

Small Financial Institution Employs Hybrid DDoS Protection Posture to Protect Their Network

OVERVIEW

The Challenge

Financial institution battles Application-Layer and TCP-Flood-DDoS attacks that their service provider's always-on cloud solution could not identify and manage effectively.

The Solution

- Arbor Edge Defense® (AED)
- Arbor Cloud®

The Results

Once the AEDs and Arbor Cloud were implemented, the client experienced a very noticeable drop in the familiar firewall attacks that they had been experiencing throughout the year while using their always-on, cloud-only solution.



Customer Profile

This Regional Financial Institution is a short-term financial solutions company. They employ sophisticated technologies to manage a diverse range of online, mobile and branch-based consumer financial and loan services as well as applications.

The Challenge

The organization embarked on a traffic analysis project with an eye toward understanding malicious traffic that could be traversing their network. Their initial decision was to employ one of our competitors, which specializes in an always-on cloud solution that is provided through a service provider. The always-on cloud solution employs a service assurance solution as the back-end to provide access to scanned traffic. What they found was that the traffic analysis for malicious traffic and identification of volumetric DDoS attacks were sufficient but what they didn't plan on were the other DDoS attack vectors that the cloud solution would have trouble identifying because it is typically designed and configured to trigger mitigation on traffic volume spikes.

The Solution

While discussing service assurance and traffic analysis with the client in an effort to replace the back-end service assurance solution that was feeding the always-on (always-monitoring) DDoS cloud solution, the NETSCOUT® team changed direction by providing an update on the security division of NETSCOUT and what value it provides to our customers plus the value it could bring to them. To begin the DDoS discussion, they led with the question "What are you doing about the other types of DDoS attacks beyond volumetric?" For example, there are at least two other vectors that the cloud solution will not be effective at mitigating with one being low and slow Layer 7 application attacks and the other being attacks that are targeting the TCP

Tables within your stateful devices, such as NGFWs and VPN Concentrators. Both of these attacks may slip by a cloud solution unnoticed because they have a small footprint and will not trigger volumetric alarms. Once the client heard this, they explained that they had been experiencing firewall attacks all year long even after implementing the always-on, cloud only solution. The NETSCOUT team then made a recommendation that the organization review a hybrid approach with AEDs on premise within each data center to protect the edge of the network and stateful devices from low-volume yet effective attacks while collaborating with Arbor Cloud to mitigate the volumetric attacks. This would cover them for complex, multi-vector DDoS attacks.

Summary

This financial vertical has been subject to cyber-attacks via political “hactivism” for many years. The hackers today are becoming more brazen, and the attacks are more complex. Financial institutions need to look at a hybrid approach to stopping DDoS attacks. By employing the NETSCOUT recommended hybrid solution, this financial institution gained the ability to identify and mitigate DDoS attacks at every level in the application stack.

LEARN MORE

For more information about NETSCOUT solutions visit:

<http://www.netscout.com>



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