NETSCOUT®

| WHITE PAPER |

Traffic Capacity Management

Defending from DDoS Attacks while Scaling Operations

SECURITY

Supporting growth and demand are sometimes two opposing forces that impact network operations. On one side you have growth from the business which is usually focused on supporting increased utilization, customer growth or some combination of two. On the other side of that spectrum you have increased operational demand from your users and the ever-growing frequency and size of DDoS attacks. Like all risks, you take a measured approach, and based on your business requirements establish a plan that addresses the demands on network capacity while accepting the risks that are associated with your capacity plan.

Predictability in network and cost are two key metrics large organizations spend analyzing and measuring as we all continue into that digital frontier. If we follow the path from device and from user to internet, our reliance on the Service Provider and the ever-expanding peering networks is absolutely critical to get to our final destination. And the demand we all are placing on access to the internet from ISVs and carriers is high.

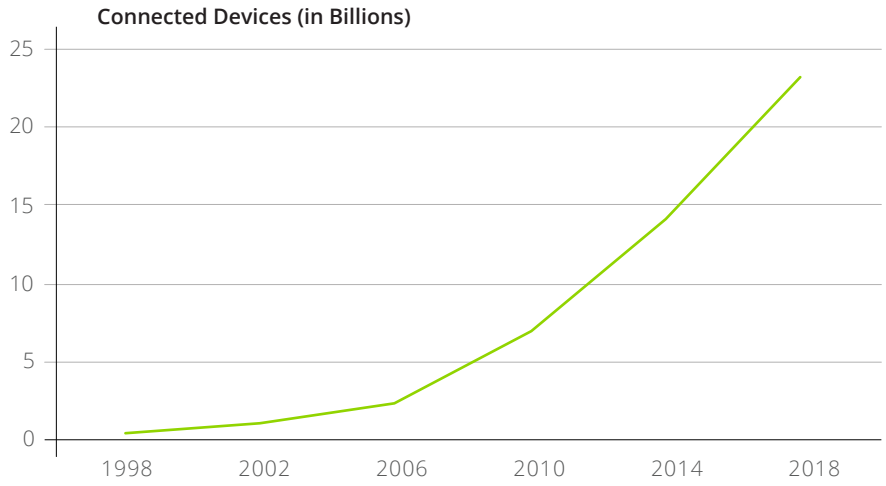

Figure 1: Growth if IoT devices over time.

There have been numerous reports on the increase of data, devices, mobility and internet access, but the most compelling numbers focus on how many connected devices are making it to the market and into users' hands. Figure one shows the proliferation of connected devices (IoT devices) over time, and trends show us that this number has no sign of slowing down. In fact, as more and more users obtain access to the internet – through increased broadband access and increased mobile availability – this number will continue to accelerate. Figure 2 shows the increased availability of internet access through users. It is predicted by the end of 2022, more than 75% of all humans will have access to and use the internet. What these numbers don't tell us is that we continue to increase our dependence on the internet to fulfill our daily activities.

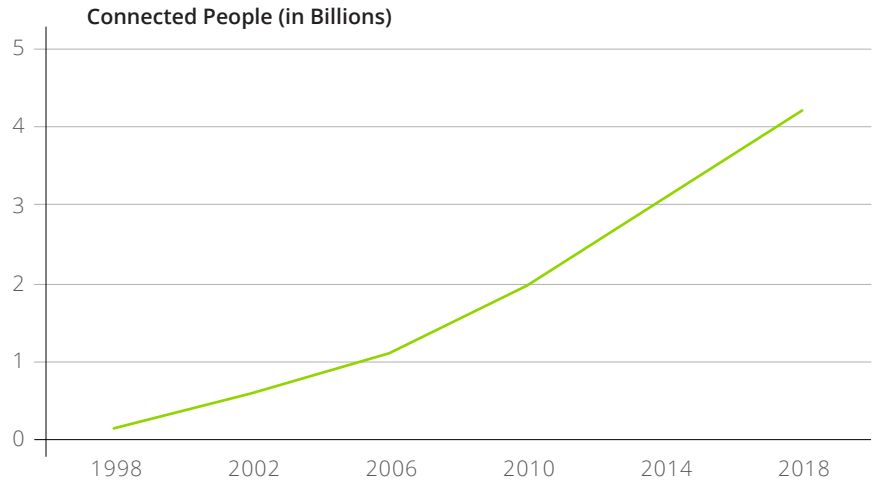

Figure 2: Number of people with Internet access over time.

This creates a landscape ripe for exploiting weaknesses in your defenses. The more we use our connected devices and the more devices we use to stay connected all have an impact on our exposure to threats...which are prevalent today and growing.

Aligning your Capacity Planning Model to Your Attack Exposure

With the accelerating growth in user, device and bandwidth, Service Providers are challenged with predicting their capacity planning for everyday internet access. With growth comes greater risk to core infrastructures and to end users. To be prepared to address the increased risk, Service Providers must have the ability to absorb and defend against threats that consume their customers' access, but more importantly, they need to be able to predict the demands that unwanted traffic places on their backbone and either absorb them or protect their network from these attacks. The first step to predicting this type of demand is through high-level visibility.

Network visibility is key to differentiating network traffic patterns and peering connections. High-fidelity traffic analysis is key to understanding patterns, identifying trends and mitigating threats. This type of visibility can help prevent capacity bloating and ensure that you are not over-investing in your network protection platform. This is key for DDoS protection since building a DDoS defense infrastructure can be quite expensive, complex and underutilized if not combined with effecting traffic visibility and routing analysis.

Managing Mitigation Capacity for Core Networks

Once a capacity management plan has been designed, the next step is to determine the design of the delivery architecture. Depending on preference, budget and overall capacity needed, a DDoS mitigation architecture can be designed to fit any environment using almost any delivery model desired. The key is identifying a vendor that can support the unique needs that your network requires for effective protection and delivery of service:

Hardware Expansion

The tried and true design, the hardware chassis, has been regarded as the premium model. With hardware designed to support unique capabilities, performance is usually unparalleled. Not only is the performance optimized, but the reliability of the service is usually greater than in other delivery models.

Virtualized Expansion

While hardware-hardened designs have some performance advantages, Service Provider infrastructures are often customized and require a combination of designs. With the advances of SDN/NFV, a move towards virtualized networks has evolved many network environments to a point where COTS models and virtual instances of services, such as DDoS protection, are not just desired...but required. This type of expansion can be very cost effective for Service Providers looking to expand protection capacity without heavy physical infrastructure buildout and capital budgeting.

External Cloud-Based Expansion

While building out a DDoS defense architecture is a safe and effective way to protect you and your customers from attack, utilizing a cloud-based service to provide DDoS scrubbing may offer a couple benefits.

Cloud-based services do not usually require a capital investment and can be budgeted differently freeing up capital budget for other strategic initiatives. These types of services can often be brought up quickly and can be effective for massive DDoS attack support. In 2018, NETSCOUT® observed its first 1+Tbps attack. In fact, this sustained attack broke 1.7Tbps. Utilizing a cloud scrubbing service can help support these types of attacks while your own DDoS protection infrastructure can support the majority of other attacks.

Depending on the infrastructure you choose, you may even be able to signal from your environment directly to the cloud services. This could reduce the amount of time it takes to offload a large attack, but since this is using a third-party, some latency would occur. And if you have monetized your cloud scrubbing center by selling it as a service to your customers, this latency could affect SLAs associated with you customer contracts.

Most Service Providers evolve from building out a DDoS Protection infrastructure to support their own core network. Once this model has been proven, they will begin to monetize this investment by offering a scrubbing service to customers. From here, many Service Providers begin to offer their expertise through a managed security service supporting a customer's on-premise device. The service evolution is heavily dependent on having a strong core network that is capable of supporting customer demand.

Partnering with NETSCOUT

In order to right-size your DDoS protection infrastructure and establish an optimized capacity management plan, you need a combination of network visibility and a proven mitigation strategy that can support your network demands today, and address all future increases in attack size, type and duration.

NETSCOUT Arbor Insight provides comprehensive visibility into your core infrastructure and helps optimize your peering environment while helping to uncover network anomalies and identify DDoS attacks. This visibility platform provides network analysis using historical network data and combining it with real threat intelligence from NETSCOUT's ATLAS® network ensuring that you are not only aware of what is happing in your environment but also made aware of trends and threats that are happening around the world that could impact you.

While Arbor Insight offers your network operations the ability to keep your network running with high-efficiency, it can also help redirect the unwanted traffic whether through denying access or by routing it through the NETSCOUT Threat Mitigation System™ infrastructure. NETSCOUT Threat Mitigation System cleans your internet traffic. The Threat Mitigation System was designed for the Service Provider in mind. With it scalable architecture, DDoS Mitigation Capacity is limitless, and with different platform capacities and virtualized instances, a DDoS Scrubbing service can be built using a design as unique as you need it to be.

For those organizations anticipating significant attack sizes, but not a frequency that warrants a capital investment, Arbor Cloud was designed to protect organizations of any size from DDoS attacks of any size. Through the ability of cloud signaling, you can unify a hybrid architecture of on-premise protection with cloud-based scrubbing to optimize both your physical investment and your defense posture. This design has been recognized by analysts and industry experts as the best approach for effective comprehensive DDoS protection. This hybrid approach allows you to design a growth strategy that optimizes your protection needs while providing predictability in your costs (Figure 3).

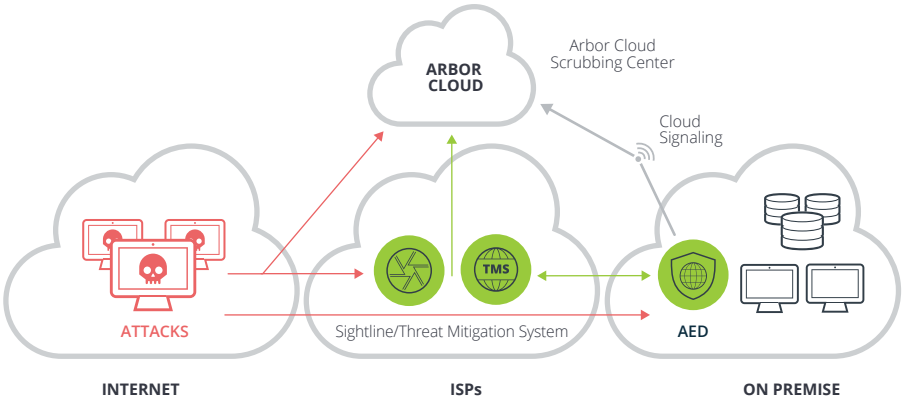

Figure 3: NETSCOUT's hybrid approach to DDoS Protection.

As you continue to invest in building out your core network and the services that come from it, designing a capacity plan that includes DDoS Protection is not only necessary, but make makes sense. While the importance of defending against attack is paramount, the nature of volumetric-based DDoS attacks is to exhaust your network capacity, so creating a DDoS protection infrastructure will help you ensure that the capacity you are building is for clean internet access. Being able to monetize this investment while expanding your footprint with customer through additional managed services is just smart business. Make sure that a DDoS defense strategy is part of your capacity plan.

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

SECWP_010_EN-2202 08/2022