Arbor Sightline

How It Works and Where It Lives in the Network

The Need for Upstream Mitigation

For an enterprise, inline protection devices can handle successfully most variants of Layer 7 attacks and state exhausting threats as long as they are lower in volume than the internet link size. To deal with volumetric attacks, upstream mitigation, like Arbor Sightline/Arbor Threat Mitigation System (TMS), is generally provided by a Volumetric Scrubbers deployed at appropriate geographic points in the upstream network.

Integrated within Core Network

Arbor Sightline is capable of detecting volumetric attacks, then diverting the attack traffic to one or more volumetric scrubbers. Since this is happening within the core network , in many cases this is transparent to the end-users who is under attack, and the problem is dealt with by the network teams. In a true hybrid setup, there is communication between on premise inline devices and the core, making the sites (or customers) under attack an active participant in the mitigation process. The scrubbing capacity of core network is generally many hundreds of Gb/s making it capable of handling the largest of attacks being levelled at end sites or customers, and/or multiple concurrent attacks against different targets at the same time.

Arbor Sightline helps to manage and secure the network in addition to provide enhanced value-added services to end users and customers. The solution relies, to achieve that, on:

- Detecting and mitigating attacks. The solution provides intelligent mitigation using TMS appliances, Access Control List (ACL) filter generation, Blackhole routing using BGP and Flow Specification (BGP FlowSpec capabilities).
- Providing vision for traffic from across the entire network (routing, transit, partners, customers, and quality of service). Sightline uses flow records, SNMP, and BGP data to build network-wide relational models of traffic.
- Providing a set of managed services which can be valuated and proposed to final customers (DDoS protection, traffic reports, MPLS/VPN visibility and mitigation).
- Monitoring and reporting on network services including VoIP and HTTP.
- Providing a web GUI to facilitate security team day to day mission.
- REST/API modules (webservice and SOAP API) available in the Sightline software.

Data Model and How Does Sightline Work

The solution by analyzing the traffic info (Netflow, BGP and SNMP) will give visibility on routers, interfaces and transported flows.

Users and Managed Objects

To protect/track a customer or a service, a managed object should be created (mainly linked to a set of IPs). Managed objects will then be monitored, and graphs made available.

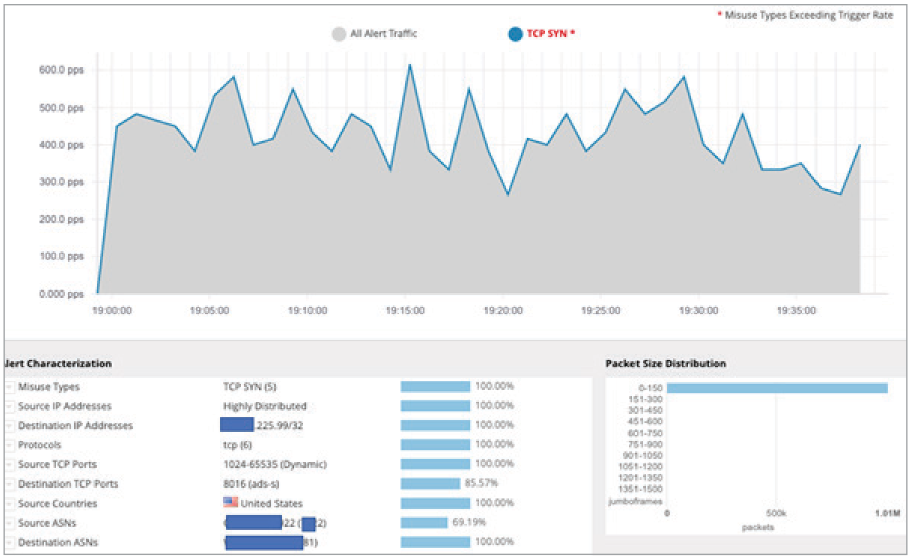
For management and visibility, a user can be created and associated to a particular Managed object. Depending on restriction chosen by the platform administrator while creating the user, following features can be made available: mitigation, created child objects, change settings and access graphs. Each user will only access data and actions associated to designated managed objects, that allows security team to propose a GUI access for visibility and control to final users (or customers), by maintaining confidentiality, security and data consistency.

Alerts and Detection

Once defining the managed objects (customers or services), settings are applied to analyze traffic and then match standard (common to all customers and present in the default config) and customized (bespoke profiles, thresholds and FCAP signatures) threats behavior or signature.

There is also a set of alerts linked to BGP issues (peering instability…), Interface predefined traffic thresholds, state errors (interface status over SNMP, router state, boundary interfaces…).

Traffic alerts reports malicious traffic and thresholds overcoming traffic are displayed by Sightline. To each alert correspond a set of graphs where the threat and packets characteristics are mapped, to define repartitions so Sightline shows at a glance relevant alert info. In the example bellow, a TCP SYN towards a single host on TCP port 8016 is ongoing. The security team can then investigate furthermore and take appropriate actions since they have all relevant info.



lert Characterization

Misuse Types	TCP SYN (5)	100.00%
Source IP Addresses	Highly Distributed	100.00%
Destination IP Addresses	[redacted].225.99/32	100.00%
Protocols	tcp (6)	100.00%
Source TCP Ports	1024-65535 (Dynamic)	100.00%
Destination TCP Ports	8016 (ads-s)	85.57%
Source Countries	United States	100.00%
Source ASNs	[redacted]22 ([redacted]2)	69.19%
Destination ASNs	[redacted]81)	100.00%

Packet Size Distribution

Arbor Sightline is capable of detecting volumetric attacks, then diverting the attack traffic to one or more volumetric scrubbers.

The scrubbing capacity of core network is generally many hundreds of Gb/s making it capable of handling the largest of attacks…

Reports and Graphs

Insight provides a large set of graphs and reports related to traffic and status of peers, customers, services, interfaces, ASN, countries, routers, managed objects, past and ongoing mitigations, TMS, and VPN.

From Netflow, BGP and SNMP collected data, Sightline build graphs for system known items (managed objects, interfaces, routers, peer), those can be pre-configured or automatically discovered by the tool with BGP/ASN analysis for example. Thus, received info (Netflow messages, traps, BGP announces) are analyzed to fill existing entries statistics (managed objects, interfaces…) and then removed. With Insight appliance, information is kept, and graphs can be generated a posteriori i.e. user can create an M-O corresponding to a customer, he will then get access to graphs of the previous days since the FlowSpec info is stored in Insight Database. Another important feature offered by Insight is the possibility to set up multidimensional filters to show graphs, where basic Sightline proposes two fields filtering.

For management and visibility, a user can be created and associated to a particular Managed object.

Detecting and Mitigating DDoS Threats

Sightline solution uses several sources to identify a threat:

- Local predefined and customized filters and thresholds (number of DNS query per source, Packets/Sec on an interface, FCAP filter list, …). DDoS attack monitoring is done per Managed Object (corresponding to a service or a customer).
- ATLAS Intelligent Feeds (AIF) which provides threats signatures (botnets, known attacks and scenarios, application signature …).
- On premises DDoS devices for which Sightline is used as “Cloud Signaling” system from which enterprise protection device (AED) requests help to handle volumetric attacks.

Once detected and according to predefined rules, some actions can be taken automatically and/or manually:

- Blackhole traffic: this is the strictest option and could be useful during very huge attack however clean traffic is also lost.
- Filterlist: from data collected on malicious traffic characteristics sources IPs, Dest IPs, IP header, Ports, Protocol, Checksum, Flags…), filters can be extracted and built to be used on the appropriate interface in order to stop the traffic.
- Apply FlowSpec policy on routers and/or interfaces: From malicious traffic analysis, packets properties can be identified and FlowSpec instructions set up to be applied on the network as upstream as possible (entry peering router, Core router, Concentrator router…).
- Send the total traffic to a mitigation platform such as Arbor Threat Management System, so malicious traffic will be dropped, and clean traffic delivered to the customer. Redirection can be done via simple BGP and GRE tunnels (to avoid loops) or via more elaborated architectures using FlowSPec, durty and clean VRF.

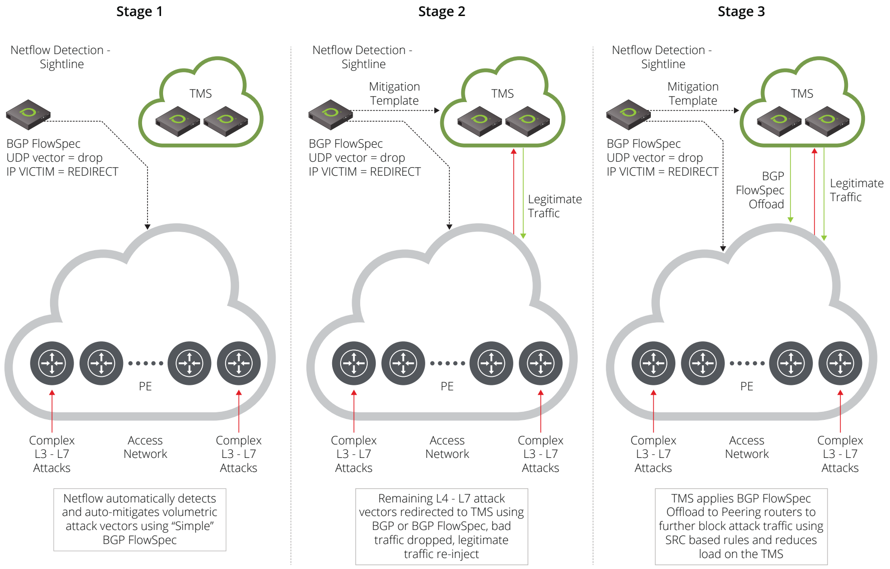
Each user will only access data and actions associated to designated managed objects…

The Role of BGP FlowSpec

BGP Flow spec is key and is used at the different steps of the protection process

1. Attack is detected, FlowSpec is used to block initial volumetric attack vectors.
2. FlowSpec is used to divert the remaining traffic to the TMS for analysis and blocking.
3. TMS, after analysis, uses FlowSpec to push Source based FlowSpec rules to further reduce the load on the TMS.

Traffic alerts reports malicious traffic and thresholds overcoming traffic are displayed by Sightline.



Netflow automatically detects and auto-mitigates volumetric attack vectors using "Simple" BGP FlowSpec

Remaining L4 - L7 attack vectors redirected to TMS using BGP or BGP FlowSpec, bad traffic dropped, legitimate traffic re-inject

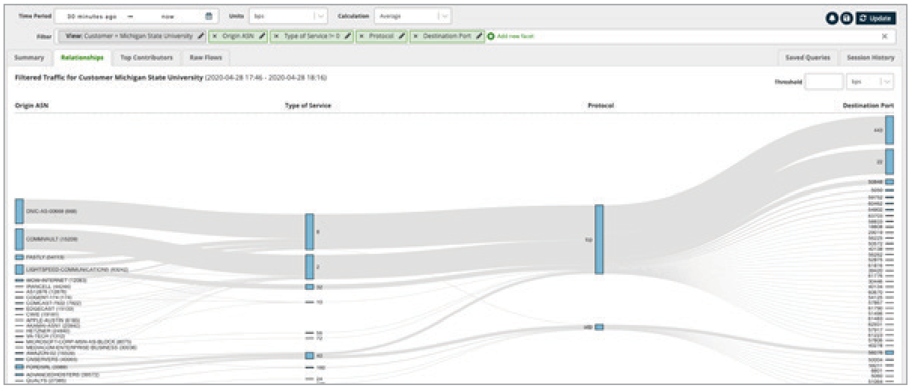
TMS applies BGP FlowSpec Offload to Peering routers to further block attack traffic using SRC based rules and reduces load on the TMS

Attack Forensics

For certain classes of DDoS attacks there might be a need for forensic to catch the attacks characteristics (source/dest, port, mechanisms ...). Arbor solutions can provide data at multiple levels of granularity when it comes to forensics. the first layer of alert details shows only the most important information so that a security operator can quickly interpret the traffic behind the attack. To study the incident in depth, an operator can drill into a second layer of details that specify attack pattern, sources and destinations in aggregated form.

To each alert correspond a set of graphs where the threat and packets characteristics are mapped...

Both of these levels of data provide useful information that network, and security operations can rely upon when reviewing an incident. However, for deeper anomaly analysis Insight can be used. Insight allows flexible requests with as many filters as are needed to isolate the traffic of interest. Below an example of using Arbor Insight database to explore DDoS traffic in a network:



Filtered Traffic for Customer Michigan State University (2020-04-28 17:46 - 2020-04-28 18:16)

Blacklist and Whitelist

Arbor Sightline offers also the possibility to blacklist/whitelist hosts, that could be also based on “on premises” devices analysis and requests. Ex. An AED detects a L7 attacks from HostA (the threat is under the global threshold set up globally). Since sightline is configured to be the Cloud Signaling of the AED, the device can send a blacklist request to Sighline to block hostA upstream. This alert can be transformed by Sighline on a BGPFlowSpec to discard all packets from HostA.

ATLAS Intelligence Feed

AIF contains information about the latest advanced threats, botnets, and web crawlers that our Active Threat Level Analysis System (ATLAS) has identified. Sightline can use this information to detect threats (malformed/invalid DNS or SIP requests, HTTP messages and Botnet packets).

Notifications

E-mails, syslog messages and SNMP traps can be configured to be sent when a configured event happens (bandwidth, system health, Cloud signaling event, protection level, change logs ...).

LEARN MORE

For more information about NETSCOUT Arbor Sightline visit:

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

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