Description of Atman AntiDDoS 2.0 service

Basic information

DDoS (Distributed Denial of Service) is an attack carried out simultaneously from many computers (so-called zombies) and infected IoT devices on computer systems of content and Internet service providers. It is impossible for classic security systems to distinguish such attack from the correct inbound traffic from other computers.

Threats

DDoS attacks have been around for a long time, but their form is getting more and more advanced. At present, such attack can be ordered by anyone, because their availability and price are not a barrier. This is one of the most common ways of maliciously blocking websites and web systems.

For an enterprise which provided online services, **business losses related to overloaded servers and access links are not only limited to** the inability to service customers during the attack, but also involve loss of confidence, financial losses and damage to their image or a potential conflict within the organization. Protection against DDoS attacks has become as important as protection of IT resources against hackers and computer viruses.

Security

DDoS attack is specific because it cannot be distinguished from normal traffic by classic security systems. The attack consists in saturating client resources (e.g. Internet links), so, **for security effectiveness purposes, it is critical to recognize and stop an attack at the infrastructure level of a telecommunications operator (e.g. ATM)**, which is capable of accepting and neutralizing an attack that is potentially very dangerous to the end customer.

Therefore, Atman offers a comprehensive solution to protect against known, unknown and evolving volumetric attacks, including DoS and DDoS. Atman's AntiDDoS 2.0 service is characterized by:

- Automatic action and **human factor elimination**
- **Very fast response time** (critical for DDoS attacks) where threat is detected and neutralized in a few seconds.
- **Unbeatable low price.**

ATM S.A.
Grochowska 21a, 04-186 Warszawa, Poland
tel: +48 22 51 56 100, fax: +48 22 51 56 600, info@atman.eu

Technical description of service

Service model

Atman AntiDDoS 2.0 is an additional service that extends the Internet access service. It assumes that the client network is covered with additional inbound traffic monitoring and, if a DDoS attack is detected, it is automatically redirected to nodes filtering DDoS attacks deployed in the Atman's backbone network.

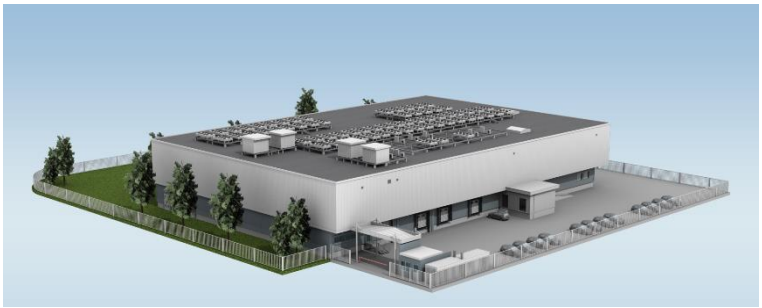
Solution components

The solution is based on hardware components and application. Hardware components include Sensor and Scrubber, which are installed in the Atman Data Center WAW-1 and Atman Data Center WAW-2.

- Sensor - device connected to the Atman's distribution switch. It is designed to analyze in real time the sample traffic through the client's Internet link.
- Scrubber - device connected to the Atman's backbone switch. Scrubbers have a configured BGP session to the backbone router. They are used to redirect traffic to the attacked host, which is then subjected to a cleaning process.
- Software - specialized redGuardian software installed on both Sensor and Scrubber.

Atman WAW-1

Atman WAW-2



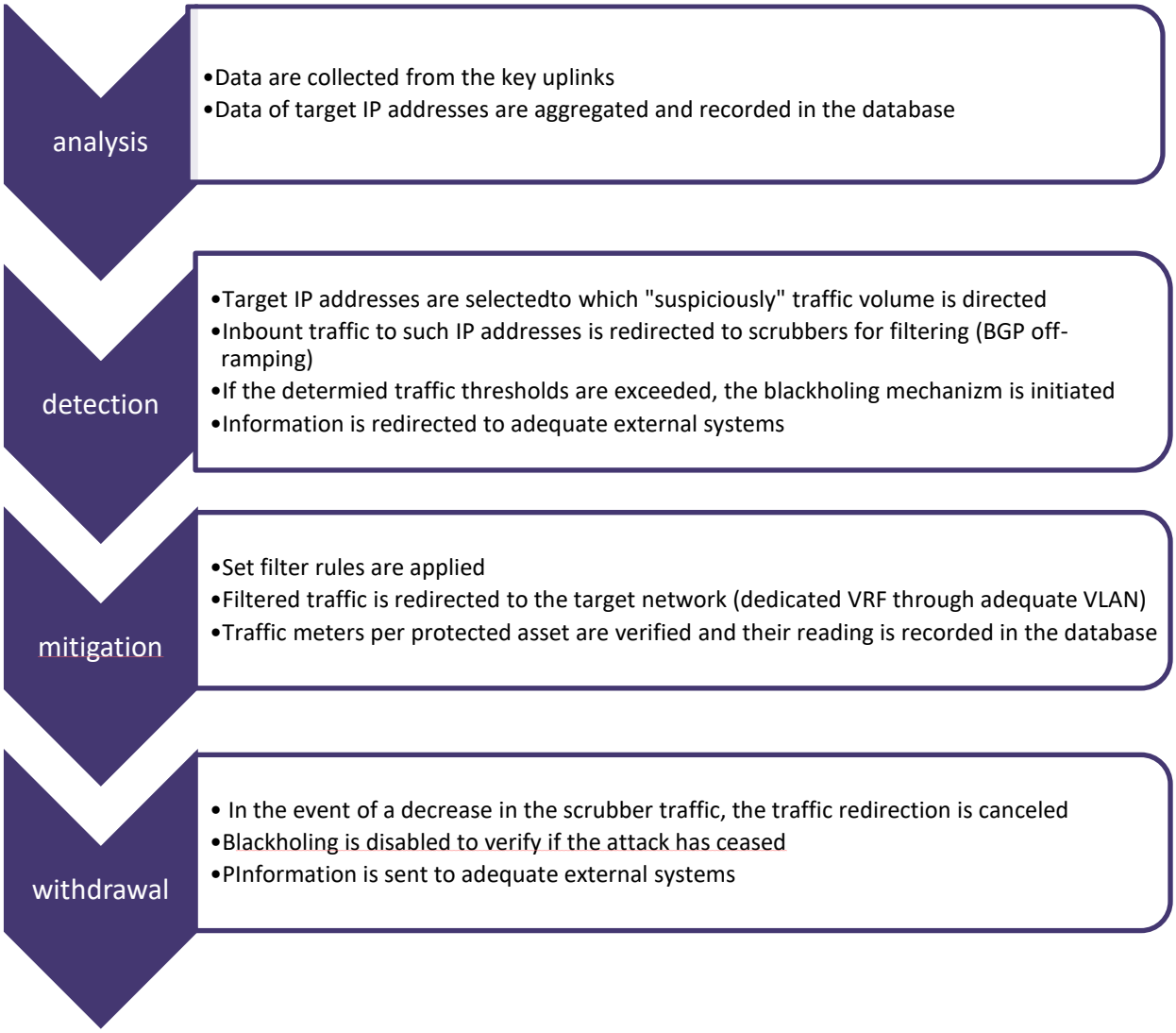
From a customer perspective, the implementation of the service does not involve any changes to its existing infrastructure.

Method of operation

Atman AntiDDoS 2.0 system analyzes and responds to traffic volume indicators, but does not include features met by IDS/IPS systems. Customer resource protection is complementary, in principle, which means that Atman AntiDDoS provides the customer with the bandwidth and availability of the infrastructure, while it is up to the customer to arrange for FW/IDS in the upper layers.

Address pools are identified in the system which are to be observed. When the alarm threshold is exceeded, an anomaly is signaled.

The standard response to the anomaly is to run a filter. Then the scrubbers send for BGP to the Atman prefix/32 backbone router with the filtered host address, which redirects the attacked host to scrubbers to mitigate the DDoS attack. Filtered traffic is sent back to the client by its primary link.



The **main advantages** of this architecture are as follows:

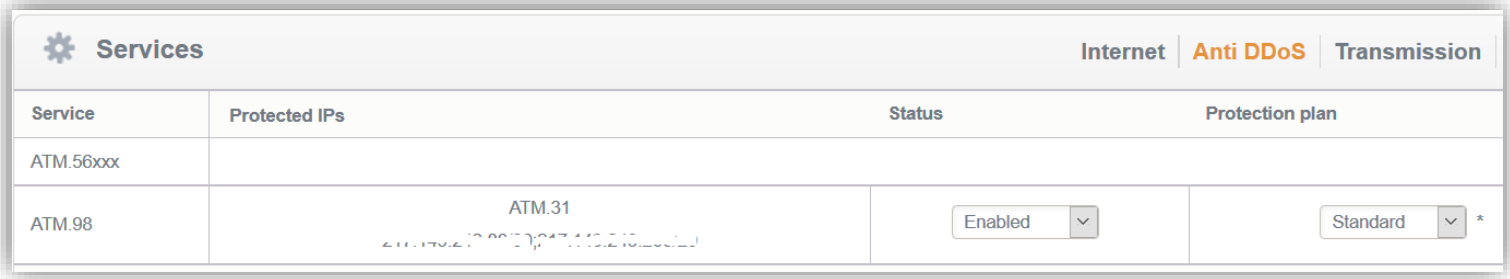
- addresses which are not under attack run continuously on the primary link
- system failure has no impact on the Internet access service whatsoever.

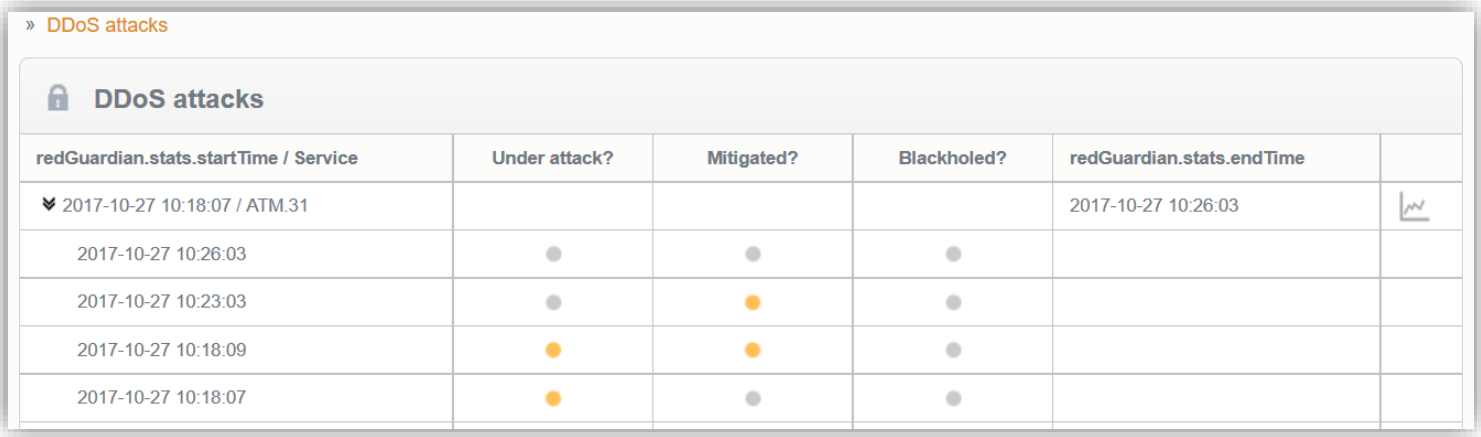
Atman Customer Portal

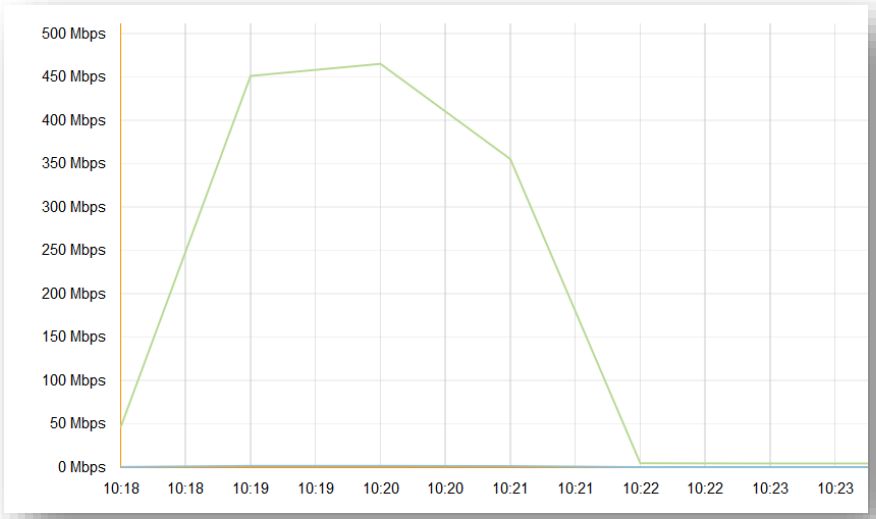
On the Atman Customer Portal the user may:

- Periodically disable protection
- Change the protection plan
- View attack statistics
- Define the addressees of e-mail notifications

Basic views:







A user with administrator privileges may define users who are to receive e-mail notifications of occurrence or discontinuation a DDoS attack.

Sample e-mail massage:

Dear Sirs or Madams,

We kindly inform that an attack on Test.56e is underway. The traffic has been redirected to the cleansing center.

This e-mail has been generated automatically. Do not respond to it.

Kind regards,

bok@atman.pl

Protection plans

At the time of launching Atman AntiDDoS 2.0 service, "Standard Plan" is set by default as the protection plan. The plans are not "better" or "worse", only more or less sensitive.

Protection plan	Mitigation parameters	Blackholing parameters
Standard plan	200 Mbps, 100 kpps	5Gbps, 5 Mpps
Pro Plan	500 Mbps, 200 kpps	5Gbps, 5 Mpps
Max Plan	1 Gbps, 500 kpps	10 Gbps, 14 Mpps

The defined parameters apply to a single IP address and not to the entire link.

If any of the thresholds are exceeded, the following action is triggered:

- ➔ scrubbing (redirection and filtering)
- ➔ blackholing (also upstream)

The parameters are selected for the typical traffic generated by one user, a popular service server. The pps (packets per second) parameter, usually ignored, (e.g. 1Gbit/s is 1.48 Mpps in small packages, but only 81 kpps in full packages) is essential here. DDoS can have only a few hundred Mbit/s, but several hundred thousand of pps SYN Flood, which will paralyze the link.

A change of plans in PKA should be reflected in the setting of new security parameters within 2 minutes.

Service parameters and limitations

- The Internet access service for which Atman AntiDDoS 2.0 service is running must be provided by Atman
- AntiDDoS protection cannot be run for Thinx IX (OpenPeering.PL) service
- Response type: automatic
- Response time from detection to mitigation: max. 60 seconds
- Number of analyzed IP addresses: unlimited
- The protection lasts up to 10 minutes after the end of the attack - preventively. In the meantime, traffic is analyzed at the scrubber entry to check if the attack is not repeated

Service launch

Typical launch up to 7 DR.

To enable the service, the customer should specify a service window when Atman engineers will modify the protected Internet access service on Atman's router. No change of configuration by the customer is required.