allot
See. Control. Secure.

Allot DDoS Position Paper

Beat DDoS Attacks on 5G with Inline DPI/Next Gen Firewall

April 2022

Contents

5G Networks Demand Comprehensive Security and QoE Assurance

5G is a technological revolution. Unlike the transition from 3G to 4G, which was an evolutionary change – slightly bigger pipes, slightly faster data speeds – 4G to 5G is a whole new ballgame. From distributed architecture, through multi-access edge computing sites (MECs) to cloud native deployments, 5G is much more than 4G on steroids. Massive broadband, ultra-low latency, and millions of IoT devices are truly a quantum leap. New services and applications, like AR/VR-powered gaming and autonomous vehicles, that take advantage of these characteristics are certain to surprise and delight.

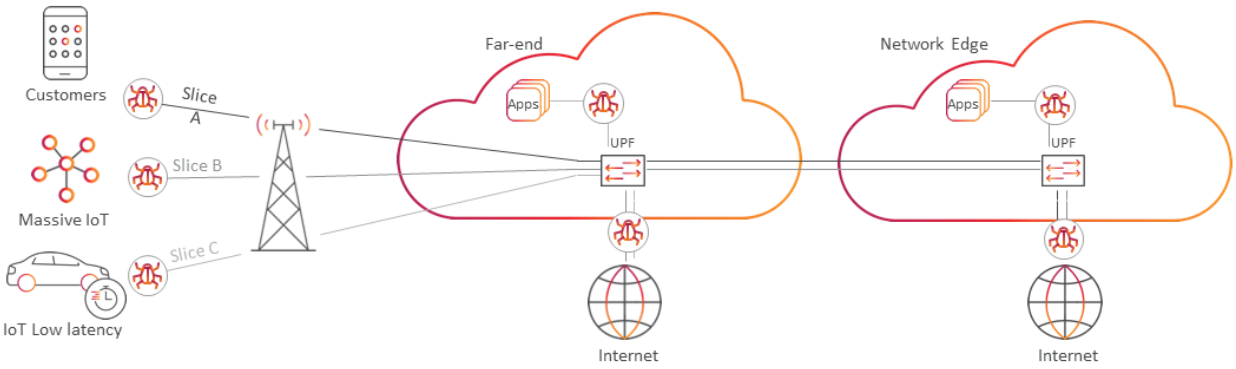
To meet the hype-driven expectations, 5G networks must be protected against service-impacting attacks, which decrease bandwidth, add latency, and cripple performance. Why is this a problem, and how can communication service providers best protect their new 5G networks?

The 5G Security Challenge

As explained in a recent IDC Technology Spotlight whitepaper,

> "The 5G/MEC/IoT architecture, now tasked with meeting these customer expectations, has the potential of exposing a communications SP's network to a growing security attack surface. Little industry attention has been given to identifying and eliminating risk vulnerabilities in this new environment."

The following diagram makes this clear.



5G Architectural Vulnerabilities

5G networks have many more points of attack. The 10s, 100s or even thousands of MECs that are needed to provide local breakout points in support of ultra-reliable low latency services (URLLC) are potential attack entry points, which can easily be taken out of service by even low-volume attacks. What you don't see in this diagram is the expected millions of IoT devices that are another great benefit planned for 5G. Massive

Machine Type Communications will enable a range of exciting services such as smart cities, smart cars, smart energy, smart health, and more. But IoT devices are overwhelmingly poorly secured, single-function devices. They can be easily taken over by threat actors to form massive DDoS attacks from both inside and outside the network that can utilize their enhanced mobile broadband (eMBB) to ruin the ability of 5G to deliver on its promise.

LIMITATIONS OF TRADITIONAL DDOS MITIGATION APPROACHES

DDoS mitigation solutions use network data as their primary source for detecting network-layer attacks. This information is processed by various technologies to detect, alert, and mitigate attacks when they occur. The two most common network data sources used by DDoS mitigation solutions are deep packet inspection and flow-based statistical traffic sampling. It is our position that, especially in the context of 5G DDoS challenges, inline deep packet inspection is far superior.

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. 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, and the damage done. In 5G networks where URLLC is expected to be a significant use case and source of revenue, these short attacks can introduce enough latency to degrade these services. Although 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.

NetFlow systems also aggregate their data samples before exporting them. Aggregation means a loss of data specificity, so attacks that require correlation between different flows, which are related to a specific attack, are more difficult to detect through this data. Finally, to reduce the data export load, NetFlow systems typically sample data rather than checking all of it. 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.

The Advantages of DPI-based DDoS Mitigation

DPI-based detection, as its name implies, requires an inline deep packet inspection element to be deployed with 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 significant 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. Allot's DPI-based inline solution uses a high-scale, machine learning-based detector, designed to handle large amount of information. This means the detection is much faster and more accurate, with higher confidence in triggering mitigation.

NetFlow mitigation systems, on the other hand, typically reroute the traffic that contains suspected attack data to a scrubbing center where the data is examined in detail, "scrubbed," and then the clean data is routed back to the network. By definition, this process introduces latency, in addition to routing costs.

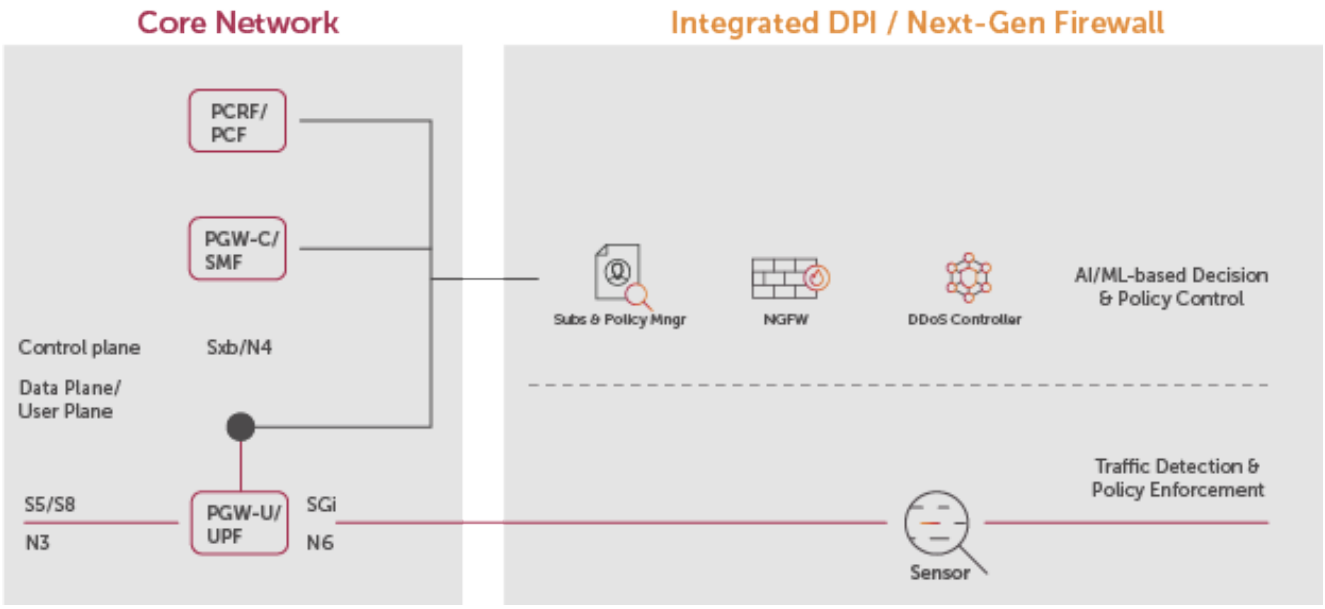
Inline mitigation dynamically filters out attack traffic while clean traffic of legitimate customers goes through, unimpeded, without the latency costs associated with scrubbing centers. Inline DPI mitigation collects granular and detailed information. The more detailed the data, the more precise the 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.

Combining DPI-based DDoS Mitigation with Next Generation Firewalls

Despite the best-in-class protection of DPI-based anti-DDoS solutions, one cannot completely discount the increase in end-to-end latency due to its in-line deployment. Although this was negligible in previous network generations, it can become significant in 5G, where even fractions of milliseconds can impact latency-sensitive use cases.

However, firewalls are another security solution that are deployed inline in 5G networks, on the user data path, to prevent unauthorized access to network resources and prevent traffic to/from compromised sites and domains. As an inline node, firewalls already increase latency.

An integrated firewall/DPI solution could separate the traffic monitoring and threat detection functions and process them in parallel. This would significantly reduce the inserted latency. This one-pass approach enables additional functional expansion, for example to prioritize specific traffic threads, with no risk of additional latency – preserving one of the major KPIs in 5G networks.



THE DPI-BASED DDOS DETECTION, ADDED VALUE BONUS

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, Allot's inline DDoS mitigation solutions utilize DPI collectors for implementing the mitigation policy.

The additional capabilities of 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 threatened most.

CONCLUSION

Given the constantly changing attack surface - featuring multi-vector attacks, zero-day attacks, growing volumes of malicious traffic, and increased numbers of cyber incidents - a combined firewall and DPI-based DDoS solution is the only future-proof approach that efficiently protects CSP network services without increasing latency.

Such a solution provides comprehensive protection from both inbound and outbound attacks, as well as the advanced traffic management and application detection capabilities to protect the performance of mission critical applications during cyberattacks.

Finally, unifying user interfaces and shared functionality enable the overall reduction of TCO for the combined, comprehensive solution.