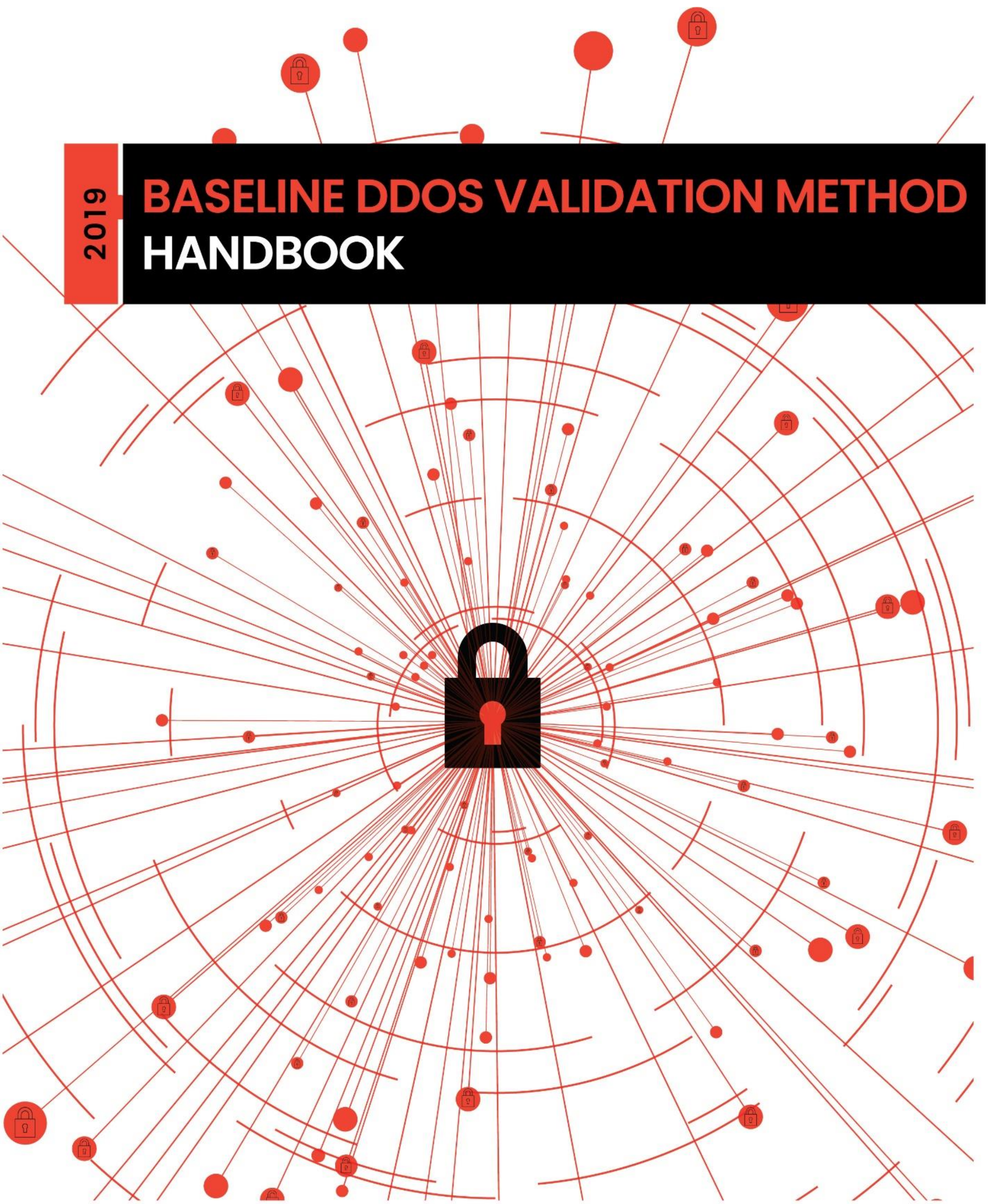
2019

BASELINE DDOS VALIDATION METHOD HANDBOOK



MAZEBOLT

TABLE OF CONTENTS

INDEX OF TABLES

LIST OF FIGURES

INTRODUCTION –BASELINE DDOS VALIDATION METHODOLOY STANDARD

Online is the new reality - Organizations are more reliant than ever on various types of online transactions and digital transformation (DX). **This** is now a common term among all businesses, essentially, we are transitioning all our business services online.

Businesses that depend on being online and active 24x7 or 9 to 5, are at risk from a single DDoS attack, disrupting their online services and IT infrastructure. In most cases these attacks result in downtime and financial losses.

ALL ORGANIZATIONS MUST PREVENT DOWNTIME BEFORE IT HAPPENS

We need to be efficient - The BaseLine ***DDoS Validation Methodology*** is a concept designed to 'proactively', 'continuously' and 'quickly' alert activation, to avoid the risk of downtime, due to a successful DDoS attack.

How a successful DDoS Attack can bring down an online system can be read here.

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

Evaluating this vast landscape can be close to impossible, without a thorough method and structure.

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, HULK

Eliminating DDoS Risk through simplicity - Adding to the complexity, in order to mitigate these DDoS attacks, there is no single "silver bullet", but rather, various types of DDoS mitigations.

These include: Cloud based scrubbing centers (BGP), Customer Premise Equipment (CPE) mitigation devices, CDN, or combinations of all of these methods. (See Figure 1 below)

UNDERSTANDING BASELINE DDOS VALIDATION METHODOLOGY

Organizations need to deal with **DDoS complexity.** They either need to validate and optimize 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 always to **proactively validate the network**, to understand how vulnerable the DDoS Mitigation is to any kind of DDoS attacks.

The bottom line is, organizations don't want **any downtime**.

The only way to effectively and manageably prevent downtime from DDoS attacks, is through the **BaseLine DDoS Validation methodology.**

The **BaseLine DDoS Validation Methodology** is a concept of DDoS validation.

It is aimed at proactively **preventing interruption and downtime** of an organization's IT infrastructure.

It prevents disruption to online services from DDoS attacks. It effectively highlights the most important DDoS vulnerabilities in the mitigation configurations, allowing security personnel to make the least amount of changes. At the same time it builds a robust and strong IT infrastructure against DDoS attacks.

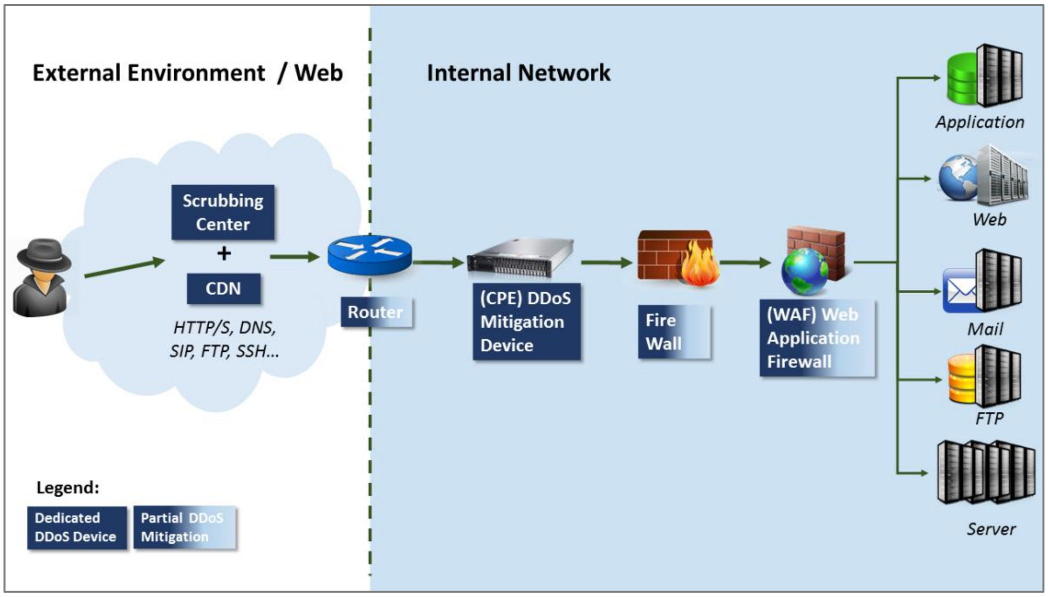


Figure 1 - Typical DDoS Mitigation Setups (Part or all of the above)

The BaseLine DDoS Validation Methodology can be achieved in 2 ways.

Traditional DDoS Pen Testing (One-off with minimal coverage) -

- This is disruptive and needs a 3-hour maintenance window.
- It can only test a maximum of 5 IPs at a time with 18 or less DDoS attack vectors.
- Read more about Traditional DDoS Pen Testing here.

MazeBolt's DDoS Radar® (Ongoing with, Full Coverage) -

- This is **non disruptive**, continuous, 24/7, and can validate the entire network at a time with 100+ (full coverage) DDoS attack vectors.
- Read more about **DDoS Radar®** here.

Traditional DDoS Pen Testing	**MazeBolt's DDoS Radar®**
One off - Simulation of DDoS attacks against the organization.	**Progressively and continuously -** Strengthens an organization against DDoS attacks.
Once or twice a year – This test is run once or twice a year to test DDoS Vulnerabilities.	**Ongoing validation -** 24x7 validates DDoS Mitigation configuration.
Needs a maintenance window – This requires halting of all production on the network to run tests. This is a basic requirement.	**No maintenance window needed** Tests are carried out live on the production network without disruption and so therefore doesn't need any maintenance window.
Handpicked web facing IPs - Pen-tester produces a report (based on downtime) that shows whether the handpicked web facing IPs are being protected by DDoS Mitigation.	**Entire network -** Simulates DDoS attacks on the entire network to identify vulnerabilities and reports on whether the underlying network is being protected through DDoS Mitigation.
Cannot revalidate - If the corrective measures taken to fix DDoS vulnerabilities have not been revalidated, they may not have worked.	**Can revalidate –** Can be checked to ensure that the corrective measures taken to fix the DDoS Vulnerabilities have been fixed and revalidated.

The core reasoning behind BaseLine DDoS validation methodology is **efficiency**. This is done by initially selecting as few DDoS attacks as possible, to give the most value to an organization's defenses as fast as possible.

With **MazeBolt's DDoS Radar®**, the idea is to start fine tuning defenses based on a few typical DDoS attack vectors. When it's confirmed that defenses are defending against all these **19 attack vectors**, the rest of **81+** DDoS attacks are also heavily mitigated. Therefore, less fine tuning is required on an ongoing basis.

The 100+ DDoS attacks are still actively validated against each external internet facing IP.

Traditional DDoS testing can only really give you a couple of snapshots twice a year of your systems vulnerability against 19 DDoS attack vectors, and this is in the best case scenario. It can be thought of as a litmus test of vulnerability validation.

The BaseLine DDoS Validation Methodology utilizes an easy to understand **scoring metric** to communicate DDoS vulnerabilities, making communication between mitigation vendors and clients easy and clear. It also reinforces DDoS mitigation technology to **automatically** mitigate DDoS attacks which organizations are likely to face.

To achieve Baseline DDoS Validation Methodology, MazeBolt has introduced three progressive steps of coverage

Level 1 - BaseLine (Can be achieved with **DDoS Radar®** or with **Traditional DDoS Pen Testing**)
Level 2 - BaseLine⁺ (Only possible with **DDoS Radar®**)
Level 3 - Full coverage (Only possible with **DDoS Radar®**)

WHY MOVE FROM `BASELINE DDOS TESTING' TO `BASELINE DDOS VALIDATION'?

MazeBolt was the **first company** to introduce **BaseLine DDoS testing** in 2013 (now changed to "BaseLine DDoS Validation").

Originally BaseLine DDoS testing, launched 19 **disruptive DDoS attacks** (using **Traditional DDoS Pen Testing**), against an organization's environment, to identify weaknesses in the DDoS mitigation posture.

However, **DDoS Radar® product** has brought a paradigm shift product that makes the traditional method of DDoS Pen Testing almost insignificant.

DDoS Radar® enables the advantages of **Non-Disruptive DDoS validation capabilities** and in turn, the Baseline DDoS Validation Methodology, can be fully achieved **without impacting** the production environment.

In other words, **no maintenance period is required** to validate the **production environment** against all current 19 BaseLine DDoS attack vectors.

This offers up a range of new possibilities.

Due to the very nature of non-disruptive DDoS validation technology the BaseLine DDoS Validation Methodology has been expanded to three progressive **levels of coverage** including:

Level 1 - **BaseLine** - 19 attack vectors.

Level 2 - **BaseLine⁺** - 21 attack vectors.

Level 3 - **Full coverage** - 60 attack vectors.

Today Baseline DDoS Validation Methodology developed by MazeBolt, allows for a faster understanding and a far more accurate remedy of DDoS vulnerabilities, with its patented **DDoS Radar® product.**

DDoS Radar® is a **patented product** that is used to carry out Baseline DDoS Validation Methodology for all **3 Levels** of coverage.

Its capabilities however, are not restricted solely to validation.

Once **DDoS Radar®** (DDR) starts operating alongside a DDoS Mitigation system, it enables a Proactive Feedback Module.

INTRODUCTION TO VPV (VULNERABILITY PROBING VECTOR)

This Proactive Feedback Module continuously, in real-time validates an enterprise's changing production environment and identifies how those changes impact on the in-line DDoS mitigation policies deployed. The proactive feedback module runs 24x7 together with the existing DDoS Mitigation system.

DDoS Radar® through a series of ongoing Vulnerability Probing Vectors (VPV's), investigates the DDoS Mitigation Policy Configurations in production across the web facing IP addresses. It also identifies DDoS vulnerabilities created due to misconfigurations.

- The VPV's at **any point in time** can be **configured** to represent all known attack vectors.
- VPV's power works in a controlled manner to identify DDoS Vulnerabilities **without impacting** an enterprises **production network.**
- This makes it non disruptive and allows it to run continuously.
- VPV's allow for ongoing validation of your production environment. Tens of thousands of DDoS validations continue per annum, to ensure DDoS vulnerabilities are identified and eliminated and revalidated.

BASELINE DDOS VALIDATION METHODOLOGY POWERED BY MAZEBOLT'S DDOS RADAR

Non-disruptive BaseLine DDoS Validation - powered by the **DDoS Radar**® (DDR) product - is a way of validating an enterprise's DDoS mitigation configuration in the production environment 24x7. Its VPV technology ensures that DDoS Mitigation configuration **is always up to date** even during a working environment.

Table 2 - MazeBolt VPV's vs Traditional DDoS Pen Testing Simulation

Parameters	**Traditional DDoS Pen testing simulation**	**MazeBolt's VPV**
Actual DDoS attack traffic against a production environment	Yes	Yes
Requires a maintenance period scheduled due to expectation of downtime on the production environment	Yes	No
Number of Attack Vectors checked during the year e.g. SYN Flood, Brobot attack, HULK etc.	18	100+
Number of IP's (Targets) in a production environment checked annually	< 10 in most cases	Unlimited
Number of individual simulations (VPV or Traditional DDoS Attack vectors) during the year (Simulation = Attack Vector + Target).	~40 (requires disruption)	>24,000 to unlimited (no-disruptions)
Hours per year (8760 hours per year), production DDoS mitigation policies validated for their effectiveness	Maximum of 10 hours	Maximum of 8760 hours
Full Validation Coverage for each IP address, against all DDoS attacks at minimum once a year (assuming even a 50 IP address network) in a production environment.	No (Not even once)	Yes (Many times)
Launched against production IT environment to assess DDoS vulnerability	Yes	Yes
Validation 24x7 of DDoS defences taking place during ongoing production?	No	Yes
Mitigation Effectiveness Understanding does my company receive granular data on how much of the attack traffic leaks through?	No	Yes

BASELINE DDOS VALIDATION METHODOLOGY – 3 LEVELS OF COVERAGE

The MazeBolt DDoS validation methodology is designed to provide organizations with a systematic three phased (**Level 1** – BaseLine, **Level 2** – BaseLine+ and **Level 3** – Full Coverage) progressive approach, to validate that DDoS defenses are working, as required both from a DDoS mitigation and operational perspective.

Different levels of coverage are mentioned below:

Table 3 – Levels of coverage

Level of Coverage	**Phase**	**Goal**	
		DDoS Mitigation Coverage	**Operational**
Level 1 - BaseLine	**Basic** - (Can be accomplished by Traditional DDoS pen testing or **DDoS Radar®**)	19 attack vectors validate that the company's mitigation can **automatically** withstand the most common types of DDoS attacks	**Most common DDoS attack vectors** that validate the main DDoS mitigation mechanisms, responsible for mitigating over 95% of the DDoS attack vectors. Validation aims at DDoS attack vectors getting **automatically mitigated** by the defensive solution deployed, prior to moving onto Baseline$^+$ validation
Level 2 - BaseLine$^+$	**Advanced** - (Can only be accomplished only using **DDoS Radar®**)	**Additional intense 21** DDoS attack vectors to the BaseLine Group for a total of 40 DDoS attack vectors	Provides a **greater extensive validation** of Out-of-State' and anomalous packet mitigation mechanisms as well as validating **additional Layer 7 attacks**
Level 3 - Full Coverage	**Complete coverage –** this is to eliminate sneakier and smarter DDoS attacks. Attacks (Can only be accomplished with **DDoS Radar®**)	**Adds extremely powerful 60+ DDoS attack vectors** to the BaseLine$^+$ Group for a total of 100 DDoS attack vectors	Verifying DDoS mitigation technology can **withstand and adapt to recently evolved sneakier and smarter DDoS Attacks** across the web-facing IP addresses without interrupting the production environment

REQUIREMENTS TO ACCOMPLISH BASELINE DDOS VALIDATION METHODOLOGY

Here are the following requirements to perform Baseline DDoS Validation Methodology:

Traditional DDoS Pen Testing	MazeBolt’s DDoS Radar®
Maintenance Window Required - In over **95%** of testing schedules, regardless of industry or organization size, **downtime is experienced** during this type of testing. That is why this is performed during maintenance time.	**No Maintenance Window Needed -** Level 1 to 3 of coverage doesn’t require a maintenance window. It runs ongoing in the Production Environment and because VPV technology is used, there is **no disruption.**
3 Hours Long - Traditional DDoS 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).	**On Going and Continuous -** Enterprises can continuously run 24x7 in an ongoing manner during validation of DDoS Mitigation. Once the vulnerabilities are fixed by the DDoS Mitigation vendor, enterprises can then re-validate the vulnerabilities once more, to ensure configurations were accurately applied.
Measurement - The goal of any Traditional DDoS Test is to see if an attack vector brings **the system down.** Considering the goal is to bring the system down, KPIs of Traditional DDoS Testing are PROTECTED, PARTIALLY PROTECTED, PARTIALLY VULNERABLE and VULNERABLE. All KPI’s are **determined on downtime & NOT leakage.**	**Measurement -** The goal of VPV KPIs (**DDoS Radar®**) is to understand if the mitigation mechanisms are triggered, through determining leakage. i.e. PROTECTED, PARTIAL PROTECTED, VULNERABLE. All KPI’s are **determined based on actual attack leakage, detection and blocking mechanisms triggers. (No downtime).**
Limited Coverage - validates only the environment for which it is run against. Therefore, if it’s run against a staging environment, the results will likely be different for production.	**Complete Coverage -** This covers all the Internet Facing IP Addresses in real-time, to validate the production environment.
1 Level of coverage offered - i.e. BaseLine coverage is offered with mentioned (below) 19 attack vectors at the BaseLine level. It covers the bare minimum possible validation for Layer 3, Layer 4 and Layer 7 attacks.	3 Levels of coverage are offered - with total 100+ Attack Vectors. MazeBolt believes that with this comprehensive coverage running across the network real-time, this reduces industry standard DDoS Risk from 45% to under 2%. It covers best possible validation for Layer 3, 4 and 7 attacks and attack vectors are refreshed weekly to include latest attack vectors.

ATTACK VECTORS USED IN BASELINE DDOS VALIDATION METHODOLOGY

Coverage Level 1 – BaseLine

BASELINE					
#	DDoS Attack Vectors	DDoS Attack Layer	#	DDoS Attack Vectors	DDoS Attack Layer
1	ACK-PSH Flood	Layer 4	11	ICMP_PING Flood	Layer 3
2	All TCP Flags Flood	Layer 4	12	IP Fragmented Garbage	Layer 3
3	Brobot HTTPS Simulation	Layer 7	13	RST Flood	Layer 4
4	Brobot Simulation	Layer 7	14	Slowloris Test	Layer 7
5	Empty Connection Flood(R)	Layer 4	15	SSL Negotiation Flood	Layer 7
6	FIN Flood	Layer 4	16	SYN Flood	Layer 4
7	HTTP Flood - Browser Simulation	Layer 7	17	UDP Flood	Layer 4
8	HTTP Flooder	Layer 7	18	UDP Garbage Flood	Layer 4
9	HTTPS Flood - Browser Simulation	Layer 7	19	URG Flood	Layer 4
10	HTTPS Flooder	Layer 7			

Coverage Level 2 – BaseLine^{+}

Baseline^{+}					
#	DDoS Attack Vectors	DDoS Attack Layer	#	DDoS Attack Vectors	DDoS Attack Layer
20	ACK Flood	Layer 4	31	RST-SYN Flood	Layer 4
21	ACK-FIN Flood	Layer 4	32	THC-SSL Test	Layer 7
22	ACK-RST Flood	Layer 4	33	URG-ACK Flood	Layer 4
23	ACK-SYN Flood	Layer 4	34	URG-ACK-PSH-RST Flood	Layer 4
24	DNS	Layer 7	35	URG-ACK-RST Flood	Layer 4
25	DNS Response	Layer 7	36	URG-FIN Flood	Layer 4
26	HTTP Range	Layer 7	37	URG-PSH Flood	Layer 4
27	ICMP Destination unreachable Flood	Layer 3	38	URG-PSH-FIN Flood	Layer 4
28	PSH-RST Flood	Layer 4	39	URG-PSH-SYN-FIN Flood	Layer 4
29	PSH-RST-FIN Flood	Layer 4	40	URG-RST-FIN Flood	Layer 4
30	PSH-RST-SYN Flood	Layer 4			

Coverage Level 3 – Full Coverage

Full Coverage								
#	DDoS Attack Vectors	DDoS Attack Layers	#	DDoS Attack Vectors	DDoS Attack Layers	#	DDoS Attack Vectors	DDoS Attack Layers
41	URG-RST-SYN-FIN Flood	Layer 4	61	PSH-RST-SYN-FIN Flood	Layer 4	81	URG-PSH-RST-FIN Flood	Layer 4
42	AB - Apache HTTP server benchmarking tool	Layer 7	62	PSH-SYN Flood	Layer 4	82	URG-PSH-RST-SYN Flood	Layer 4
43	ACK-PSH-FIN Flood	Layer 4	63	PSH-SYN-FIN Flood	Layer 4	83	URG-PSH-RST-SYN-FIN Flood	Layer 4
44	ACK-PSH-RST Flood	Layer 4	64	URG-ACK-PSH-RST-FIN Flood	Layer 4	84	URG-PSH-SYN Flood	Layer 4
45	ACK-PSH-RST-FIN Flood	Layer 4	65	URG-ACK-PSH-RST-SYN Flood	Layer 4	85	URG-RST Flood	Layer 4
46	ACK-PSH-RST-SYN Flood	Layer 4	66	URG-ACK-PSH-SYN Flood	Layer 4	86	URG-RST-SYN Flood	Layer 4
47	ACK-PSH-RST-SYN-FIN Flood	Layer 4	67	URG-ACK-PSH-SYN-FIN Flood	Layer 4	87	URG-SYN Flood	Layer 4
48	ACK-PSH-SYN Flood	Layer 4	68	URG-ACK-RST-FIN Flood	Layer 4	88	URG-SYN-FIN Flood	Layer 4
49	ACK-PSH-SYN-FIN Flood	Layer 4	69	URG-ACK-RST-SYN Flood	Layer 4	89	GET Request Flood*	Layer 7
50	ACK-RST-FIN Flood	Layer 4	70	URG-ACK-RST-SYN-FIN Flood	Layer 4	90	POST Request Flood*	Layer 7
51	ACK-RST-SYN Flood	Layer 4	71	URG-ACK-PSH-RST-FIN Flood	Layer 4		Hash Collision Flood*	Layer 7
52	ACK-RST-SYN-FIN Flood	Layer 4	72	URG-ACK-PSH-RST-SYN Flood	Layer 4	92	Dynamic GET Flood*	Layer 7
53	ACK-SYN-FIN Flood	Layer 4	73	URG-ACK-PSH-SYN Flood	Layer 4	93	Dynamic POST Flood*	Layer 7
54	DNS SEC	Layer 7	74	URG-ACK-PSH-SYN-FIN Flood	Layer 4	94	DELETE Request Flood*	Layer 7
55	Empty Connection Flood(F)	Layer 4	75	URG-ACK-RST-FIN Flood	Layer 4	95	HEAD Request Flood	Layer 7
56	GoldenEye HTTP Test	Layer 7	76	URG-ACK-RST-SYN Flood	Layer 4	96	PUT Request Flood*	Layer 7
57	HULK Flood	Layer 7	77	URG-ACK-RST-SYN-FIN Flood	Layer 4	97	CONNECT Request Flood*	Layer 7
58	ICMP_Time_exceeded Flood	Layer 3	78	URG-ACK-SYN Flood	Layer 4	98	OPTIONS Request Flood*	Layer 7
59	PSH Flood	Layer 3	79	URG-ACK-SYN-FIN Flood	Layer 4	99	TRACE Request Flood*	Layer 7
60	PSH-FIN Flood	Layer 4	80	URG-PSH-RST Flood	Layer 4	100	PATCH Request Flood*	Layer 7

WHAT YOU GET – THE BENEFITS OF BASELINE DDOS VALIDATION METHODOLOGY

BaseLine DDoS Validation Methodology offers a variety of benefits.

It **strengthens** enterprises DDoS Defenses. It identifies vulnerabilities and helps in **fine tuning DDoS Mitigation configurations**. The objective of BaseLine DDoS Validation Methodology is to **reduce DDoS risk fast,** by ensuring that the underlying network is defended by DDoS Mitigation deployed.

Efficiency of existing DDoS Mitigation is **increased**, and DDoS Risk is **reduced** with the help of Reporting and Measurable KPIs as explained below:

Efficiency

BaseLine DDoS Validation Methodology is a useful way to understand the state of existing DDoS Mitigation defenses and improves the defenses based on thorough analysis.

Traditional DDoS Pen Testing	MazeBolt’s DDoS Radar®
Testing a few IPs - DDoS Mitigation vulnerabilities are identified by testing marginal IPs.	**Validates all Internet facing IPs -** DDoS vulnerabilities are identified across the production network irrespective of its global location.
Finetuned one-off but NOT revalidated - DDoS Mitigation is fine tuned for the few identified vulnerabilities.	**Finetuned and revalidated ongoing -** DDoS Mitigation is fined-tuned for vulnerabilities to be identified and revalidated, and to ensure that they are fixed.
3 hours with major disruption - Tests are carried out on IPs with 3 hours maintenance and using the involvement of the entire team. This requires a lot of manual intervention.	**24x7 and without disruption –** The entire network remains in live production, the environment is validated ongoing and without interruption. No manual intervention is needed to simulate DDoS Attack Vectors.
Limited reporting for technical team - In-house security teams receive an easy to understand report on vulnerabilities and can fix them with the help of mitigation vendor.	**Intelligent reporting for Executives and technical teams -** and Executives can measure the progress month on month for the vulnerability gaps and justify investments & security Level. In-house security teams can understand exactly where (every IP wise analysis) the DDoS Vulnerability is. This is then communicated effectively with DDoS Mitigation Vendor and revalidated once the mitigation vendor fixes vulnerability.
Reports can be used for one-time analysis only - As tests performed are on select IPs only during maintenance period, reports are valid for a limited time and cannot be used again.	**Continuous analysis makes reports relevant all the time -** Reports present a single dashboard of vulnerabilities across the globe for subsidiaries, businesses, and locations. Since tests performed are ongoing and continuous, they are valid for analysis all the time.

DDoS Risk Reduction

Traditional DDoS Pen Testing	MazeBolt's DDoS Radar®
~31% Ongoing Risk	<2% Ongoing Risk
DDoS risks are mitigated for a limited time - but get new risk is generated quickly as the underlying production network continuously changes. Therefore, the network remains at risk of around 31% ongoing at best.	**DDoS risks are 24/7 continuous and in real-time mitigation -** to keep them under 2% ongoing.
Frequency Once or twice in a year - is the maximum that testing can be carried out, as money is lost during downtime.	**Continuous, ongoing, 24/7 Frequency –** to validate DDoS mitigation across the network.
Coverage of testing is limited to approximately 5 IPs or a few more, leaving other IPs unassessed and **assumed** that the few tested IPs represent the entire attack surface.	**Coverage is the entire attack surface in live production** environment validated to leave **no** chance for **assumptions**.
Downtime required - In order to test the production network, downtime is essential	**No Downtime needed -** Live production network in action is validated against basic, new sneakier and sophisticated DDoS attacks.
Revalidation is not possible: Revalidation of fixed DDoS vulnerabilities **is not possible** forcing organizations to trust that measures taken have closed all vulnerabilities.	**Revalidation is possible:** Once the vulnerabilities are fixed by DDoS Mitigation vendor, they are re-validated to ensure that no further vulnerabilities are open to exploitation.

Reporting

Traditional DDoS Pen Testing offers reporting during testing time. The reports show attack traffic metrics, such as, PPS (Packets Per second), Gbps (Gigabits per second), CPS (Connections Per second).

Traditional DDoS Pen Testing shows a UDP Garbage Flood as illustrated in the screenshot below:

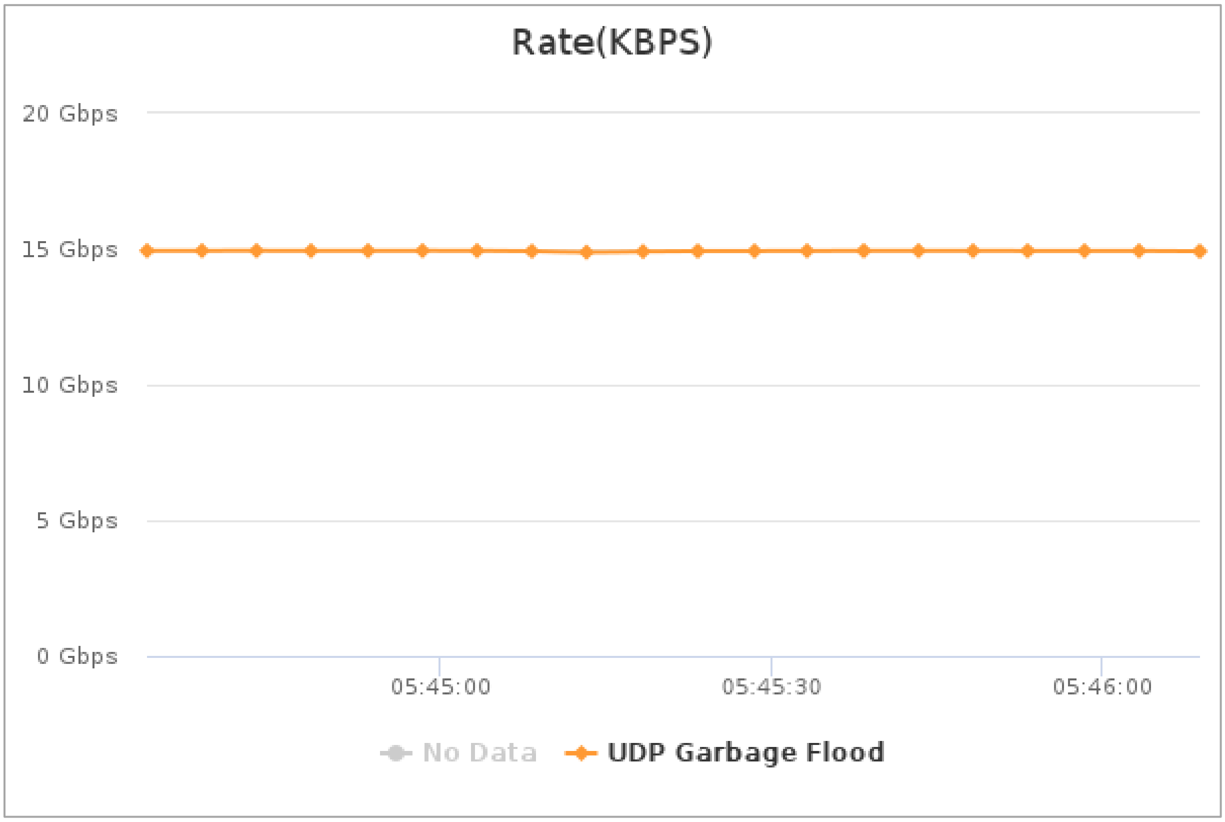


Figure 2 - Screenshot of Traditional DDoS Pen Testing Module

MazeBolt's DDoS Radar®

Offers complete transparency and easy to understand clear metrics. It offers tangible progress in DDoS mitigation vulnerability postures, for executives to monitor the milestones that have been achieved against the goal to be achieved. At the same time, it offers concise information for cybersecurity teams to undertake the task of communicating vulnerability scenarios with DDoS Mitigation vendors. Below is a glimpse of several screenshots:

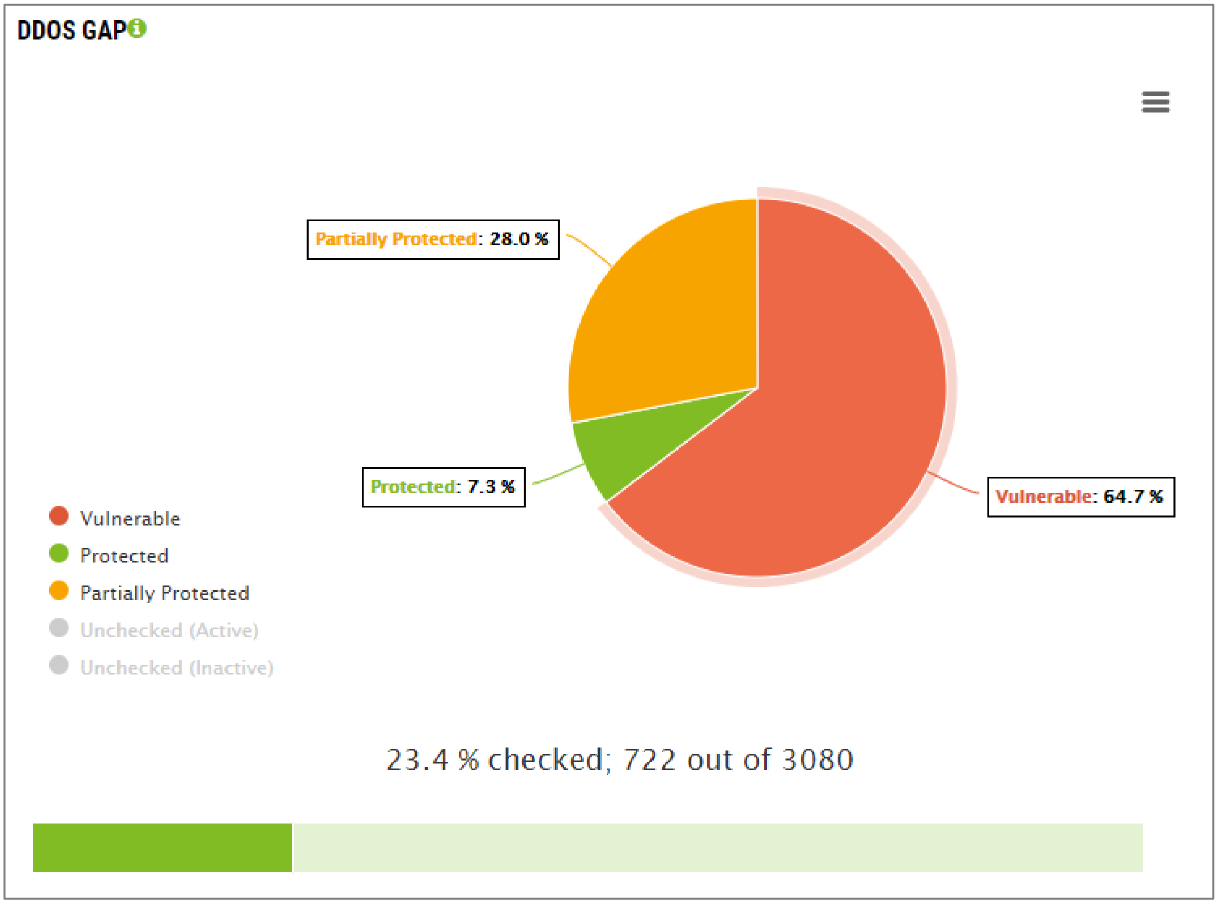


Figure 3 - Ongoing – Current DDoS Gap status report

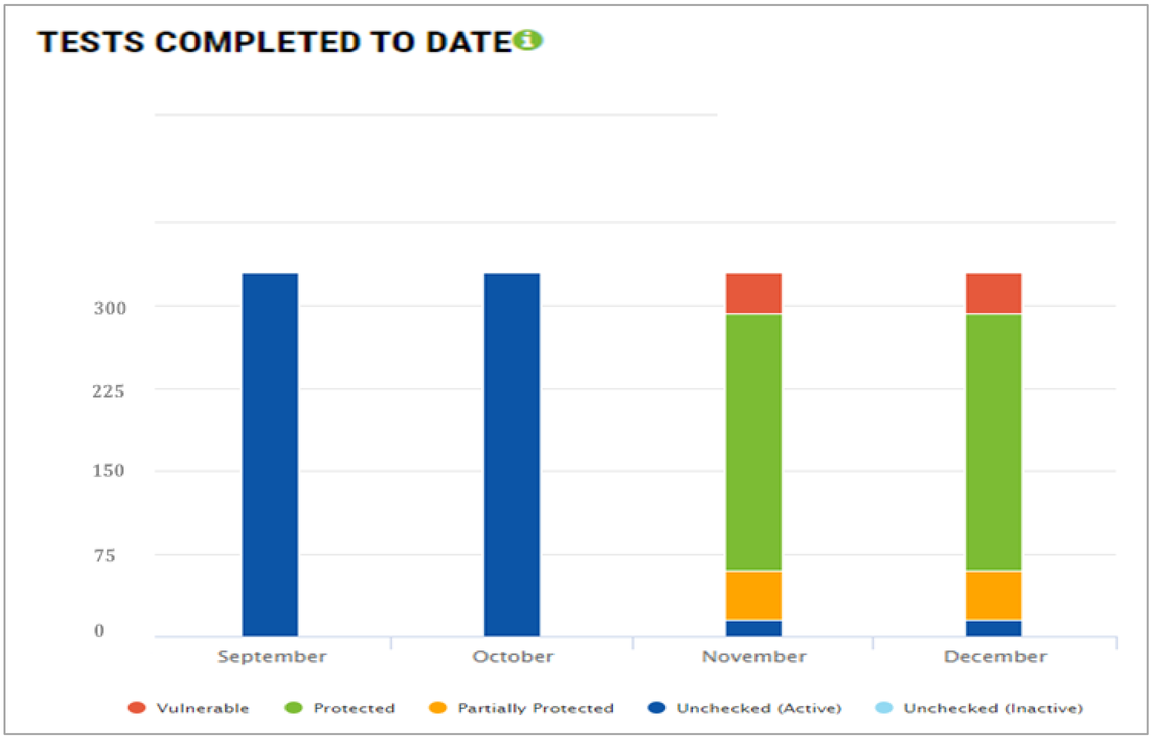
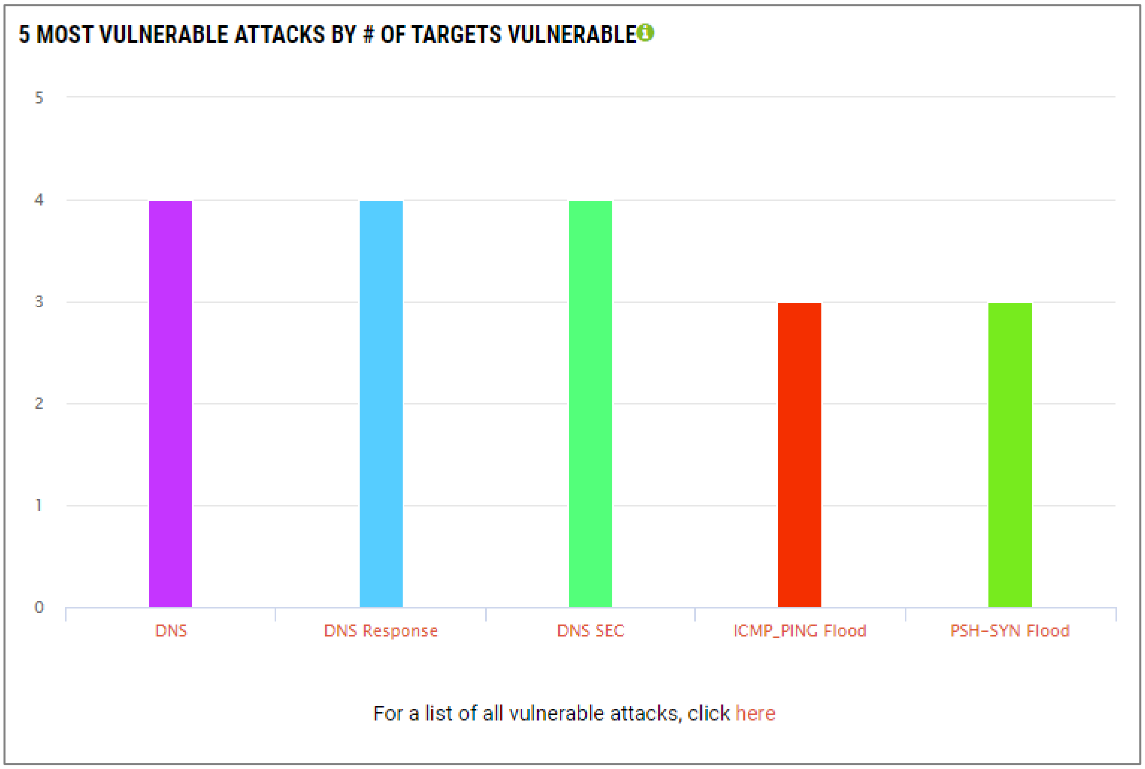


Figure 4 – Ongoing Monthly Report



For a list of all vulnerable attacks, click here

Figure 5 – Ongoing – Overview of most vulnerable attack vectors

Each VPV has its attacker sending and received metrics stored in the MazeBolt UI

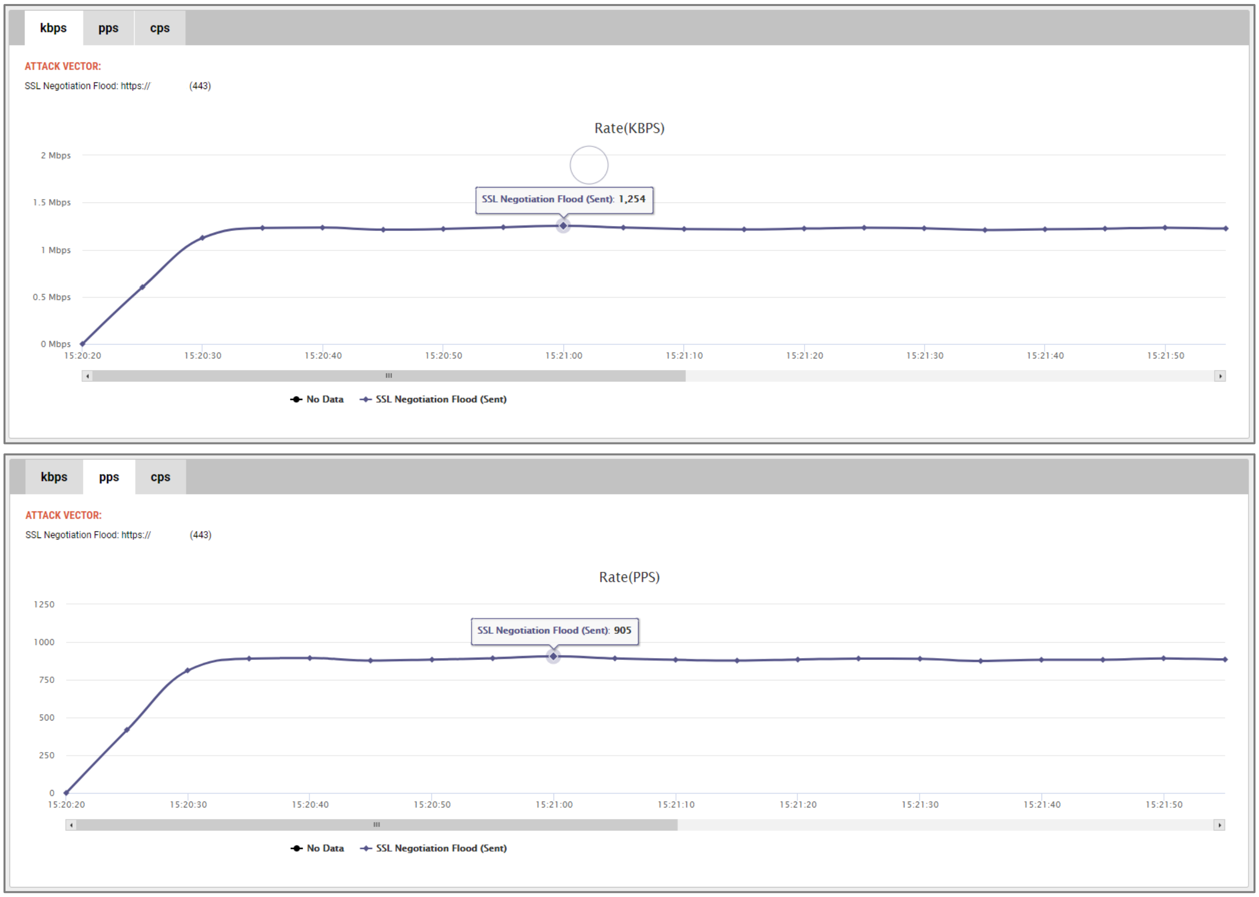


Figure 6 - An ACK-PSH-RST flood's recording

Additionally, while the VPV was running, *response monitoring* is being recorded,which in turn shows the response time average from 3 different continents where the services are being monitored.

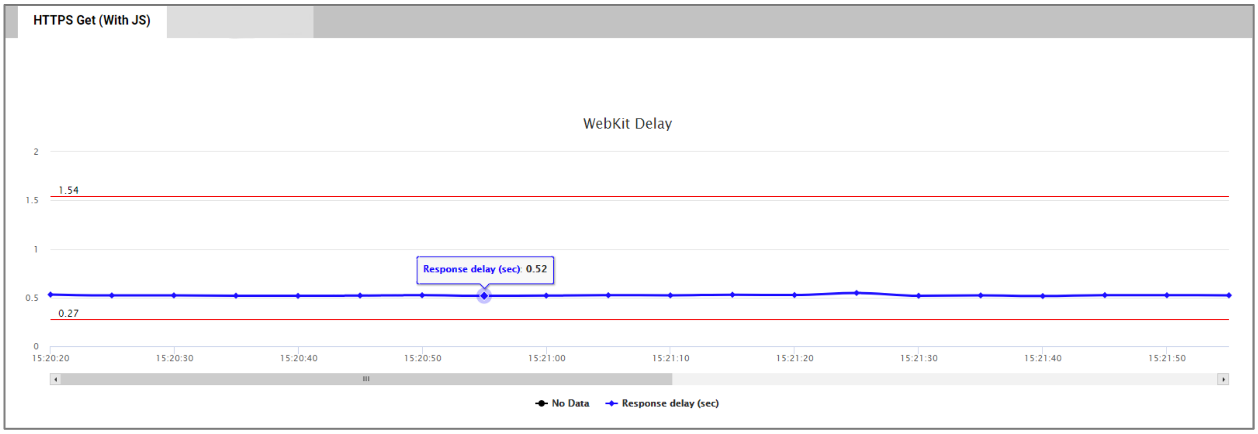


Figure 7 – Response Monitoring

Measurable Key Performance Indicators (KPIs)

It should be noted that:

Traditional DDoS Testing KPI's are decided upon whether the system **remains up or goes down by specific DDoS attack vector**.

DDoS Radar® concludes results by **analyzing how much traffic leaks through DDoS mitigation systems**.

Most importantly, Baseline DDoS Validation Methodology reports clearly indicate strengths and weaknesses of any DDoS Mitigation system deployed (Scrubbing or CPE). It also allows customers to analyze the traffic behavior, packets sent and received, and overall analysis of the validations performed.

With Traditional DDoS Pen Testing

The goal of traditional DDoS Pen Testing is to **bring the system down** using varied DDoS Attack vectors, its Key Performance Indicators (KPI's) are mentioned below:

Table 4 - KPIs of Traditional DDoS Pen Testing

Result	Description
PASS	The site/service was not affected, and the network devices were not affected. Mitigation was automatic.
PARTIAL PASS	Passed overall. The site or 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 or 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. The site or service being tested was mostly down.
FAIL	The site went down and stayed down. There was no mitigation throughout the test.

With MazeBolt's DDoS Radar®

For each MazeBolt's **DDoS Radar®** report, one of the following metrics is assigned in the final report the organization receives. It should be noted that, these **KPIs are based on how much traffic was successfully passed during the attack.**

Table 5 - KPIs of MazeBolt's DDoS Radar

Result	Description
PROTECTED	This KPI indicates that the attack was mitigated and there was no disruption to the IT service tested.
PARTIALLY VULNERABLE	The attack may have been mitigated, however, there was some slowdown to the service tested. This would further mean that the slowdown was probably due to some mitigation defensive mechanism triggering. Alternatively, it could be a very weak device in the chain of DDoS defenses or a false positive with one or more of the defenses blocking legitimate traffic.
VULNERABLE	The DDoS attack simulation traffic generated reached the targeted IT service. It means that this DDoS attack vector would most likely cause disruption or complete downtime to the IT service targeted. The infrastructure is vulnerable to this DDoS attack vector.

WHAT `IF' SCENARIOS – EVALUATE YOUR NEED FOR BASELINE DDOS VALIDATION

1. What happens when my IT infrastructure is unavailable because of a successful attack?
   a. Is there a financial impact?
   b. Is there a customer retention impact?
   c. Can this type of PR effect current business or new customers?
   d. Is downtime a possibility in my business (even a minute)?
2. What if my cyber management systems are disconnected from my central and my satellite locations due to a DDoS attack?
   a. At that point can risks be identified in other locations and the central location?
   b. Can an ongoing attack be analyzed in real-time?
   c. In order to assist in defending against the attack real-time can information be provided to the vendor quickly and in real-time?
3. If I'm the subject of a ransom request for $100K or DDoS attack, can I confidently not pay the criminals and not face severe ongoing downtime?
   a. In the decision-making process is there data on-hand to explain to management?
   b. Is there a visibility into a complete DDoS risk across the organization in real-time?
   c. Are services vendors, or SLA's online technology working to prevent long and protracted downtime?
   d. If the intermittent downtime lasts for the next few days, will it impact cost and profits?
4. When a DDoS attack hits my 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)?
5. 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 this is the case, could previously un-exploited vulnerabilities now be exploited?
   b. Will a DDoS attack severely limit the ability to control security apparatus devices deployed worldwide over VPN's if my main NOC is under attack?
6. 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.

If, however, any of the above questions are of potential concern to your company, it means you should be utilizing the BaseLine DDoS Validation method.

CONCLUSION OF BASELINE VALIDATION METHODOLOGY

- ✓ MazeBolt Baseline DDoS Validation Methodology is the **de-facto industry standard** of DDoS testing.
- ✓ BaseLine DDoS validation method **strengthens resistance to DDoS attacks** through a standardized DDoS testing methodology.
- ✓ Baseline DDoS Validation Methodology **eliminates DDoS Risk** (varied depending on how it is executed by either Traditional DDoS pen testing or **DDoS Radar®**)
- ✓ With **DDoS Radar®**, enterprises can **validate** their **entire production** environment **24x7**, across internet facing IPs **continuously without any disruption**, for BaseLine Validation method's Level 1,2 and 3.
- ✓ **Fortune 500 and NASDAQ listed companies trust** the MazeBolt standard of the BaseLine DDoS Validation Methodology.
- ✓ Baseline DDoS Validation Methodology 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 Validation Methodology is **continuously reviewed** to ensure its **relevance to the threats** our customers face daily.

Any organization that has any uptime SLA/internal assumptions cannot know **any** of their resistance to DDoS attacks without having performed at least a single BaseLine DDoS validation test Level 1.

The BaseLine DDoS validation method, facilitated through **DDoS Radar®**, **eliminates DDoS risk almost entirely**.

No maintenance time is needed to carry out all 3 levels of the BaseLine DDoS Validation Methodology with progressive steps.

It is **non-disruptive** to the production environment and **validates it in real-time**.

ABOUT MAZEBOLT

MazeBolt is a company that specializes in **proactive DDoS mitigation technologies**, which currently **include DDoS Radar®** and Traditional DDoS pen testing.

MazeBolt's patented technology eliminates DDoS Risk through installing its **DDoS Radar®** technology (Proactive Feedback Module) in an enterprise's DDoS Mitigation.

For any enterprise responsible for 24/7 service availability **downtime isn't an option**.

Existing DDoS Mitigation solutions cannot detect vulnerabilities originating from changes made to the production environment network and IT services. This leaves companies with an average of 48% DDoS risk.

DDoS Radar® - a **patented technology**, is an essential Proactive Feedback Module that completes any in-line, production, DDoS mitigation system. This allows companies to safely make ongoing changes to their production environment's underlying networks and IT services, while eliminating DDoS risk.

The **DDoS Radar®** supports the following:

1. **DDoS Vulnerabilities are identified continuously in the live production environment** – Validation takes place continuously 24x7 (across the network) and is kept under 2% ongoing without disruption to live operations.
2. **New DDoS mitigation GAPs are instantly identified -** with a Proactive Feedback Module. Once discovered DDoS vulnerabilities can be closed and then again verified against closure, using the Proactive Feedback Module.
3. **Actionable insight -** Network security personnel or DDoS mitigation vendors, provide visibility, by showing everyday reports that are easy to understand.
4. They are user friendly and are necessary to resolve identified DDoS Vulnerabilities.
5. **Executive reports - every** quarter there will be clear indicators of the performance of DDoS Mitigation with past vulnerabilities, vulnerabilities fixed, milestones achieved and current DDoS Risk.

Visit us at: www.mazebolt.com