Arbor Sightline, Threat Mitigation System (TMS) and Arbor Edge Defense (AED)

How They Work Together

DDoS Threats

DDoS attacks uses different types of vectors and scenarios to affect the targets. For each type there is a solution which the best protects from it. Obviously, all Arbor solution share some characteristics which makes them relevant for DDoS protection, those are stateless built-in process and solution and ATLAS Intelligent feed compatibility. Stateless makes Arbor solution robust to state exhaustion attacks and highly scalable to handle packets received during a volumetric attack. AIF provides signatures and info about latest known attacks and botnets, that keeps the devices' threats data base up to date.

AED: Targeted, L7 and Volume-Limited Attacks

AED (on premises protection device) is enough to handle this kind of attacks and is also the best placed to do so. Since this kind of attacks could be too small to be seen by a protection device placed upstream in the Core network where millions of flows are transiting.

For this kind of attacks, AED will use local settings and ATLAS feeds to detect threats and then to mitigate them (automatically or manually depending on the config).

AED can see every packet entering the site since it sits inline (Arbor recommend installing it between the router and the FW). This full visibility gives the AED more accuracy in analyzing and acting on the traffic.

AED stands synchronized with a "Cloud Signaling" system, that is Sightline. AED can then ask help as follow

- Blacklist/Whitelist any source which is causing threats or is trusted partner
- Ask for mitigation while an attack occurs

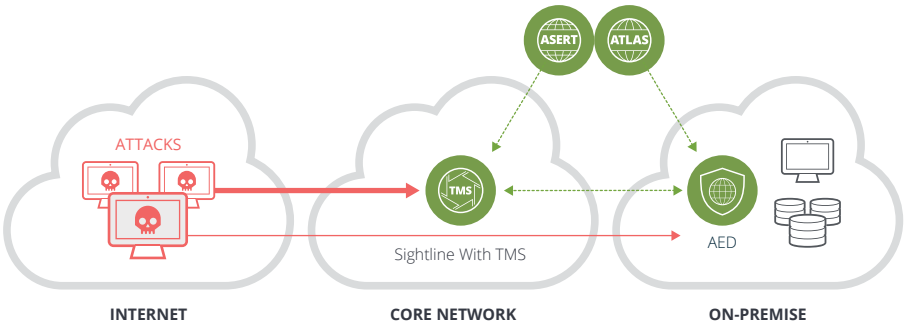
Sightline: Volumetric Attacks

In case of an attack which can saturate the uplink of the final site, Sightline can be alerted thanks to its configuration (ex. IPs to protect) and to AIF, Sightline can analyze inputs received from the network (Netflows, SNMP and GBP data).

Sightline monitors traffic to provide reports and detect threats, it's also synchronized with the AED which sits on site. That's key for the network teams to be aware of the limited/small attacks which can only be seen by an inline device installed in end site, that is AED.

Once an alert is detected or reported by an AED, Sightline will apply the required action (even automatically or upon admin action depending on local configurations and settings):

- Blacklist/Whitelist source/destination detected or reported by AED
- Apply BGPNetflow mitigation on impacted routers
- Blackhole the traffic towards the target
- Launch a TMS mitigation (Threat Management System)



TMS Mitigation

While instructed by Sightline, TMS absorb all traffic towards protected IPs (services, machines, customers...). TMS will then apply countermeasures as configured and according to threats feeds received from AIF.

Traffic re-routing solution is configured in Sightline and should be implemented in the Core routers so once Sightline sends instructions to the routers, those will be able to manage them and carry the traffic according to the global schema (clean/dirty VRF, BGPFLowSpec, DNS redirect, BGP+GRE tunnels...).

The main duty of TMS is to receive traffic, identify legitimate traffic to send it back to the destination, all other packets are discarded. Obviously, TMS, provides data and monitoring information about dropped traffic to Sightline. Graphs are then available in the UI for troubleshooting and reporting.

Protection Actions

- On premises, AED can run mitigation by discarding malicious traffic and deliver legitimate traffic. AED can also request from Sightline/TMS to block the attack upstream in the Core Network. That's very useful in case of volumetric attacks which overcomes uplink capacity.
- In Core Network, Sightline is monitoring the traffic and keeps synchronized with on-premises devices (AED). While a threat is detected or reported, Sightline can
  - Blacklist the source of the attack
  - Apply BGP FlowSpec policy to drop unwanted traffic
  - Blackhole the destination (in some rare and extreme cases, that could be a solution ex. very large volume attack on a non-critical server)
  - Request TMS mitigation to clean the traffic

LEARN MORE

For more information about NETSCOUT solutions visit:

Arbor Sightline
https://www.netscout.com/product/arbor-sightline

Arbor Threat Mitigation System (TMS)
https://www.netscout.com/product/arbor-threat-mitigation-system

Arbor Edge Defense (AED)
https://www.netscout.com/product/netscout-aed

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECJTF_004_EN-2001 06/2020