Going Over The Top

DDoS Protection Assurance with Arbor Cloud for Service Providers

Over-Sizing is So Over

General best practices in early cloud adoption was to ensure that capacity was always available by doubling the capacity needed. This was done for many reasons, but primarily in case a usage spike occurred. This practice ensured that almost all problems could be absorbed. This also helped to ramp up services quickly, so customers received the promise of speed, scale and security. With the exception of transit links, organizations have reduced this double-capacity practice even though demands on cloud environments and bandwidth consumption are growing. The practice of optimizing capacity while managing growth has created operational management conflict.

While some traffic patterns and volume increases are predictable, the underlining fact is that traffic capacities are growing at an accelerated rate. This pattern also applies to attack traffic. Attack traffic, however is less predictable and creates havoc on optimized and restricted network environments. As businesses continue to move to more optimized environments, their capacity buffer has decreased, so volumetric attacks, or large data operations can impact network performance and availability. Consumer demand and consumption is changing, and the market is demanding more flexible options to fall in line with end user requirements. We are moving to an Everything-As-A-Service (EAAS) model. Security will need to be at the forefront of this change in utilization. On demand services are now the norm.

As a Service Provider, you have a good idea of how your traffic is growing, and you continuously expand and optimize your environment to support the demands coming from your customers. But how do you handle those exceptions? How do you mitigate those attacks that mean to clog your infrastructure and block access to your customers data, websites and systems? And how do you manage while ensuring your fully optimized environment does not get overloaded with attack traffic?

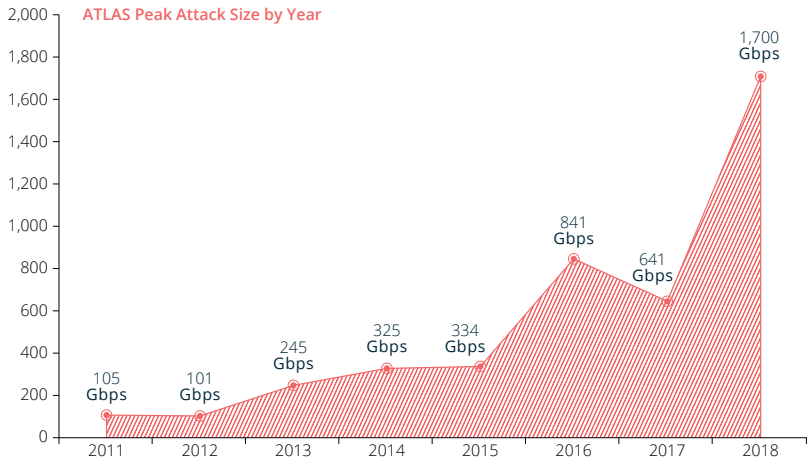

Figure 1: Largest attack size detected, NETSCOUT Arbor ATLAS platform, 2011-2018.

WITH ARBOR CLOUD YOUR ORGANIZATION CAN:

- Ensure only DDoS-free traffic is traversing your core infrastructure;
- Defend your backbone from sustained volumetric attacks;
- Protect your network capacity with budgetary predictability.

Like all other security threats to your business, DDoS attacks are growing in size, frequency and sophistication. Large-scale collateral damage from security breaches continue to be at the forefront of the C suite, especially with new legislation and compliance restrictions. Protecting infrastructure and core clients is becoming a broader problem as organizations migrate to Cloud. Whilst not always prevalent in your network environment, they continue to have an impact on your customers. In fact, the Memcached-driven attacks this year have broken 1 Terabit per second. In March of 2018 NETSCOUT® ATLAS® monitored a sustained attack that reached 1.7Tbps (See Figure 1).

While attacks like the one identified in Figure 1 are rare, their size and sustainability can have long-term implications on business. Building a defense infrastructure to absorb such attacks is not feasible for most companies, so how can you ensure availability without heavy investment? And even if you can absorb large-scale attacks, how quickly can you spin up the needed capacity?

Persistence of Volumetric Attacks

The plain and simple truth regarding volumetric-based DDoS attacks is that they are cheap to launch and sustain. As the cost for bandwidth continues to decline the ability to use sizeable internet traffic to impact large organizations is in the hands of anyone with an internet connection. Couple this easy access to networking capacity with the fact that there are billions of connected devices, and you have the makings of a sizeable botnet army. These factors increase the risk to your customers that large-scale attacks will impact their business, and with respect your core infrastructure. It has become a perfect storm, and shows no signs of stopping with the ever-increasing IOT landscape.

Prepare for the Coming Storm

Unlike the debate on climate change, network-based attacks are 100% manmade, and these attacks are only growing stronger. The investment needed to support these multi-Gbps attacks may be too much to build out, but you cannot expose your customers to any attack. But what if you could ensure that you have the ability to protect your core infrastructure, and your customers connectivity without heavy infrastructure changes or investment?

With Arbor Cloud from NETSCOUT, your organization can realize the benefits of an infrastructure that can absorb volumetric attacks of every size without the need to spin up capacity or involve your core infrastructure in attack defenses.

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

SECSB_012_EN-2001 01/2020