MAZEBOLT

2018

BaseLine DDoS Testing Handbook

"The de-facto industry standard of DDoS testing"

www.mazebolt.com

Table of Contents

Table of Tables

Introduction – Why a BaseLine Testing Standard?

Organizations whose business depends on being online and active 24x7 or 9x5, are at risk from a single DDoS attack disrupting their online services and IT infrastructure. In most cases these attacks result in downtime and both direct and indirect financial losses.

BaseLine DDoS testing is designed to 'proactively' and 'continuously' mitigate the risk of downtime due to a successful DDoS attacks.

DDoS attacks may strike your network at different OSI (Open Systems Interconnection) layers, taking many different forms within each OSI layer, complicating identification of the DDoS attack (See Table 1 for examples).

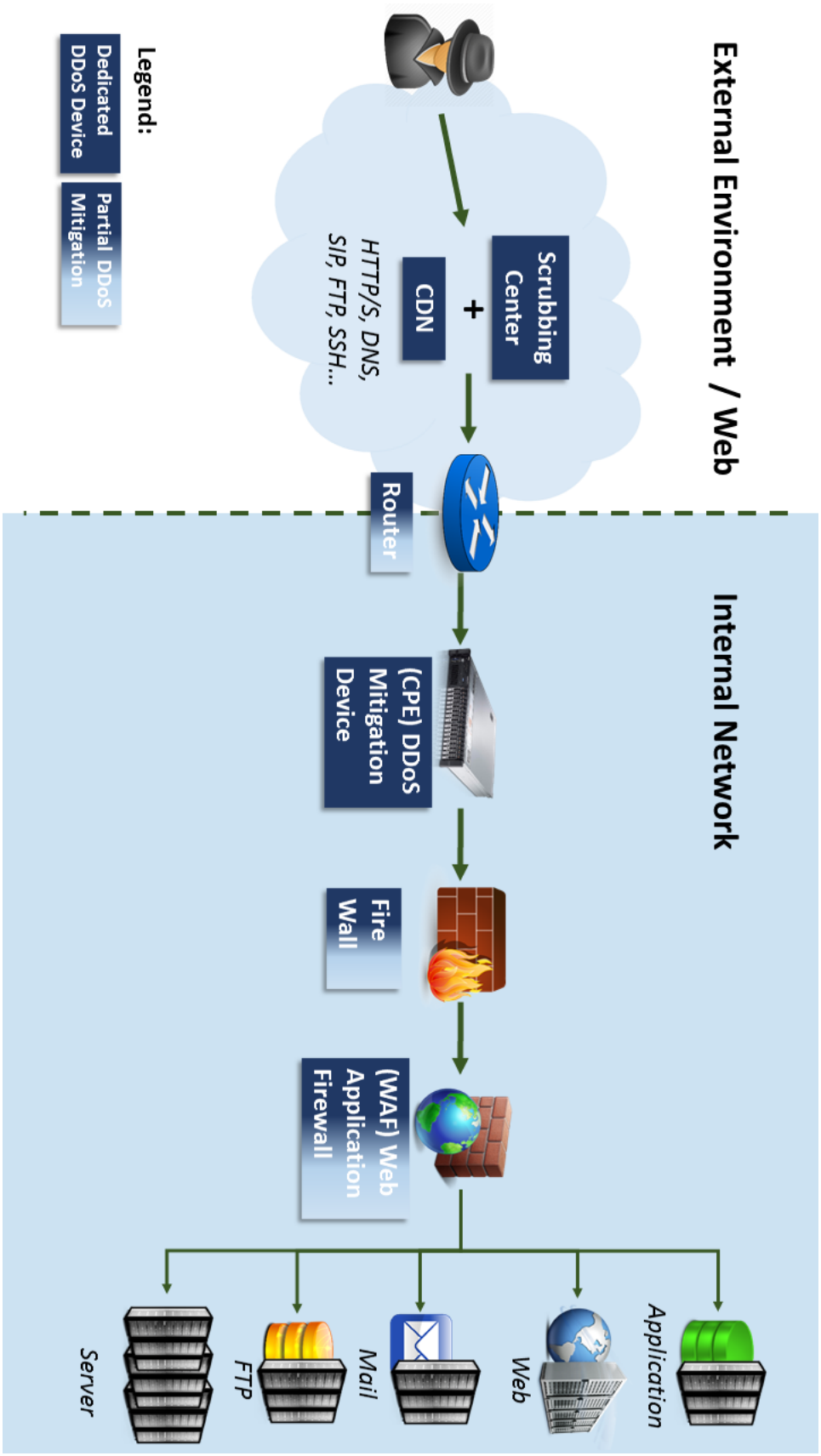
Table 1 – Examples of DDoS Attacks by OSI Layer

OSI Layer (#)	Attack Types
Network (3)	ICMP, Malformed IP, IP Fragmented
Transport (4)	SYN, UDP Flood, Empty Connection, PSH+ACK Flag, URG Flag
Application (7)	Brobot, SlowLoris, DNS Request, HTTPS, SSL Negotiation

To add to the complexity, mitigating DDoS attacks has no single "Silver bullet" but rather various types of DDoS mitigation such as: Cloud based scrubbing centers, Customer Premise Equipment (CPE) mitigation devices, CDN or combinations of these (See Figure 1 below).

Organizations need to deal with "DDoS complexity", either by validating and optimizing existing DDoS defenses**,** or if no defenses are deployed**,** to decide which type of DDoS defense technology best suits their environment. The first stage is to always proactively test their network to understand how vulnerable they are to DDoS attacks.

Figure 1 – Typical DDoS Mitigation Setups (Part or all of the below components)



What is the BaseLine Testing Methodology?

The BaseLine Testing methodology is based on **iteratively** hardening an organization against DDoS attacks with an **ongoing validation** program.

BaseLine DDoS testing is designed to validate DDoS mitigation systems can **automatically** mitigate the most common types of DDoS attacks organizations are likely to face.

MazeBolt was the first company to introduce BaseLine DDoS testing in 2013. BaseLine testing is designed to validate and understand an organization's level of DDoS vulnerability to enable effective communication between DDoS mitigation vendors and their clients on the DDoS defense needed.

MazeBolt BaseLine DDoS testing allows for a **faster** understanding and more **accurate** remediation of DDoS vulnerabilities – regardless of which type of DDoS mitigation is deployed.

BaseLine testing is aimed at proactively preventing disruption and downtime of an organization's IT infrastructure and preventing disruption to online services. It effectively highlights the most important DDoS vulnerabilities in the mitigation apparatus and/or architecture, allowing security personnel to make the least amount of changes, and at the same time the biggest impact in strengthening the IT infrastructure against DDoS attacks.

BaseLine testing is aimed at validating both the technological DDoS mitigation equipment or services as well as internal or external process & procedure handling during a DDoS attack.

BaseLine DDoS testing utilizes an easy to understand scoring metric to communicate DDoS vulnerabilities, making communication between mitigation vendors and clients easy and clear.

Since 2013, MazeBolt BaseLine DDoS testing has become the ***de-facto*** Industry Standard for organizations worldwide, across the industry spectrum, to communicate their DDoS vulnerabilities. Many **Fortune 1000** and **NASDAQ** listed companies now use BaseLine DDoS testing to strengthen their resistance to DDoS attacks.

MazeBolt's DDoS BaseLine Testing Cycles

MazeBolt's DDoS Testing Cycles are designed to provide an organization with the **optimal and** systematic process to validate that their DDoS defenses.

A BaseLine Cycle consists of three stages, which are detailed below in Table 2:

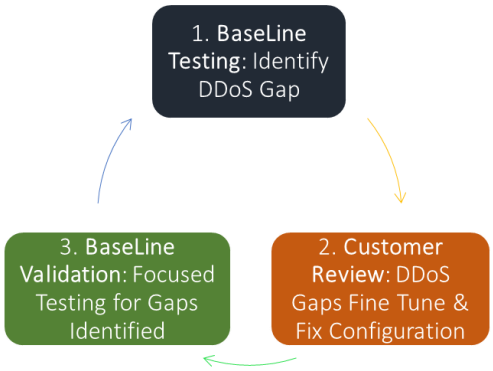


Table 2 – MazeBolt DDoS Testing Methodology

Stage	Activity	Testing Goal	
		DDoS Mitigation Technology	**Operational**
#1. BaseLine	BaseLine Testing	Validate a company's mitigation can **automatically** withstand the most common types of DDoS attacks	Familiarize IT Operations Team with DDoS attack scenarios and standard responses, continuous improvement of DDoS mitigation configurations and procedures. BaseLine DDoS tests should be **automatically** mitigated by the defensive solution deployed, prior to moving onto APT DDoS testing.
#2. Customer Review / Action Plan	Review & Remediate	Fix vulnerabilities & resolve SLA issues with DDoS mitigation vendors and scrubbing service providers	1. Internal DDoS response playbook 2. Lines of communications with vendors (Mitigation & Scrubbing)
#3. Validation	Validation Testing	Focus only on vulnerable attack vectors and retest to ensure mitigation posture has improved.	

MazeBolt BaseLine DDoS Testing

To start with, DDoS mitigation (**if** configured correctly) should be able to **automatically** block the most common types of DDoS attacks without requiring any 'human' intervention i.e. manual changes. This **automatic** DDoS mitigation capability is a critical factor that translates to minimal disruption to the target organization's online services and IT infrastructure when under attack.

MazeBolt's BaseLine testing is designed as an entry level test to verify DDoS defense mechanisms are working automatically against the most common DDoS threats in the wild, regardless of whether the organization is using CPE, Scrubbing center services or a combination of the two.

From the operational perspective, BaseLine DDoS tests help familiarize the Operations team with the DDoS attack response scenarios and processes to ensure optimal (**automatic** mitigation of all BaseLine DDoS tests) performance when the company comes under attack.

How does MazeBolt BaseLine testing work?

BaseLine DDoS testing involves running a sequence of highly controlled DDoS simulations against an environment in order to determine how well the company's DDoS mitigation operates.

These are 7 basic BaseLine testing characteristics:

1. **Maintenance Window** – BaseLine testing requires a maintenance window. In over **ninety five percent** of BaseLine tests performed, regardless of industry or organization size, downtime is experienced; this is generally due to configuration, technological or architectural weaknesses discovered during testing.
2. **3 Hours Long** – BaseLine testing is designed to be run over a **three** hour period, with up to a maximum time of **six** hours in a single testing session (for larger environments). Our experience shows that testing for longer periods of time has proven ineffective in terms of observing network and security apparatus behavior.
3. **Validate "automatic" mitigation** – DDoS mitigation technology deployed should be able to be mitigate ALL tests run without human intervention.
4. **Vendor Agnostic** – The testing should be done in a DDoS mitigation vendor agnostic manner, i.e. the attack is either mitigated or it's not.

5. **Testing coverage efficiency** – The testing should cover Layer **3**, **4** and **7** DDoS attacks online services and IT infrastructure is likely to be subjected to. These tests should validate the most common mitigation mechanisms deployed by all vendors, E.g. Behavioral, statistical, challenges, rate limiting etc.
6. **Measurement** – KPIs should be easy to understand and resolved i.e. PASS, PARTIAL PASS, PARTIAL FAIL and FAIL. These results should be easy for Mitigation Vendors to use as a guide to resolve their vulnerabilities. Each individual DDoS test run is assigned a result in the report received by the company post BaseLine test. See Table 4 below for details)
7. **Target specific** – BaseLine testing validates only the environment for which it is run against, so if run against a staging environment, the results will likely be different for production. Where possible MazeBolt recommends testing the production environment in a maintenance period.

BaseLine DDoS Testing Process Steps

A typical test will involve the following process steps:

1. **Targets to Validate** - Understand the IT infrastructure that has to be validated to DDoS attacks.
2. **BaseLine Test Plan** - MazeBolt SOC submits a BaseLine test plan to the organization for approval; included here are all the details of how the test will be run, such as testing rate, time, targets, etc.
3. **Run the BaseLine Test** – At the scheduled maintenance period MazeBolt SOC together with the organization will together execute the approved test plan;
4. **BaseLine Report** – MazeBolt SOC will provide the organization with a detailed report utilizing its unique corporate resistance metric of each DDoS test performed .e.g. (i) PASS, (ii) PARTIAL PASS, (iii) PARTIAL FAIL & (iv) FAIL.

Baseline Tests Run

MazeBolt BaseLine testing currently consists of the following tests, to provide the best possible validation for Layer 3, 4 and 7 attacks (Current BaseLine tests in Table 3, subject to change at any time).

Table 3 – BaseLine DDoS Tests by OSI Layer

No.	BaseLine DDoS test	OSI Layer
1.	IP Fragmented Garbage Flood	Layer 3
2.	ICMP Flood	Layer 3
3.	UDP Flood	Layer 4
4.	UDP Garbage Flood	Layer 4
5.	URG flood	Layer 4
6.	Empty Connection Flood	Layer 4
7.	PSH+ACK Flood	Layer 4
8.	ACK Flood	Layer 4
9.	RST Flood	Layer 4
10.	FIN Flood	Layer 4
11.	HTTPs Flood	Layer 7
12.	HTTP Flood	Layer 7
13.	Brobot HTTP	Layer 7
14.	Brobot HTTPs	Layer 7
15.	HTTP/s Flood With Browser emulation	Layer 7
16.	SlowLoris (HTTP/s)	Layer 7
17.	SSL Renegotiation Attack	Layer 7
18.	THC-SSL Attack	Layer 7

MazeBolt Baseline Validation DDoS Testing

The BaseLine Validation DDoS test focuses only on DDoS attack vectors that were identified as vulnerable in the BaseLine Test I.e. FAIL, PARTIAL FAIL and PARTIAL PASS. These attacks are rerun in order to verify the fixes and remediation efforts are working as expected.

All tests run during the BaseLine Validation test will be a subset of the initial BaseLine Test.

What you get – The benefit of BaseLine testing

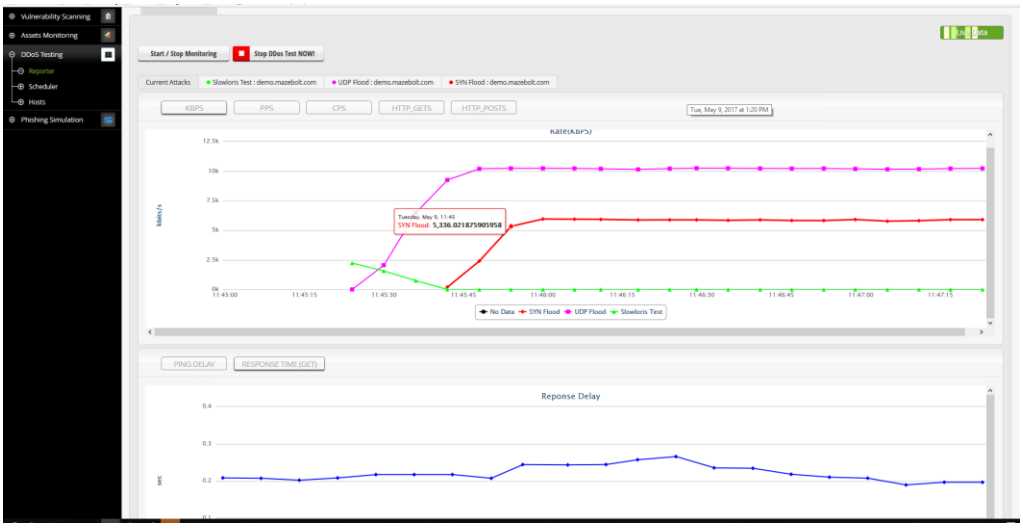
A Starting Point for tangible improvement

MazeBolt's BaseLine Testing methodology and simple reporting KPI's provide enterprises with both a **tangible starting point** and the **terminology** required to effectively **manage** the strengthening process of their DDoS mitigation posture.

Transparency

MazeBolt conducts the BaseLine testing from its DDoS testing module, a cloud based platform that provides companies with complete transparency as illustrated in the screenshot below:

Figure 2 - Screenshot of MazeBolt DDoS Testing Module



Reporting

A clear report, portraying a realistic understanding of your organizations strengths and weaknesses to DDoS attacks. MazeBolt utilizes its own proprietary KPIs to assist in strengthening the environment's resistance to DDoS attacks.

Table 4 - MazeBolt's Resistance to DDoS Metrics

For each BaseLine test run in Table 3, one of the following metrics is assigned in the final report the organization receives.

Result	Description
PASS	The site/service was not affected also the network devices were not affected. Mitigation was automatic.
PARTIAL PASS	Passed overall, the site/service did not go down straight away**;** however**,** there may have been intermittent slowdown or downtime; some network devices may have been affected.
PARTIAL FAIL	The site/service went down immediately and network devices may have been affected. However after some time the attack may have been mitigated. Mitigation was either delayed or manually applied. If the site or service being tested was mainly down.
FAIL	The site went down and stayed down, there was no mitigation throughout the test.

The report may be used to guide DDoS mitigation vendors to tweak the organization's DDoS security configurations, regardless of whether it is a CPE or scrubbing center deployment.

The BaseLine report provided is a guide on where to focus organization resources and may be provided to DDoS mitigation vendors to make configuration specific changes and in some cases may prove the current technology deployed to be unsuitable for the organizations requirements.

What you don't get – Limitations of BaseLine testing

Ongoing reporting

BaseLine testing is only valid for the **time of testing**, See below the section: "How often should BaseLine DDoS testing be performed?" for more details.

Vendor Specific Details

BaseLine testing is mitigation vendor agnostic and does not provide vendor specific configuration changes. BaseLine testing will provide a high-level overview of where the organization should focus their resources based on test results.
BaseLine testing is a compass of where the DDoS mitigation vendors are succeeding but more importantly where they are not succeeding and may be leaving the organization vulnerable to DDoS attacks.

How often should BaseLine DDoS testing be performed?

That depends; answers to these below questions will ascertain frequency of BaseLine DDoS testing:

Questions to understand your need of DDoS testing:

1. What happens when my IT infrastructure is unavailable because a successful DDoS attack targeted your organization?
    a. Is there a financial impact?
    b. Is there a customer retention impact?
    c. Can this type of PR effect current or new customers?
    d. Is downtime a possibility in my business (Even a minute)?
2. Can a DDoS attack affect my security posture to allow other attack vectors to succeed?
    a. Do my WAF's/IPS systems go into a fail-open status when under load, if so could previously un-exploitable vulnerabilities now be exploitable?
    b. Will a DDoS attack severely limit the ability to control security apparatus devices deployed worldwide if my main NOC is under attack?
3. Do I have regulatory requirements?
    a. If I have service availability issues can a regulatory authority fine me?
    b. If I have service availability issues can a customer SLA make me subject to a fine?

    Answers to these questions will differ in different organizations. However, if any of the above questions are of potential concern it means you should most likely be performing BaseLine DDoS testing at a minimum **bi-annually** per physical infrastructure that falls into those concerns.

    Most organizations having serious concerns about the questions listed above should plan for a BaseLine testing **per quarter**, the reason being that DDoS mitigation defenses require continuous tweaking, and *the strengthening of IT infrastructure against DDoS attacks is an iterative one*.

Conclusion of Baseline Testing Method

- ✓ BaseLine DDoS testing strengthens resistance to DDoS attacks through a standardized DDoS testing methodology.
- ✓ MazeBolt BaseLine DDoS testing is the ***de-facto*** industry standard of DDoS testing.
- ✓ BaseLine DDoS testing is designed to validate DDoS mitigation systems ability to **automatically** mitigate the most common types of DDoS attacks they are likely to face.
- ✓ BaseLine DDoS testing will generally consist of a BaseLine Cycle, which is a combination of an initial BaseLine Test next a Customer review and then a further BaseLine Validation test to ensure the DDoS gaps have been closed.
- ✓ Many Fortune 1000 and NASDAQ listed companies trust the MazeBolt standard of DDoS testing.
- ✓ MazeBolt BaseLine DDoS testing is continuously reviewed to ensure its relevance to the threats our customers face on a daily basis.

Any organization that has any uptime SLA/internal assumptions cannot know their true resistance to DDoS attacks without having performed at least a single BaseLine DDoS test. A BaseLine DDoS test report is only true for that particular point in time and the results may change with any network or configuration changes to the IT infrastructure tested.

Most organizations will require a regular schedule of BaseLine DDoS testing to ensure uptime and smooth service availability of their online services and IT infrastructure.

Organizations that are engaged in MazeBolt BaseLevel DDoS testing programs may also be ready to perform MazeBolt APT (Advanced Persistent Threat) testing to verify that their DDoS mitigation can withstand DDoS attacks from determined groups of cybercriminals.

About MazeBolt

MazeBolt strengthens companies' resistance to cyberattacks. MazeBolt has developed a unique Threat Assessment Platform (TAP) that consolidates threat assessment for the three main cyber-attack vectors, namely:

- DDoS Testing – Validate your defenses against DDoS Attacks are working as expected
- Phishing Awareness Programs – Strengthen your employees' resistance to Phishing through ongoing phishing simulation and dynamically adaptive awareness training campaigns
- Vulnerability Exploitation – Scan your external environment for over 32,000 possible threats

MazeBolt's TAP allows organizations to control all aspects of their cyber vulnerabilities with a unified interface that provides actionable insight, detailed reporting and most importantly – full control over cyber threats.

Visit us at: www.mazebolt.com