Opis Przedmiotu Zamówienia Część II

Przedmiotem zamówienia jest usługa dostępu do sieci Internet w lokalizacjach Zamawiającego oraz dostępu do usługi VPN w celu połączenia sieci korporacyjnych Zamawiającego.

I. ZAMAWIAJĄCY

Ministerstwo Rozwoju i Technologii
Plac Trzech Krzyży 3/5
00-507 Warszawa

II. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest usługa dostępu do sieci Internet dla Ministerstwa Rozwoju i Technologii w lokalizacji przy pl. Trzech Krzyży 3/5 i przy ul. Chałubińskiego 4/6 w Warszawie oraz usługa VPN w celu połączenia sieci korporacyjnych dwóch lokalizacji Ministerstwa – przy Placu Trzech Krzyży 3/5 i przy ul. Chałubińskiego 4/6 w Warszawie jako usług zapasowych.

Na przedmiot zamówienia składa się:

1) Usługa dostępu do sieci Internet w lokalizacji przy pl. Trzech Krzyży 3/5 w Warszawie, za pomocą łącza symetrycznego o gwarantowanej przepustowości 1000 Mbps wykonane w technologii światłowodowej jako zapasowego dostępu do sieci Internet.
2) Zapewnienie Zamawiającemu dostępu do usługi VPN w celu połączenia sieci korporacyjnych, dwóch lokalizacji Ministerstwa – przy pl. Trzech Krzyży 3/5 oraz przy ul. Chałubińskiego 4/6, jako zapasowej usługi VPN między lokalizacjami ministerstwa.

OPIS Minimalnych wymagań w zakresie realizacji przedmiotu zamówienia:

1) Usługa dostępu do sieci Internet w lokalizacji przy pl. Trzech Krzyży 3/5 w Warszawie, w pomieszczeniu 48.
2) Zapewnienie Zamawiającemu dostępu do usługi VPN w celu połączenia sieci korporacyjnych, dwóch lokalizacji Ministerstwa – przy pl. Trzech Krzyży 3/5 oraz przy ul. Chałubińskiego 4/6.
3) Usługa dostępu do sieci Internet w lokalizacji przy pl. Trzech Krzyży 3/5 w Warszawie, w pomieszczeniu 48, będzie realizowana za pomocą łącza o gwarantowanej przepustowości 1000 Mbps wykonane w technologii światłowodowej;
   Usługa dostępu do sieci Internet w ww. lokalizacji zostanie zrealizowana poprzez:
   a) podłączenie i konfigurację dostępu Zamawiającego do sieci Internet w terminie najpóźniej do 5 dni przed rozpoczęciem świadczenia usługi, tj. 01.04.2026 r.;
   b) zapewnienie łącza z adresacją potrzebną do uruchomienia usługi;
   c) skonfigurowanie i uruchomienie na łączu protokołu BGP;
   d) zapewnienie łącza z 32 zewnętrznymi adresami IP;
   e) świadczenie Zamawiającemu usługi dostępu do sieci Internet od dnia 01.04.2026 r. przez **okres 3 miesięcy;**
4) Zapewnienie Zamawiającemu dostępu do usługi VPN w celu połączenia sieci korporacyjnych, dwóch lokalizacji Ministerstwa – przy pl. Trzech Krzyży 3/5 oraz przy ul. Chałubińskiego 4/6 będzie realizowane w szczególności poprzez:
   a) zestawienie łącza pomiędzy ww. lokalizacjami o przepustowości gwarantowanej min. 300 Mbps;
   b) zestawienie łącza VPN o przepustowości gwarantowanej min. 300 Mbps pomiędzy ww. lokalizacjami;
   c) świadczenie usługi transmisji danych Zamawiającego pomiędzy dwoma ww. lokalizacjami poprzez zestawione łącze VPN;
   d) wykonanie prac wymienione w pkt a) i b) w terminie najpóźniej do 5 dni przez rozpoczęciem świadczenie usługi, tj. do 01.04.2026 r.
   e) rozpoczęcie świadczenia usług wymienionych w pkt c) nastąpi najpóźniej do dnia 01.04.2026 r. i będzie realizowane przez **okres 3 miesięcy.**

III. Wymagane minimalne warunki techniczne:

1) Wykonawca będzie świadczył Zamawiającemu usługi dostępu do sieci Internet opisane w pkt II zgodnie z poniżej podanymi wymaganiami:
    1. Zapewni łącze symetryczne dla lokalizacji pl. Trzech Krzyży 3/5, 00-507 Warszawa o przepustowości gwarantowanej 1000 Mbps wykonane w technologii światłowodowej.
    2. Zapewni dostęp do sieci internet zakończony w lokalizacjach Zamawiającego urządzeniami pracującymi w warstwie L2 pełniącymi funkcję urządzeń demarkacyjnych, do konwersji sygnału optycznego na elektryczny. Urządzenia te będą wpięte do sieci Wykonawcy i przez niego zarządzane i monitorowane.
    3. Konfiguracja routingu (BGP) zostanie zestawiona pomiędzy routerem będącym własnością Zamawiającego a routerem brzegowym wewnątrz sieci Wykonawcy.
    4. Zapewni obsługę ruchu generowanego przez Zamawiającego przy pomocy dynamicznego protokołu routingu BGP w wersji 4.
    5. Zapewni brak ograniczeń w ilości i rodzaju przesyłanych danych.
    6. Zapewni na łączu uruchomienie i skonfigurowanie ruchu sieciowego przy pomocy protokołu Ipv4, z możliwością konfiguracji do Ipv6.
    7. Zapewni zakończenie łączy: Ethernet 10/100/1000 Mb/s,
    8. Opóźnienia pakietów na łączu od routera brzegowego Zamawiającego do styku sieci Wykonawcy z Internetem będą na poziomie mniej niż 15 ms,
    9. Miesięczną dostępność dla usług na poziomie minimum 99,8%,
    10. Udostępni Zamawiającemu dostęp do monitoringu i statystyk online wykorzystania oraz dostępności łącza
    11. Udostępni Adresy IP niezbędne do uruchomienia łącza.
    12. Straty pakietów IP – nie więcej niż 0,5% (Pomiar straty pakietów jest zdefiniowany, jako stosunek liczby pakietów straconych do liczby pakietów wysłanych w danym okresie pomiarowym. Przy czym za stracone uznaje się pakiety, które nie zostały odebrane lub są znacznie opóźnione (powyżej 3s). Straty pakietów IP = (Pw – Po)/Pw *100% gdzie: Pw – pakiety wysłane, Po – pakiety odebrane).
    13. Zapewni Zamawiającemu ochronę przed Atakami DDoS, w tym atakami wolumetrycznymi, na usługi uruchomione przez Zamawiającego w publicznej sieci Internet poprzez:
        a) monitorowanie ruchu sieciowego kierowanego do i z sieci Zamawiającego pod kątem prób ataków DDoS na udostępnione usługi w trybie 24/7/365 z ukierunkowaniem na wykrycie anomalii mogących skutkować wysyceniem łącza i utratą ciągłości procesów biznesowych;
        b) monitoring odbywający się wyłącznie na urządzeniach Wykonawcy bez przekierowywania ruchu poza teren (granice) Rzeczpospolitej Polskiej. Monitoringiem i obsługą incydentów związanych z atakami musi zajmować się wyspecjalizowana jednostka realizująca funkcję wyłącznie nadzoru pracująca w sposób ciągły (24/7/365);
        c) linię wsparcia, która będzie pełnić funkcję monitoringu i operacyjnej ochrony przed atakami oraz prowadzić ciągły dyżur;
        d) ochronę przed wolumetrycznymi atakami DDoS;
        e) ochronę co najmniej przed następującymi typami ataków: TCP SYN flood, UDP flood HTTP GET flood, HTTP POST flood, ICMP flood, IGMP flood, invalid packets, IP fragments, IP NULL, DNS flood, SIP request flood, SSL negotiation;
        f) platforma/system/scrubbing center realizujące ochronę przed atakami ddos musi obsłużyć ataki o wielkości min 100 gbps
        g) powiadamianie Zamawiającego (poprzez ustalone kanały komunikacji) w ciągu 15 minut od pojawienia się zagrożeń wskazujących na wystąpienie ataku DDoS;
        h) przekierowywanie ruchu w przypadku podejrzenia wystąpienia ataku do dedykowanych do tego celu zasobów wewnętrznych Wykonawcy, zlokalizowanych na terytorium Rzeczpospolitej Polskiej, w ciągu 20 minut od zgłoszenia przez Zamawiającego;
        i) zastosowanie filtrowania ruchu za pomocą „blacklist” oraz „whitelist” w czasie nie dłuższym niż 2 godziny od wykrycia incydentu;
        j) filtrowanie ruchu sieciowego (odrzucanie pakietów pochodzących ze źródeł ataku, zanim właściwy ruch zostanie przekazany do Zamawiającego) przy możliwie jak

najmniejszym wpływie na ruch uprawniony oraz przekierowywanie odfiltrowanego ruchu do Zamawiającego;

k) dostęp dla Zamawiającego do panelu administracyjnego usługi DDoS za pośrednictwem, którego będzie dostęp do historii i szczegółów dotyczących alarmów, uruchomionych mitygacji oraz monitoringu bieżącego ruchu

l) przygotowanie dla Zamawiającego raportu po zakończeniu oczyszczania ruchu po zaistniałym ataku DDoS.

2) Wykonawca zobowiązany jest:
   1. Posiadać centrum obsługi klienta i centrum zarządzania siecią z całodobowym monitoringiem świadczonej usługi. Obsługa klienta musi być w języku polskim.
   2. Posiadać całodobowy, dedykowany numer telefoniczny do zgłaszania awarii w języku polskim.
   3. Posiadać bezpośrednie styki z operatorami międzynarodowymi o łącznej przepustowości 30 Gb/s oraz bezpośrednie styki z operatorami krajowymi o przepustowości 100Gb/s łącznie.
   4. Posiadać symetryczne połączenie do węzła wymiany ruchu internetowego PLIX lub TPIX o przepustowości, co najmniej 40Gb/s.
   5. Posiadać symetryczne połączenie do międzynarodowego punktu węzła wymiany ruchu internetowego DEC-IX lub AMS-IX o przepustowości co najmniej 20Gb/s.

3) Wykonawca zapewni Zamawiającemu dostęp do usługi VPN w celu połączenia sieci korporacyjnych, dwóch ww. lokalizacji Ministerstwa zgodne z poniżej podanymi wymaganiami:
   a) Łącze VPN musi polegać na usłudze transmisji danych typu punkt – punkt pracującej na warstwie Ethernetowej bez szyfrowania pozwalającej na połączenie dwóch lokalizacji Zamawiającego przy pl. Trzech Krzyży 3/5 oraz ul. Chałubińskiego 4/6 i umożliwiać odseparowaną logicznie od innych usług telekomunikacyjnych transmisję danych pomiędzy lokalizacjami. Transmisja danych szyfrowana będzie na urządzeniach Ministerstwa.
4) Wykonawca zagwarantuje usługę typu SLA, w tym:
   a) obowiązek ciągłego monitorowania łączy. Do zarządzania siecią i urządzeniami nie wolno korzystać z gwarantowanej przepływności łączy;
   b) ciągłe monitorowanie parametrów SLA oraz obciążenia wszystkich łączy;
   c) możliwość generowania co najmniej miesięcznych i rocznych raportów z parametrów SLA, w postaci tekstowej oraz graficznej;
   d) usunięcia awarii usług łącza w ciągu … godzin (zgodnie z deklaracją zawartą w ofercie, ale w czasie nie dłuższym niż 8 godzin) od momentu jej zgłoszenia przez Zamawiającego lub wykrycia przez Wykonawcę;
   e) dostępność służb technicznych 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku.
5) Warunki zgłaszania awarii:
   a) Zamawiający zobowiązuje się do zgłoszenia Wykonawcy awarii, usterek, wad lub innych nieprawidłowości w świadczeniu usługi dostępu do sieci Internet lub dostępu do usługi VPN, zwanego dalej „zgłoszeniem”, niezwłocznie po ich stwierdzeniu.
   b) Zamawiający zobowiązuje się do zapewnienia Wykonawcy całodobowego dostępu do urządzeń w celu przeprowadzenia napraw i konserwacji (po uprzednim uzgodnieniu terminu wykonania tych czynności). Naprawy i konserwacje będą wykonywane przez osoby uprzednio zgłoszone przez Wykonawcę w obecności osoby reprezentującej Zamawiającego.
   c) Zgłoszenia będą przyjmowane przez Wykonawcę całodobowo przez 7 dni w tygodniu, telefonicznie pod numerem …, mailem pod adres …
   d) Wykonawca zobowiązuje się do przystąpienia do usunięcia awarii w czasie do 2 godzin.
   e) Wykonawca potwierdzi przystąpienie do usunięcia awarii poprzez wysłanie mail’a do Zamawiającego na adres ……...
   f) W przypadku konieczności przeprowadzenia prac konserwacyjnych lub modernizacyjnych, Wykonawca może, po wcześniejszej pisemnej zgodzie Zamawiającego, zawiesić usługę dostępu do sieci Internet. Okresowe zawieszenie

usługi może odbyć się wyłącznie w godzinach 23.00-5.30.