**Załącznik nr 1 do umowy nr ... z dnia ................**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. Przedmiotem zamówienia jest:
   1. Dostarczenie zapasowego łącza internetowego o parametrach określonych poniżej na okres 36 miesięcy.
2. Wymagane minimalne parametry dla łącza.
3. Łącze symetryczne o przepustowości nie mniejszej niż 10 Gbps w kierunku od/do Zamawiającego (upload/download).
4. Łącze musi posiadać funkcjonalność routingu BGP.
5. Łącze musi być doprowadzone do siedziby Oddziału Informatycznego Sądu Apelacyjnego we Wrocławiu ul. Borowska 283b (Data Techno Park).
6. Łącze do obiektu musi być doprowadzone stałym, jednorodnym łączem optotelekomunikacyjnym – światłowód.
7. Łącze musi być doprowadzone do routera Zamawiającego za pośrednictwem interfejsu Ten Gigabit Ethernet fizycznie zakończonego złączem LC wraz z wkładką SFP+ współpracującą z routerem CISCO C8500-12X.
8. Łącze z gwarancją przepustowości na pełnym poziomie CIR (ang. Committed Information Rate) = EIR (ang. Excess Information Rate) - w obu kierunkach od/do Zamawiającego (download/upload).
9. Wykonawca zapewni działanie łącza w pełnej funkcjonalności routingu BGP w wersji 4 oraz 6, w zakresie przesyłania pełnych tablic routingu BGP do routerów Zamawiającego oraz dystrybucji (rozgłaszania w Światowym BGP) sieci Zamawiającego do sieci Internet.
10. Wykonawca zapewni publiczne adresy sieci połączeniowej (IPv4) z własnej puli adresowej. Zmawiający zastrzega możliwość sprawdzenia adresacji w bazie RIPE - <https://apps.db.ripe.net/db-web-ui/query> gdzie Wykonawca musi być wskazany jako organizacja odpowiedzialna (Responsible organisation) za adresację.
11. Wykonawca przekaże wszystkie informacje potrzebne do konfiguracji routingu do sieci Dostawcy.
12. Specyfikacja usługi AntyDDoS

Jako usługę AntyDDoS Zamawiający definiuje usługę przeciwdziałania atakom typu DDoS (Distributed Denial of Service) na kierunku ruchu do sieci Zamawiającego z Internetu. AntyDDoS musi być świadczony bez żadnych ograniczeń w ilości analizowanych danych. Wymagany czas reakcji na zdarzenia nie może być dłuższy niż 3 minuty od wykrycia zdarzenia.

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

* system monitorowania w czasie rzeczywistym Routerów PE(Provider Edge) lub innych urządzeń we własnej infrastrukturze, w celu sporządzenia profilu typowego ruchu w kierunkach od i do Zamawiającego;
* system wykrywania anomalii ruchu przynajmniej za pomocą sygnatur, przekroczenia zdefiniowanych progów ruchu dla określonego typu pakietów i protokołów, analizy profilu ruchu w oparciu o profil standardowego ruchu;
* system usuwania ataku (filtrowania) przy możliwie jak najmniejszym wpływie na pozostały ruch w kierunkach od i do Zamawiającego;
* panel zdalnego dostępu dla klienta poprzez dedykowaną stronę WWW dostępną z dowolnego miejsca w Internecie, umożliwiający dostęp dla minimum 5 pracowników Zamawiającego. Panel klienta musi umożliwiać przynajmniej sprawdzenie:
* statystyki aktualnego ruchu w kierunkach od i do klienta wraz z wartościami ekstremalnymi;
* aktualnego stanu wykrytych ataków i aktualnego stanu działań zabezpieczających;
* raportów dziennych/tygodniowych z wykrytych ataków, po każdym ataku i podjętych działań, także raportów historycznych z minimum dwóch poprzednich miesięcy.

W przypadku braku dedykowanego panelu raportowego Zamawiający dopuszcza udostępnienie raportów poprzez ich przesyłanie na wskazaną skrzynkę mailową po każdym ataku (nie później niż 24h po jego wystąpieniu i usunięciu) oraz raportów tygodniowych. W raporcie powinno być zawarte co najmniej czas wystąpienia ataku, rodzaj ataku, czas trwania ataku, podjęte działanie oraz adres systemu atakowanego. Jednocześnie Wykonawca udostępni panel klienta przez który Zmawiający będzie mógł przeglądać dane dotyczące poszczególnych ataków na stronie www.

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

1. Usługa AntyDDoS musi umożliwiać skonfigurowanie do dziesięciu tzw. obiektów zarządzanych (managed object) umożliwiających niezależne skonfigurowanie parametrów mitygacji dla dziesięciu grup adresów IP, przy czym jedna grupa musi obligatoryjnie obejmować całą pulę publicznej adresacji IP Zamawiającego, a pozostałe grupy pule adresów IP wydzielone z całej publicznej adresacji IP Zamawiającego, na których wystawione są w Internecie określone usługi Zamawiającego, np. WWW, VPN, DNS.
2. System wykrywania anomalii ruchu musi obejmować przynajmniej:

* wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu w sieci Internet, w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS;
* wyznaczanie oczekiwanej wartości ruchu w kierunkach do i od Zamawiającego, o danej porze dnia w danym dniu tygodnia;
* wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanych tego ruchu;
* ochronę przed wysyceniem łączy telekomunikacyjnych przeznaczonych dla usługi dostępu do Internetu.

1. System usuwania ataku musi obejmować przynajmniej:

* filtrowanie ruchu z błędnymi nagłówkami IP/TCP/UDP;
* odrzucanie lub przepuszczanie na bazie zdefiniowanych dla Zamawiającego filtrów operujących na informacjach w nagłówkach L3 i L4 modelu ISO/OSI;
* filtrowanie ruchu na określonych portach UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne;
* filtrowanie ruchu na określonych portach TCP na podstawie zawartości pola danych w oparciu o wyrażenia regularne;
* ochronę przed atakami z udawanymi adresami źródłowymi IP (spoofing) poprzez autentykację sesji TCP, zapytań DNS oraz zapytań HTTP;
* filtrowanie nieprawidłowych zapytań DNS;
* ograniczenie zapytań DNS do zadanej wartości zapytań na sekundę;
* filtrowanie oparte o wyrażenia regularne definiujące zakres stosowania autentykacji DNS oraz ograniczania liczby zapytań DNS;
* filtrowanie nieprawidłowych zapytań HTTP;
* blokowanie ruchu do serwisu Zamawiającego przekraczających progi dla operacji HTTP na sekundę na dany serwer lub na dany URL;
* filtrowanie oparte o wyrażenia regularne definiujące zakres stosowania autentykacji HTTP lub ograniczania liczby zapytań HTTP;
* filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków HTTP;
* ochronę przez atakami typu Slow Lories poprzez resetowanie połączeń, które pozostają nieaktywne przez zadany okres czasu;
* ochronę przez atakami typu Slow Lories poprzez resetowanie sesji TCP, której aktywność jest poniżej zadanej liczby bajtów przesyłanej w zadanym okresie czasu;
* wykrywanie ruchu kierowanego z serwerów CDN proxy i stosowanie algorytmów filtrowania na podstawie oryginalnego źródła ruchu;
* wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS, które są poza sekwencją;
* blokowane sesji jeżeli podczas negocjacji SSL/TLS klient zarządza nadmiernej ilości metod kryptograficznych lub rozszerzeń użytkownika. Próg dla tych wartości musi być definiowalny;
* wykrywanie i rozłączanie sesji jeżeli negocjacja SSL/TLS nie zakończy się w zadanym czasie;
* blokowanie ruchu ze stacji, dla których występuje nadmierna liczba nieprawidłowych, nadmiarowych lub niekompletnych sesji SSL;
* ochronę przed atakami pochodzącymi od sieci botnetowych (komputerów zainfekowanych w sposób umożliwiające zdalne sterowanie przez hackerów) poprzez filtrowanie na podstawie na bieżąco aktualizowanych sygnatur zawierających listę adresów IP;
* ochronę przed atakami poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości. Wartości progowe muszą być definiowalne zarówno dla całości ruchu jak i do części ruchu zdefiniowanego za pomocą filtru.

1. Ze względu na wymaganą w Umowie poufność monitoring i obróbka ruchu pod kątem ataków DDoS musi odbywać się wyłącznie w infrastrukturze Wykonawcy.
2. Specjaliści dedykowani do obsługi AntyDDoS muszą odpowiadać przynajmniej za:

* analizę ruchu w celu identyfikacji typu i natury ataku;
* powiadamianie Zamawiającego o podejrzeniu wystąpienia ataku;
* rozpoczęcie usuwania ataku w porozumieniu z Zamawiającym, przy czym automatycznie musi być uruchamiania obrona dla alarmów o uzgodnionym poziomie zagrożenia;
* modyfikację zestawu użytych mechanizmów przeciwdziałania tak, aby uzyskać maksymalny poziom filtracji ruchu niepożądanego przy minimalnym wpływie na ruch prawidłowy;
* klasyfikację alarmów typu DDoS jako:
* atak prawdziwy - zweryfikowany,
* atak fałszywy – zweryfikowany,
* nagły wzrost ruchu – zweryfikowany (pożądany).

1. Szczegółowy sposób powiadamiania Zamawiającego, inicjowania, awaryjnego przerwania i zakończenia procedury filtrowania w przypadku wykrycia ataku zostanie uzgodniony na etapie wdrożenia.
2. Po zakończeniu operacji filtrowania ruchu po zaistniałym ataku DDoS każdorazowo wymaga się sporządzania przez Wykonawcę i przekazywania Zamawiającemu raportu z wykrytego ataku. Raport musi zawierać przynajmniej następujące informacje:

* rozmiar ataku, liczniki pakietów, procent całości ruchu wyrażony także w Gb/s;
* czas trwania ataku;
* jeżeli jest możliwe do ustalenia - główne źródła ataku wraz z geograficznym położeniem tych źródeł;
* typ i naturę ataku;
* wdrożone metody eliminacji ataku;
* wielkość oczyszczonego ruchu;
* czasy związane z wykonywaniem usługi AntyDDoS, tj.:
  + godzina początku ataku,
  + godzina powiadomienia Zamawiającego,
  + godzina wdrożenia procedur obronnych,
  + godzina zakończenia ataku,
  + godzina przywrócenia normalnej pracy sieci.

1. Wymaga się sporządzania przez Wykonawcę i przekazywania Zamawiającemu raportów cotygodniowych za poprzedni tydzień lub miesięcznych zawierających przynajmniej:

* statystykę ruchu w kierunkach od i do Zamawiającego;
* maksymalne wartości ruchu;
* listę zarejestrowanych ataków wraz z ich klasyfikacją;
* listę usuniętych ataków.

1. Wykonawca zapewni dla 2 osób wskazanych do realizacji Umowy po stronie Zamawiającego uczestnictwo w dedykowanym instruktażu technicznym z zakresu aspektów ochrony przed atakami DDoS realizowanym na potrzeby usługi dostarczonej dla Zamawiającego.

Instruktaż techniczny ma trwać przynajmniej 4 godziny oraz zostanie przeprowadzony w siedzibie Zamawiającego z zastrzeżeniem, że Zamawiający zobowiązuje się do zapewnienia sali oraz nieprzerwanego w czasie trwania instruktarzu oddelegowania 2 pracowników lub w formie sesji zdalnej z wykorzystaniem systemu wideokonferencyjnego. Instruktaż techniczny ma zostać przeprowadzony w terminie uzgodnionym z Zamawiającym w ramach zamówienia, przed jego końcowym odbiorem.

1. Wykonawca zapewnia, że:
2. posiada, co najmniej 3 niezależne, bezpośrednie punkty styku z Międzynarodowymi Dostawcami Internetowymi o przepustowości min. 10 Gb/s każdy, które zostaną sprawdzone przez stronę [https://www.peeringdb.com](https://www.peeringdb.com/) lub [https://bgp.tools](https://bgp.tools/) Nie dopuszcza się realizacji powyższego wymogu za pośrednictwem podmiotów trzecich.
3. posiada, co najmniej 3 punkty styku z Krajowymi Dostawcami Internetowymi o przepustowości min. 10 Gb/s każdy, które zostaną sprawdzone przez stronę [https://www.peeringdb.com](https://www.peeringdb.com/) lub [https://bgp.tools](https://bgp.tools/) Nie dopuszcza się realizacji powyższego wymogu za pośrednictwem podmiotów trzecich.
4. Jest uczestnikiem w co najmniej dwóch Punktach Wymiany Ruchu Internetowego – Internet Exchange (np. EPIX, PL-IX);
5. dokona wszelkich ustaleń z administratorami i służbami technicznymi budynku, w którym świadczona będzie usługa. Zamawiający nie poniesie z tego tytuły żadnych dodatkowych kosztów.
6. Pozostałe wymagania:
7. Termin uruchomienia usługi 60 dni od dnia podpisania umowy. Zamawiający zastrzega przeprowadzenie testów połączeniowych i sprawdzających przepustowość łącza, co najmniej 10 dni roboczych przed wymienionym terminem uruchomienia usługi.
8. czas usunięcia pojedynczej Awarii nie dłuższy niż 4 godziny. Pod pojęciem Awarii Zamawiający rozumie zdarzenie powodujące przerwę w działaniu Usługi lub uniemożliwiające korzystanie przez Zamawiającego z Usługi lub niedochowanie wymaganych parametrów Usługi
9. miesięczna dostępność łącza na poziomie nie gorszym niż 99,6 %
10. gwarancja przepustowości łącza na poziomie 99 %.
11. czas reakcji na zgłoszenie Awarii nie dłuższy niż 1 godzina.
12. zapewnienia punktu dostępowego do dokonywania zgłoszeń awarii łącza dostępny 24/7 365 dni w roku. Punkt dostępowy umożliwi dokonywanie zgłoszeń przez Zamawiającego za pomocą poczty elektronicznej, fax-u, linii telefonicznej lub dedykowanego portalu zgłoszeniowego.
13. Zamawiający dopuszcza okno serwisowe przeznaczone na planowe prace konserwacyjne. Okno serwisowe musi być uzgodnione z Zamawiającym z wyprzedzeniem co najmniej 7 dni roboczych. Planowane prace konserwacyjne mogą być prowadzone w godzinach od 00:00 do 4:00 rano oraz w soboty, niedziele i w dni ustawowo wolne od pracy. Pojedyncze okno serwisowe nie może być dłuższe niż 2 godziny od momentu rozpoczęcia prac. Planowane prace konserwacyjne nie mogą być prowadzone częściej niż 1 raz w miesiącu. Przerwy w dostarczaniu usługi spowodowane oknami serwisowymi Zamawiający traktuje jako zachowanie ciągłości usługi.
14. Dodatkowe wymagania dla łącza zapasowego.
15. Zamawiający wymaga współpracy przy konfiguracji protokołu BGP w celu prawidłowego rozgłaszania adresacji przypisanej do będącego w posiadanego Zamawiającego numeru AS (ang. Autonomous System) 204066.
16. Wykonawca będzie współpracował z Operatorem podstawowego łącza w celu skonfigurowania wszelkich parametrów dla sesji BGP oraz konfiguracji routera brzegowego.
17. Łącze zapasowe musi być niezależnym, fizycznie oddzielonym łączem od łącza podstawowego i musi być dostarczone od innego operatora ISP (ang. Internet Service Provider) niż łącze podstawowe.