NETSCOUT

The NETSCOUT Team Provides Expertise to Assist Large South American Company Defend Against Overwhelming DDoS Attacks

The Situation

As COVID 19 swept across South America and pressed countries in the region to go into quarantine, many organizations began to acknowledge that there was an uncontrolled increase in DDoS attacks throughout the area. One of the largest companies in the energy sector was finding that their mitigation capacity was consistently being overwhelmed by the attacks and were looking for help to ensure that they could continue to offer availability and services to their internal as well as external customers.

The Details

Due to a strong ongoing relationship, NETSCOUT was asked to come in and assist with the issue. The NETSCOUT team suggested a layered defense strategy augmenting their current mitigation capability by employing Sightline with TMS integrated with Arbor Cloud. This layered defense which is endorsed by a variety of analysts provides granular control of the visibility and mitigation of local traffic, while also handling upstream attacks which threaten to overwhelm both local capacity and peering links. They chose NETSCOUT to assist in this situation primarily due to 3 factors.

- Prior established working relationship between technical resources from both organizations.
- Familiarity with the implementation, configuration and administration of our technology.
- High level of confidence in the value of our global mitigation capacity, our managed services and ASERT team's expertise and our PoP (Point of Presence) in Brazil.

The Solution

After the initial emergency engagement to get the current DDoS Attacks under control by employing Arbor Cloud, the organization moved forward with a purchase of Arbor Cloud to protect their system going forward. The implementation effort and initial recommendations around a layered defense provided by NETSCOUT Resources prompted the organization to look at other NETSCOUT products for following reasons:

- Augment their DDoS mitigation capability to attend to a variety of other potential attacks that could require a hybrid or layered approach to DDoS mitigation.
- Attain visibility into their network traffic for operations and network engineering needs.
- For both of these they looked at and purchased Sightline and TMS (Threat Mitigation System).

Because of an established relationship, the organization's initial instinct was that the NETSCOUT team would be the solution to the ongoing DDoS Attacks. After further inspection through the engagement and exposure to the expertise provided by the NETSCOUT Team, they realized the value the NETSCOUT Team and NETSCOUT products would deliver to their security, operations and engineering teams.

Employing a layered DDoS Defense to knock down overwhelming 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.
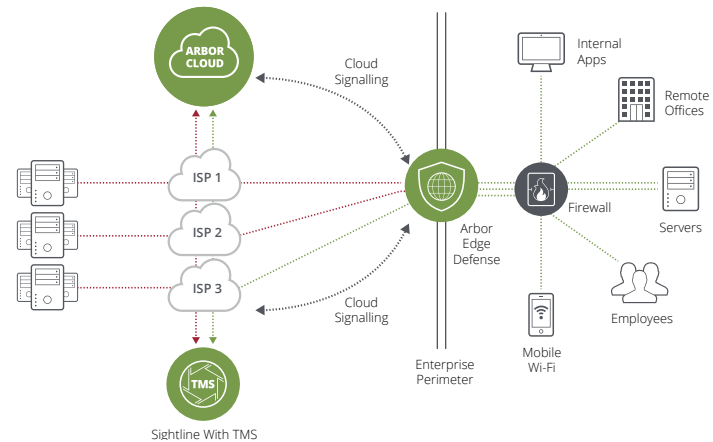
On-Premise Protection

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 inbound 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.