MAZEBOLT

2018

Tailoring DDoS Mitigation to Your Needs

www.mazebolt.com

Table of Contents

Table of Figures

MazeBolt Introduction

MazeBolt is a cybersecurity threat-assessment company that strengthens enterprises' resistance to cyber-attacks. MazeBolt's pioneering DDoS Testing & Phishing Simulation & Awareness solutions are used by Fortune 1000 & NASDAQ-listed companies in over 50 countries.

MazeBolt's leading DDoS Testing solutions cover both:

Traditional DDoS Testing:

The commonly available DDoS Testing technology that is disruptive to ongoing operations and requires maintenance windows. MazeBolt's traditional BaseLine DDoS Testing Methodology – the ***de-facto*** industry standard – is the most effective method of traditional testing that provides validation of over 95% of all DDoS attack vectors in just 3 hours.

****NEW** Non-Disruptive DDoS Testing**:

MazeBolt's **DDoS Radar** has ZERO impact on ongoing operations that allows it tests a company's entire networks against hundreds of DDoS attack vectors continuously 24/7. MazeBolt's patent pending DDoS Radar is the only DDoS testing method that unlike traditional DDoS Testing (that is limited in time (maintenance window) and network (up to 5 IPs)), provides a unique, comprehensive answer to the challenge of DDoS prevention.

"The more complex your DDoS mitigation system is, the more likely failure will be due to configuration issues."

Matthew Andriani, CEO, MazeBolt

Executive Summary

Generally the more complex the mitigation system, the more likely failure will be due to configuration issues. This is because most Enterprise IT organizations don't have the time or resources to ensure that every part of their DDoS Mitigation posture is updated, integrated, and running the right settings for their specific environment.

No matter what the level of complexity or robustness, your mitigation system most likely has some combination of the following components:

- Scrubbing Center (BGP)
- Content Delivery Network (CDN)
- Vendor Appliances (CPE Equipment)
- Intrusion Detection System/Intrusion Prevention System
- Web Application Firewall

This document reviews the most common network devices from the DDoS mitigation perspective to provide clarity regarding the role each element plays in mitigating DDoS attacks.

Questions this document answers:

- Do WAFs, Firewalls and Load balances protect against DDoS Traffic?
- What is the difference between an Intrusion Prevention System (IPS) and a DDoS mitigation system?
- Does a CDN completely replace DDoS mitigation?
- What are the crucial systems my specific network needs for optimal DDoS mitigation?
- Does cloud based mitigation (scrubbing) deprecate on-prem DDoS mitigation?

Components of a DDoS Mitigation System

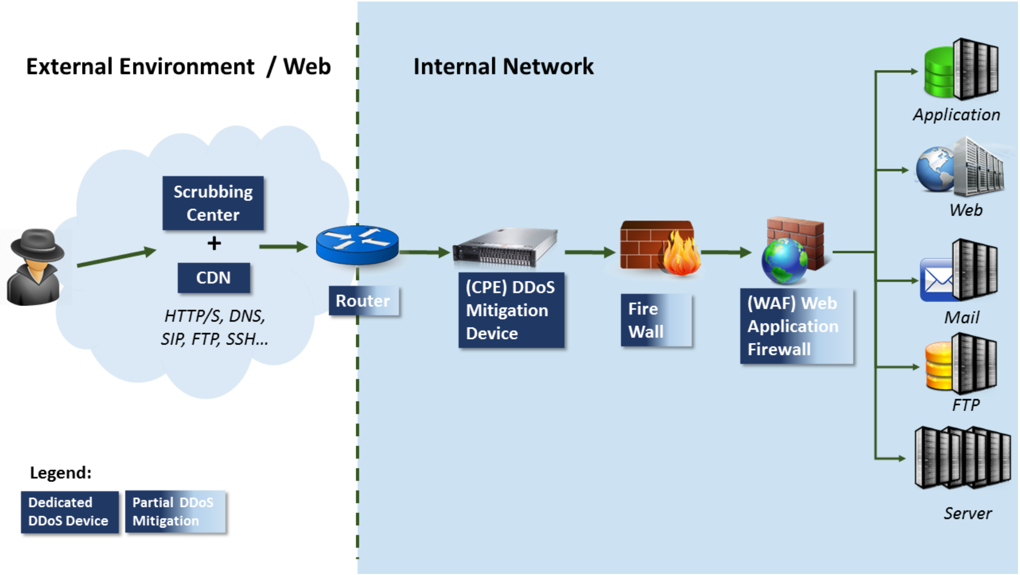
There are generally three types of DDoS mitigation postures: Cloud based, On-Prem solutions, and lastly, hybrid combinations of the two. Each has its own advantages and disadvantages and the decision of which to use largely depends on the company's infrastructure.

Most mitigations systems consist of a combination of components. This combination is essential because each component is proficient in responding to different types of attacks.

Most companies today opt for a hybrid setup. At the very least they would include a scrubbing center to protect their bandwidth. Without it, their internet pipe is very likely to be easily saturated, even if the attack traffic does not enter their internal network.

That being said, companies that host their infrastructure exclusively in the cloud (AWS, Google, Azure) cannot have on-prem mitigation devices (as they just don't have an infrastructure premises), but should still have a scrubbing center.

Figure 1: Illustration of a Typical Hybrid DDoS Mitigation Posture



Approaches to Mitigation Activity

DDoS mitigation generally takes one of two approaches:

- Proactive, “always on” – Goes into effect automatically. All traffic is inspected, and suspicious traffic is separated out before it gets to your infrastructure, preventing it from going down.
- Reactive, “on demand” – Also known as Monitoring Mode. Components that take this approach do not block automatically, they monitor and wait for a block order. This isn’t always automated, which means by the time the mitigation provider discovers the problem – often reported via a client calling the customer service line – it may be too late to prevent downtime.

Cloud Based Solutions

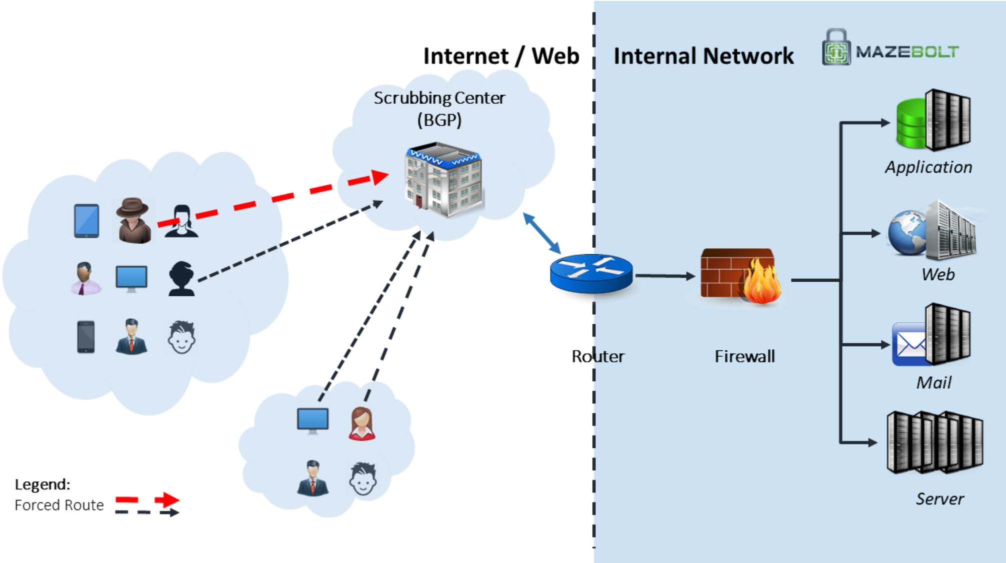
1. Scrubbing Center

Component Snap Shot	Deployment Location:	**Cloud-based**
	Functional Role:	**Scalable Data Cleanser**
	DDoS Mitigation Capabilities:	**Layer 3 & 4** – Strong **Layer 7** – Conditional on SSL visibility

Most scrubbing centers are cloud-based. They are the first source of defense for most volumetric attacks, which send an enormous number of packets in an attempt to overwhelm your network resources and saturate bandwidth.

Most Application Layer (Layer 7) traffic is encrypted, this means that the ability of a scrubbing service to effectively mitigate malicious Application Layer traffic is highly dependent on whether it has the relevant decryption keys – i.e. “SSL Visibility”.

Figure 2: Illustration of a Cloud Scrubbing Service



Scrubbing centers are essentially data cleansers – They review traffic going through them and remove packets that don’t adhere to the rules and guidelines defined.

The reason they are used mostly against large volumetric attacks is because of their ability to scale and match even some of the largest floods exceeding 10Tbps.

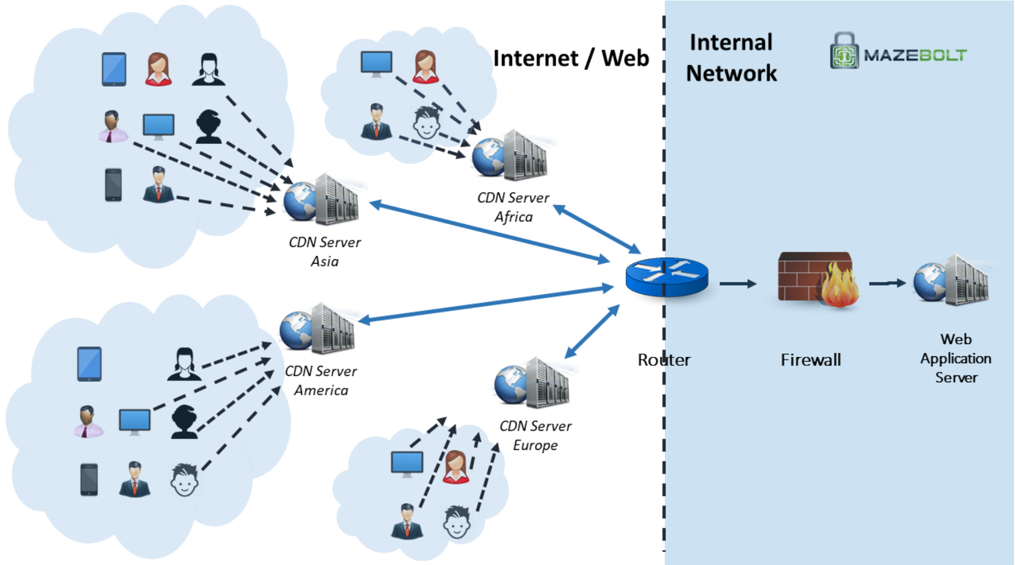
Scrubbing centers generally use the Border Gateway Protocol (BGP). BGP routes traffic according to rule-sets, policies and metrics. It forces all traffic to go through the scrubbing center, where the incoming attack traffic is cleaned before being forwarded to the organizations' IT infrastructure. Using a scrubbing center will protect an organization against an attacker targeting the name (DNS name) of your organization or the numerical IP address.

2. Content Delivery Network (CDN)

Component Snap Shot	Deployment Location:	**Cloud-based**
	Functional Role:	**Static Content Serving**
	DDoS Mitigation Capabilities:	**Good - Situational**

Content Delivery Networks (CDNs) use the DNS (Domain Name System) protocol to route traffic through the CDN provider's system.

Figure 3: Illustration of a Content Distribution Network (CDN)



In its most basic form, a Content Deliver Network is used to improve your customers' access to your website's content. CDNs cache some of the site's resources, and only forward requests it cannot handle, that is, only Layer 7 traffic. Incidentally, that means that Layers 3 and 4 traffic is never forwarded by a CDN to the organization's IT infrastructure, thus protecting it against volumetric attacks.

However, CDNs will only protect organizations against attacks that use the DNS names as their target. For example: An attacker targeting www.bankingplusonline.com will be forced to go through the CDN. But, if the attacker targets the same organization by inputting the site's IP address directly, i.e. 10.249.3.2 – you are not protected because your CDN provider never even sees the attack.

A CDN can only be a part of a bigger DDoS mitigation scheme. Usually more advanced attackers can find and attack the source IP of the website directly, circumventing the CDN completely.

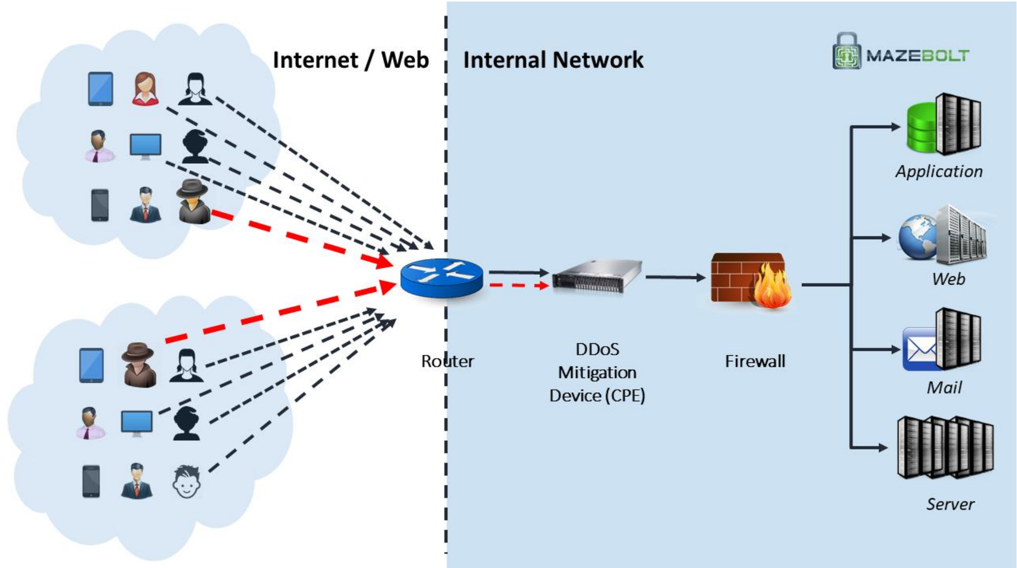
On-Prem. Based Solutions

3. Vendor Appliances (Customer Premises Equipment - CPE)

Component Snap Shot	Deployment Location:	**On-Prem.**
	Functional Role:	**DDoS Mitigation and Protection**
	DDoS Mitigation Capabilities:	**Strong**

Vendor appliances contain a variety of proprietary technologies, but, at their core, they are all tuned to detect and stop DDoS attacks. DDoS CPE equipment is generally located at the very edge of the organizations network, after the router but before reaching the internal network infrastructure, E.g. Firewalls, Load Balancers etc.

Figure 4: Illustration of Dedicated On-Prem DDoS Mitigation Equipment



The appliances vary from being a combination of other components – to being a completely proprietary device consisting of highly specialized software and hardware fine-tuned to protect against DDoS attacks.

Many of the devices deliver in-depth traffic analysis, bandwidth monitoring, and anomaly reports, allowing for better network traffic planning and DDoS attack analysis. Detection of malicious packets triggers filters, that only allow the legitimate traffic to get through. Post-attack forensics may provide lessons learned, so the systems can be better tuned for mitigation of future attacks.

Processing speed varies among vendors, with some offering over 100Gbps throughput.

With the increasing use of AI, vendors are including more specialized detection software based on behavioral analysis, better-tuned anomaly detection, and active intelligence gathering.

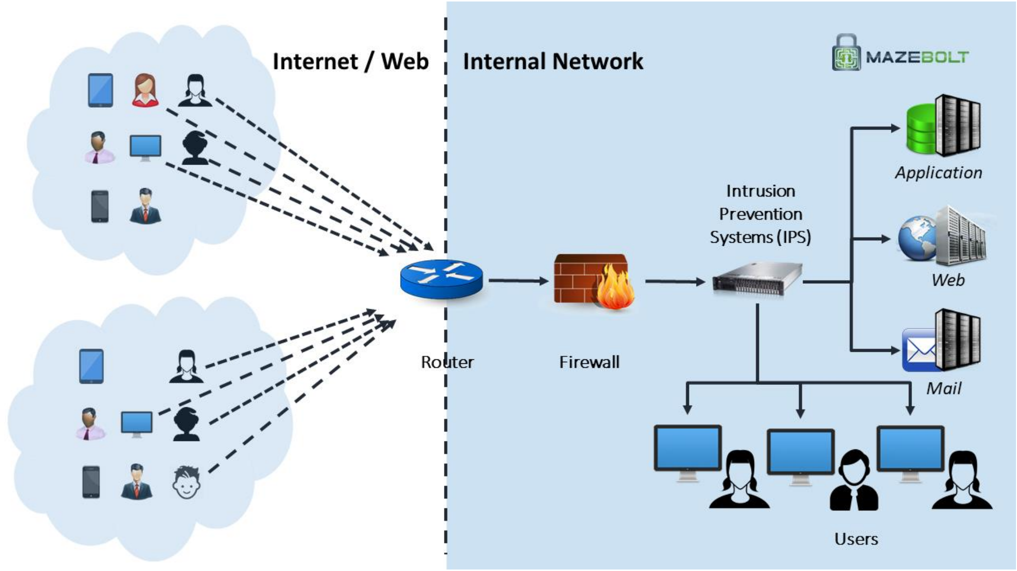
CPE equipment without a scrubbing center will not protect against large volumetric attacks, even if the CPE equipment is well configured. The CPE alone will not provide protection against internet pipe saturation.

4. Intrusion Prevention Systems (IPS)

Component Snap Shot	Deployment Location:	**On-Prem.**
	Functional Role:	**Detecting and Stopping Cyber Attacks**
	DDoS Mitigation Capabilities:	**Poor**

These appliances specifically monitor suspicious activities within the network. They can be part of the router system, integrated into the firewall, serve as a back-up to a firewall, or sit deeper within the network infrastructure.

Figure 5: Illustration of an Intrusion Prevention System (IPS)



They inspect and scan packets based on pre-existing rule sets, signatures, protocol status, or anomaly detection, creating alerts and/or blocking when any type of cyberattack is suspected.

The underlying design is focused on blocking security breaches, and is not set to stop a DDoS attack. These systems generally have some layer 3, 4 and 7 protection capabilities, but can only be used to help filter out leakage from components up stream, or potentially to block prolonged Layer 7 attack campaigns.

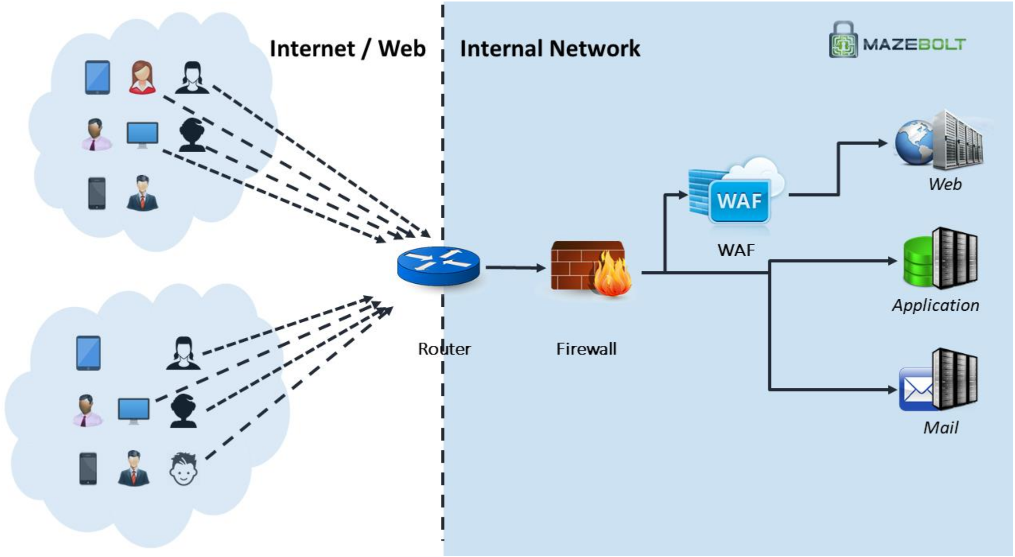
Generally most DDoS attacks cannot be mitigated using IPS systems and having to use an IPS system to block an attack most likely means the organization targeted is under a very advanced DDoS attack campaign in which CPE and or scrubbing center services are failing to mitigate Layer 7 attack traffic.

5. Web Application Firewalls (WAFs)

Component Snap Shot		
	Deployment Location:	**On-Prem./Cloud-based**
	Functional Role:	**Protection against Layer 7 Application Attacks**
	DDoS Mitigation Capabilities:	**Mild**

WAFs perform multiple functions – intrusion detection and DDoS attack detection and prevention. They analyze application traffic, distinguishing potential risks from legitimate usage, controlling access to applications or services by applying a set of rules to incoming HTTP traffic. They perform deep-packet inspections, locating, identifying, classifying, rerouting and/or blocking packets with specific data or code payloads.

Figure 6: Illustration of a Web Application Firewall (WAF)



WAFs depend on white-listing and black-listing, which means they must be updated continuously. Legitimate user traffic will be allowed through, while suspicious traffic will be routed elsewhere for further inspection or simply blocked.

The web application firewall can be customized to your applications. For example, protecting from certain attacks against functionality – they generally protect against layer 7 attacks, which directly affect applications. The inspection process does increase latency and affects the user experience, so efficiency is key.

The WAF can also be cloud-based via a service provider like AWS. Still, it generally does not protect against volumetric attacks on layers 3 and 4 that target network availability.

6. Load Balancer

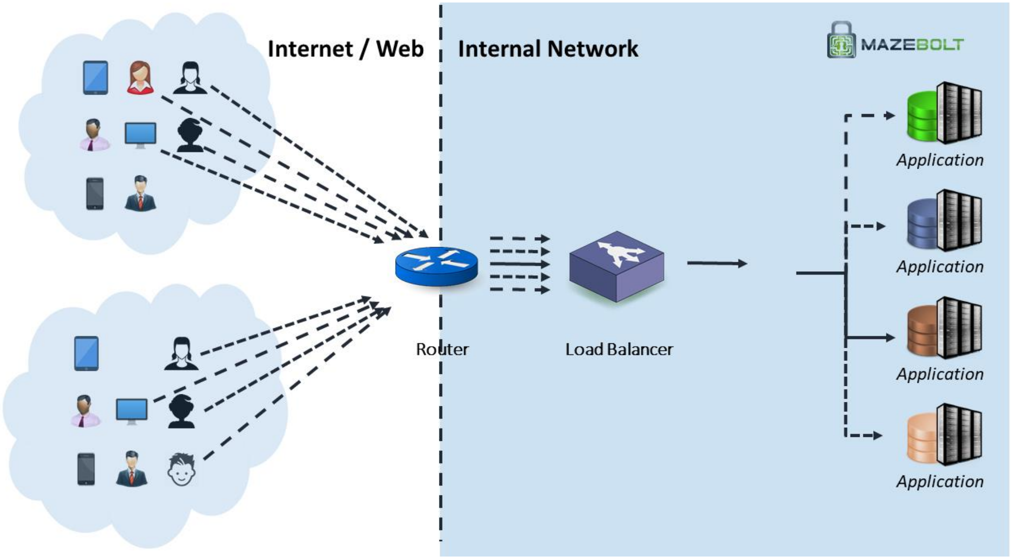
Component Snap Shot		
	Deployment Location:	**On-Prem.**
	Functional Role:	**Distributing Incoming Traffic**
	DDoS Mitigation Capabilities:	**Poor**

A Load Balancer receives traffic from many clients and distributes that traffic evenly between multiple application servers of the same type. In many cases multiple servers are preferred over a single stronger server for the increased reliability and availability they provide.

A Load Balancer acts as a man-in-the-middle. Clients connect to it on one end, and the load balancer creates a connection to one of the application servers on behalf of the client. In this way, the load balancer has to keep track of every connection's state i.e. the load balancer is a stateful device.

Like many other stateful devices, the load balancer is vulnerable to state-table saturation attacks e.g. HTTP attacks and a SYN flood.

Figure 7: Illustration of a Load Balancer



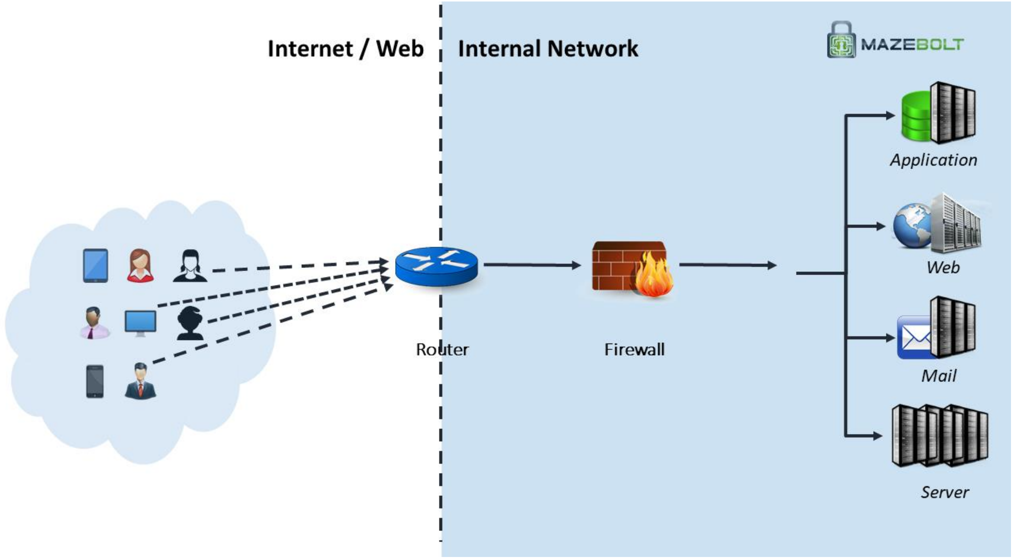
A Load Balancer can help offset DDoS Attacks by distributing the malicious traffic between the application servers. Unfortunately, without a stronger DDoS mitigation component upstream to filter out most of the attack traffic, the load balancer will not be enough to stop your site from being overwhelmed.

7. Firewall

Component Snap Shot		
	Deployment Location:	**On-Prem.**
	Functional Role:	**Rule-based Traffic Filtering**
	DDoS Mitigation Capabilities:	**Mild**

The Firewall guards the entrance to your internal network, preventing certain types of packets or requests from reaching your servers. It does so using rules defined at setup time, and mostly filters according to allowed packet types and the connection states.

Figure 8: Illustration of a Firewall



A Firewall keeps a record of the state of every connection opened between external clients and the internal servers and uses those records to filter out any packet that is out-of-state. Unsurprisingly, that qualifies the Firewall as a stateful device.

Like many other stateful devices, the firewall is vulnerable to state-table saturation attacks e.g. HTTP attacks and a SYN flood.

A Firewall can filter the packets that are part of a DDoS attack, but is usually not optimized for the amount of incoming packets that a DDoS entails. It will become overloaded very quickly, and will go into a fail-open or fail-closed state, both of which are sure to cause downtime.

8. Components Summary

No.	Component	Network Location	DDoS Mitigation Capabilities	Comments
1.	Scrubbing Center	Cloud-based	**Layer 3 & 4** – Strong	The main protection against volumetric attacks
			Layer 7 – Conditional on SSL visibility	
2.	CDN	Cloud-based	Good – Situational	Can mitigate DDoS Attacks but will not stop skilled attackers.
3.	CPE	On-Prem.	Strong	The main on-site protection
4.	IPS	On-Prem.	Poor	Unsuitable for DDoS Mitigation
5.	WAF	On-Prem. /Cloud-based	Mild	Cannot process the volume of traffic a DDoS attack entails.
6.	Load Balancer	On-Prem.	Poor	Has no defensive capabilities
7.	Firewall	On-Prem.	Mild	Cannot process the volume of traffic a DDoS attack entails.

Conclusion

Choosing the right combination of mitigation devices requires an understanding of how each devices' capabilities matches your environments needs together with an objective look at the corporate requirements – risk, available resources, budget, personnel, existing network infrastructure.

No matter how the technology is mixed and matched, it needs to be stress tested to ensure that it works when DDoS attacks strike. BaseLine testing is critical.

Sources

1. https://en.wikipedia.org/wiki/Application_firewall
2. https://www.techwalla.com/articles/what-are-the-advantages-and-disadvantages-of-using-a-firewall
3. https://searchnetworking.techtarget.com/definition/deep-packet-inspection-DPI
4. https://arxiv.org/pdf/1710.08628.pdf
5. http://www.ijiss.org/ijiss/index.php/ijiss2/article/view/248/pdf_561
6. https://www.sans.org/reading-room/whitepapers/intrusion/summary-dos-ddos-prevention-monitoring-mitigation-techniques-service-provider-environment-1212
7. http://www.infosecurityeurope.com/__novadocuments/22581
8. https://en.wikipedia.org/wiki/Data_monitoring_switch