CASE STUDY

NEAR REAL-TIME DNS REPORTING MITIGATES DDOS ATTACKS

DDOS ATTACKS ARE GROWING

Distributed Denial-of-Service (DDoS) attacks are powerful forces that can bring down even the most popular websites by overloading servers with more requests than they can handle. DDoS attacks have increased 200 percent in the first quarter of 2019 compared to the same time period in 2018, and DDoS attackers are now combining multiple attack methods.[1] The rapidly expanding Internet of Things (IoT) provides DDoS attackers with a large attack surface filled with minimally secured devices. These coordinated attacks can quickly take a system offline resulting in revenue loss, reputation damage and exposure to other types of attacks.

One major Service Provider wanted to minimize the risk of internal DDoS attacks on its subscriber Domain Name System (DNS)—the same type of attack that occurred with the 2016 Mirai botnet malware. The service provider's existing DDoS defense platform did not have the visibility and reporting capabilities to meet its end-customer requirements and was not able to efficiently scale to handle large volume attacks.

The Service Provider wanted to:

- Easily append existing DNS infrastructure with an out-of-band DNS solution that would clean network bandwidth of DDoS traffic
- Quickly view and analyze DNS current activity and attacks
- Increase transparency through real-time reporting both inside and outside the DNS team
- Gain a real-time dashboard to help security teams instantly see and respond to DDoS attacks

PARTNERING FOR SUCCESS

The Service Provider's Chief Engineer responsible for perimeter security, partnered with F5 engineers to better secure its DNS and security posture. The F5 team helped to identify gaps in the Service Provider's existing systems and develop a solution that would meet its real time, out-of-band requirements.

The solution they implemented consists of F5® BIG-IP® Advanced Firewall Manager, F5 BIG-IP i15800 appliances and F5® BIG-IQ® Centralized Management. This tightly integrated policy control and enforcement solution hyperscales and secures DNS responses geographically to survive DDoS attacks and also mitigates DDoS threats by blocking resolution to malicious domains. The BIG-IQ web-based UI provides easy-to-use configurations with centralized dashboards as well as advanced logging, statistics and reporting—all easily exportable to third-party analytics platforms.

GRANULAR VISIBILITY INTO DNS AND DDOS MITIGATES ATTACKS

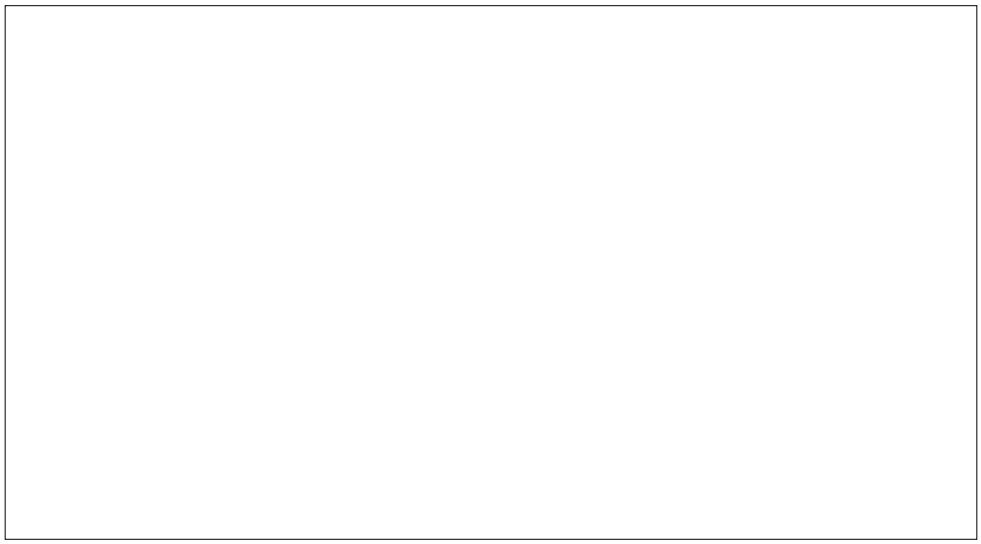
Integral to the solution, the BIG-IP i15800 appliance excels in delivering high-performance DNS visibility, reporting and analysis. The BIG-IP i15800 incorporates a front-end field programmable gate array (FPGA) to clean the incoming data of DDoS traffic. The FPGA offers 100X throughput performance improvement versus using standard CPU clock cycles.

The DNS DDoS filtering solution was implemented using a hybrid approach which included using an out-of-band “tap” to monitor traffic. When an attack is detected, a border gateway protocol (BGP) announcement of “default-originate” is made directing all traffic to the F5 BIG-IP appliances. When the attack is over, they reroute traffic back to the regular DNS servers. This granular visibility into DNS and DDoS helps mitigate attacks.

The other half of the solution, F5 BIG-IQ, centrally manages the BIG-IP DNS services and policies and captures DNS statistics and other pertinent reporting metrics. BIG-IQ enables the Service Provider to gain visibility into the DNS servers and detect when they are underperforming. The system allows them to drill down into specific attacks or review current traffic trends. All application visibility and reporting (AVR) statistics are sent from the BIG-IP to the BIG-IQ for in-depth analysis, reporting and policy augmentation as needed.

Figure 1 shows the F5 BIG-IQ DNS DDoS summary page which displays both DNS activity analytics along with DDoS metrics. This gives both Security Operations Center (SOC) and DNS Network Operations Center (NOC) engineers the tools to accurately determine what is happening in their DNS infrastructure at a glance. In addition to displaying DNS activity, it shows the top 25 attacked URLs, top 10 attackers, attack heat map, and a list of the top 10 attack types.

Figure 1: F5 BIG-IQ DNS DDoS Summary Page



The attack heat map provides an easy-to-consume view of the top attacks on the infrastructure, sorted and color coded by size and severity. For networks that experience thousands of DNS attacks a day, this is the most efficient way to zero in on the attacks that matter most.

Figure 2 shows the BIG-IQ DDoS traffic dashboard which provides a consolidated view of data coming from all BIG-IQ managed BIG-IPs. It shows all the DDoS attacks against the network for the selected time regardless of the attack type. It can display attack type, size, flow history, source and destination IP address, Geo IP map and status. The attack type details show in/drop requests, the amount of traffic that has been filtered, the status indicating whether the attack is ongoing or has been mitigated, the start and end date of the attack, and how much traffic has been observed by each F5 BIG-IP appliance.

Figure 2: F5 BIG-IQ DNS and DDoS Traffic Dashboard

SERVICE PROVIDER'S RESULTS

The Service Provider successfully implemented an out-of-band solution with near real-time abilities to clean incoming traffic of DDoS attack packets and respond to attacks. The BIG-IQ dashboards provide a high level, at-a-glance view of DNS and DDoS traffic details from which the Service Provider can review current traffic trends or drill down into specific attacks with criteria like attack type, size, flow history and source, and destination IP address.

For more information contact F5 or go to https://www.f5.com/solutions/service-providers

[1] Comparitech–DDoS Attack Statistics and Facts for 2018-2019.