**1. Usługa AntyDDos powinna :**

* Umożliwiać definiowanie własnych białych, czarnych list portów i protokołów;
* Umożliwiać wysyłanie powiadomień o akcjach obronnych wysyłanych na wskazany przez klienta adres e-mail ;
* Umożliwiać definiowanie list obiektów oraz list wykorzystywanych portów i protokołów
* możliwość określenia, które z obiektów wykorzystują komunikację UDP;
* definiować wielkości ruchu mierzonej w pps i bps dla poszczególnych adresów IP, przekroczenie której spowoduje uruchomienie alarmu;
* definiować wielkości ruchu mierzonego w pps i bps dla poszczególnych adresów IP, przekroczenie wartości spowoduje automatyczne uruchomienie obrony;
* umożliwiać określenie, czy podczas ataku adresy źródłowe powinny zostać ograniczone do terytorium Polski / innych obszarów geograficznych;
* Rozwiązanie DDos powinno umożliwiać zdefiniowanie minimum 20 chronionych obiektów;
* Umożliwiać zmianę sposobu reakcji na atak – automatyczna / ręczna dla każdego z obiektów;
* Umożliwiać zdefiniowanie dedykowanego scenariusza obsługowego;
* Umożliwiać do pięciu zmian konfiguracji w miesiącu;
* realizacja usługi musi odbywać się na łączach dostawcy rozwiązania DDoS;
* Rozwiązanie DDos powinno zabezpieczać Klienta przed atakami o wolumenie nie mniejszym niż 70 Gbps ;
* Umożliwiać aktywny monitoring 24/7/365 bezpieczeństwa zasobów IT klienta i reagowanie na ataki;
* Klient powinien mieć dostęp do raportów dotyczących ruchu i ataków;
* Klient oczekuje pełnego wsparcia ze strony ekspertów na wszystkich etapach wdrożenia rozwiązania, obejmującym analizę istniejącej infrastruktury dla potrzeb wdrożenia usługi DDos;
* gwarancja parametrów niezawodnościowych - Service Level Agreement (SLA)
* Dostępność minimum jednego punktu kontaktowego – BOK 24/7/365

SLA

* Próba kontaktu z klientem nastąpi nie później niż 15 minut od chwili wykrycia alarmu
* Obrona zostanie uruchomiona w czasie nie dłuższym niż 15 minut po potwierdzeniu przez klienta
* W przypadku ochrony uruchamianej w sposób automatyczny, rozpoczęcie filtrowania ruchu nastąpi nie później niż 5 min od chwili wykrycia ataku.

Wykaz odpieranych ataków przez rozwiązanie DDoS nie mniej niż:

1. ICMP - smurf attack

2. CMP - ping flood

3. LAND

4. Christmas tree

5. TCP SYN Flood

6. UDP flood

7. NTP reflected/amplification attack

8. DNS reflected/amplification attack

9. CLDAP Amplification / Reflection attack

10. CHARGEN Amplification / Reflection attack

11. L2TP Amplification / Reflection attack

12. MSSQL Amplification / Reflection attack

13. NetBIOS Amplification / Reflection attack

14. RCPBIND Amplification / Reflection attack

15. RIPv1 Amplification / Reflection attack

16. SNMP Amplification / Reflection attack

17. mDNS Amplification / Reflection attack

18. SSDP Amplification / Reflection attack

19. Memcached Amplification / Reflection attack

20. UDP/IP Fragments

21. Generic UDP Reflection

22. QOTD Reflection

23. DNS Query Flood

24. Invalid packets - IP checksum

25. Invalid packets - IP NULL

26. Invalid packets - TCP flags

27. Invalid packets - Bad UDP Payload length

28. TCP Fragments

29. TCP RST Flood

Metody obrony/blokowania nie mniej niż:

* blokowanie/czasowe zawieszanie źródłowych adresów IP;
* blokowanie wybranych pakietów;
* kombinacja blokowania adresów IP bazująca na nagłówkach pakietów oraz progach ilościowych;
* blokowanie adresów IP na podstawie danych geolokalizacyjnych;
* obsługa BGP Flowspec;
* obsługa BGP Blackhole;

Mechanizmy używane w trakcie obrony nie mniej niż:

* SYN Filter
* Token Bucket Filter
* WHITE/BLACK LIST
* DROP
* Invalid Packet Filter
* Adaptive Filter
* GeoFilter
* Automatycznie aktualizowana black list