NETSCOUT

International IP Transit Provider Uses Network Visibility to Increase Revenue via Capacity Planning

The Situation

An international IP transit provider, which sells internet connectivity to other ISPs globally by connecting to one or more of their PoPs (Points of Presence), has employed NETSCOUT® Visibility Solutions to execute network analysis for capacity planning and revenue generation.

The key to managing this type of complex and fluid network plus optimize each customer's experience is network planning. Visibility into the network's traffic can provide a variety and multitude of details about their customers' and prospective customers' traffic. This will help to drive new investments, such as additional capacity in existing PoPs, or by adding new ones. From the NetOps Team standpoint, when pressed for economics, it came down to "avoiding waste" or increased efficiencies plus network optimization.

The Details

General network planning without traffic visibility is mostly based on peering negotiations with other IP transit and Tier 1 providers. The lack of detailed visibility into the large amounts of traffic driven by CDNs and OTT providers make those negotiations more challenging, as the parties argue about who's behind those large flows of content and who should pay for transiting it.

A DNS-probe solution would not be feasible and would not scale in their environment due to higher costs.

This provider currently employs the Sightline and TMS for the purpose of traffic analysis and DDoS Mitigation. The primary focus of this organization's strategy is based on bandwidth and capacity provisioning, or more precisely, standing up PoPs, and traffic analysis for Service Assurance.

The TMS capacity is for infrastructure protection and Managed DDoS Protection Services that are now seen as an indispensable part of the company portfolio.

NETSCOUT Visibility solutions help inform the decision to open a new PoP by providing traffic flow matrices between existing and prospect customers and partners to uncover new market opportunities within existing regions or by expanding in new geographies.

They also used the capabilities of our solution to offer customers the ability to capture visibility on their specific network traffic as well as mitigating DDoS attacks. This has become a revenue opportunity for them.

The Results

The benefits were realized in network design and capacity analysis, driven by network visibility and analysis. For example, when they open new PoPs, they can identify potential partners and content providers on this PoP based on traffic.

Other benefits are recognized in customer satisfaction due to fewer support tickets and a decrease in ticket resolution time. In addition, their customers also enjoy add-on services that show them what is happening on their networks, if they are moving a lot of traffic, plus how to avoid service problems and close customer complaints faster.

Network Design and Capacity Analysis Driven by Visibility and Analytics Identify Potential Revenue Opportunities.

SECURITY

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.
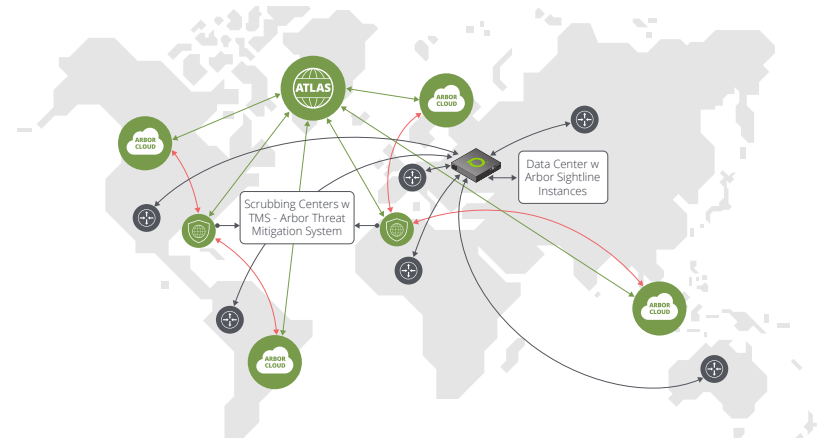
NETSCOUT.

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