

**SPECYFIKACJA TECHNICZNA PRZEDMIOTU UMOWY
DOTYCZĄCA CZĘŚCI AKTYWNEJ ŁĄCZA**

1. Wytyczne dotyczące części aktywnej łącza:

- 1) Wykonawca zapewni gwarantowane pasmo (CIR) **2 Gbit/s (2 Gb/s)** pobieranie danych i **2 Gb/s** wysyłanie danych) do sieci Internet, a transmisja danych będzie przebiegać poprzez etherchannel złożony z dwóch linków podłączonych do routera BGP poprzez dwa porty 1G.
- 2) Wykonawca zapewni wymianę ruchu BGP w zakresie przesyłania pełnych tablic routingu BGP do routerów Zamawiającego oraz dystrybucji (rozgłaszania w Światowym BGP) sieci Zamawiającego do sieci Internet;
- 3) Wykonawca po przeprowadzeniu wizji lokalnej dostarczy dwie odpowiednie wkładki **Cisco (duplex)** do routera brzegowego BGP serii Cisco ASR zapewniające odpowiedni zasięg do zestawienia poprawnej transmisji, a Zamawiający udostępni dwa porty 1Gb/s w routerze BGP;
- 4) Wykonawca prześle wszystkie informacje potrzebne do konfiguracji routingu do sieci Dostawcy;
- 5) Wykonawca zapewni rozgłaszanie adresacji Zamawiającego za pomocą protokołu BGP pod własnym numerem ASN Zamawiającego (IPv4);
- 6) Wykonawca zapewni publiczne adresy sieci połączeniowej (IPv4) z własnej puli adresowej;
- 7) Wykonawca prześle informacje o serwerach DNS dostawcy oraz zapewnieniu zapasowy serwer DNS u Dostawcy, dla wszystkich domen których właścicielem jest Zamawiający;
- 8) Wykonawca umożliwi Zamawiającemu dostęp do całej puli prefixów w sieci Internet;
- 9) Wykonawca musi posiadać, co najmniej dwa niezależne, bezpośrednie punkty styku z Międzynarodowymi Dostawcami Internetowymi;
- 10) Wykonawca musi posiadać, co najmniej 3 punkty styku z Krajowymi Dostawcami Internetowymi, w tym jeden z nich powinien być bezpośredni z siecią TPNET;
- 11) Wykonawca musi posiadać, styk do węzła wymiany ruchu Polish Internet Exchange PLIX;
- 12) Nie dopuszcza się stosowania łączy radiowych;
- 13) Zamawiający przyjmuje, że Straty pakietów są wyrażonym w % wynikiem pomiarów realizowanych przez co najmniej jednokrotne wysłanie 1500 64-bajtowych pakietów ICMP (ping), co godzinę w 24-godzinny okres pomiaru przez internetową sieć szkieletową Dostawcy do OPP (Ostatni punkt pomiarowy – OPP oznacza ostatni router w sieci Dostawcy, który posiada bezpośredni styk z operatorem międzynarodowym). W celu uzyskania odpowiednich statystyk strat pakietów Wykonawca będzie monitorować drogę od routera brzegowego Zamawiającego do OPP;

- 14) Wynik testów akceptacyjnych opisanych w pkt. 13 uznaje się za pozytywny jedynie w przypadku gdy zaobserwowane straty pakietów z routera brzegowego Zamawiającego wynoszą średnio nie więcej niż 2%, w czasie 24 godzin od chwili rozpoczęcia testu.
- 15) Wykonawca dokona pomiaru obciążenia łącza z sieci Zamawiającego w celu sprawdzenia rzeczywistej przepustowości zamawianego łącza.

**SPECYFIKACJA TECHNICZNA PRZEDMIOTU UMOWY
DOTYCZĄCA OCHRONY PRZED ATAKAMI DDoS NA ZAMAWIANE ŁĄCZE**

Definicje:

Atak DDoS – zdarzenie w publicznej sieci Internet o charakterze ataku na system komputerowy lub usługę sieciową Zamawiającego, w celu naruszenia bezpieczeństwa oraz uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów sieciowych po stronie Zamawiającego, przeprowadzane równocześnie z wielu hostów w sieci Internet, poprzez generowanie Ruchu Sztucznego.

Ruch Sztuczny – ruch w sieci Internet generowany w kierunku sieci i adresów IP Zamawiającego, zakłócający pracę systemów komputerowych Zamawiającego, jego usług sieciowych, oraz urządzeń Zamawiającego.

Zdrowy Oczyszczony Ruch Sieciowy – odfiltrowany ruch pochodzący z Ataku DDoS w kierunku Zamawiającego bez uwzględniania Ruchu Sztucznego.

Celem Zamawiającego jest zakup usługi dostępu do Internetu zabezpieczonej poprzez system ochrony przed atakami DDoS, który wykrywając atak DDoS na łącza/sieć Zamawiającego, blokuje niepożądany ruch, odfiltrowuje z niego ruch prawidłowy i przesyła pożądaną ruch do sieci Zamawiającego specjalnie do tego przygotowanym tunelem GRE

1. W ramach ochrony przed Atakami DDoS na zamawiane łącze Wykonawca zapewni:
 - 1) ciągłość usługi dostępu do Internetu oraz bezpieczeństwo przed wszystkimi rodzajami Ataków DDoS w szczególności:
 - a) powodującymi przepełnienie i wysycenie pasma potrzebnego do świadczenia usług;
 - b) mającymi na celu zalanie datagramami ICMP/UDP;
 - c) powodującymi wyczerpanie zasobów systemu świadczącego usługę np. przez zalanie pakietami z flagą TCP SYN;
 - d) Atakami DDoS z wykorzystaniem dużej ilości sesji na konkretną aplikację wykorzystywaną do świadczenia usługi;
 - 2) monitoring ruchu internetowego do klienta za pomocą protokołów takich jak NetFlow, SNMP i innych;
 - 3) ochronę następującej ilości obiektów:
 - a) 195.182.9.0/24;
 - b) dodatkowych klas Zamawiającego, które zostaną uruchomione w trakcie trwania umowy;
 - 4) monitorowanie w sposób ciągły (24/7/365) ruchu sieciowego Zamawiającego, wykrywanie anomalii względem standardowego ruchu internetowego Zamawiającego mogących skutkować wysyceniem łącza i utratę ciągłości procesów biznesowych;

- 5) usługę ochrony przed Atakami DDoS, która musi być wykonana na urządzeniach zlokalizowanych na terenie Polski;
- 6) całodobową gotowość Wykonawcy administratorów do podjęcia przeciwdziałań (czas reakcji: 15 minut od wykrycia Ataku DDoS przez Zamawiającego;
- 7) reakcję na Atak DDoS na infrastrukturę Zamawiającego poprzez zastosowanie posiadanych przez Wykonawcę wszelkich systemów i narzędzi obrony oraz przeciwdziałanie nowym Atakom DDoS o nieznanych sygnaturach;
- 8) dodatkowe narzędzia takie jak: blackholing, filtry międzynarodowe, które pozwolą na filtrowanie ruchu Zamawiającego za pomocą „blacklist” i „whitelist”;
- 9) przekazanie informacji i wszelkiej wiedzy potrzebnej do prawidłowej konfiguracji i eksploatacji narzędzi ochrony DDoS, na wniosek Zamawiającego;
- 10) realizację poniższych wytycznych:
 - a) ochronie musi być poddany cały ruch na łączu internetowym;
 - b) system musi zapewniać możliwość dostępu Zamawiającego do danych dotyczących stanu bieżącego oraz historii pracy systemu, statystyk, monitoringu ruchu i szczegółów Ataków DDoS;
 - c) system musi zapewniać możliwość definiowania różnych polityk ochrony dla wybranych adresów IP;
 - d) system musi posiadać możliwość zdefiniowania zaufanych adresów, dla których ruch nie będzie blokowany;
 - e) system musi być dostępny przez 365/7/24 z czasem reakcji na wykrycie Ataku DDoS do 2 minut;
 - f) system musi automatycznie zapobiegać Atakom DDoS na obiekty Zamawiającego do przepustowości minimum **[zgodnie z ofertą Wykonawcy]** Gbps;
 - g) Wykonawca przeprowadzi wywiad z Zamawiającym i zbierze wszelkie niezbędne informacje techniczne (np. zebranie statystyk z routera pozwalających wykryć anomalie w ruchu przychodzącym) niezbędne do zdefiniowania i skonfigurowania prawidłowo działającej ochrony DDoS na zaproponowanym przez Wykonawcę formularzu po podpisaniu umowy;
 - h) Wykonawca w uzgodnionym z Zamawiającym czasie przeprowadzi testy usługi ochrony DDoS polegające na symulacjach Ataków DDoS, które potwierdzą prawidłowo skonfigurowaną i w pełni działającą usługę ochrony przed Atakami DDoS;
- 11) aplikację online do obserwowania aktualnych statystyk, historii ruchu na zamawianym łączu oraz do obserwowania działania systemu ochrony przed Atakami DDoS z możliwością generowania przez Zamawiającego raportów o przeprowadzonych Atakach DDoS, podejrzanych pakietach i wolumenie ruchu;
- 12) przeprowadzenie prezentacji z świadczonej przez Wykonawcę usługi ochrony przed Atakami DDoS w siedzibie Zamawiającego oraz przeszkolenie z obsługi aplikacji online o której mowa w pkt. 11) dla administratorów Zamawiającego w ciągu 14 dni od uruchomienia usługi DDoS.

- 13) dostarczenie szczegółowych raportów do Zamawiającego na temat monitorowanego ruchu oraz ilości Ataków DDoS przeprowadzanych na infrastrukturę Zamawiającego na życzenie Zamawiającego, z zadanego przedziału czasu. Zamawiający nie będzie żądał więcej niż 4 raporty w miesiącu;
2. Usługa ochrony DDoS musi zostać zrealizowana w oparciu o rozwiązania firmy Arbor Networks lidera rozwiązań w zakresie ochrony przed atakami DDoS (lub rozwiązanie równoważne).
3. Rozwiązanie musi zapewnić Geolokalizację adresów IP umożliwiającą blokadę ruchu przychodzącego z danego kraju bądź obszaru geograficznego.
4. Rozwiązanie musi zapewnić sposób blokady niedozwolonych zapytań DNS, http.
5. Rozwiązanie musi zapewnić ochronę serwerów DNS przed atakami typu DNS reflection attack, cache poisoning, resource exhaustion poprzez przepuszczenie zapytań DNS zgodnych z RFC oraz pochodzących z właściwych źródeł.
6. Rozwiązanie musi zapewnić ochronę serwerów SIP poprzez przepuszczenie zapytań zgodnych z RFC oraz pochodzących z właściwych źródeł.
7. System ochrony DDoS, musi zapewnić trzy rodzaje mechanizmów detekcji:
 - 1) sygnatury,
 - 2) przekroczenie progów dla określonych typów pakietów i protokołów,
 - 3) analiza profilu ruchu Zamawiającego i wykrywanie nieoczekiwanych zmian w ruchu w odniesieniu do tego profilu.
8. Rozwiązanie (aplikacja online) musi zapewnić dostęp do statystyk i panelu zarządzania w trybie do odczytu, w szczególności musi zapewnić:
 - a) dostęp do statystyk ruchu na podstawie NetFlow,
 - b) dostęp do raportów generowanych przez system,
 - c) dostęp do listy wykrytych ataków,
 - d) dostęp do listy akcji wykonywanych w celu ograniczenia wpływu ataku,
 - e) możliwość zapisywania raportów w formie PDF,
 - f) możliwość wysyłania raportów w formacie PDF za pomocą email, bezpośrednio z aplikacji,
 - g) dostęp do zarządzania powinien odbywać się szyfrowanym kanałem https.
9. Raporty o których mowa w pkt. 8) ppkt. b) muszą zawierać co najmniej:
 - a) przedział czasowy wystąpienia ataku DDoS,
 - b) wykres przedstawiający wielkość ruchu przychodzącego, wielkość ruchu oczyszczonego, w przedziale czasowym,
 - c) typ ataku, krótki opis rodzaju ataku,
 - d) kierunek ataku,
 - e) źródła ataku (adres IP hostów, adres sieci, porty źródłowe,
 - f) docelowe adresy IP ataku, porty docelowe,
 - g) wykorzystany protokół,
 - h) ilość pakietów pps, wielkość ruchu w bps,

- i) wielkość ruchu całkowitego, wielkość ruchu zdrowego, wielkość ruchu który został oczyszczony i odrzucony.

10. W przypadku Ataku DDoS:

- 1) system ochrony DDoS dokona weryfikacji czy ewentualne zagrożenia związane są z rzeczywistym Atakiem DDoS, powiadomi Zamawiającego i uruchomi odpowiednie narzędzia, które wyeliminują Atak DDoS, Ruch Sztuczny oraz podejrzane pakiety, tak aby do Zamawiającego trafił jedynie pożądaný Zdrowy Oczyszczony Ruch Sieciowy;
- 2) Wykonawca dokona dokładnej analizy i prześle do Zamawiającego raport końcowy, zawierający szczegółowe informacje na temat monitorowanego ruchu oraz ilości Ataków DDoS przeprowadzanych na infrastrukturę Zamawiającego, w ciągu 24 godzin od zakończenia Ataku DDoS.