Opis usługi Atman AntyDDoS 2.0

Podstawowe informacje

DDoS (ang. Distributed Denial of Service) to przeprowadzany równocześnie z wielu komputerów (tzw. zombie) i zainfekowanych urządzeń IoT atak na systemy komputerowe dostawców treści i usług internetowych. Atak taki jest niemożliwy do odróżnienia przez klasyczne systemy zabezpieczeń od prawidłowego ruchu z innych komputerów.

Zagrożenia

Ataki typu DDoS są powszechne już od dłuższego czasu, ale ich forma jest coraz bardziej zaawansowana. Obecnie taki atak może zamówić każdy, ponieważ ich dostępność i cena nie stanowią żadnej bariery. Jest to jeden z najpowszechniejszych sposobów złośliwego unieruchamiania witryn i systemów internetowych.

Dla przedsiębiorstwa świadczącego swoje usługi przez Internet **straty biznesowe związane z przeciążonymi serwerami i łączami dostępowymi nie ograniczają się jedynie** do niemożliwości obsługi klientów w czasie samego ataku, ale rozciągają się również na utratę zaufania, straty finansowe oraz wizerunkowe czy też potencjalny konflikt wewnątrz organizacji. Ochrona przed atakami DDoS stała się równie ważna jak ochrona zasobów IT przed hakerami i wirusami komputerowymi.

Zabezpieczenia

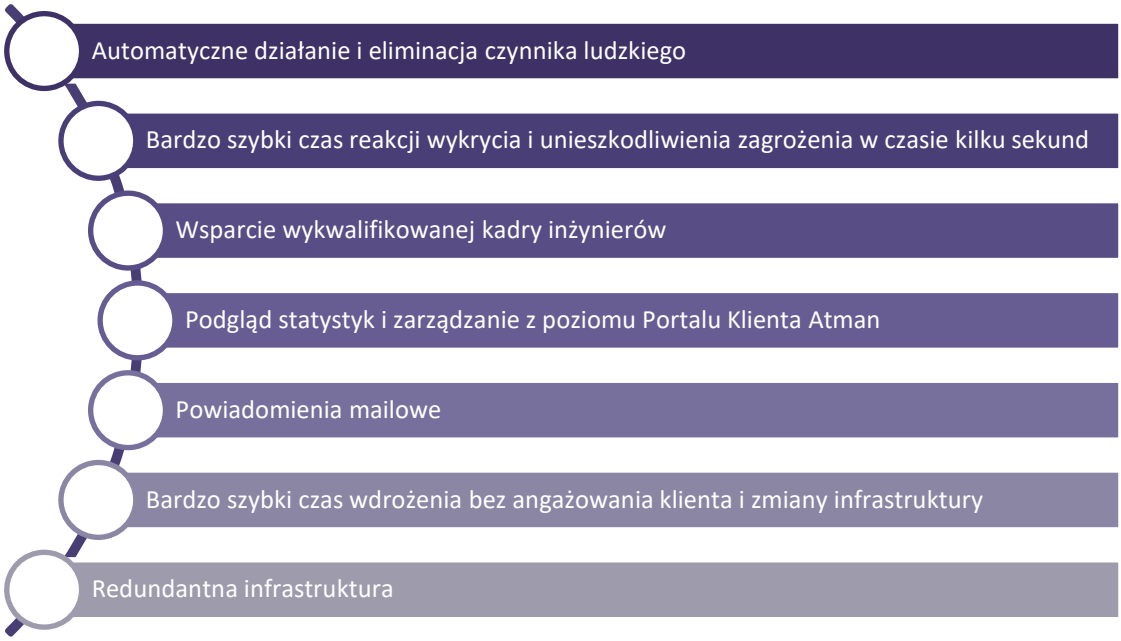
Atak typu DDoS jest specyficzny z uwagi na niemożliwość jego odróżnienia od zwykłego ruchu przez klasyczne systemy zabezpieczeń. Atak polega na wysyceniu zasobów klienta (np. łączy internetowych), więc **dla skuteczności ochrony kluczowe jest rozpoznanie i zatrzymanie ataku na poziomie infrastruktury operatora telekomunikacyjnego (np. ATM),** który ma możliwość przyjęcia i neutralizacji ataku, potencjalnie bardzo niebezpiecznego dla klienta końcowego.

W związku z powyższym Atman oferuje kompleksowe rozwiązanie zapewniające ochronę przed znanymi, nieznanymi i ewoluującymi atakami wolumetrycznymi, w tym DoS i DDoS. Usługę Atman AntyDDoS 2.0 charakteryzuje:

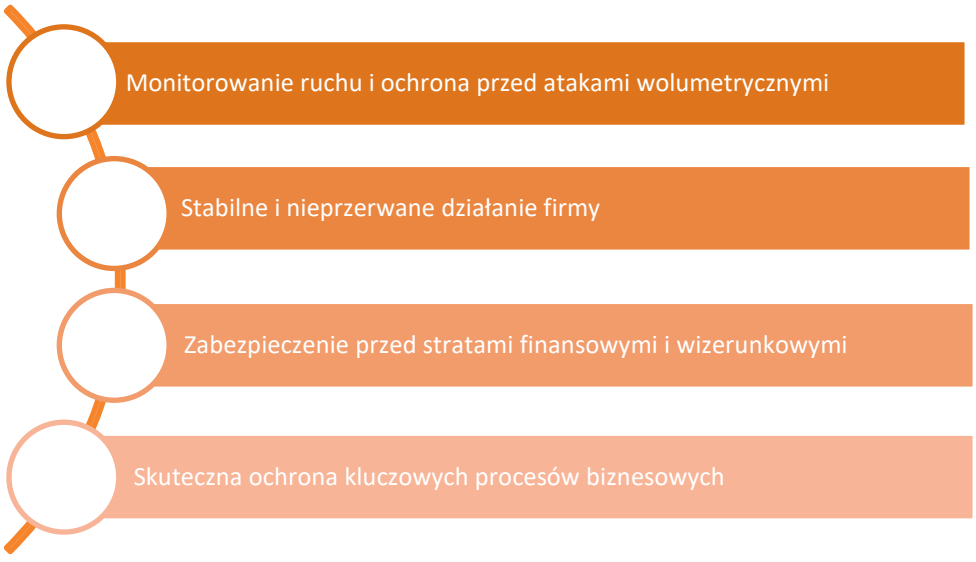
- Automatyczne działanie i **eliminacja czynnika ludzkiego**
- **Bardzo szybki czas reakcji** (kluczowy przy atakach DDoS), gdzie zagrożenie jest wykrywane i unieszkodliwiane w ciągu kilku sekund
- **Bezkonkurencyjnie niska cena.**

ATM S.A.
ul. Grochowska 21a, 04-186 Warszawa
tel. 22 51 56 100, faks 22 51 56 600, info@atman.pl

Podstawowe zalety rozwiązania



Podstawowe korzyści z wdrożenia



Opis techniczny usługi

Model usługi

Atman AntyDDoS 2.0 jest usługą dodatkową, rozszerzającą usługę dostępu do Internetu. Zakłada ona objęcie sieci klienta dodatkowym monitoringiem poziomu ruchu przychodzącego i w przypadku wykrycia ataku DDoS, automatycznym przekierowaniem go na węzły filtrujące ataki DDoS rozlokowane w sieci szkieletowej Atman.

Komponenty rozwiązania

Rozwiązanie funkcjonuje w oparciu o komponenty sprzętowe oraz aplikację. Komponenty sprzętowe to Sensor i Scrubber, które zainstalowane są w Centrum Danych Atman WAW-1 oraz Centrum Danych Atman WAW-2.

- Sensor – urządzenie podłączone do przełącznika dystrybucyjnego Atman. Ma za zadanie w czasie rzeczywistym analizować próbkowany ruch przepływający przez łącze internetowe klienta.
- Scrubber – urządzenie podłączone do przełącznika szkieletowego Atman. Scrubbery mają skonfigurowaną sesję BGP do routera szkieletowego. Służą do przekierowania ruchu do atakowanego hosta, który następnie poddany jest procesowi czyszczenia.
- Oprogramowanie – specjalistyczne oprogramowanie redGuardian zainstalowane zarówno na Sensorze, jak i na Scrubberze.

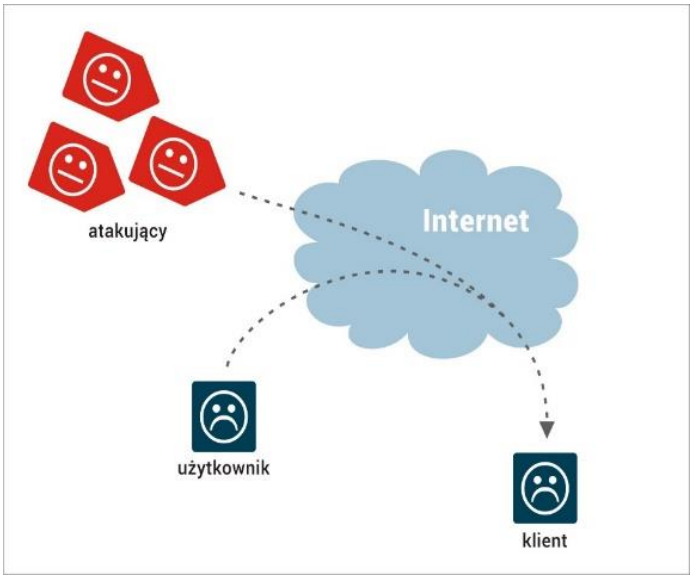
Atman WAW-1

Atman WAW-2

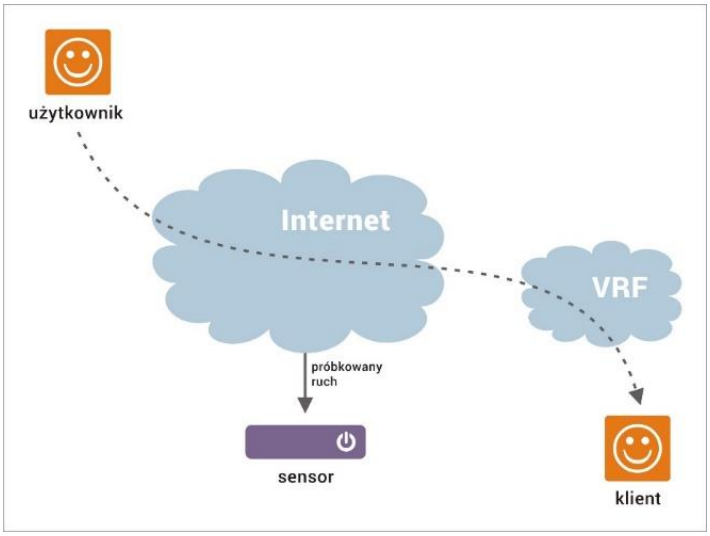
Z perspektywy klienta, wdrożenie usługi nie wiąże się z żadnymi zmianami w obecnej jego infrastrukturze.

Poniżej obrazowo przedstawiono zasadę działania:

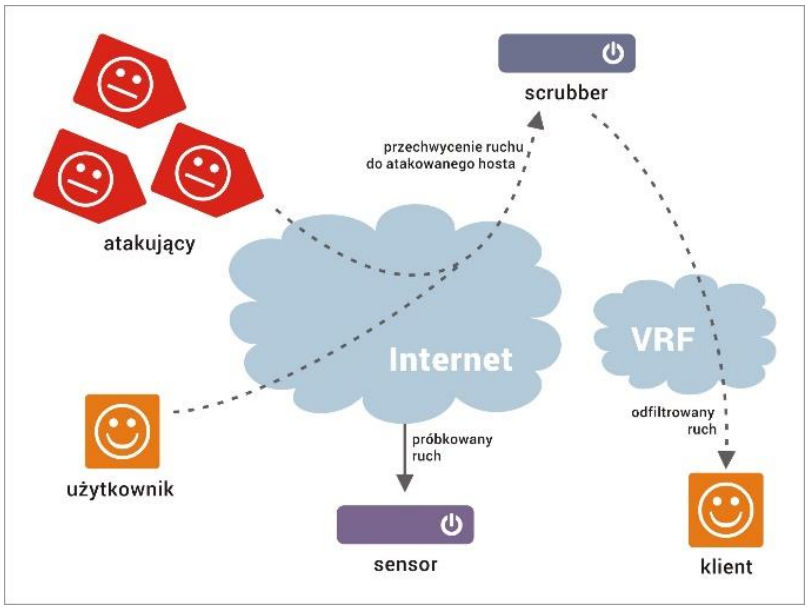
1. Usługa dostępu do Internetu bez ochrony przed atakami DDoS



2. Usługa dostępu do Internetu z włączoną ochroną przed atakami DDoS (bez ataku)



3. Usługa dostępu do Internetu z włączoną ochroną przed atakami DDoS (w trakcie ataku)

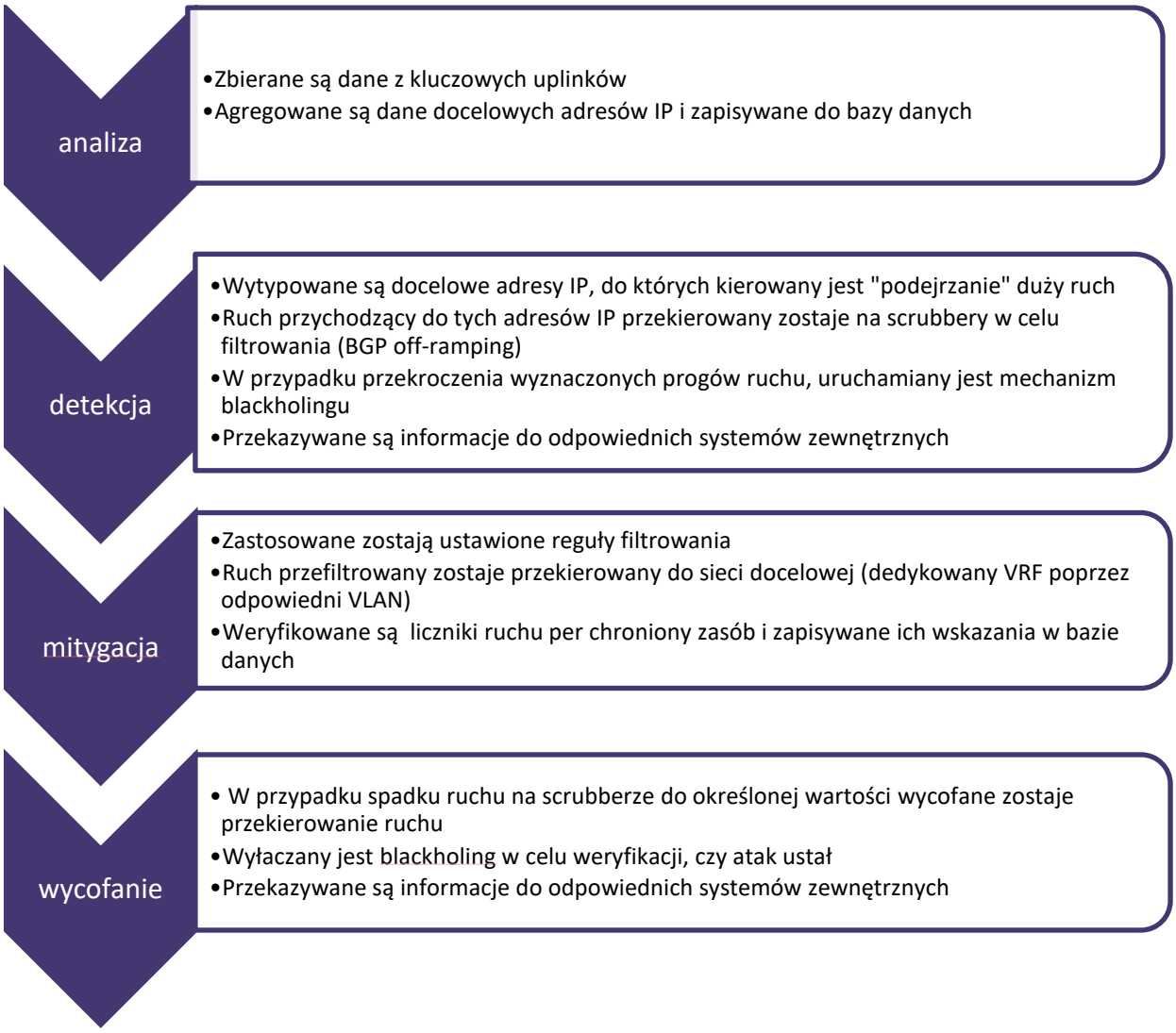


Sposób działania

System Atman AntyDDoS 2.0 analizuje i reaguje na wskaźniki wolumetryczne ruchu, jego działanie natomiast nie obejmuje funkcji spełnianych przez systemy typu IDS/IPS. Ochrona zasobów klienta jest z założenia komplementarna, czyli Atman AntyDDoS zapewnia klientowi pasmo i dostępność infrastruktury, zaś po stronie klienta leży zadbanie o ochronę FW/IDS na wyższych warstwach.

W systemie zostają zdefiniowane pule adresowe, które system ma obserwować. Po przekroczeniu progu alarmowego sygnalizowana jest anomalia.

Standardową reakcją na anomalię jest uruchomienie filtrowania. Wówczas scrubbery wysyłają po BGP do routera szkieletowego Atman prefix /32 z adresem filtrowanego hosta, co powoduje przekierowanie ruchu atakowanego hosta do scrubberów w celu mitygacji ataku DDoS. Ruch odfiltrowany jest odsyłany do klienta jego podstawowym łączem



Podstawowe zalety takiej architektury są następujące:

- adresy niebędące pod atakiem działają nieprzerwanie na łączu podstawowym
- awaria systemu nie wpływa w najmniejszym stopniu na usługę dostępu do Internetu.

Rodzaje mitygowanych ataków DDoS

Wolumetryczne:

- Odbite floods, m.in.:
  - odpowiedzi NTP MONLIST
  - DNS
  - SSDP
  - TFTP
  - SNMP
  - Chargen
  - QOTD
  - RIP
  - Portmapper
  - NetBIOS
  - Sentinel
  - Valve/Steam
  - MSSQL
  - LDAP
- IP fragment flood
  - TCP ACK Flood

Stanowe:

- TCP SYN flood
- TCP RST flood
- TCP FIN flood

Pozostałe:

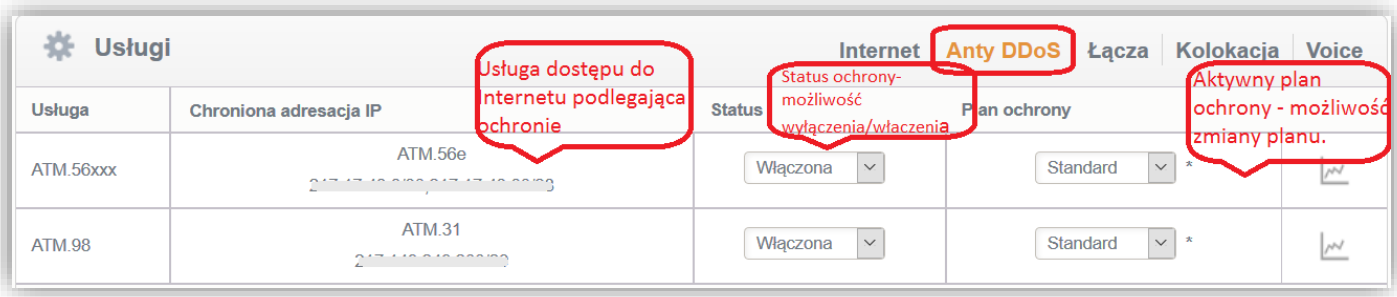
- ICMP flood
- Podejrzane i nieprawidłowe pakiety
- Mieszane

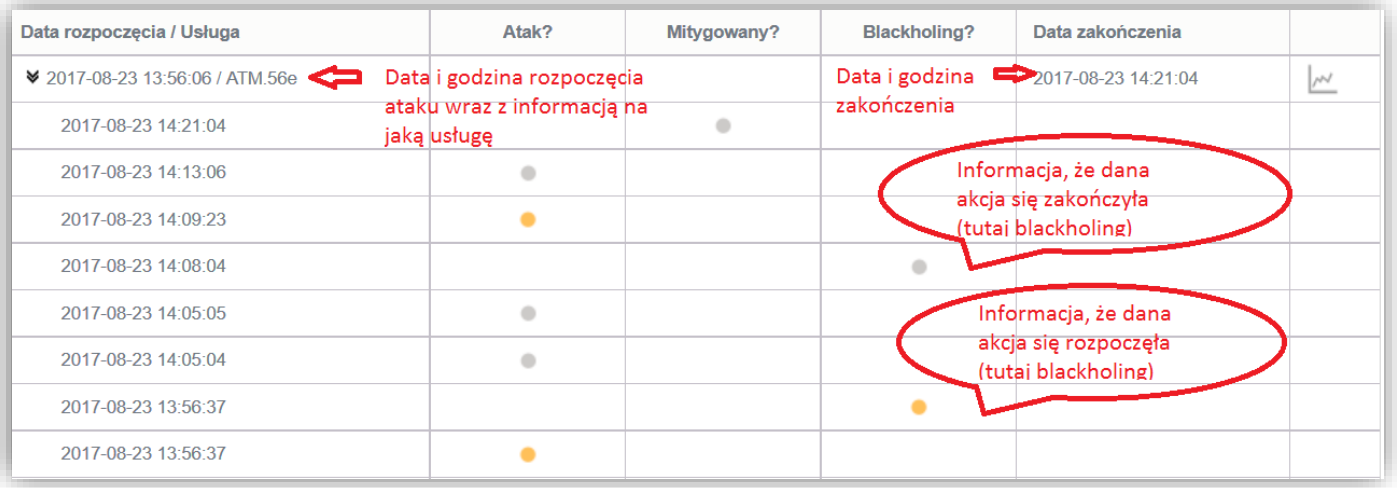
Portal Klienta Atman

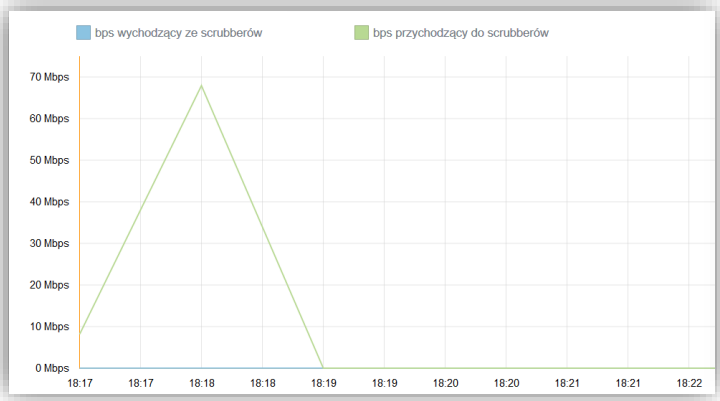
Użytkownik ma możliwość w Portalu Klienta Atman :

- Okresowego wyłączenia ochrony
- Zmiany planu ochrony
- Podglądu statystyk z ataków
- Zdefiniowania adresatów powiadomień email

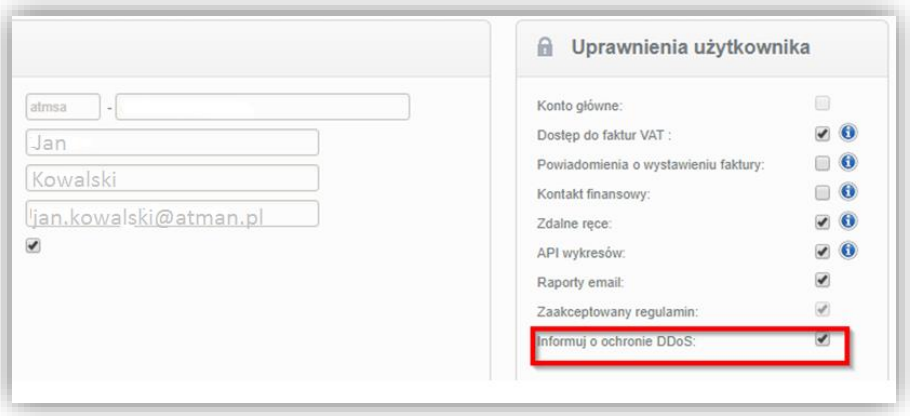
Podstawowe widoki:







Użytkownik posiadający uprawniania administratora ma możliwość zdefiniowania użytkowników, którzy mają otrzymywać powiadomienia email o wystąpieniu czy ustaniu ataku DDoS.



Przykładowa wiadomość e-mail:

Szanowni Państwo,

uprzejmie informujemy, że trwa atak na usługę Test.56e. Ruch został skierowany do centrum oczyszczania.

Mail został wygenerowany automatycznie. Prosimy na niego nie odpowiadać.

Pozdrawiamy

Portal Klienta Atman bok@atman.pl

Plany ochrony

W momencie uruchamiania usługi Atman AntyDDoS 2.0 domyślnie ustawiany jest plan ochrony „Plan Standard". Plany nie są „lepsze" i „gorsze", tylko mniej lub bardziej czułe.

Plan ochrony	Parametry mitygacji	Paramatery blackholowania
Plan Standard	200 Mbps, 100 kpps	5Gbps, 5 Mpps
Plan Pro	500 Mbps, 200 kpps	5Gbps, 5 Mpps
Plan Max	1 Gbps, 500 kpps	10 Gbps, 14 Mpps

Zdefiniowane parametry dotyczą pojedynczego adresu IP a nie całego łącza.

Przekroczenie dowolnego z progów wyzwala akcję:

- scrubbing (przekierowanie i filtrowanie)
- blackholing (także u upstreamów)

Parametry są dobrane pod kątem typowego ruchu, jaki generuje jeden użytkownik, serwer popularnej usługi. Kluczowy jest tutaj parametr pps (pakiety na sekundę), zwykle ignorowany (np. 1Gbit/s to 1.48Mpps w małych pakietach, ale zaledwie 81kpps w pełnowymiarowych pakietach). DDoS może mieć zaledwie kilkaset Mbit/s, ale kilkaset tys. pps SYN Flood , który sparaliżuje łącze.

Zmiana planów w PKA powinna mieć odzwierciedlenie na ustawienie nowych parametrów ochrony w przeciągu 2 minut.

Parametry i ograniczenia usługi

- Usługa dostępu do Internetu, dla której jest uruchamiana usługa Atman AntyDDoS 2.0, musi być świadczona przez Atman
- Ochrona AntyDDoS nie może być uruchomiona dla usługi PWR Thinx (OpenPeering.PL)
- Typ reakcji: automatyczny
- Czas reakcji od wykrycia do mitygacji: maks. 60 sekund
- Liczba analizowanych adresów IP: bez ograniczeń
- Ochrona trwa jeszcze do 10 min po zakończeniu ataku – prewencyjnie. W tym czasie analizowany jest ruch na wejściu scubbera czy czasem atak nie jest ponowiony

Uruchomienie usługi

Typowe uruchomienie do 7 DR.

W celu włączenia usługi klient powinien wskazać okno serwisowe, w trakcie którego inżynierowie Atmana dokonają modyfikacji, na routerze Atmana, usługi dostępu do Internetu objętej ochroną. Po stronie klienta nie jest wymagana żadna zmiana konfiguracji.