MAZEBOLT

WHITEPAPER

Testing DDoS Mitigation Effectiveness

Table of Contents

Index of Tables

Executive Summary

Many companies offer an "outside-in" approach, where they get into the mind of the threat actor and perform testing accordingly. While that's important, it's only one side of the equation. Comprehensive understanding of both the attacker's perspective and the defense perspective are critical to properly execute DDoS testing.

Mitigation systems are very similar; while some vendors' individual approaches and technologies vary, the systems are generally tuned to protect against a broad range of attacks. The environments in which they operate vary significantly on a case-by-case basis. That's where the points of failure regularly occur – a generally tuned device is installed within an environment with very specific requirements. When the device is tuned effectively, potential failures are significantly reduced.

> ***"Newly published research suggests that while there has been a marked increase in spending to mitigate against Distributed Denial of Service (DDoS) attacks, organizations are still falling victim."***
> Davey Winder, Security Journalist, SC Magazine UK

Effective DDoS mitigation at the enterprise level is typically comprised of both on-premises - customer premises equipment (CPE) - mitigation and/or a scrubbing service. For optimal mitigation, you must fine-tune both the CPE and trust that your scrubbing service will effectively mitigate DDoS attacks and have the right response team available when you do come under attack.

Hundreds of different types of DDoS attacks variants exist in "the wild," with new DDoS attack types identified on a regular basis. Protecting networks against these dynamic, continuous DDoS threats is a complex, ongoing, and iterative effort.

With these thousands of variations of DDoS attacks and new ones popping up constantly, appropriate testing is critical. That is why knowledge of the interaction between attacks and mitigation needs to be the starting point for effective DDoS testing.

Approaches to DDoS Testing

The Knowledge Perspective

The best approach to DDoS testing occurs within the context of knowledge attainment:

1) You don't know what you don't know, so it is difficult to formulate the right questions.
2) You realize what you don't know, so you can ask the right questions.
3) You have knowledge.

You don't know what you don't know, so it is difficult to formulate the right questions.

What this means in regard to DDoS testing is that during knowledge stage one, you know that you have vulnerability to DDoS attacks, but don't know how to go about identifying or even recognizing your weaknesses, much less why they exist.

Some vendors offer DIY solutions, where they provide a specific catalog of DDoS attacks and allow you to directly test your systems. At the first stage of knowledge, many people have a general, but not a comprehensive understanding about the many devices within their networks, how they interact with the mitigation systems, how well tuned they are to each other, and the specific areas in which they're vulnerable.

A DIY system can give them all the answers they want about what tests their systems fail. The problem is that they cannot apply that knowledge appropriately to understand exactly what needs to be fixed to prevent those failures. Or even if they were checking the correct tests in the first place.

You know what you don't know, so you can ask the right questions.

In this stage of knowledge, you are in a position to start understanding all of the things you don't know. After your systems fail a DIY test, you can begin to try to figure out where the failures occurred and why. The problem is the size of your system – what's the logical point to start your investigation so you can find the points of failures? Do you have the time and resources for the investigation?

You have knowledge.

When you are at this stage, you understand that the complexity of DDoS attacks is such that a DIY solution is not going to be able to give you a comprehensive, detailed overview of what attacks your system is vulnerable to, where those vulnerabilities lie, and how to fix them.

That's why a methodological approach to DDoS testing is required.

BaseLine DDoS Testing Methodology

Protecting against DDoS attacks requires the right tools configured in the right way against the most common and most likely DDoS attacks, combined with the ability to recognize and protect against the less common and less likely DDoS attacks. Every mitigation vendor's system protects against attacks; the nature of the configurations are generally the points of failure. Therefore, BaseLine DDoS testing needs to take the comprehensive approach to push each generally configured system to the limit to ensure that it can be fine-tuned to protect within the specific environment in which it is operating.

BaseLine DDoS Testing provides enterprises with the optimal tool for managing the complexity of dealing with DDoS mitigation. The three main considerations that need to be addressed in an effective DDoS mitigation strategy are detailed below:

The three main considerations that need to be addressed in an effective DDoS mitigation strategy are detailed below:

Table 1 – The Three Key Aspects in DDoS Mitigation

Aspect	Complexity	DDoS Mitigation
Technical	How well do my mitigation systems **automatically** work against Layer, 3 4 and 7 attacks?	Validate each layer and attack mechanism at play in DDoS defenses.
Vendor SLAs	If I have a scrubbing center, how well does my SLA work with my vendor?	Validate that the scrubbing center switchover and the mitigation capabilities work as expected. Ensure it identifies false positive triggering.
HR	How will my personnel react?	Ensure team's ability and capacity to respond to a DDoS attack scenario. It improves response handling and reduces downtime during a real DDoS attack.

The Mitigation Perspective

Examining the hundreds of different DDoS attack variants in the wild, it becomes apparent that when viewed from the perspective of DDoS mitigation that DDoS attacks can be grouped according to the various mechanisms used to mitigate them.

Generally, five main DDoS mitigation mechanisms are used. (See Table 2 below). Therefore, testing can be highly targeted and efficient, applied to verify these mechanisms within a realistic timeframe. For example: *Attack name: HTTP with browser emulation attacks.*

This attack uses a webkit to perform an HTTP-based DDoS attack. Hundreds of such variants exist, all with a unique name. However, testing that you are protected against this **single attack** will likely ensure you are protected against **other similar variants**.

Mitigation generally occurs using a Layer 7 challenge or a signature technology that identifies the webkit itself. (See Table 2 below for details)

Table 2 is a high-level description of how the different DDoS mitigation mechanisms work – **keeping in mind that all vendors use very similar methodologies implemented in slightly different ways**.

Table 2 - Main DDoS Mitigation Mechanisms

No.	Mitigation Mechanisms	Details
1	Signature-based	The mitigation mechanisms work by identifying certain rates and strings in packets for Layers 3, 4 and 7 from SRC IPs. This is generally done to block or suspend SRC IPs. The mitigation mechanisms vary based on the vendor, but they all take a similar approach.
2.	Behavioral-based	These mechanisms use various algorithms to identify malicious DDoS traffic, such as a normal baseline rate against IPs that deviate from the normal baseline rate, as well as baseline deviation. Protection occurs with the application of some type of or dynamic signature, etc. These mechanisms generally block based on SRC IP but may have more complex and granular blocking mechanisms, again, depending on the vendor.
3.	Challenge-based	When an anomaly has been discovered, a challenge may be issued to specific or all new connecting IPs. This challenge may be Layer 7 or Layer 4. For example, a SYN cookie challenge, DNS challenges, or JS/302 redirect challenges, etc. There are a few variants depending on vendor.
4.	Out-of-state packet	Some DDoS mitigation devices in certain deployments may also enforce stateful sessions or deliver partial enforcement for TCP traffic.
5.	Rate-based	It's a primitive, fallback method used when no other option is available. It's very false-positive prone.
6.	Botnet detection	Having on hand a known list of attacking IPs and applying this list to perimeter defenses. This method is part of a wider toolbox for mitigating attacks because it's only as good as the list –there will always be IPs not known to the list you are using.

Cutting Through the Noise – Mapping DDoS Testing to DDoS Mitigation Mechanisms

Even with the most sophisticated DDoS mitigation and testing solutions deployed, most companies are left with a staggering 48% DDoS vulnerability level. The vulnerability gap stems from DDoS mitigation solutions & infrequent Red Team DDoS testing being reactive, instead of continuously evaluating and closing vulnerabilities.

Working with any mitigation solution installed, RADAR™ offers superior DDoS coverage and automated DDoS protection. RADAR™ simulates over 100 attack vectors with all public facing IPs 24/7, giving real time visibility to all DDoS vulnerabilities with zero downtime.

Table 3 - DDoS Attacks Mapped to DDoS Mitigation Mechanisms

Layer	Attack Type	Mitigation Mechanism Tested
3	IP Fragmented Flood	- Behavioral - Signature
3	ICMP Flood	
4	UDP Flood	
4	UDP Garbage Flood	
4	URG Flood	- Behavioral - Signature - L4 Challenge - Out-of-state
4	Empty Connection Flood	
4	PSH + ACK Flood	- Behavioral - Signature - Out-of-state
4	ACK Flood	
4	RST Flood	
4	FIN Flood	
7	HTTPs Flood	- Layer 7 Challenge - Signature
7	HTTP Flood	
7	Brobot HTTP	
7	Brobot HTTPs	
7	HTTP/s with Browser	
7	SlowLoris	
7	SSL Renegotiation Attack	
7	THC-SLL Attack	

Conclusion

For a completely different perspective, think about DDoS testing in the context of standard lab work. When you go for a physical and they do a CBC (complete blood count), you get information about your red blood cells, your white blood cells, your hemoglobin, your hematocrit, and your platelet numbers. Analyzed together, they can greatly clarify the clinical picture. RADAR™ does the same thing for your security protection against DDoS attacks.

About MazeBolt

MazeBolt introduces a new standard in DDoS coverage, automatically detecting, analyzing, and prioritizing remediation across the network, doubling coverage, and virtually eliminating DDoS exposure without shutting down organizational operations. MazeBolt's continuous defense supercharges the performance of CISOs as well as the mitigation service provider.

Free E-Book `A Simple Guide to DDoS Mitigation'

Download Now!

