NETSCOUT Assists Large Southeast Asian Telecom Company Mitigate Volumetric DDoS Attacks

The Situation

Over the first half of the year, one of the largest Telecommunications and Service Providers in Southeast Asia was experiencing 3 to 5 volumetric DDoS attacks per month. These attacks saturated many of their connections to other ISPs as well as their overseas links to PoPs in other Southeast Asian countries. This problematic assault impacted their entire internet service but was primarily focused on their mobile infrastructure including their NAT IPs. These attacks were affecting many of their customers and the issues were being escalated through to management all the way to the C-Suite. The organization was starting to see some customer churn due to the availability issues and began to look for a solution.

The Details

The operations team worked diligently to solve the problem. As a temporary fix, the provider tried to work with upstream providers to blackhole the malicious traffic. Unfortunately, technical limitations in the network and the nature of the attack made this approach difficult to get in place. The effort took a great deal of time which impacted their customers experience and the internal teams KPIs.

For organizations that have no other means of blocking an attack, blackholing is a widely available option but cannot discriminate any good traffic from the bad. Unfortunately, sophisticated attacks will use varied IP addresses and attack vectors, which limits the effectiveness of blackhole as a mitigation option. Blackhole routing indiscriminately blocks good and bad traffic, so the consequence is that the attacker has essentially accomplished their goal of disrupting traffic to the target network or service. Blackhole routing can still be useful when the target of the attack against an inconsequential part of a larger network. When critical services are in jeopardy, a more surgical mitigation option is needed.

The Results

The organization itself is a long-time user of Arbor Sightline and TMS equipment, but these were not able to prevent upstream links from becoming overwhelmed. BGP blackhole and Flowspec filtering in cooperation with their upstream providers were used to tamp down some of the attack traffic. This improved their situation, but some collateral damage was being seen.

NETSCOUT® recommended a layered defense consisting of their local Sightline and TMS deployment and Arbor Cloud. This hybrid solution provides granular control of the visibility and attack mitigation for local traffic, while also handling the attacks which threaten to overwhelm the capacity of their peering links. With the integration of Arbor Cloud with Sightline and TMS as a layered defense strategy, they now have the ability to mitigate any size of attack and they can confidently provide clean pipe managed services to their enterprise customers.

CONTACT AN EXPERT ▶

Employing a layered DDoS Defense to knock down volumetric DDoS attacks.

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.

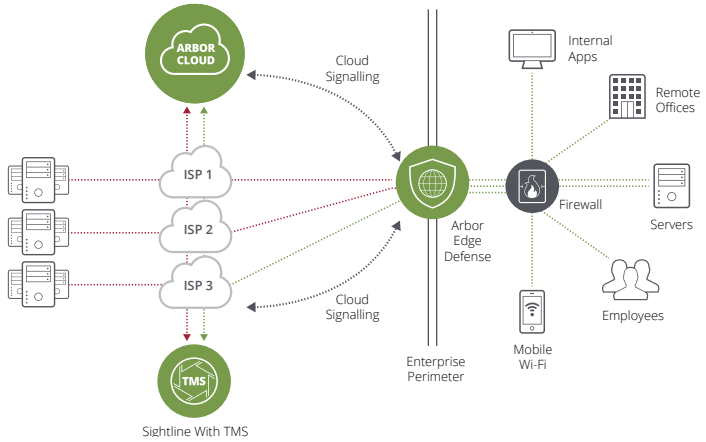
On-Premise Protection

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_013_EN-2001 10/2020