allot
See. Control. Secure.

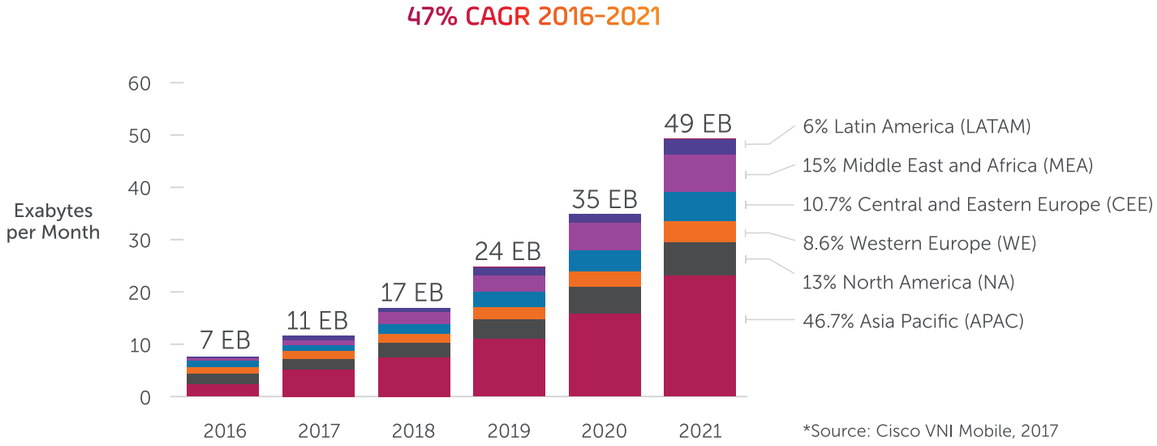
Congestion Management

QoE Assurance through Automated QoS & DDoS Mitigation

INTRODUCTION

It is has become a truism in transportation and data transport: ***If you build it, they will come***. The more roads and highways that get paved, the more cars, buses and trucks clog the byways. In telecom, the more transport that gets deployed and the higher the bandwidth that can be achieved, the bigger the demand for high definition, high speed data traffic.
Service providers learned long ago that simply adding more bandwidth is not a cost-effective solution in the long run. No matter how much bandwidth you provide, today's applications and users will demand more. Furthermore, recurring capacity investments have not been backed by corresponding increases in revenue because ARPU is either stable or even declining in most markets. And looking at the latest Cisco VNI projections, the situation will get worse, around the world, even as 5G is deployed in an attempt to keep up with surging demand. Mobile data traffic will reach the following milestones within the next 5 years:

- Monthly global mobile data traffic will be 49 exabytes by 2021, and annual traffic will exceed half a zettabyte.
- Mobile will represent 20 percent of total IP traffic by 2021.
- The number of mobile-connected devices per capita will reach 1.5 by 2021.



*Source: Cisco VNI Mobile, 2017

The cost to CSPs in CAPEX and OPEX, constitutes **a huge drain on their bottom line**, a problem that is exacerbated by the dropping ARPU rates seen worldwide.
In this reality, the ability to get the most out of already deployed infrastructure has become a critical business challenge. That is why most operators have implemented traffic management and congestion control solutions to optimize bandwidth utilization and network efficiency. But are these solutions optimal?

CONGESTION

Normal congestion refers to the situation where QoE begins to suffer as bandwidth demand outstrips supply. When this happens, users experience slow response time, excessive buffering, erratic video streaming, and other symptoms of poor service.

The traditional approach to this problem is: deploy more transport, upgrade infrastructure technologies, increase BW, attempt to optimize across different technologies etc. Operators also employ traffic management systems that monitor bandwidth and attempt to optimize capacity by rerouting traffic or throttling demand. There are two main problems with this approach. Using bandwidth as the trigger only approximates user Quality of Experience (QoE) and the attempts to remedy (and later restore) the situation may be too early or too late. In addition, throttling demand across the board may not meet Quality of Service (QoS) requirements.

A more optimal approach would be to monitor specific performance attributes that reflect actual QoE, at the correct network elements, per technology; i.e. within a mobile cell, a BRAS interface, DSL interface or a CMTS channel/bonding group. When QoE suffers in conjunction with bandwidth demand, an advanced traffic management solution should automatically adjust the specific bandwidth demands to the current available capacity by re-allocating the bandwidth to applications and users according to the QoS policies that have been configured in the system. Because bandwidth demand is not constant, such a system must "breathe" automatically, incrementally adjusting the demand up and down, in keeping with configured policies, based on ever changing conditions.

MALICIOUS CONGESTION

Unfortunately, the above normal congestion is not the only problem that CSPs face in their struggle to provide consistent and superior QoE. An increasing percentage of available bandwidth is rendered unusable by deliberate volumetric DoS/DDoS attacks carried out in CSP networks, either as a means to attack other targets or as an attack on the CSP infrastructure itself. These attacks are growing in both frequency and size for a number of reasons. One reason is that the explosive proliferation of IoT devices provides hackers with a growing landscape from which to launch these attacks. IoT devices bring lots of value – remote automated metering, security cameras, smart utility grids, etc. However, most IoT devices are essentially stripped-down, single purpose computers with little or no security. They are easily hacked and converted into soldiers in a botnet army, triggering ever growing floods of DDoS attacks. Another reason is that although they are technologically sophisticated, the tools needed to launch these attacks are widely available and easy to use. As highlighted in the recent takedown of a large international service for paid DDoS attacks, there is huge industry of DDoS attack tools for hire. Network capacity continues to grow and will jump significantly with the coming deployment of 5G. This will enable many positive applications but it will also enable even bigger DDoS attacks.

Malicious congestion is obviously worse than ordinary congestion. This kind of congestion is unpredictable, both in timing and in scale. In worst case scenarios it can bring down routers, firewalls and other infrastructure components causing heightened vulnerability and even complete loss of services.

BALANCE OF POWER

CSPs ARE LOSING THE BATTLE

Common attempts to solve these problems are not working and the problem is getting worse. Typically, 15% of a CSPs network suffers from congestion and a great deal of CAPEX and OPEX is allocated in trying to keep up with this congestion by deploying more infrastructure. Clearly it would be much more cost-effective if malicious traffic could be eliminated and normal congestion could be managed in a way that ensures QoS policies are met and QoE impact is minimal. Allot has found at multiple CSP customers that 20 - 30% of network capacity can be freed-up by a holistic solution which combines more optimal traffic management and inline DDoS mitigation. Every CSP must make their own calculation, but our experience shows that Allot's two-pronged approached, detailed below, has a typical ROI of one year.

CONGESTION MANAGEMENT:

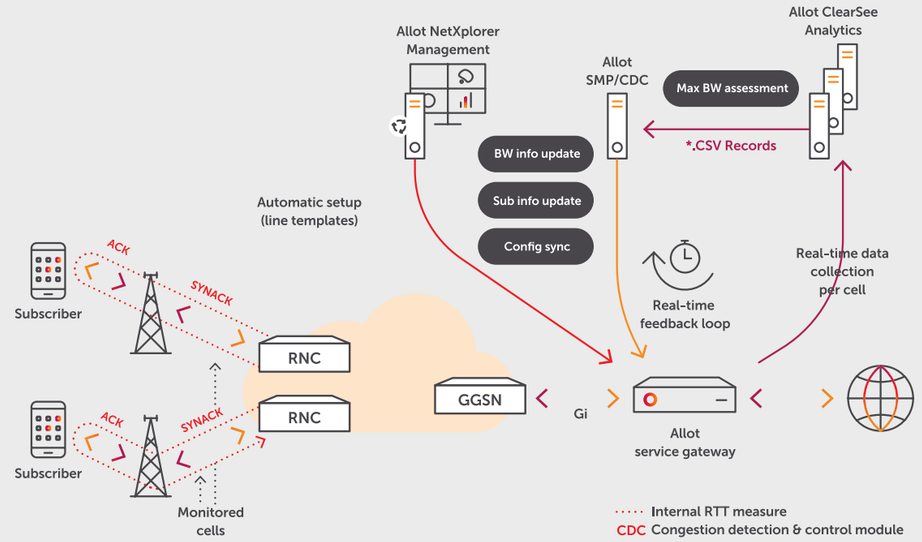
A TWO-PRONGED APPROACH

By combining automated QoE-based congestion management with bidirectional, inline DDoS mitigation, CSPs can save up to 30% of their expansion budget, by better allocating demand and eliminating DDoS traffic, saving or delaying the corresponding portion of their network growth.

QOE-BASED CONGESTION MANAGEMENT

As mentioned above, bandwidth demand and availability are not accurate enough measures of QoE. To know precisely when and where to adjust demand, operators need an automated closed-loop system that measures attributes that more directly correspond to actual end-user QoE. In addition, the differential throttling of user demand must take into account each user-application combination and the relative policy priorities that are configured for each scenario. **Allot QualityProtector does exactly this**. Every second, Allot QualityProtector samples Key Quality Indicators (KQI) to ascertain the QoE being delivered in a given Network Unit. Based on the Network Unit's QoE score, Allot Service Gateway automatically adjusts the bandwidth demand to the current available capacity by re-allocating the bandwidth to applications and users according to the same QoS or service plan policy that the service provider had set in the system. The available bandwidth is assessed based on QoE indicators sampled in real-time every second by Allot Congestion Detection & Control (CDC) technology covering KQIs such as Internal Round Trip Time, Internal TCP Retransmissions and External TCP Retransmissions. Baseline conditions are calculated and then quality is monitored and compared every 15 seconds (by default).

When the calculated congestion crosses a defined threshold a corresponding congestion management policy is triggered. QoE indicators continue to be sampled, providing real-time feedback on how bandwidth adjustments are affecting the QoE level. Fine tuning continues until bandwidth adjustments are sufficient and congestion in the Network Unit is released.



BI-DIRECTIONAL, INLINE DDOS MITIGATION

As mentioned above, DDoS traffic is a growing threat for CSPs. Even when they are not the specific target of the attack, the large volumes of malicious traffic traversing their networks negatively impact the QoS they can deliver to their customers. This uncontrolled and unpredictable "background noise" contributes to network congestion in an ongoing basis. In worst case scenarios, services grind to a halt and/or the CSP is seen as propagating an attack and ends up getting blacklisted by other organizations and suffers tremendously from customer churn.

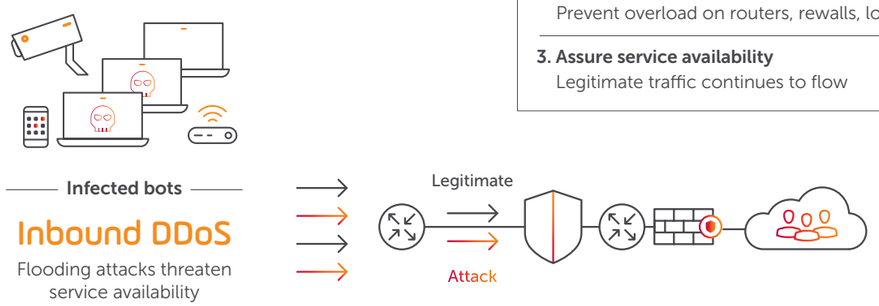
Traditional, high-end scrubbing centers are too costly for most CSPs, have difficulty detecting attacks in asymmetric traffic and tend to miss short-lived flood and low volume attacks since they operate by sampling traffic. Low-end, repurposed enterprise solutions do not scale to meet CSP requirements.

What is needed is a **cost-effective approach to DDoS** that both meets todays challenges and can effortlessly scale to handle tomorrow's larger and unknown attacks, protecting CSP networks and customers, all the time and on time. This new approach, exemplified by Allot's DDoS Secure, runs on the same platform as the QoE-based Congestion Management solution described above. DDoS Secure consists of a highly scalable, inline DDoS mitigation system that stops both inbound and outbound volumetric attacks, uses machine learning to detect previously unknown patterns and is fully integrated with DPI functionality to ensure the quality of legitimate traffic during attacks.

Because DDoS Secure is inline, it is always on and responds in seconds – so there is no latency introduced. Because the solution is integrated with DPI, its application and user awareness ensures policy-based prioritization of critical traffic, even during the largest attacks. Finally, because it uses machine learning to centrally analyze ratios of inbound and outbound traffic, it detects unfamiliar patterns to provide future proof security.

Allot Inbound DDoS Protection

1. **Mitigate attacks in seconds**
   Eliminate congestion on costly transit links
2. **Protect the perimeter**
   Prevent overload on routers, rewalls, load balancers
3. **Assure service availability**
   Legitimate traffic continues to flow



Allot Outbound Bot Containment

1. **Guarantee QoE**
   Prioritize delivery of critical apps during attack
2. **Block botnet traffic**
   Only botnet traffic is blocked while legitimate traffic behind NAT IP flows freely
3. **Isolate the bots**
   Isolate from the network and block attempts to spread infection

CONCLUSION

Congestion is a constant and growing problem for CSPs, necessitating over-provisioning of network resources to meet worst case scenarios. An ideal solution will get rid of spurious congestion caused by malicious traffic and will automatically optimize the reallocation of available bandwidth when genuine congestion occurs – by taking into account the impact on end-user quality of experience and matching available capacity to preconfigured policies for users and their applications. Allot provides both of these integrated solutions on a fully virtualized multi-service gateway that ensures unlimited, elastic scalability and optimal utilization of network resources.

For more information, visit: https://www.allot.com/enterprise