Technical Brief

Protecting Against Application DDoS Attacks with BIG-IP ASM: A Three-Step Solution

Today's security threats increasingly involve application-layer DDoS attacks mounted by organized groups of attackers to damage web-facing applications by exhausting resources. F5 BIG-IP ASM provides application-layer protection against DDoS attacks.

By Or Katz
Principal Security Engineer

Contents

Introduction

In the past few years, organizations have reported a growing number of incidents involving groups of attackers trying to damage commercial and institutional web applications by exhausting their resources through distributed denial-of-service (DDoS) attacks. Attacker groups understand that preserving application availability is a high priority for most organizations because availability influences application revenue, and therefore any reduction in the quality of service can reduce revenue as well as damage the organization's reputation.

Application-level DDoS attacks are popular specifically because it's a challenge to completely protect against them. By design, the application level of the network is generic in nature; each application has unique characteristics, but the interfaces and mechanisms used to deliver those applications are similar. As a result, the application layer is vulnerable to a wide range of threats, including relatively unsophisticated attacks. For instance, analysis of recent DDoS attacks on a major credit card company involved in the 2009 WikiLeaks incident indicated that when the company's website first experienced downtime, 940 computers were participating in the attack, which used brute-force HTTP traffic to the application.[1] This case shows how easily even a simple attack can bring a web application to its knees. With more sophisticated DDoS tools, attackers can identify specific vulnerabilities in applications and their delivery methods, enabling them to use less bandwidth and more distributed resources to exhaust application resources across the network.

A good example of how easily public vulnerabilities can be found and exploited was shown by the recently discovered vulnerability of web servers running a certain combination of PHP5, Java, and ASP.NET. Specially crafted HTTP requests targeted towards this very specific platform combination can result in collisions of the web server's hashing function when unique requests return non-unique and overlapping responses. An attacker could send many "hash busting" requests at the same time to successfully create a denial of service event on the web server, starving legitimate resources.

Fortunately, by focusing on how users interact with applications in real-time and how those applications are delivered over the network, organizations can predict how attackers and attacks will evolve. When looking at the threat from a protective point of view, it becomes possible for application and network administrators to work together to detect and protect against DDoS threats.

1 "'Tis the Season of DDoS," PandaLabs blog, December 2010

The appropriate Application Delivery Controller (ADC) can serve an invaluable role. F5® BIG-IP® Application Security Manager™ (ASM), which resides between applications and users, can detect and protect against an attack in real-time by:

- Detecting that an application is under attack.
- Identifying attacker information, including whether the attack is distributed or coming from a single location.
- Effectively mitigating the attack without damaging application availability, thus minimizing the effects on innocent users.

By controlling access, implementing challenge/response and anomaly detection engines, and applying the ability to understand application behavior, BIG-IP ASM defends against malicious connections and keeps attackers from overwhelming applications.

Step 1	Detect that an application is under attack
Step 2	Identify attacker information
Step 3	Mitigate the attack

Figure 1: F5 BIG-IP ASM is a web application firewall that detects and mitigates the threat of application DDoS attacks based on the ability to understand the application layer and its behavior.

Three-Step Application Protection

Step One: How to Detect an Application Attack

Recent application-level DDoS incidents show that such an attack can be described as a mass of HTTP requests to the web application from as many sources as possible. Before DDoS was the attack du jour, the standard, single-point denial-of-service (DoS) attack was a tried and true staple of the attacker community. Unlike its distributed cousin, a standard DoS attack uses a single source that sends as many requests as possible to affect application availability, where a DDoS attack is mounted from multiple, geographically distributed locations as it tries to bypass traditional protection methods.

From a security standpoint, this difference between DoS and DDoS attacks dictates the way a security filter can detect and mitigate the attack. A security filter can easily detect an abnormal rate of HTTP requests sent from one source, as happens

in a traditional DoS attack. Once detected, the attack can be mitigated easily by blocking access from the single source.

While the DoS scenario seems trivial from a protective point of view because it's so easy to detect and mitigate, the DDoS is much more complex, since it includes a multi-source attack with each source sending many HTTP requests. These attacks are usually conducted by ranks of 'zombie' PCs: devices infected by malware and controlled remotely by an anonymous attacker, often without the machine's owner having any knowledge that an attack is underway. To detect this type of attack, DDoS protection policies need to study how the attacked application is legitimately used. This can only be done by learning how the application is accessed over time, including all the characteristics of valid traffic. These characteristics typically include:

- **Access rate over time.** This identifies access rate to the application during different hours and days of the week. For example, some applications may draw Monday morning rush-hour traffic levels significantly different from their traffic at other hours and on other days of the week.
- **Rate per application resource.** The application is not one organism; each resource of the application has its own characteristics. For example, there is no doubt that the access rate for an application login page is greater than for other pages in the application.
- **Response latency.** The application response latency for each application resource (and for the entire application) indicates when a resource is being exhausted.
- **Rate of application responses.** The rate of application responses such as 404 (page not found errors) and 500 (application errors) will change according to how the application is used.
- **Geographical locations.** User access rate can be segregated according to the users' geographical location, and in many cases, web application administrators can predict their users' location(s). For example, U.S. government web application administrators might anticipate that most users, for most applications, will be accessing those applications from within the U.S.

The detection of these traffic characteristics should be based on anomaly detection, or in other words, changes in the application behavior. For example, if the access rate of an application's search page is typically 500 transactions per second and suddenly that rate jumps to 5000 transactions per second, it is usually safe to assume that the search page is being abused and possibly attacked. Depending

on the source locations of each of those requests, the application may be subject to DDoS attack. In this example, the security filter should not monitor the source of attack, but rather the resource under attack.

BIG-IP ASM detects such attacks by learning how the application is normally accessed. Depending on configuration, BIG-IP ASM generally accomplishes this by collecting the following information:

- Transactions per second for each URL in the application.
- Web server latency for each URL in the application.
- Transactions per second for each source IP that accesses the application.

BIG-IP ASM will detect an attack when there is a change in the way an application is being accessed compared to the normative values it has already learned.

Step Two: How to Identify Attacker Information

After detecting that an application is under DDoS attack, the next step in defense is to determine who is attacking the application—or at least, what information about the attacker(s) can be discerned. By definition, a DDoS attack is not mounted by one source that needs to be blocked, but rather by many. In the above example of unusual search page requests, there might be multiple users trying to perform searches on the application. Some of these sources of traffic will be valid users, while others are participants in the attack, and the challenge is to differentiate between the legitimate and the illegitimate searches.

The best way to differentiate is to challenge users by distinguishing between normal users who work with browsers and malicious automatic tools that send requests directly to the application. One example for such a challenge is the CAPTCHA authentication test, which is used on many application login pages and attempts to repel brute-force attacks by requiring the user to respond to a random or personal challenge.

Another example of an effective challenge, and one used by BIG-IP ASM, is the injection of JavaScript to the user. Only clients who use a browser pass this challenge, while malicious automated tools fail it. As a result, BIG-IP ASM can selectively pinpoint and block those automated tools.

Detection and attacker identification are not always decisive, of course. The complexity of the scenario affects the accuracy of detection efforts, and challenging detection tasks may result in false positives. In addition, failure to respond to a

security challenge does not necessarily equate to an attack. For example, a challenge can fail to receive a response as a result of the users' browser limitations or configurations. Nonetheless, security measures with the ability to discern information about potential attackers and pose one or more challenges to suspicious users can more effectively detect and thus mitigate threats.

Three: How to Mitigate an Attack

As noted, application delivery is often a primary business goal and may be an organization's dominant—or only—customer interaction. In such cases, dropping application users' transactions is unacceptable, even when suspicious users fail to respond to a security challenge. Instead, efforts to mitigate DDoS attacks should apply these principles:

As possible, protect the application from DDoS attacks.

If an attack occurs, mitigate the attack's effects on the application. Preserve application availability so it remains intact for other users.

One mitigation option that conforms to these principles is to increase the overall availability of an attacked resource by lowering the rate at which suspicious sources can access the application, thus maintaining application availability and preventing the DDoS attack at the same time. The benefits of this approach are that:

- Application quality of service remains intact. The reduction of service availability for suspicious users will be determined based on total available resources for the application.
- Attackers are less likely to recognize that the attack is being mitigated.

Using this approach, the worst case scenario becomes a false positive that slows user connectivity to the application but does not prevent user service, thereby maintaining availability for legitimate users. In actual attacks, the application is protected as well.

If attack is suspected, delay access or drop connections.

During a potential attack, several mitigation options are available:

- Delay access from suspicious source IPs
- Delay access to URLs that are under attack
- Drop connections for suspicious source IPs
- Drop connections for URLs that are under attack

Administrators can manage the balance that BIG-IP ASM provides between application protection and availability by setting policies to influence how aggressively suspicious connections should be dropped.

Reporting

BIG-IP ASM uses a unique, bi-directional approach to detecting DDoS attacks and identifying attacker information, thereby preserving quality of service and mitigating the effects of an attack at the same time. Because BIG-IP ASM sits between users and applications, it can maintain awareness of both to:

- **Monitor application resources behavior.** BIG-IP ASM learns normal application latency and transactions per second rates and limits access when those rates dramatically exceed the learned values.
- **Challenge suspicious users and respond appropriately.** BIG-IP ASM injects a JavaScript challenge to application responses and limits application availability to users or agents who fail to reply.

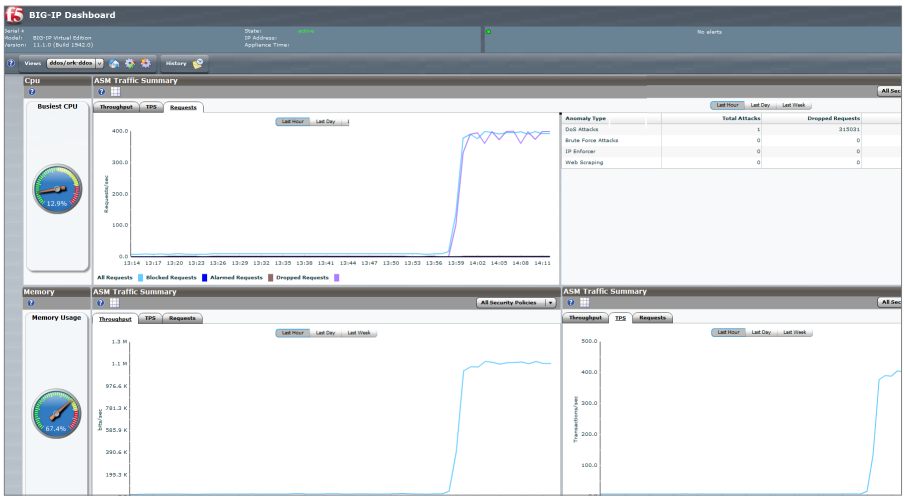

Figure 2: The BIG-IP ASM dashboard provides executive reporting on application availability and traffic, including availability during DoS and DDoS attacks.

BIG-IP ASM also keeps IT administrators apprised of both normal and potentially abnormal application activity through operational dashboards and reporting. In addition to the management dashboard, which routinely displays operational data such as connections, throughput, and availability, BIG-IP ASM provides specific reports on DoS and DDoS incidents. Administrators gain an easy reference to

detailed views of detected anomalies, the mitigation response including dropped connections, and the suspicious IP addresses involved. With this data, organizations can understand the frequency and level of DoS and DDoS attacks against their networks, as well as the effects those attacks may have had on availability, so management decisions can be made with confidence.

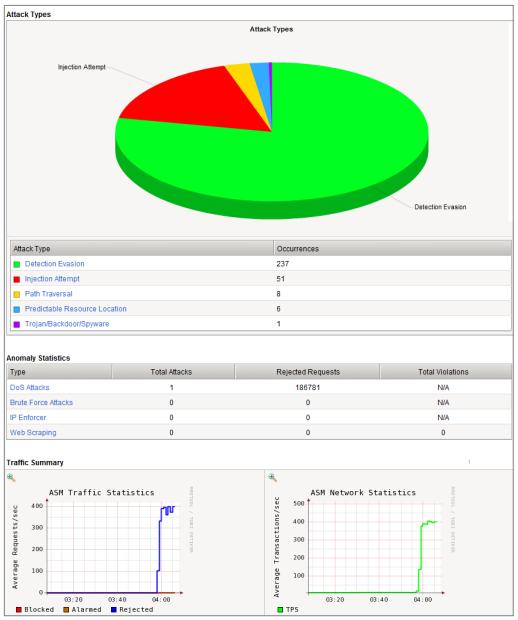

Figure 3: BIG-IP ASM reporting delivers in-depth statistics on attack types, anomaly statistics, top requested URLs, and top requesting IP addresses.

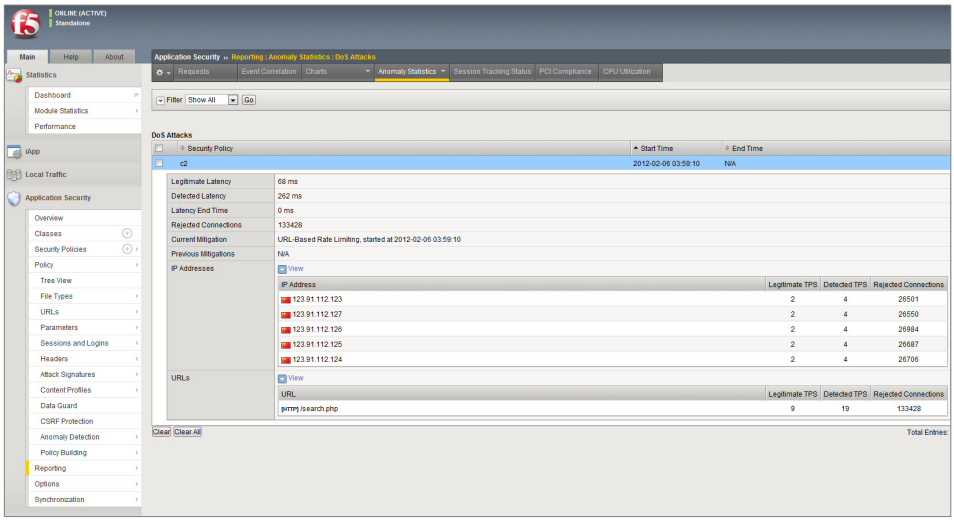

Figure 4: BIG-IP ASM specifically reports on DoS and DDoS incidents.

Conclusion

Web applications are both crucial to the operations and customer service of many organizations and particularly vulnerable to the DDoS attacks occurring with such prevalence today. Detecting attack is the first step to mitigating it and preserving application availability. When trying to determine whether an application is under a DDoS attack, any change in the behavioral characteristics of the application should be taken under consideration, because combining information such as access and response rates can give us clear view of the state of the application.

F5 BIG-IP ASM offers an all-in-one solution for protecting applications and organizations from DDoS attacks by:

- Learning application behavioral properties.
- Detecting changes in the routine behavior of the application.
- Mitigating the attack using a variety of responses and options that preserve availability and repel attackers.
- Providing detailed reporting for increased management insight on application and security status.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com