ISP's DDoS Mitigation and Reporting Cuts Costs and Provides Revenue via Managed DDoS Services

The Situation

A large US-based ISP discovered during DDoS events that sometimes very large-volume attacks caused regional outages beyond just the intended victims, as edge and near-edge equipment was overwhelmed. Existing monitoring and reporting tools were focused only on network performance making detection and forensic investigation of DDoS events extremely difficult and time consuming. Often times expensive truck rolls were ordered to inspect equipment before the problem was fully understood and could be alleviated. Additionally, the ISP realized its customers were unable to implement their own DDoS mitigation solutions, due to various limitations including manpower, expertise, and cost. The ISP wanted to protect its own infrastructure and reduce costs such as truck rolls, as well as provide a managed DDoS service for its customers.

The Details

The ISP saw several needs:

- A means of rapid detection to determine the nature and scope of the attack. This would prevent unnecessary or duplicate effort when moving to solve the problem, allow for quicker response, and even automated orchestration of mitigation.
- A way to block attack traffic as rapidly and effectively as possible. This includes traffic at the ISP peering edge utilizing BGP Flowspec, as well as dedicated hardware positioned to remove attack traffic directly at the peering edge minimizing the potential for collateral damage.
- Reporting mechanisms to clearly and distinctly identify the types and volumes of blocked traffic. This aids in rapidly being able to adapt countermeasures to prevent over-blocking of good traffic. It also allows the ISP to be able to accurately report to its commercial DDoS customers the effectiveness of the overall mitigation strategy, regardless of where and how the bad traffic was blocked.

The Solution

Arbor Sightline provides the most comprehensive reporting for network utilization and DDoS protection. Combining Arbor Sightline with Arbor Sightline With Sentinel and Arbor TMS, security operators can detect attacks rapidly, orchestrate mitigation across their networks, and have full visibility into understanding exactly what mitigations are happening, why they're active, and how, with full reporting.

With Arbor Sightline and TMS, the ISP can rapidly detect DDoS attacks and affect mitigation extremely quickly. This resulted in reduced operational overhead, lowered time to resolution, and prevented unnecessary and costly responses such as truck rolls. Additionally, Arbor Sightline with Sentinel provides comprehensive reporting across the entire mitigation response including traffic blocked by the Network with BGP FlowSpec.

With this combination of comprehensive mitigation and reporting, the ISP also began offering DDoS mitigation to their customers as a supplement to their Internet service. With the ISP-provided DDoS mitigation, Customers can now have on-demand or always-on protection as part of their overall Internet service and SLA with the ISP. The ISP utilizing Arbor Sightline With Sentinel is able to generate usage reports outlining all aspects of a DDoS mitigation – both the volume and types of attacks. Customers can now see with full clarity what traffic was dropped, where it was dropped, and why, and the ISP can validate and report on both their own and their customer's usage levels.

CONTACT AN EXPERT ▶

Intelligently orchestrated DDoS attack mitigation and comprehensive reporting cuts costs and produces revenue via managed DDoS protection service.

Intelligently Automated, Best Practice Hybrid DDoS Protection, Backed by Global Visibility and Threat Intelligence

The facts are clear – DDoS attacks continue to rise in size, frequency and complexity. Modern-day DDoS attacks are a dynamic combination of:

1. Volumetric
2. TCP State Exhaustion
3. Application-layer attack vectors

Industry-best practice for DDoS defense is a multi-layer, or hybrid approach that takes into account the different types and targets of DDoS attacks. Just as important, the solution must have an intelligent form of communication between these two layers backed by up-to-date threat intelligence to stop dynamic, multi-vector DDoS attacks.

In-Cloud Protection

Arbor Cloud™ is an ISP agnostic, in-cloud, fully managed DDoS Protection service. Employing 14 scrubbing centers located throughout the US, Europe and Asia, Arbor Cloud provides over 11 Tbps of global mitigation capacity. Enterprises can seamlessly integrate their on-premise Arbor Edge Defense (AED) protection with Arbor Cloud to obtain comprehensive DDoS attack protection. Service Providers can also use Arbor Cloud for extra mitigation capacity and expertise.

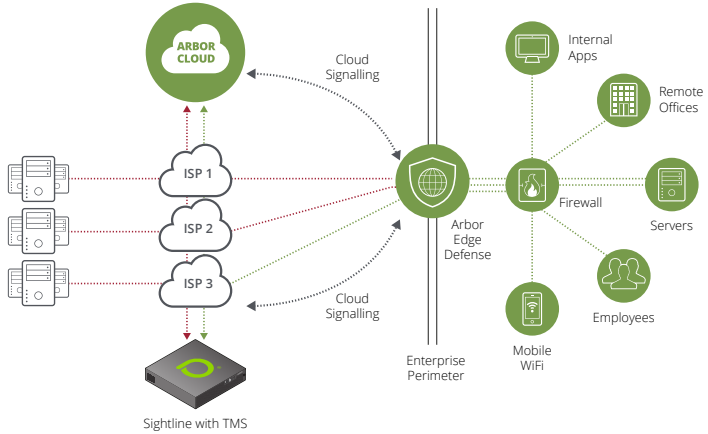
On-Premise Protection

For larger networks and more experienced DDoS attack mitigation teams, Arbor Sightline and Arbor Threat Mitigation System (TMS) provide pervasive network visibility and DDoS attack detection. Upon attack detection, Arbor Sightline can automatically re-route attack traffic to the Arbor TMS for surgical mitigation of all types of DDoS attacks. For smaller networks, Arbor Edge Defense (AED) is an always-on, in-line, DDoS attack detection and mitigation solution which can stop in-bound DDoS attacks. For larger DDoS attacks, AED's Cloud Signaling™ will intelligently link to Arbor Cloud.

Global Visibility and Threat Intelligence

Arbor Security Engineering & Response Team (ASERT) leverages a 20-year, worldwide deployment of Arbor products and third-party intelligence – otherwise known as ATLAS® – to gain unmatched visibility into global threat activity. The global insight derived from ATLAS/ASERT continuously arms all Arbor products and services in the form of features, integrated workflows and the ATLAS Intelligence Feed (AIF).

Arbor Products	
Arbor Cloud DDoS Protection Products and Services	• A fully managed, tightly integrated combination of in-cloud and on-premise DDoS protection. • 24/7 managed DDoS protection with 14 scrubbing centers around the world providing over 11 Tbps of mitigation capacity.
NETSCOUT Arbor Edge Defense	• Always-on, in-line, detection and mitigation of DDoS attacks ranging from sub 100 Mbps to 40 Gbps. • Can stop inbound and outbound DDoS attacks, malware, and C2 communication.
Arbor Sightline & Threat Mitigation System (TMS)	• Arbor Sightline provides pervasive network visibility and DDoS attack detection. • Arbor TMS provides out-of-path, stateless, surgical mitigation at up to 400 Gbps per 2U device.
Arbor Sightline with Sentinel	• Intelligently optimize mitigation based on infrastructure capability to block attacks in the most efficient and scalable way. • Share attack data and request mitigation help from other networks. • Detailed reporting to see exactly what is being dropped, where, and why.



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

SECSS_012_EN-2001 08/2020