An Elastic and Adaptive Anti-DDoS Architecture Based on Big Data Analysis and SDN for Operators

Liang Xia Frank.xialiang@huawei.com Tianfu Fu Futianfu@huawei.com
Cheng He hecheng@huawei.com Tobias Gondrom tobias.gondrom@gondrom.org
Danping He ana.hedanping@huawei.com

Abstract

This article analyzes the new challenges today's DDoS attacks pose to operators and enterprises and proposes a new innovative elastic and adaptive Anti-DDoS architecture to identify attacks early, adapt to them and mitigate them. It focuses on several key points, especially for large network operators: security extension of IP packet sampling, performance and adaptability, automation and operational involvement and business benefits. Based on this analysis, we propose an elastic and adaptive Anti-DDoS architecture. This architecture leverages big data analysis and Software Defined Networks (SDN) for operators. We explore these innovative technologies and how they can be integrated into a modern comprehensive Anti-DDoS solution architecture to achieve great new benefits and opportunities.

1 New Challenges of Today's DDoS Attacks

Distributed Denial of Service (DDoS) attacks have been widely acknowledged as the most serious types of attacks to operators and enterprises due to the serious risks they pose to the availability of networks, services and applications. Over the last few years, DDoS attack vectors have dramatically evolved to a new stage, with the potential to now seriously threaten the business operation of many large organizations.

First, new and more and more powerful attacks are becoming possible due to advanced attack reflective techniques combined with attackers controlling massive-sized and growing botnets at their disposal. With the widespread use of DNS/NTP/SDDP/SNMP reflective amplification attack technologies, the traditional volumetric flood attack can grow in size to dozens or even hundreds of Gbps. This large scale attack traffic can easily saturate the network bandwidth and bring even large scale target systems to their knees. In such cases, the network operators are most suited to combat the attack, as on-premise enterprise security devices can often not handle such massive amounts of traffic. In the past, the attacks could be detected and mitigated by specialized (high performance and expensive) Anti-DDoS devices deployed at critical locations. However, as DDoS attack traffics grow rapidly, the specialized Anti-DDoS devices may be easily overwhelmed and will be unable to handle volumetric flood attack effectively.

Second, specific DDoS attack techniques are also evolving dramatically, becoming much more intelligent and sophisticated. In addition to the existing wide variety of DDoS attacks in Layer 3-7, new attacks emerge very quickly. And often the specific attack may even adapt to deployed defense strategies within minutes while the attack is still ongoing. Furthermore, application-level DDoS attacks have the common "low-and-slow" characteristic, which can make their proper detection more difficult. The traditional signature-based detection method must evolve to a comprehensive method consisting of signature, behavior analysis, flow pattern identification and more.

Third, more and more DDoS attacks camouflage themselves and make it difficult to mitigate them, using spoofed addresses and distributed attack sources and traffic. This change requires that the Anti-DDoS solution involves more network devices in its defense strategy, especially devices connected closest to the attack sources to mitigate the attack traffic, which can make counter-measures more effective compared to if only conducted by a specialized security devices.

Traditional Anti-DDoS defense approaches deploy specialized detecting devices at important locations in the network to inspect all traffic through them, and then divert malicious traffic to clean pipe devices for filtering and returning back clean traffic. Due to the dramatic evolution of DDoS attacks in size and sophistication, traditional methods reach their limits and severe challenges with regards to cost, elasticity, detection precision and adaptability. Thus additional comprehensive network scale Anti-DDoS solutions should be provided to overcome today's Anti-DDoS functions provided by isolated and rigid individual devices.

2 Requirements for Operations

Analyzing a multitude of real-world deployments by network operators, we find several points that need to be considered when deploying Anti-DDoS solutions for their network infrastructure.

These can be categorized into the following sections:

2.1 Security Extension of IP Packet Sampling

Current IP packet sampling methods (i.e., netflow, ipfix, etc) have the following limitations:

1. Several research projects [N. DUFFIELD, 2003], [D. BRAUCKHOFF 2006] show that packet sampling impacts on small flows (with only few packets) due to the smaller sampling probability compared to larger flows, unfortunately attacks such as SYN-Flood, ACK-Flood all have small flow characteristics, which means that packet sampling may impair the detection performance for small flow based DoS attacks;
2. Although the communication is 2-way between source and destination, today's packet sampling is applied independently in each direction, which leads to difficulties correlating the statistic of both sides, despite that those metrics are essential indicators in detecting attacks such as SNMP/DNS Reflected Amplification (i.e. where there are not much or even no traffic in the opposite direction of the attacking flow);
3. Today's packet sampling cannot provide detailed information of traffic between communication peers, which makes it impossible to distinguish some of the attacks, such as IP fragment attack and Slowloris HTTP attack, from ordinary traffic.

In order to enhance anomaly detection, a layer 4 connection oriented sampling method is recommended as security extension of the current IP packet sampling method: Rather than sampling a small part of packets in the traffic between the communication peers, the connection sampling records all TCP/UDP connection packets (including packets during connection setup and close phase if there is) between them once that connection is selected to be sampled.

2.2 Performance and Adaptability

Operator network bandwidths are rapidly increasing all the time. And so do traffic and attack flows. An effective Anti-DDoS solution for them must be highly scalable in terms of performance to adapt and expand with it accordingly. Specialized Anti-DDoS devices are often reaching their limits when trying to keep up with ever increasing performance requirements, due to their hardware models and high costs. An anomaly detection based big data analysis platform can be a more effective solution in this case, because it has very high and easily scalable performance by itself. Cloud-based or NFV-based Anti-DDoS solutions can offer a similar advantage.

In addition to that, because of the very dynamic and fast evolution of today's DDoS attacks, Anti-DDoS solutions must be self-learning, self-adapting and self-modeling. Big data analysis can offer the ideal method to drive Anti-DDoS solutions to be more proactive compared to the current more reactive approaches.

2.3 Automation and Operational Involvement

A network scale Anti-DDoS solution involves a large number of NEs, i.e., routers, anomaly detection system, DPI devices, traffic clean pipe devices, etc. It also needs to control frequent communication and negotiation between these NEs to fulfill its essential functions, i.e., packet sampling, traffic diversion, sending security policy, etc. All these NEs and related control processes can be integrated into an SDN control architecture to improve the automation level and reduce operational involvement in DDoS attack management.

2.4 Summary

Based on the above analysis, we recommend an elastic, adaptive and cost-effective Anti-DDoS solution to operators. The solution has the following features:

- Support layer 4 connection oriented sampling,
- Sufficiently high performance and easily to be scale-out,
- Have capabilities of self-learning, self-adapting and self-modeling to provide the proactive and superior attack protection,
- Centralized intelligence provided by SDN to control and manage the scalable, global distributed Anti-DDoS capabilities to minimize the operational overhead for operators.

When operators have such mature and very cost-effective security defenses, many additional business benefits will come along with them and can be further leveraged by the operator, such as:

- Saving high cost of interconnection traffic by filtering large amount of junk traffic among them,
- Providing Anti-DDoS as a service to SMEs (Small, and medium Enterprises), allowing for additional or increased revenue streams,
- Guaranteeing higher application layer QoS (Quality of Service) due to the capability of application layer attack protection.

3 Proposed Solutions

3.1 Big Data Analysis for Anti-DDoS

During the era of Mobile / Fix Broad Band, the complexity of DDoS attacks is growing rapidly with the explosion of big data and large networks. This has brought enormous challenges to network management and operation. Traditional Anti-DDoS solutions with signature detection capabilities are having difficulties handling various mutations of DDoS attacks in such high-speed IP networks in real-time, because they often face the challenges of limited hardware resources, large data volume, fast change of flow patterns, etc. Fortunately, with the progresses of big data analytical technologies, addressing such security issues is not an impossible task anymore. Compared with traditional signature based device embedded solutions, big data analysis focuses more on the behaviors and patterns of the data flows other than on the content of the payload. Multi-dimensional to ultra-high dimensional models can be built to accurately profile the data flows on-line, which allows detecting and even predicting DDoS attacks in real-time. By so doing, operators can greatly reduce the CAPEX (capital expenditure), as complicated and expensive detecting devices with Deep Packet Inspection (DPI) will no longer be essential.

Furthermore, compared to big data offline / batch analysis, big data online learning / stream mining techniques can provide additional advantages like:

- Avoiding to re-train processes when adding new instances,
- Strong adaptability to changing environments,
- Can built on theoretical proofs and guarantees,
- High efficiency and easy scalability,

By combining an online learning framework with batch analysis techniques, as well as expert knowledge, and even online deep learning techniques in the future, we can have powerful tools successfully defending against future attackers and detecting anomalies in time.

3.2 SDN for Anti-DDoS

With the advantages of centralized controlling, SDN can manage the overview of the whole network to detect and mitigate network security attacks. The basic SDN architecture is shown in Fig. 1.

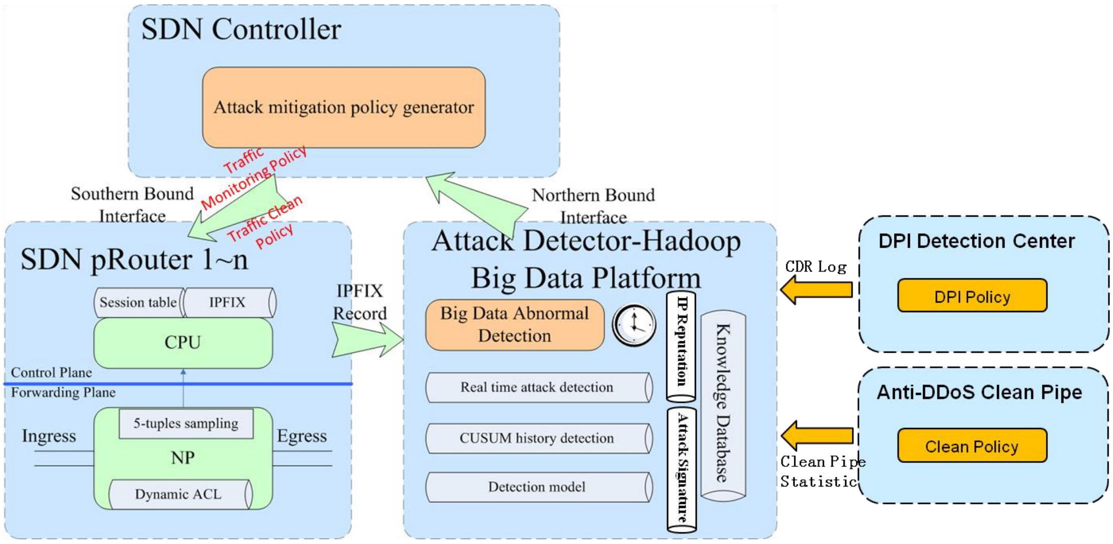

Figure 1 Architectural Overview of SDN-based Anti-DDoS Solution

The SDN controller, routers, and big data platform form a closed-loop control system. The SDN controller sends traffic monitoring policies and traffic clean policies to routers. The routers perform the packet sampling functions and possible traffic diversion actions (to DPI or Anti-DDoS clean pipes). The big data platform performs detection of abnormal traffic by running data mining based on received packet sampling records and feeds back the detection results to SDN controller. Based on this, the SDN controller takes the decision on adequate mitigation and configuration steps.

In addition to that, the big data platform can also receive the Call Data Record (CDR) Log from a DPI detection center, as well as the statistics information from an Anti-DDoS clean pipe, to help it improve and derive further intelligence by self-learning.

3.3 Overall Anti-DDoS Solution for Operators

Joining big data analysis and SDN together, the overall Anti-DDoS solution is a multilayered architecture as shown in Fig. 2.

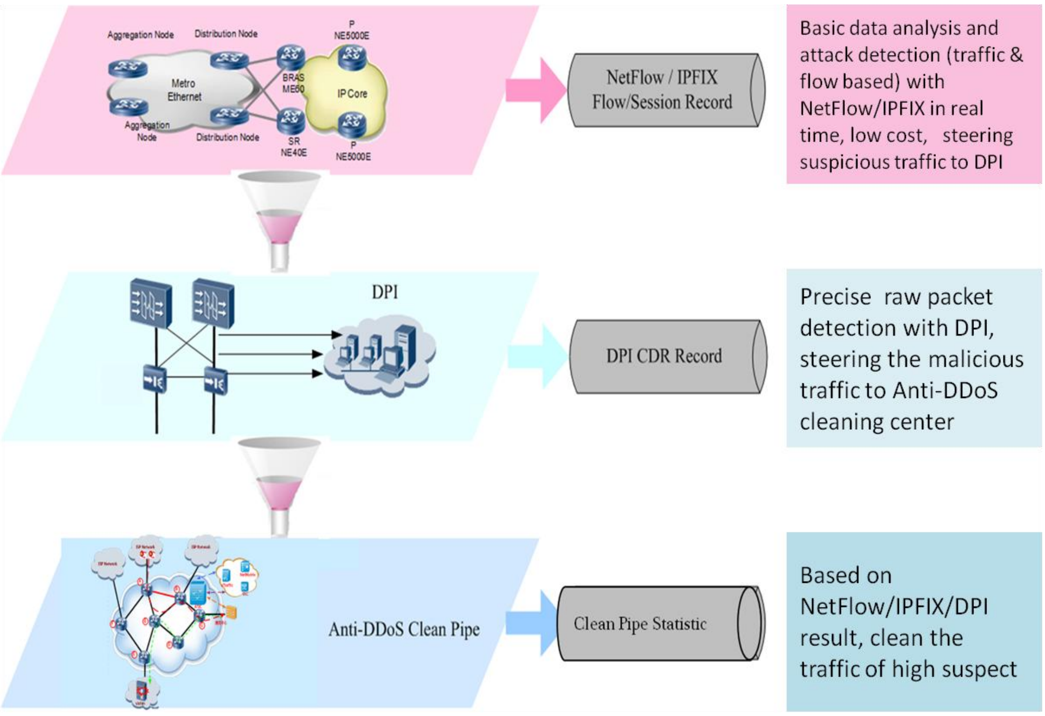
Aggregation Node
Distribution Node
P
NE5000E
Metro
Ethernet
BRAS
ME60
IP Core
Aggregation
Node
Distribution Node
SR
NE40E
P
NE5000E
NetFlow / IPFIX
Flow/Session Record
Basic data analysis and attack detection (traffic & flow based) with NetFlow/IPFIX in real time, low cost, steering suspicious traffic to DPI
DPI
DPI CDR Record
Precise raw packet detection with DPI, steering the malicious traffic to Anti-DDoS cleaning center
Anti-DDoS Clean Pipe
Clean Pipe Statistic
Based on NetFlow/IPFIX/DPI result, clean the traffic of high suspect

Figure 2 Multilayered Anti-DDoS Solution Joining Big Data Analysis and SDN

This multilayered attack protection architecture can take the full advantage of the high performance and powerful filtering capabilities of the big data platform, coupled with the entire network scheduling capability of SDN. It will greatly enhance the cleaning efficiency and can significantly reduce overall costs.

Fig. 3 shows the detailed process of information exchange and the corresponding actions to further explain the overall architecture from an alternative viewpoint.

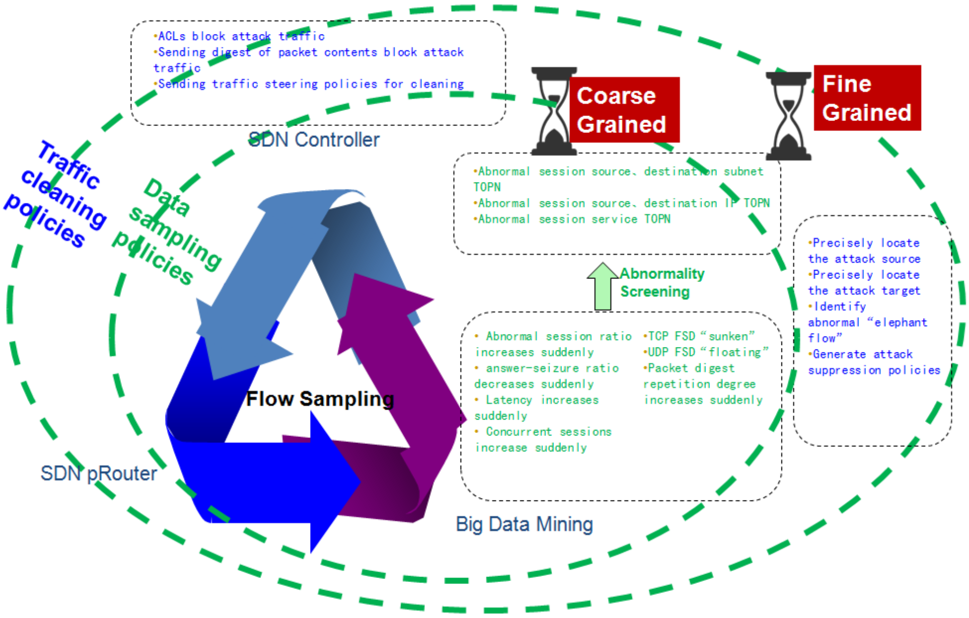
•ACLs block attack traffic
•Sending digest of packet contents block attack traffic
•Sending traffic steering policies for cleaning
SDN Controller
Coarse Grained
Fine Grained
Traffic cleaning policies
Data sampling policies
•Abnormal session source、destination subnet TOPN
•Abnormal session source、destination IP TOPN
•Abnormal session service TOPN
Abnormality Screening
•Precisely locate the attack source
•Precisely locate the attack target
•Identify abnormal “elephant flow”
•Generate attack suppression policies
• Abnormal session ratio increases suddenly
• answer-seizure ratio decreases suddenly
• Latency increases suddenly
• Concurrent sessions increase suddenly
•TCP FSD “sunken”
•UDP FSD “floating”
•Packet digest repetition degree increases suddenly
Flow Sampling
SDN pRouter
Big Data Mining

Figure 3 Workflow of Information Exchange and Corresponding Actions

4 Conclusion

Along with the continuing growth in both size and sophistication of DDoS attacks, the trend of requiring Anti-DDoS architecture to be more elastic and adaptive is becoming increasingly evident.
Enhanced by big data analysis and SDN, the integrated Anti-DDoS solution can be significantly more powerful and more cost-effective, better fulfilling business requirements and even creating new business opportunities for network operators. We like to invite and welcome operators and other vendors to jointly develop with us open standards and solutions for these proposed technologies together and to improve DDoS protection for the Internet overall.

5 Reference List

[N. DUFFIELD, 2003]: DUFFIELD, N., LUND, C., AND THORUP, M., Estimating Flow Distributions from Sampled Flow Statistics. In ACM SIGCOMM, Karlsruhe, August 2003.

[D. BRAUCKHOFF 2006]: Brauckhoff, D., Tellenbach, B., Wagner, A., May, M. and Lakhina, A., Impact of packet sampling on anomaly detection metrics. In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement (IMC '06). ACM, New York, NY, USA, 159-164.