząd Zamówień Publicznych, Warszawa, ul. Postępu 17A

1. Dane podstawowe

Okres raportowania: od ..... do .....

Data sporządzenia raportu: .....

Wykonawca: .....

Przedstawiciel Wykonawcy: .....

Zamawiający: Urząd Zamówień Publicznych

Przedstawiciel Zamawiającego: .....

2. Dostępność usług (SLA)

Usługa	Wymagana dostępność (%)	Dostępność w okresie raportowania (%)	Liczba przerw	Uwagi
Łącze podstawowe	≥ 99,5			
Łącze zapasowe	≥ 99,5 (światłowód) / ≥ 99,0 (radiolinia)			
Usługi DNS	≥ 99,9			
Ochrona AntyDDoS	≥ 99,9			

3. Zgłoszenia, awarie i czasy reakcji

Data zgłoszenia	Typ zgłoszenia (awaria/incydent/serwis)	Usługa	Czas reakcji [min]	Czas naprawy [h]	Status	Uwagi
(data)						

- Średni czas reakcji: ..... min
- Średni czas naprawy: ..... h
- Liczba zgłoszeń przekraczających SLA: .....
- Opis przyczyn przekroczeń SLA (jeśli wystąpiły): .....

4. Testy failover

- Data przeprowadzenia testu: .....
- Czas przełączenia (w sekundach): ..... (wymagane ≤ 60 s)
- Utrata sesji krytycznych: ☐ NIE ☐ TAK (szczegóły: .....)
- Uwagi do testu:
  .....

5. Incydenty bezpieczeństwa i ochrona AntyDDoS - istotne

Data incydentu	Typ ataku/incydentu	Usługa/adres IP	Rozmiar ataku [Gbps]	Czas trwania [min]	Zastosowane środki	Skuteczność mitygacji	Uwagi
(data)							

- Liczba incydentów przekraczających progi raportowania: .....
- Powiadomienia e-mail: ☐ TAK ☐ NIE
- Raporty po incydentach: ☐ przekazano ☐ nie przekazano

6. Weryfikacja usług DNS

- Secondary DNS: ☐ działa poprawnie ☐ nie działa
- revDNS: ☐ działa poprawnie ☐ nie działa
- Panel zarządzania rekordami: ☐ dostępny ☐ niedostępny
- Uwagi:
  .....

7. Wnioski i rekomendacje

- Ocena realizacji SLA: ☐ spełnione ☐ niespełnione (szczegóły poniżej)
- Rekomendacje dotyczące poprawy jakości usług: .....
  .....
- Inne uwagi: .....

8. **Podpisy**

..... Przedstawiciel Wykonawcy (data, podpis)

..... Przedstawiciel Zamawiającego (data, podpis)

Załączniki do raportu:

- Zestawienia wszystkich zgłoszeń i incydentów (PDF/XLSX)
- Wyniki testów (wydruki, screeny)
- Raporty po incydentach bezpieczeństwa (jeśli wystąpiły)

Załącznik 5: Wytyczne Adgar Plaza do wykonywania prac w kompleksie **(w formie plików PDF załączonych do OPZ)**

Załącznik nr 6 do OPZ - Formularz ofertowy

1. Dane Wykonawcy

- Pełna nazwa Wykonawcy:
  .....
- Adres siedziby:
  .....
  .....
- NIP: ..... REGON: .....
- Osoba do kontaktu (imię, nazwisko, telefon, e-mail):
  .....

2. Oferowana cena za realizację zamówienia podstawowego

Lp.	Nazwa elementu	Jednostka	Ilość	Cena jednostkowa netto [PLN]	Wartość netto [PLN]	VAT [%]	Wartość brutto [PLN]
1	Abonament miesięczny za łącze podstawowe (światłowodowe) wraz z usługami: dostęp do Internetu, DNS, AntyDDoS, serwis, monitoring, raportowanie, opłaty dla zarządcy	miesiąc	24				
2	Abonament miesięczny za łącze zapasowe (światłowodowe/radiowe) wraz z usługami: dostęp do Internetu, DNS, AntyDDoS, serwis, monitoring, raportowanie, opłaty dla zarządcy	miesiąc	24				
3	Koszt miesięczny za udostępnienie puli 32 publicznych adresów	miesiąc	24				

	IPv4 (PA) dla UZP (adresacja podstawowa)		
4	Instalacja, konfiguracja i uruchomienie usługi (obejmuje oba łącza, urządzenia CPE, konfigurację failover, szkolenie, dokumentację)	ryczałt	1
	RAZEM wartość netto		
	RAZEM wartość brutto		

Uwaga:

- Wartości należy podać z dokładnością do dwóch miejsc po przecinku.

3. Cennik opcji (zgodnie z rozdz. 10 OPZ)

3.1. Dodatkowe, stałe adresy IPv4 (maks. 12 adresów)

Lp.	Nazwa opcji	Jednostka	Cena jednostkowa netto [PLN]	VAT [%]	Cena jednostkowa brutto [PLN]
1	Dodatkowy, stały adres IPv4 (publiczny, dostępny na obu łączach, ochrona AntyDDoS, DNS)	adres/miesiąc			

3.2. Rozszerzenie przepustowości łącza podstawowego do 2 Gbps

Lp.	Nazwa opcji	Jednostka	Cena miesięczna netto [PLN]	VAT [%]	Cena miesięczna brutto [PLN]
2	Rozszerzenie przepustowości łącza podstawowego do 2 Gbps (wraz z	miesiąc			

	modyfikacją ochrony AntyDDoS)				

3.3. Wydłużenie okresu obowiązywania umowy (opcja)

Lp.	Nazwa opcji	Jednostka	Cena miesięczna netto [PLN]	VAT [%]	Cena miesięczna brutto [PLN]
3	Wydłużenie okresu obowiązywania umowy o kolejne 12 miesięcy (wszystkie usługi jak w zamówieniu podstawowym)	miesiąc			

4. Oświadczenia Wykonawcy

1. Oświadczam, że zapoznałem się z treścią OPZ i zobowiązuję się do realizacji zamówienia zgodnie z wymaganiami Zamawiającego.
2. Oświadczam, że oferowane usługi i urządzenia spełniają wszystkie wymagania funkcjonalne, techniczne i jakościowe określone w OPZ.
3. Oświadczam, że posiadam wpis do rejestru przedsiębiorców telekomunikacyjnych UKE oraz certyfikat ISO/IEC 27001.
4. Oświadczam, że ceny wskazane w formularzu obejmują wszystkie koszty realizacji zamówienia, w tym koszty instalacji, konfiguracji, szkoleń, dokumentacji, opłat dla zarządcy oraz wszelkie inne koszty niezbędne do prawidłowej realizacji zamówienia.
5. Oświadczam, że ceny opcji są stałe przez cały okres obowiązywania umowy i nie podlegają zmianom, z wyjątkiem waloryzacji przewidzianej w umowie.

6. Podpis Wykonawcy

..... (miejscowość, data)

..... (podpis osoby upoważnionej do reprezentowania Wykonawcy)