allot
See. Control. Secure.

Fast and Accurate DDoS Mitigation for 5G CSPs

02 November 2020

1 Introduction

An unexpected outcome of the Covid-19 pandemic has been to focus attention on the impact that Distributed Denial of Service (DDoS) attacks have on Communications Service Provider (CSP) networks. Covid-19 lockdowns generated tremendous growth in internet traffic and, unfortunately, explosive growth in DDoS attacks as well. CSPs have experienced more attacks, new attack techniques, and an increase in both attack size and severity. CSPs suffer both as primary targets and as unintended victims when DDoS attacks traverse their networks.

As CSPs build out their 5G networks to enable exciting new services that require orders of magnitude increases in bandwidth and machine-to-machine communications as well as ultra-reliable low latency, it is time to reconsider the kind of DDoS mitigation solution that will best block DDoS attacks aiming to cripple these new services.

A lot has been said about different approaches for mitigating DDoS attacks, but the nature of the data the different approaches use to detect attacks has not received enough attention. DDoS mitigation solutions use network data as their primary source for detecting network-layer attacks. This information is processed by various technologies in order to detect, alert, and mitigate attacks when they occur. This document will focus on the two most common network data sources used by DDoS mitigation solutions, deep packet inspection and flow-based statistical traffic sampling, and will highlight the advantages of deep packet inspection in the context of 5G DDoS challenges.

2 The Pros and Cons of Flow-based DDoS Detection

Network flow statistics are an abundant data source in any CSP network because most routing and switching devices can export some form of NetFlow/sFlow/jFlow/IPFIX.

Using flow information to detect an incoming DDoS attack, therefore, appears to be convenient. However, there are also substantial drawbacks to using NetFlow, which may impact detection speed, accuracy and cost, and should, therefore, be carefully considered.

Flow-based detection solutions are convenient, but reliance on statistics and sampling leave them vulnerable to:

- Small, “under the radar” attacks
- Fragmented “bits and pieces” attacks
- Costly upgrades to processing power

2.1 Every Second Counts

A big factor in flow-based DDoS detection is the speed at which the routers or switches can export their flows. Most devices are configured to export flow records when the flow is 60 seconds old. This represents a full minute of delay before the router starts sending evidence of an ongoing attack. Given the latest trend of pulse attacks (over 50% of attacks), which are characterized by massive, short spikes, this method completely fails. By the time the data arrives at the DDoS detection component and mitigation can be triggered, the pulse may already be over. In other words, the

damage is done before the defense even knows there was an attack to mitigate. While most devices allow setting the flow record export to 15 or even 10 seconds, such frequent exports have an associated cost. When routers export more data for detecting DDoS attacks, more processing power is required, and the solution becomes much less cost effective.

2.2 Aggregation Means Losing Data

NetFlow information is collected in data buckets before it is exported to a DDoS detection system for further analysis. To lower the load on the collection process and avoid bucket overflow, NetFlow-based solutions often aggregate flow data, keeping less data per flow. The aggregation process uses an aggregation key that defines which attributes and statistical counters will be kept in the aggregated data bucket. Naturally, to reduce load, the attributes that are often included in the key are those with low or reasonable diversity. As a result, attacks that require correlation between different flows, which are related to a specific attack, are more difficult to detect through this data. Detection mechanisms that rely on NetFlow information are therefore inherently less sensitive. For large voluminous attacks, this might not be such a big problem. But smaller and stealthier attacks may go undetected or take more time to detect, while still causing significant damage. Hackers have recently adopted a new attack technique called “bits and pieces,” which distributes the attack volume across millions of pieces (10 million) either by targeting multiple IPs, or via multiple fragments. In this way, they evade DDoS detection systems that rely on massive aggregation of flow statistics.

2.3 Sampling Errors May Lead to False Detection

DDoS solutions that use NetFlow statistics as their data source require an integration between the DDoS detection system and the router. Although NetFlow is considered a fairly standard format, there is a data export integration challenge. The DDoS detection component is not typically a big data system and, to overcome limitations in data capacity, NetFlow routers and switches use sampling techniques to reduce the export load. Sampling means that the system does not inspect all the flows, but rather selects a smaller portion of the flows for statistical collection and then normalizes the numbers to represent the entire network. When sampling 1:10,000 flows (a commonly used sample rate), the extrapolation can introduce significant errors because normalized statistics may not accurately represent the actual network traffic. As a result, a bigger deviation from normal traffic is needed to confidently determine that a DDoS attack is happening. This, of course, means that smaller (yet still large) attacks might be missed. Conversely, inline DDoS protection solutions, which use DPI to inspect all packets, include a detection component that is specially designed to handle the large amounts of data extracted from the network without sampling, and therefore can use more accurate thresholds that do not miss smaller attacks. In addition, because the various solution components (data collection, detection, and mitigation) are all delivered by the same vendor, no integration is required, thereby relieving the CSP from an unnecessary headache.

3 The Advantages of DPI-based DDoS Detection

DPI-based detection, as its name implies, requires an inline deep packet inspection element to be deployed at the CSP. This element is capable of obtaining complete traffic captures, including both headers and payload, without aggregation or sampling. The DPI devices are typically high-speed elements that do not introduce any latency to the network (microsecond scale). The granular data they inspect not only help to detect attacks, but also serve a variety of important network performance and security services. CSP requirements, especially those related to 5G eMBB, mMTC and URLCC, highlight some of the advantages of this method of detection over others.

Inline DPI rapidly inspects every packet, in both directions, and:

- Avoids sampling and statistics-driven errors
- Detects & mitigates every attack, rapidly and accurately
- Captures traffic data for forensics

3.1 Granularity Increases Speed and Confidence

While conventional flow tools instantly lose granularity as they create their minute-by-minute (or even 5-minute-by-5-minute) data flow buckets, DPI-based collection does this differently. The detailed network data is stored on the DPI sensor, and the detection system extracts the required amount dynamically, without losing granularity. A DPI-based inline solution also uses a high-scale, machine learning-based detector, designed to handle the large amount of information. This means the detection is much faster and more accurate, with higher confidence in mitigation triggering.

3.2 Surgical Filtering and Quality Forensics

Granular and detailed information is especially important for the DDoS mitigation process. In the mitigation process, mitigation patterns are formed by dynamically filtering out attack traffic while clean traffic of legitimate customers goes through, unimpeded. The more detailed the data, the more precise the mitigation, enabling surgical removal of attack traffic without false positive errors that can harm customers. The deep inspection of traffic not only improves the mitigation accuracy, but also delivers quality forensics, which the CSP can use to strengthen defenses, either in real-time during attacks, or through post-attack analysis.

3.3 Not All Attacks are Created Equal

Not all DDoS attacks are equally easy to pick up. Large volumetric attacks, such as SYN floods, UDP floods, and reflection attacks, are more straightforward because they are very “loud” and intense in their nature. Some attacks are designed to evade systems or travel “under the radar” using techniques such as short spikes, fragmentation, distribution to many targets, small volume with high bitrates, etc. Such attacks often require more detailed network data for rapid, accurate detection. For example, a fragmented DDoS attack will require the IP fragment bit information, which is often excluded from the NetFlow router’s aggregation key in an effort to reduce the amount of data. Attacks that fall “under the radar” cannot be detected automatically and require human

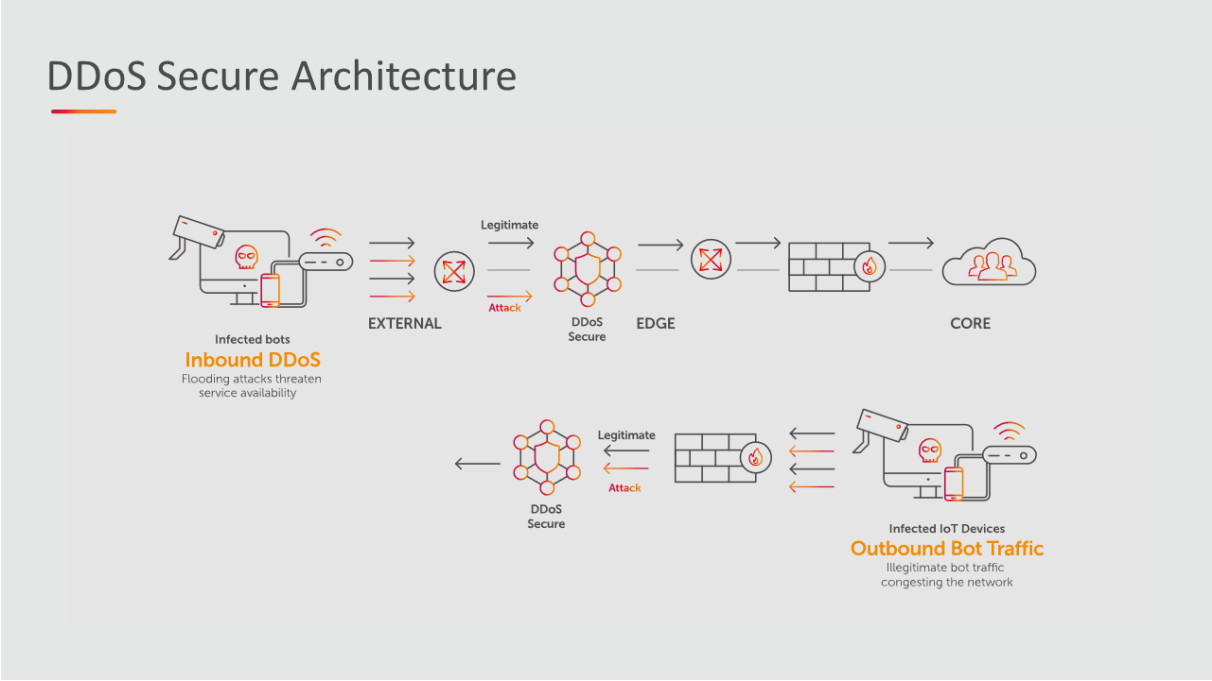
intervention in order to generate the right countermeasure. This involves hidden costs of both time and money. However, DPI-based DDoS mitigation systems extract all information by default and will, therefore, successfully detect and mitigate these otherwise “under the radar” attacks automatically and in real time.

3.4 DPI Systems are Much More than Just Collectors

DPI solutions were originally designed to efficiently manage subscriber traffic with capabilities such as congestion management, application awareness, rate limiting, and advanced filtering at wire speed, without introducing any latency. Such capabilities, combined with the fact they are already deployed inline, make them a quality data source for detecting attacks, as well as an ideal mitigation system. Indeed, there are inline DDoS mitigation solutions that utilize the DPI collectors for implementing the mitigation policy. The additional congestion management and application awareness complement DDoS mitigation in a synergic manner, as they assure subscriber quality of experience (QoE) during attacks, when QoE is at highest risk. DPI-based DDoS solutions also possess many of the functions of traditional and next generation firewalls, such as stateful packet filtering, network-layer access control, application control, anti-malware, IP reputation blacklisting, and web content filtering. Having these functions included in the DPI DDoS protection platform saves on costs, and completely removes the need to deploy a separate inline firewall function in the network, relieving the CSP from another set of problems.

3.5 Pre-emptive Protection of Valuable Assets

Critical network elements, such as DNS servers and firewalls, are ideal targets for DDoS attacks. If they fall or fail, the impact on the entire network is significant. DPI inline solutions can provide pre-emptive protection for these critical elements, minimizing the potential damage of a DDoS attack by enforcing rate-limits on the traffic to such elements and enforcing acceptable usage policies. As a result, such elements will not receive more traffic than they can handle. Inline DPI solutions also monitor individual subscriber and IoT activity. This enables them to detect and block malicious bot activity such as port scans, brute force login to vulnerable devices, malware download, and command & control communications. This capability preempts in-network attacks before they occur, preventing any damage to the CSPs’ two most valuable assets: their reputation, and their customers’ QoE.



The Allot inline, DPI-based, DDoS mitigation solution

4 Summary

The DDoS threat landscape continues to worsen, and attackers are discovering gaps in traditional defenses. Service providers must ensure their network infrastructure is not disabled during DDoS attacks and that the DDoS protection solution does not impact subscriber QoE – an especially challenging goal in 5G networks.

DDoS protection solutions that employ DPI as their source of data can detect any attack on the CSP network, big or small, and automatically mitigate it quickly, without over-blocking legitimate user traffic or introducing any delay that can threaten the 5G experience. Inline DPI collectors, which enable DDoS mitigation and incorporate application and session awareness as well as traffic shaping capabilities, enable proactive protection of critical network infrastructure elements and eliminate network congestion, assuring a high customer QoE at all times.

5G service providers are best served by DPI-based DDoS mitigation solutions that offer rapid detection and mitigation times along with advanced protection, scalability, and performance.