Załącznik nr 1

do REGULAMINU ŚWIADCZENIA PUBLICZNIE DOSTĘPNEJ USŁUGI TELEKOMUNIKACYJNEJ OCHRONY INFRASTRUKTURY ABONENTA PRZED ATAKAMI TYPU DDoS (Distributed Denial of Service) dla Podmiotów realizujących zadania publiczne oraz Podmiotów istotnych z punktu widzenia bezpieczeństwa RP

I Opis Usługi anty-DDoS

1. Usługa anty-DDoS polega na ochronie Infrastruktury Abonenta przed Atakami DDoS, a w szczególności:
   a) powodujących przepełnienie i wysycenie pasma potrzebnego do świadczenia usług;
   b) mających na celu zalanie ww. infrastruktury pakietami IP;
   c) powodującymi wyczerpanie zasobów systemu świadczącego usługę.
2. W zależności od danych zawartych w nadesłanych NASK Ankietach technicznych, poziom ochrony jest przez NASK dostosowany dla danego Abonenta i specyfiki jego infrastruktury. Usługa anty-DDoS jest realizowana w trzech Wariantach wskazanych w Regulaminie, wybór Wariantu świadczenia Usługi anty-DDoS wskazany jest w Porozumieniu.
3. Usługa anty-DDoS w Wariancie II i III w zakresie dotyczącym Infrastruktury Sieciowej Abonenta jest świadczona dla wszystkich pul publicznych adresów IP wskazanych przez Abonenta, których maska ma maksymalnie 24 bity. Pule adresowe stanowią stałą lub czasową własność Abonenta i są rozgłaszane poprzez protokół BGP do sieci Internet z Autonomicznego Systemu Abonenta (jednolita sieć Abonenta zarządzana przez wewnętrznych administratorów). Jeżeli Abonent w Ankiecie technicznej:
   a) wskazał mniejszą maskę, wówczas ochronie może podlegać jedna lub więcej pul adresowych z maską do 24 bitów;
   b) wskazał większą maskę puli adresowej, wówczas ochroną obejmuje się wskazane Aplikacje Abonenta.
4. Usługą anty-DDoS jest objęta Infrastruktura Abonenta w skład której wchodzą rutowalne adresy IP lub aplikacje dostępne z publicznej sieci Internet.
5. W ramach realizacji Usługi anty-DDoS Wykonawca zapewnia:
   a) analizę ruchu w Infrastrukturze Abonenta w wybranym Wariancie, w celu identyfikacji typu i natury Ataku DDoS, wykonywanej na podstawie danych zebranych z urządzeń Abonenta, w oparciu o technologię netflow, IPFIX lub inną ustalaną przez Wykonawcę i Abonenta w trybie roboczym,
   b) powiadamianie Abonenta o podejrzeniu wystąpienia Ataku DDoS,
   c) Mitygację Ataku DDoS, przy czym możliwa jest:
      i. Automatyczna Mitygacja Ataku DDoS;
      ii. Mitygacja Ataku DDoS na żądanie - na podstawie Zatwierdzenia lub Zlecenia Mitygacji - w przypadku Usługi anty-DDoS mającej za przedmiot Infrastrukturę Sieciową Abonenta;
   d) modyfikacja zestawu użytych mechanizmów przeciwdziałania Atakom DDoS w celu maksymalnego poziomu filtracji niepożądanego ruchu w Infrastrukturze Abonenta, przy minimalnym wpływie na ruch prawidłowy w tej Infrastrukturze,
6. Wykonawca zapewnia efektywną identyfikację potencjalnych Ataków DDoS z wykorzystaniem poniższych mechanizmów:
   a) detekcja sygnatury,
   b) przekroczenie progów ruchu dla określonych typów pakietów i protokołów,
   c) wykrywanie nieoczekiwanych zmian ruchu w odniesieniu do tego profilu oparte na analizie profilu ruchu Abonenta.

NASK-PIB
ul. Kolska 12
01–045 Warszawa

nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01

Projekt finansowany ze środków Ministra Cyfryzacji

7. W przypadku:

   a) Wariantu I – Wykonawca zapewnia wykrywanie anomalii ruchu w Aplikacjach Abonenta polegających na znaczącym przekroczeniu wolumenu tego ruchu oraz wykrywanie potencjalnych ataków w warstwie aplikacyjnej dla poszczególnych Obiektów w stosunku do wcześniej wyznaczonych wartości oczekiwanych.

   b) Wariantu II – Wykonawca zapewnia wykrywanie anomalii ruchu w Infrastrukturze Abonenta polegających na przekroczeniu wartości uważanych za normalne w ruchu Internetowym, w szczególności pakietów TCP SYN, TCP RST, TCP Null, ICMP, błędnych pakietów IP /TCP, fragmentowanych pakietów IP, DNS, NTP, pakietów adresowanych prywatnymi adresami IP, UDP.

   c) Wariantu III – ochrona obejmuje wykrywanie anomalii ruchu wskazanych dla Wariantu I i II powyżej;

8. Usługa anty-DDoS ma na celu ochronę przed typowymi rodzajami Ataków DDoS, w tym co najmniej:

   1. UDP floods (volumetric)
   2. NTP amplification (volumetric)
   3. DNS amplification (volumetric)
   4. SYN floods (protocol)
   5. DNS Query floods (layer-7)
   6. HTTP(S) GET request floods (layer-7)
   7. TCP ACK floods (volumetric & proto)
   8. Tsunami SYN flood (volumetric)
   9. CHARGEN amplification (volumetric)
   10. Memcache amplification (volumetric)
   11. SSDP amplification (volumetric)
   12. SNMP amplification (volumetric)
   13. HTTP(S) POST request floods (layer-7)
   14. TCP RST floods (protocol)
   15. SSL negotiation floods (protocol)
   16. SlowLoris attack (protocol)
   17. TCP connect() floods (protocol)
   18. SMTP request flood (layer-7)
   19. GRE-IP UDP floods (volumetric)
   20. Fragmented attacks (protocol)
   21. CLDAP attacks (volumetric)
   22. CoAP (volumetric & protocol)
   23. WS-DD (volumetric & protocol)

Projekt finansowany ze środków Ministra Cyfryzacji

24. ARMS (volumetric)
25. Jenkins (volumetric)
26. DNS Water Torture (volumetric)

9. Usługa anty-DDoS jest realizowana w środowisku wyizolowanym (bez konieczności pobierania sygnatur i innych składowych z Internetu) i zapewnia ochronę przed zagrożeniami min. OWASP TOP TEN. Oczyszczanie ruchu ma minimalny wpływ na ten ruch (bardzo niewielkie prawdopodobieństwo tzw. false positives, tj. potencjalnej możliwości blokady i zakłócenia prawidłowego ruchu w Infrastrukturze Abonenta w przypadku braku wystąpienia Ataku DDoS).
10. Ze względu na charakter chronionych serwisów i lokalizacje zasobów Abonentów Wykonawca deklaruje, że wykorzystuje minimum dwa centra oczyszczania ruchu na terenie Europejskiego Obszaru Gospodarczego.
11. Dekrypcja ruchu SSL/TLS (w ramach Wariantu I lub III dla Aplikacji Abonenta) realizowana jest na terenie Europejskiego Obszaru Gospodarczego.

II Wymagania wobec Abonenta

1. W celu realizacji Usługi anty-DDoS w Wariancie I niezbędne jest posiadanie przez Abonenta:
    a) Serwisu dostępnego z publicznej sieci Internet poprzez protokół https,
    b) Uprawnień administracyjnych do zarządzania danym serwisem,
    c) Możliwości zmian rekordów w serwisie DNS lub zlecania takich zmian operatorowi, który hostuje serwis Abonenta,
    d) Posiadanie certyfikatu przydzielonego przez zaufany urząd certyfikacji (CA).
2. W celu realizacji Usługi anty-DDoS w Wariancie II niezbędne jest posiadanie przez Abonenta:
    a) numeru Systemu Autonomicznego przydzielonego przez RIPE,
    b) publicznej adresacji IPv4 o maksymalnym rozmiarze 24 bitów (256 adresów IP)
    c) możliwości podłączenia do sieci NASK jedną z wybranych metod:
        i. łącze bezpośrednie do jednego z węzłów NASK,
        ii. łącze realizowane poprzez publiczną sieć Internet jako tunel GRE,
        iii. łącze realizowane poprzez sieć GOVnet,
    d) możliwości konfiguracji protokołu BGP (eBGP) między NASK a Abonentem,
    e) możliwości modyfikacji segmentu TCP,
    f) możliwości wysyłania/exportowania próbek ruchu przychodzącego do Centrum Czyszczenia,
    g) możliwości modyfikacji danych zapisanych w publicznej bazie RIPE DB w zakresie
        i. tworzenia obiektu route w zakresie chronionej podsieci,
        ii. modyfikacji obiektu ROA (Route Origin Authorization) – jeżeli już został taki obiekt utworzony.

Projekt finansowany ze środków Ministra Cyfryzacji

III Opis działania Usługi anty-DDoS

Wariant I – Aplikacje Abonenta:

1. Usługa anty-DDoS realizowana jest w modelu ciągłym (always on). Oznacza to, iż ruch cały czas przekierowany jest przez Centrum Czyszczenia, a Mitygacja Ataku DDoS następuje w czasie zbliżonym do rzeczywistego. Proces wdrożenia Usługi anty-DDoS realizowany jest w modelu self service.

2. Na podstawie danych kontaktowych użytkowników oraz parametrów technicznych zawartych w Ankiecie Technicznej NASK utworzy Konto w Portalu Administracyjnym. Abonent dostanie Informację o utworzeniu takiego Konta. Na podstawie własnej dokumentacji, umiejętności i wiedzy nabytej po przeprowadzonym Instruktażu, Abonent po zalogowaniu się, będzie mógł rozpocząć proces uruchomienia Usługi anty-DDoS dla danego serwisu (tzw. onboarding). Uruchomienie ochrony obejmuje następujące elementy:

    a) Wprowadzenie danych serwisu obejmowanego ochroną wraz z nazwą DNS oraz adresem IP pod którym serwis jest osiągalny,

    b) Wygenerowanie lub wgranie certyfikatu i przypisanie go do danego serwisu,

    c) Zmianę konfiguracji DNS lub zlecenie wykonania takich zmian,

    d) Aktualizację listy dostępowej do danego serwisu (access list/ACL) ograniczającej jego widoczność z sieci publicznej Internet tylko do zaufanych adresów IP będących w posiadaniu Dostawcy usługi ochrony przed atakami,

3. Schemat działania Usługi anty-DDoS w Wariancie I został zaprezentowany na schemacie nr 1 poniżej.

Wariant II - Infrastruktura Sieciowa Abonenta:

1. Usługa anty-DDoS realizowana jest w modelu na żądanie (on-demand). Oznacza to, że w przypadku wystąpienia Ataku DDoS następuje uruchomienie ochrony poprzez przekierowanie ruchu do Centrum Oczyszczania. Uruchomienie Usługi anty-DDoS następuje automatycznie i inicjowane jest przez Centrum Oczyszczania na podstawie zebranych próbek z ruchu przychodzącego lub na podstawie zgłoszenia żądania włączenia Usługi anty-DDoS;

2. Na podstawie Ankiety technicznej NASK zgłosi klasy adresowe, które będą objęte Usługą anty-DDoS. Jeżeli Abonent jest właścicielem klasy adresowej o rozmiarze większym niż /24 wówczas ochronie będą podlegały wszystkie sieci /24 które wchodzą w skład posiadanej Infrastruktury Sieciowej. Przykładowo: jeżeli Abonent zgłosił w celu objęcia Usługą anty-DDoS sieć /22 wówczas ochroną zostaną objęte wszystkie sieci /24 mieszczące się we wskazanej /22 (w omawianym przykładzie będą to 4 klasy adresowe). Jeżeli Abonent posiada jedną lub więcej sieci /24, wówczas uruchomienie Usługi anty-DDoS będzie realizowane jednocześnie ze wstrzymaniem rozgłoszenia tych sieci do upstream providera. Ewentualnie należy prependować rozgłoszenia tych sieci. NASK potwierdzi działanie łącza między urządzeniem NASK a urządzeniem brzegowym Abonenta. Na etapie zestawiania łącza do sieci NASK, NASK dostarczy wszelkich danych niezbędnych do skonfigurowania usługi, w tym:

    a) Numer Systemu Autonomicznego do którego należy zestawić sesję BGP,

    b) Adresację IP niezbędną do zestawienia sesji BGP (sieć /30),

    c) W przypadku tuneli GRE NASK poda adres IP urządzenia do którego należy zestawić tunel GRE,

    d) Rozmiar MTU i segmentu TCP jaki należy ustawić po stronie Abonenta,

    e) Adresację IP urządzeń, do których należy dostarczać próbki ruchu,

    f) Parametry jakie należy ustawić w celu zbierania próbek ruchu przychodzącego do Abonenta,

    g) Zmiany, które należy wprowadzić w bazie RIPE.

3. W celu zachowania najwyższego poziomu dostępności Usługi anty-DDoS NASK rekomenduje zestawienie minimum dwóch połączeń z siecią NASK przy wykorzystaniu minimum dwóch sposobów realizacji łącza.

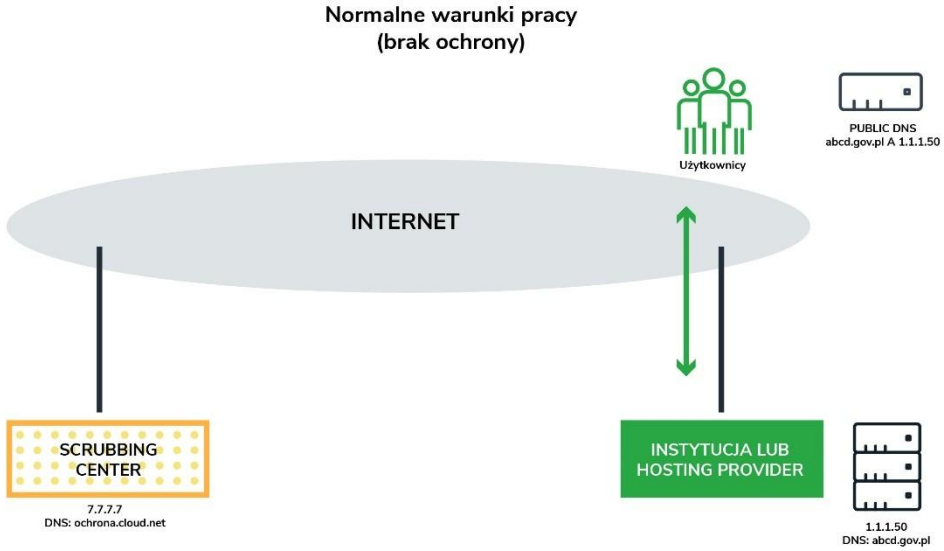
Projekt finansowany ze środków Ministra Cyfryzacji

4. Po spełnieniu wymogów określonych w lit. b Usługa anty-DDoS jest przygotowana do świadczenia. W momencie wystąpienia Ataku DDoS na Infrastrukturę Sieciową Abonenta rozgłaszana jest sieć Abonenta lub jej fragment do sieci Internet. Rozgłaszającym sieć Abonenta jest NASK za pośrednictwem Centrum Czyszczenia. W ten sposób wolumen Ataku DDoS oraz ruch prawidłowy trafia do Centrum Czyszczenia. Tam następuje oddzielenie ruchu zainfekowanego Atakiem DDoS od prawidłowego a następnie ruch prawidłowy trafia do sieci NASK, skąd zostaje przekierowany do sieci Abonenta.

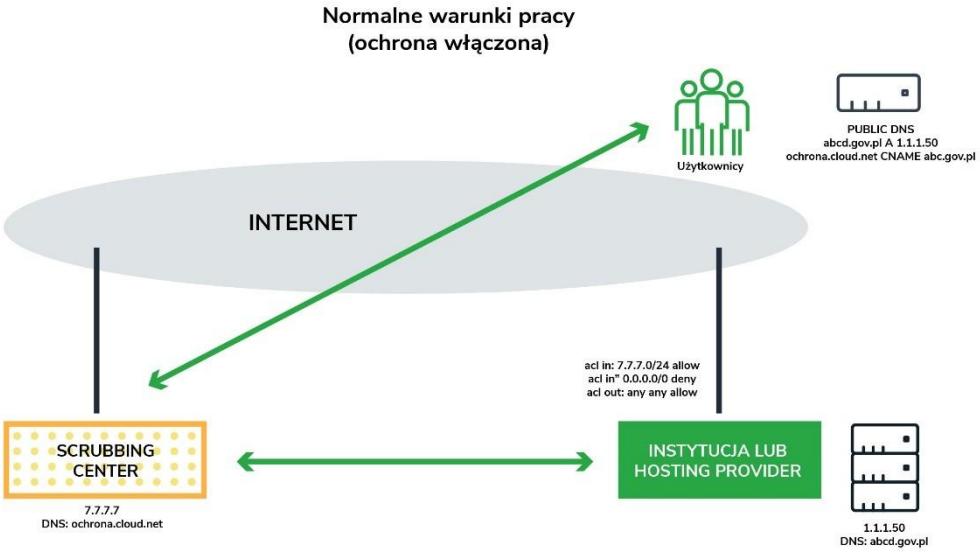
5. Schemat działania Usługi anty-DDoS w Wariancie II został zaprezentowany na schemacie nr 2 poniżej.

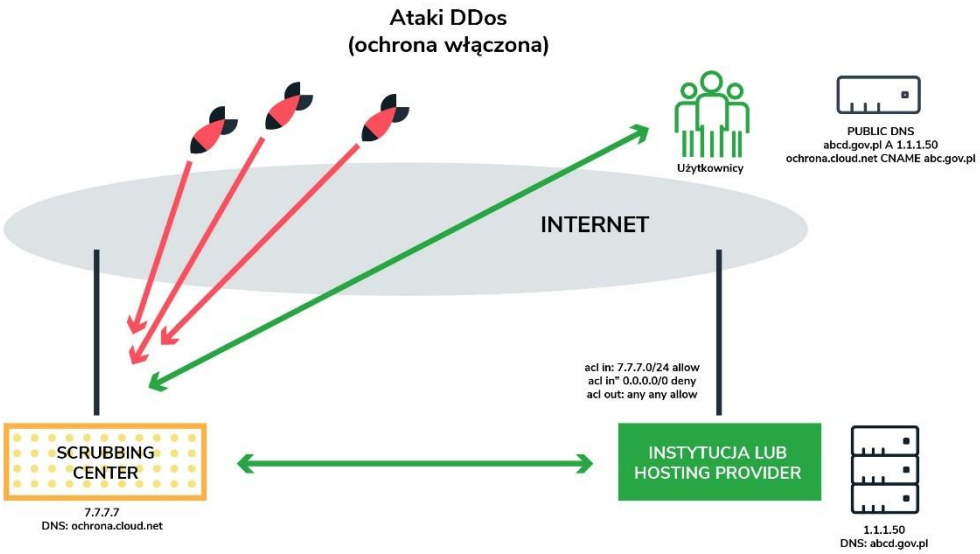
Usługa anty-DDoS w Wariancie III stanowi połączenie Wariantu I (w odniesieniu do Aplikacji Abonenta) i Wariantu II (w odniesieniu do Infrastruktury Sieciowej Abonenta).

SCHEMAT NR 1



Projekt finansowany ze środków Ministra Cyfryzacji

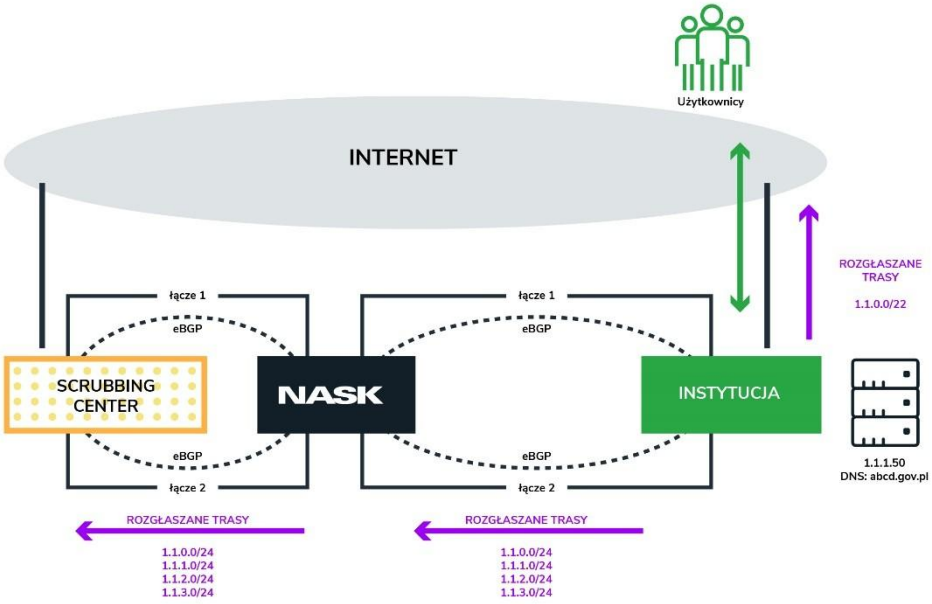




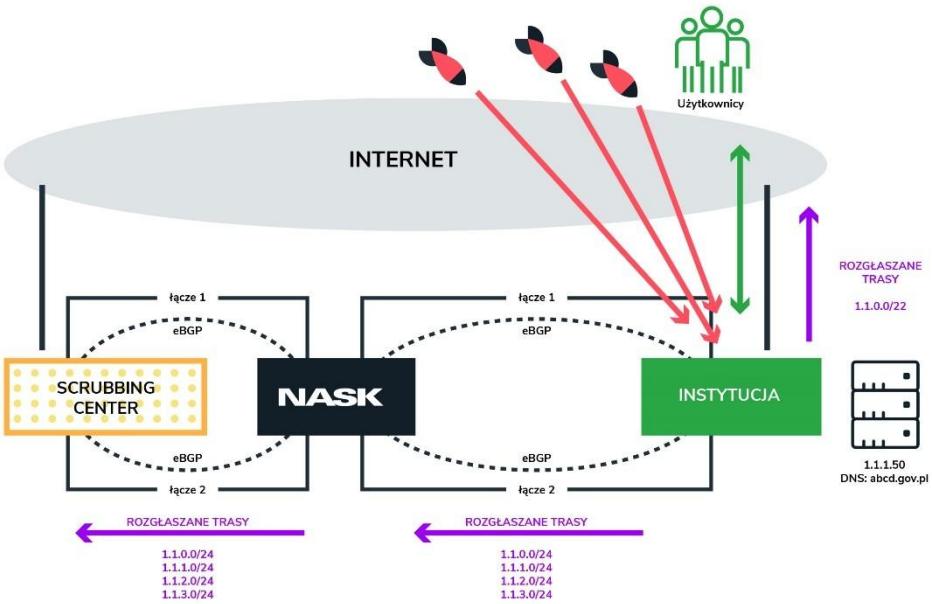
Projekt finansowany ze środków Ministra Cyfryzacji

SCHEMAT NR 2

Normalne warunki pracy
(brak ochrony)

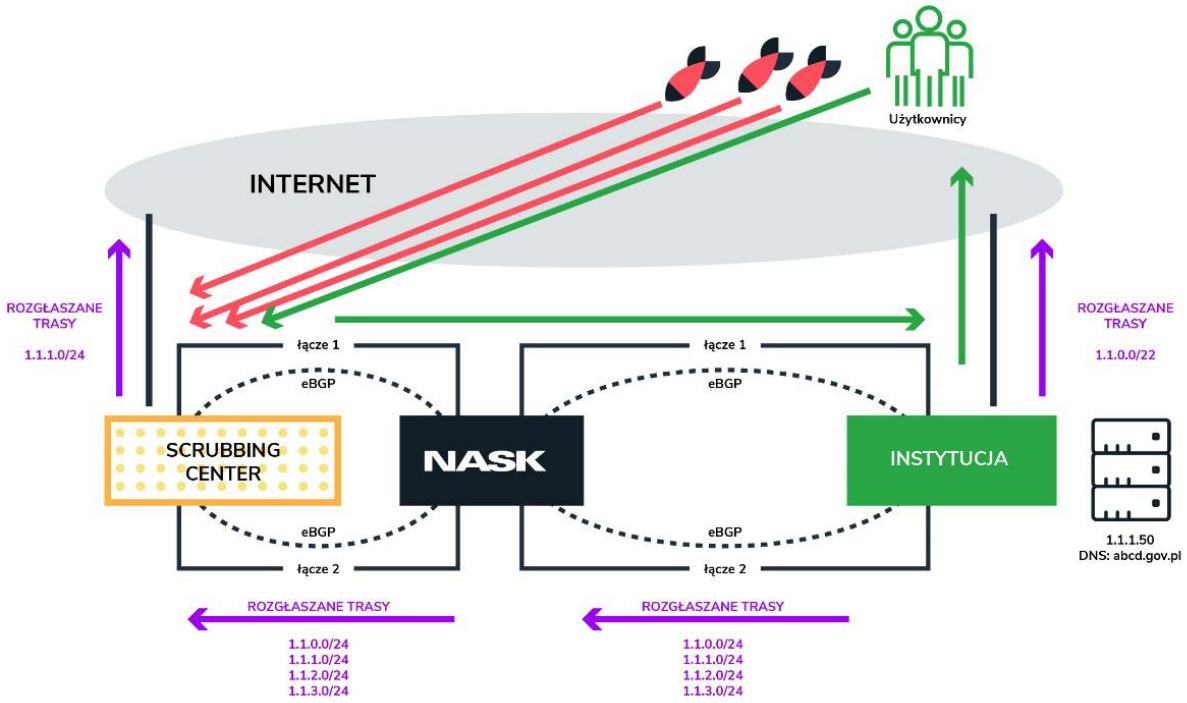


Atak DDos



Projekt finansowany ze środków Ministra Cyfryzacji

Mitygacja ataku



Projekt finansowany ze środków Ministra Cyfryzacji