

TOM III SWZ

Opis przedmiotu zamówienia

ROZDZIAŁ I. PRZEDMIOT ZAMÓWIENIA:

1. Świadczenie przez Wykonawcę usługi dostępu do Internetu na rzecz Zamawiającego w lokalizacji znajdującej się w Radomiu, ul. Samorządowa 1, od dnia zawarcia Umowy przez okres 33 miesiące ale nie wcześniej niż od dnia **01.01.2026r.** godz. 0⁰⁰.
Usługa musi być świadczona 24 godziny na dobę, przez wszystkie dni w roku, o następujących parametrach: szerokopasmowy dostęp do Internetu o przepustowości gwarantowanej 15 Gb/s wraz z ochroną AntyDDoS,
2. Zamawiający w ramach realizacji przedmiotu Umowy zastrzega sobie możliwość skorzystania z Prawa Opcji polegającego na zwiększeniu przepustowości łącza wskazanego w rozdz. I pkt 1. Wykonawca w okresie od dnia zawarcia Umowy przez 32 miesiące ale nie wcześniej niż od dnia 01.02.2026r każdorazowo na zlecenie Zamawiającego dokona zwiększenia przepustowości łącza przy założeniu, że:
 - a) zlecenie zwiększenia przepustowości nastąpi z wyprzedzeniem co najmniej 3 dni roboczych
 - b) minimalne pojedyncze zwiększenie łącza będzie wielokrotnością 1Gb/s
 - c) maksymalna przepustowość łącza po zwiększeniu nie przekroczy 20 Gb/s.
3. Wykonawca w ramach wykonywania Umowy zobowiązuje się do:
 - a) zestawienia, uruchomienia, i udostępnienia stałego łącza dostępowego, o których mowa w rozdz. I pkt. 1 wraz z urządzeniami teletransmisji niezbędnymi do świadczenia Usługi, przekazania procedur określonych w rozdz. II pkt 1 lit. f) OPZ oraz dokumentacji o której mowa rozdz. III pkt 10 lit. a) w terminie do dnia 31.12.2025 r.,
 - b) świadczenia Usług dostępu do Internetu dla lokalizacji wskazanej w rozdz. I pkt 1 w terminie od dnia zawarcia Umowy przez okres 33 miesiące ale nie wcześniej niż od dnia **01.01.2026r.** godz. 0⁰⁰, co zostanie potwierdzone Protokołami Odbioru podpisanymi przez obie Strony w terminie nie dłuższym niż 3 dni od dnia rozpoczęcia świadczenia usługi. Odbiór będzie polegał na stwierdzeniu zgodności przedmiotu Umowy w zakresie parametrów technicznych i funkcjonalnych oraz stwierdzeniu poprawności działania.;
 - c) zapewnienia ciągłości świadczenia usługi dostępu do Internetu określonej w rozdz. I, pkt. 1 oraz utrzymania poziomu parametrów określonych w OPZ , a w szczególności do:
 - i. funkcjonowania połączenia z siecią Internet o przepustowości nie niższej, niż gwarantowana,
 - ii. obsługi ruchu określonego w rozdz. II pkt 1 lit. e) OPZ ,
 - iii. obsługi QoS zgodnie z warunkami określonymi rozdz. II pkt 1 lit. f) OPZ
 - iv. zapewnienia we własnym zakresie i na swój koszt wszystkich materiałów, wyposażenia, urządzeń, narzędzi i innych elementów niezbędnych do zapewnienia prawidłowego i bezawaryjnego świadczenia Usługi przez cały okres jej realizacji;
 - d) obsługi zgłoszeń w zakresie problemów eksploatacyjnych przez 24 godziny na dobę przez wszystkie dni w roku. Zgłoszenia Awarii będą przekazywane Wykonawcy drogą poczty elektronicznej na czynny i monitorowany przez całą dobę i wszystkie dni w roku adres email

- przez upoważnione do tego osoby lub osoby nadzorujące Umowę. Wykonawca zobowiązany jest wysłać Zamawiającemu potwierdzenie odebrania zgłoszenia z zachowaniem czasu reakcji na zgłoszenie nie dłuższym niż 15 minut od momentu wysłania zgłoszenia Awarii przez Zamawiającego. W przypadku niemożności złożenia zgłoszenia drogą elektroniczną upoważniony Administrator Zamawiającego lub osoba nadzorująca zgłosi Awarię faksem na czynny i nadzorowany przez całą dobę i wszystkie dni w roku numer faksu Wykonawcy. Dodatkowo upoważniony Administrator Zamawiającego może zawiadomić Wykonawcę o Awarii telefonicznie na czynny i nadzorowany przez całą dobę i wszystkie dni w roku numer. Zawiadomienie telefoniczne nie zastępuje zgłoszenia Awarii, o jakim mowa powyżej.
- e) całkowitego usunięcia pojedynczej Awarii w dopuszczalnym czasie wskazanym rozdz. I pkt 4 OPZ.
 - f) ograniczenia dopuszczalnego łącznego czasu niedostępności Usługi w ciągu roku kalendarzowego świadczenia Usługi do 24 godzin,
 - g) wykonywania i dostarczania do siedziby Zamawiającego, po zakończonym 3 miesięcznym okresie rozliczeniowym, po wcześniejszej akceptacji przez przedstawiciela Zamawiającego, oryginałów kwartalnych raportów świadczenia Usługi uwzględniających wszystkie Awarie i odstępstwa od ustalonego poziomu świadczenia Usługi oraz statystyki wymienione w rozdz. III pkt 5 OPZ, w terminie do 15 dni od zakończenia kwartału;
 - h) wykonywania i dostarczania do siedziby Zamawiającego, po wcześniejszej akceptacji przez przedstawiciela Zamawiającego, oryginałów rocznych raportów świadczenia Usługi w terminie do 15 dni od zakończenia roku kalendarzowego.
 - i) przesłania na adres tt.raporty@mf.gov.pl raportu z incydentu każdorazowo po zaistniałym ataku zgodnie z warunkami określonymi w rozdz. III pkt 6.
 - j) Raporty wymienione w rozdz. I pkt 3 lit. g) i lit. h) powinny być wysłane do akceptacji na adres tt.raporty@mf.gov.pl
 - k) Zamawiający dopuszcza dostarczenie zaakceptowanych raportów wymienionych w rozdz. I pkt 3 lit. g) i lit. h) w wersji elektronicznej podpisanych podpisem kwalifikowanym na adres tt.raporty@mf.gov.pl
4. W przypadku braku dostępu/niesprawności/Awarii w działaniu Usługi określonej w rozdz. 1 pkt 1 Wykonawca zobowiązuje się do przywrócenia poprawnego działania w czasie nie dłuższym niż wskazanym w Formularzu ofertowym (ale nie dłużej niż wymagany przez Zamawiającego czas 4 godzin) od chwili zgłoszenia Awarii lub od momentu wykazania braku dostępu/Awarii/niesprawności w działaniu Usługi określonej w rozdz. 1 pkt 1 przez system monitorujący
5. Zamawiający dopuszcza możliwość przeprowadzenia prac konserwacyjnych przez Wykonawcę pod następującymi warunkami:
- a) Wykonawca powiadomi Zamawiającego z 2 tygodniowym wyprzedzeniem o konieczności przeprowadzenia prac konserwacyjnych i uzyska jego zgodę na ich realizację;
 - b) prace będą realizowane w godzinach nocnych (00:00-04:00),
 - c) przerwa w świadczeniu usługi nie przekroczy 30 minut,
 - d) przerwy konserwacyjne nie będą wliczane do czasu niedostępności Usługi oraz pojęcia Awarii.

ROZDZIAŁ II. SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest świadczenie przez Wykonawcę usługi dostępu do Internetu na rzecz Zamawiającego obejmującej zestawienie, uruchomienie i udostępnianie przez całą dobę (24 godziny) przez wszystkie dni w roku stałego, **symetrycznego łącza dostępowego wraz z urządzeniami teletransmisyjnymi**, zwanych dalej „Usługą” zapewniających:
 - a) szerokopasmowy dostęp do Internetu o przepustowości gwarantowanej 15 Gb/s wraz z ochroną AntyDDoS dla lokalizacji przy ul. Samorządowej 1 w Radomiu w okresie od dnia zawarcia

Umowy przez okres 33 miesięcy ale nie wcześniej niż od dnia **01.01.2026r.** godz. 0⁰⁰ przyłączonych po stronie Zamawiającego do routerów dostępowych będących w posiadaniu Zamawiającego, za pośrednictwem interfejsów 40 Gigabit Ethernet fizycznie zakończonych modułami QSFP, dostarczonymi przez Wykonawcę w ramach Usługi. Ponadto usługa musi być zrealizowana za pomocą dwóch redundantnych łącz światłowodowych, które zostaną doprowadzone do budynku w lokalizacji Zamawiającego dwoma rozdzielonymi geograficznie, odseparowanymi od siebie fizycznymi traktami (tj. nieposiadającymi żadnego wspólnego punktu) w sposób wykluczający powstanie pojedynczego wspólnego punktu awarii.

W ramach realizacji ochrony antyDDoS Zamawiający wymaga wykonania, co najmniej:

- zabezpieczenia punktu styku z siecią publiczną przed atakami DDoS o wolumenie do 60 Gbps i 60 Mpps;
- analizy ruchu w celu identyfikacji typu i natury ataku;
- automatycznego rozpoczęcia usuwania ataku
- powiadamiania Zamawiającego o wystąpieniu ataku, gdy dotyczy on jednego ze wskazanych usług/adresów IP Zamawiającego;
- zatrzymanie usuwania ataku na żądanie Zamawiającego, gdy dotyczy on jednego ze wskazanych usług/adresów IP Zamawiającego;

Szczegółowe wymagania w zakresie realizacji ochrony antyDDoS znajdują się rozdz. III OPZ

- b) dostęp do wszystkich usług i serwisów internetowych krajowych i zagranicznych;
- c) nielimitowaną ilość sesji oraz przesyłanych danych;
- d) obsługę adresów IP klasy B 145.237.0.0/16 używanych przez Zamawiającego;
- e) obsługę ruchu generowanego przez Zamawiającego przy pomocy dynamicznego protokołu routingu BGP v.4 (Border Gateway Protocol w wersji 4), w taki sposób, aby użyte w tym celu rozwiązania nie obniżały parametrów przepustowości łączy, określonych odpowiednio w rozdz. I pkt 1 OPZ, w szczególności, jeśli na rzecz obsługi protokołu BGP v.4 zarezerwowane będzie na ww. łączach dedykowane pasmo transmisyjne, to parametry tego pasma nie mogą być wliczane do przepustowości określonej w rozdz. I pkt 1 OPZ. Wykonawca na łączach dostępowych musi obsługiwać AS 34339 Zamawiającego przy użyciu protokołu BGP v.4,
- f) obsługę priorytetyzacji ruchu QoS (Quality of Service) pakietów IP przychodzących do Zamawiającego poprzez wdrożenie na urządzeniach Wykonawcy obsługujących łącze dostępne określone w rozdz. II pkt 1 OPZ procedur, umożliwiających Zamawiającemu definiowanie polityki QoS dotyczącej ruchu przychodzącego do Zamawiającego z Internetu, przy czym procedury te muszą umożliwiać Zamawiającemu okresową (nie rzadziej niż raz w miesiącu) weryfikację skuteczności tej polityki. Opis procedur oraz sposób ich użycia przez Zamawiającego (dokumentacja powykonawcza) musi być przekazany Zamawiającemu w formie elektronicznej na adres email w terminie do. 31.12.2025

ROZDZIAŁ III. Opis wymagań ochrony antyDDoS

1. Usługa dostępu do Internetu

Zamawiający wymaga uruchomienia i świadczenia ochrony przed atakami DDoS dla usługi szerokopasmowego dostępu do Internetu o przepustowości gwarantowanej dla lokalizacji wskazanej w rozdz. I pkt 1 OPZ. Usługa ochrony będzie świadczona dla adresacji IP Zamawiającego na dostarczonym w tej lokalizacji symetrycznym łączu dostępowym do Internetu.

W ramach realizacji usługi ochrony przed atakami DDoS, Zamawiający wymaga wykonywania co najmniej:

- a) monitorowania i analizy ruchu w celu identyfikacji typu i natury ataku
- b) automatycznego rozpoczęcia usuwania ataku
- c) powiadamiania Zamawiającego o wystąpieniu ataku gdy dotyczy on jednego ze wskazanych usług/adresów IP Zamawiającego;
- d) zatrzymanie usuwania ataku na żądanie Zamawiającego, gdy dotyczy on jednego ze wskazanych usług/adresów IP Zamawiającego;
- e) modyfikacji zestawu użytych mechanizmów przeciwdziałania tak, by uzyskać maksymalny poziom filtracji ruchu niepożądanego przy braku wpływu na ruch prawidłowy
- f) klasyfikację alarmów typu DDoS jako:
 - zweryfikowany atak
 - fałszywy alarm
 - nagły ruch – wzrost ruchu spowodowany inną przyczyną niż atak.

2. Wykrywanie zagrożeń

Zamawiający wymaga realizacji efektywnej identyfikacji potencjalnych ataków DDoS z wykorzystaniem, co najmniej poniższych mechanizmów detekcji:

- Sygnatury;
 - przekroczenie progów dla określonych typów pakietów i protokołów;
 - oparte na analizie profilu ruchu Zamawiającego i wykrywanie nieoczekiwanych zmian ruchu w odniesieniu do tego profilu.
- a) Usługa monitoruje ruch do i od chronionej sieci w czasie rzeczywistym
 - b) Usługa zapewnia wykrywanie anomalii polegających na przekroczeniu wartości uważanych za normalne w ruchu Internetowym w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, IP Null, IP Fragmented, DNS.
 - c) System realizujący usługę na podstawie danych historycznych wyznacza oczekiwaną wartość ruchu do i od chronionej sieci o danej porze dnia w danym dniu tygodnia.
 - d) Usługa zapewnia wykrywanie anomalii polegających na znaczącym przekroczeniu wolumenu ruchu w stosunku do wcześniej wyznaczonych wartości oczekiwanych ruchu.

3. Oczyszczanie ruchu

Zamawiający wymaga zapewnienia usługi ochrony przed atakami DDoS polegającej na usuwaniu ataku przy braku wpływu na ruch uprawniony. Efektywne działanie powinno obejmować trzy procedury:

- procedura (Off-ramping) - uruchamiana w przypadku podejrzenia wystąpienia ataku, ruch zostanie przekierowany do dedykowanych do tego celu zasobów wewnętrznych Wykonawcy
 - procedura filtrowania - oparta o wielowarstwową analizę ruchu i mechanizmy przeciwdziałania
 - procedura (On-ramping) - przekierowanie odfiltrowanego ruchu z powrotem do Klienta.
- a) Usługa zapewnia ochronę przed atakami o wolumenie do 60Gbs i 60Mpps.
 - b) W trakcie oczyszczania pakiety nie są przekierowane poza teren Unii Europejskiej
 - c) Usługa zapewnia filtrowanie ruchu z błędnymi nagłówkami IP/TCP/UDP
 - d) Usługa musi zapewniać ochronę przed co najmniej następującymi typami ataków:
 - 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/TLS negotiation;
- e) Usługa musi umożliwiać ochronę przed atakami pochodzącymi z sieci botnetowych (komputerów zainfekowanych w sposób umożliwiający zdalne sterowanie przez hackerów) poprzez filtrowanie na podstawie na bieżąco aktualizowanych sygnatur zawierających listę adresów IP.
- f) Usługa musi umożliwiać ochronę przed atakami pochodzącymi z sieci botnetowych poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości. Wartości progowe są definiowalne zarówno dla całości ruchu jak i do części ruchu zdefiniowanego za pomocą filtru.
- g) Usługa musi umożliwiać uruchamianie oczyszczania w celu nauczenia systemu wartości typowych ruchu, które następnie mogą być wykorzystywane do właściwego ustawiania progów dla algorytmów oczyszczania

4. Poziom SLA dotyczący powiadomienia o ataku

Oczyszczanie ruchu będzie włączane automatycznie dla wszystkich ataków. Dla uzgodnionych usług/adresów IP Zamawiającego będzie dodatkowo przekazywana do Zamawiającego informacja o ataku przez ustalone kanały komunikacji i w szczególnych sytuacjach na żądanie Zamawiającego oczyszczanie ruchu będzie wyłączane. Lista uzgodnionych usług/adresów IP będzie obejmować kluczowe dla Zamawiającego usługi świadczone w Internecie dla Obywateli RP, może być modyfikowana w czasie trwania Umowy.

Dla usługi ochrony przed atakami DDoS ustala się opisane poniżej trzy parametry SLA: CRA, CPZ i CRZ.

- a) Czas Reakcji na Atak (CRA)
- Przez CRA rozumie się czas, jaki upłynie od wykrycia Ataku DDoS do rozpoczęcia skutecznego oczyszczania ruchu. Wartość parametru CRA dla określonych Poziomów SLA wynosi 15 minut
- b) Czas na powiadomienie Zamawiającego o ataku w przypadku uzgodnionych usług/adresów IP (CPZ)
- Dla uzgodnionych usług/adresów IP Wykonawca przekaże Zamawiającemu informację o wystąpieniu ataku i rozpoczęciu oczyszczania ruchu na numer telefonu: +483673699 oraz adres email monit1@mf.gov.pl w czasie CPZ, który wynosi 15 min od wystąpienia ataku.
 - Czas CPZ liczony jest od momentu zaraportowania na platformie ataku do zarejestrowania w systemie teleinformatycznym Wykonawcy zdarzenia wysłania emaila.
 - Jeśli nie dojdzie do skutecznego kontaktu telefonicznego w pierwszej próbie Wykonawca zobowiązany jest do wykonania następnych prób w czasie CPZ.
- c) Czas Reakcji na Zlecenie wyłączenia oczyszczania ruchu (CRZ)
- Przez CRZ rozumie się czas, jaki upłynie od przyjęcia Zlecenia Zamawiającego z żądaniem wyłączenia oczyszczania ruchu do faktycznego wyłączenia oczyszczania ruchu.
 - W przypadku żądania Zamawiającego wyłączenia oczyszczania ruchu nastąpi ono od momentu skutecznego kontaktu Zamawiającego z Wykonawcą na numer telefonu i przekazania decyzji o wyłączeniu oczyszczania ruchu przez osoby i z numerów telefonu wskazanych przez

Zamawiającego.

- Wartość parametru CRZ dla określonych Poziomów SLA wynosi 15 minut.

5. Raport kwartalny.

Zamawiający wymaga sporządzania po każdym zakończonym 3-miesięcznym okresie świadczenia usługi, kwartalnego raportu, dotyczącego usługi antyDDoS, który będzie zawierał, co najmniej następujące statystyki,:

- a) Przekroczenia CRA, CPZ i CRZ
- b) lista zarejestrowanych i usuniętych ataków
- c) lista ataków niezmitgowanych wraz z przyczyną braku mitygacji

Uzupełnieniem Raportu kwartalnego będą wykresy graficzne pokazujące:

- a) poziom ruchu wchodzącego i wychodzącego w formie grafiki
- b) maksymalne poziomy ruchu

6. Raport z incydentu

Zamawiający wymaga każdorazowo po zakończeniu operacji oczyszczania ruchu po zaistniałym ataku sporządzenia raportu z incydentu w terminie 5 dni od zamknięcia incydentu i wysłania go na adres tt.raporty@mf.gov.pl Informacja w raporcie o incydencie zawierać będzie, co najmniej następujące statystyki:

- a) rozmiar ataku, liczniki pakietów, Gb/s oraz procent całości ruchu
- b) czas trwania ataku
- c) główne źródła ataku
- d) typ i natura ataku
- e) wdrożone metody eliminacji ataku
- f) geograficzna lokalizacja źródeł ataku
- g) wielkość oczyszczonego ruchu
- h) czasy – w szczególności: początek ataku, powiadomienie, wdrożenie procedur obronnych, zakończenie ataku, przywrócenie normalnej pracy sieci.

7. Obszar działania usługi

Zamawiający wymaga, aby ruch w sieci Zamawiającego przekierowany do oczyszczania był wysyłany wyłącznie do infrastruktury teleinformatycznej Wykonawcy lub będącej pod jego nadzorem, która znajduje się na terenie Unii Europejskiej.

8. Czas świadczenia usługi

Zamawiający wymaga świadczenia usługi ochrony antyDDoS w trybie 24/7/365.

9. Procedura przerywania oczyszczania (Fall-back Procedure)

Jeśli uruchomiona procedura eliminacji ataku DDoS ma negatywny wpływ na chronione zasoby lub usługi, Zamawiający ma możliwość zlecenia jej przerywania, co zostało opisane w rozdz. III pkt 4. Pomimo przerywania akcji, ruch Zamawiającego cały czas podlega monitorowaniu i istnieje możliwość

przywrócenia procedur obronnych w odpowiednio dostosowanym zakresie i analogicznym czasie wdrożenia.

10. Wdrożenie usługi antyDDoS.

a) Plan wdrożenia

Po podpisaniu umowy na świadczenie usługi, Wykonawca przygotowuje w uzgodnieniu z Zamawiającym dokument opisujący sposób wdrożenia/uruchomienia usługi antyDDoS. Dokument musi zawierać co najmniej:

- opis techniczny integracji usługi z siecią Zamawiającego
- opis procedur powiadamiania i eskalacji
- testy akceptacyjne
- opis procedur obsługi zgłoszeń i raportowania.

b) Implementacja

Implementacja obejmuje rekonfigurację urządzeń Zamawiającego oraz Wykonawcy pod kątem monitorowania ruchu oraz uruchomienia usługi przeciwdziałania atakom DDoS.

c) Testy akceptacyjne

Po zakończeniu Implementacji Zamawiający wraz z Wykonawcą przeprowadzą Testy akceptacyjne zgodnie z uzgodnionym Projektem wykonawczym i stanowiące test funkcjonalny platformy ochrony przeciwko atakom DDoS. Testy uwzględnią pełną weryfikację poprawności wdrożonej konfiguracji.

Przed wdrożeniem usługi Zamawiający wymaga przeprowadzenia Procesu analizy ruchu Abonenta (Learning Mitigation) - proces w którym ruch zdefiniowany w ramach danego obiektu kierowany jest do platformy ochrony przed atakami DDoS Wykonawcy. Ruch podczas learning mitigation nie podlega żadnym filtracjom i w sposób niezmienny kierowany jest do sieci użytkownika. Platforma podczas learning mitigation zbiera statystyki, na których podstawie jest w stanie określić parametry tzw. countremeasures (algorytmów mitygacji) tak, aby w trakcie ataku zachować ruch użytkowników, a odfiltrować ruch ataku.

11. Dostęp do infrastruktury Zamawiającego

W uzasadnionych przypadkach, świadczenie usługi może być powiązane z dostępem do urządzeń aktywnych zarządzanych przez Zamawiającego, w celu uzyskania statystyk ruchu otrzymywanego oraz wysyłanego do sieci Wykonawcy.