

2019

Beginner's Guide to DDoS Mitigation Technology



© MazeBolt Technologies

www.mazebolt.com

Table of Content

| | |
|--|-----------|
| MAZEBOLT INTRODUCTION | 4 |
| EXECUTIVE SUMMARY | 5 |
| QUESTIONS THIS DOCUMENT ANSWERS: | 5 |
| COMPONENTS OF A DDOS MITIGATION SYSTEM | 6 |
| APPROACHES TO MITIGATION ACTIVITY | 7 |
| CLOUD BASED SOLUTIONS | 8 |
| SCRUBBING CENTER | 8 |
| <i>Introduction to Scrubbing Center</i> | 8 |
| <i>Advantages of Cloud Scrubbing</i> | 8 |
| <i>Disadvantages of Scrubbing Centers:</i> | 9 |
| CONTENT DELIVERY NETWORK (CDN) | 9 |
| <i>Introduction to Content Delivery Networks</i> | 9 |
| <i>Advantages of CDN to mitigate DDoS</i> | 10 |
| <i>Disadvantages of CDN:</i> | 10 |
| ON-PREMISE-BASED SOLUTIONS | 10 |
| VENDOR APPLIANCES (CUSTOMER PREMISES EQUIPMENT - CPE)..... | 10 |
| <i>Introduction to Vendor Appliances</i> | 10 |
| <i>Advantages of CPE:</i> | 11 |
| <i>Disadvantages of CPE:</i> | 11 |
| INTRUSION PREVENTION SYSTEMS (IPS) | 12 |
| <i>Introduction to IPS:</i> | 12 |
| <i>Advantages of IPS</i> | 12 |
| <i>Disadvantages of IPS:</i> | 12 |
| WEB APPLICATION FIREWALLS (WAFs)..... | 13 |
| <i>Introduction to Web Application Firewalls</i> | 13 |
| <i>Advantages of Web Application Firewalls</i> | 14 |
| <i>Disadvantages of Web Application Firewalls:</i> | 14 |
| LOAD BALANCER | 14 |
| <i>Introduction to Load Balancers:</i> | 14 |
| <i>Advantages of Load Balancers:</i> | 15 |
| <i>Disadvantages of Load Balancers:</i> | 15 |
| FIREWALLS | 16 |
| <i>Introduction to Firewalls:</i> | 16 |
| <i>Advantages of Firewalls:</i> | 16 |
| <i>Disadvantages of Firewalls:</i> | 16 |
| COMPONENTS SUMMARY | 18 |
| CONCLUSION | 18 |
| BENEFITS OF DDOS RADAR® | 19 |
| SOURCES | 19 |

Table of Figures

| | |
|--|----|
| Figure 1: Illustration of a Typical Hybrid DDoS Mitigation Posture | 6 |
| Figure 2: Illustration of a Cloud Scrubbing Service | 8 |
| Figure 3: Illustration of a Content Distribution Network (CDN) | 10 |
| Figure 5: Illustration of Dedicated On-Prem DDoS Mitigation Equipment..... | 11 |
| Figure 6: Illustration of an Intrusion Prevention System (IPS)..... | 12 |
| Figure 7: Illustration of a Web Application Firewall (WAF) | 13 |
| Figure 8: Illustration of a Load Balancer | 15 |
| Figure 9: Illustration of a Firewall | 16 |



MazeBolt Introduction

MazeBolt is a cybersecurity company that offers expertise in DDoS protection and defenses.

With MazeBolt's offerings spectrum, enterprises slash their DDoS risk from an average of **ongoing 48% to an ongoing <2%**.

MazeBolt's patented product [DDoS Radar](#)[®] is a groundbreaking technology that activates [Proactive Feedback](#) to eliminate DDoS vulnerabilities.

DDoS Mitigation is incomplete as it cannot identify and mitigate vulnerabilities, generated underneath the network it protects.

Proactive Feedback Module enabled by [DDoS Radar](#)[®] completes the DDoS Mitigation, by identifying and mitigating vulnerabilities generated, underneath the network. DDoS Radar[®] in principle completes any in-line, in-production DDoS Mitigation. It therefore allows companies to safely make ongoing changes to the production environment's underlying networks, and IT services, while eliminating DDoS risk.

Enabled by the [DDoS Radar](#)[®] (Product), the proactive feedback module automatically mitigates DDoS vulnerabilities by anticipating exposures, and closing them in real time across the attack surface **before they are getting exploited**.

MazeBolt Technologies is an Israeli cybersecurity company established in 2013.

MazeBolt serves over 100 organizations across the globe and spans industries that include Fortune 500 and NASDAQ listed companies.

It has a well-established team of cybersecurity professionals with experience in handling clients from varied industries, such as banking, gaming, government, telecommunication, e-commerce and many more.

[Read more about MazeBolt](#)

[Read more about DDoS Radar](#)[®]

[Read more about Limitations of DDoS Mitigation](#)

Executive Summary

In general, the more **complex** a mitigation system, more **likely the failure** will be due to **configuration issues**. This is because most enterprises' IT cells don't have the time or resources to ensure that every aspect of their **DDoS Mitigation posture** is **updated, integrated, and is running the right settings** for their specific environment(s). This keeps enterprise security open to DDoS attacks. When an attack occurs it can be expensive in terms of downtime, leading to lost customers and business. According to Forrester, a DDoS attack costs an enterprise an estimated [US\\$2.1 million dollars lost for every four hours of downtime and US\\$27 million for a 24-hour outage.](#)

To prevent attacks, enterprises, both small and large have likely invested in one or the other mitigation solutions highlighted below:

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

This whitepaper reviews the five above mentioned mitigation solutions in detail, to provide clarity on their capabilities to mitigate DDoS attacks.

Questions This Document Answers:

- Do Web Application Firewalls (WAFs), Firewalls and Load balancers protect against DDoS Traffic?
- What is the difference between an Intrusion Prevention System (IPS) and a DDoS Mitigation system?
- Can a Content Delivery Network (CDN) replace DDoS mitigation in totality?
- What are the crucial systems a 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
- Hybrid combinations of the two.

Mitigation systems consist of a combination of these components. This combination is essential because each component is proficient in responding to certain types of attacks.

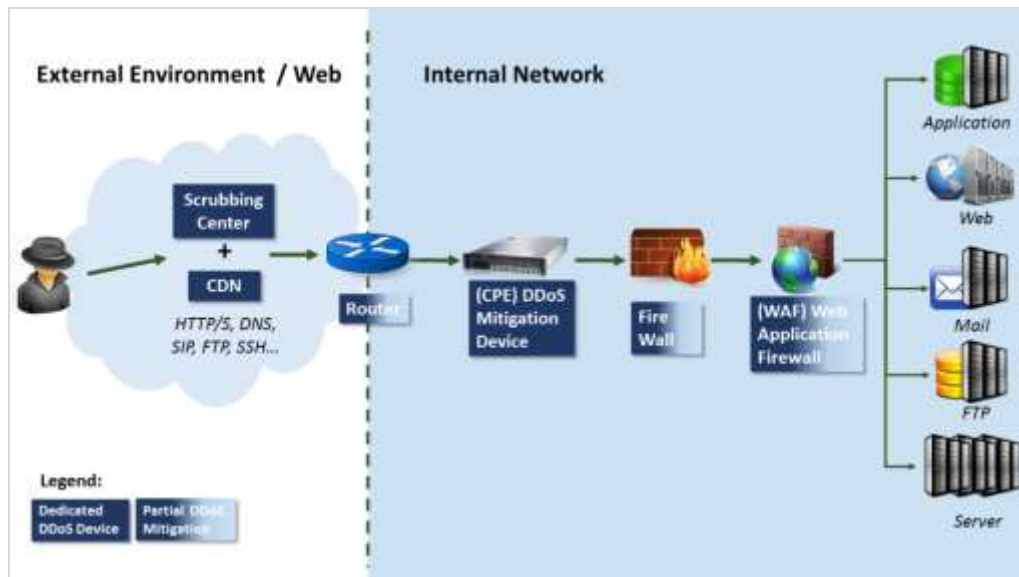
Each component has its own **advantages and disadvantages** and the decision regarding which posture is preferable depends largely on the existing infrastructure and enterprise’s business needs.

Most enterprises today opt for a hybrid setup. At the very least they would include a **scrubbing center** to protect their bandwidth. **In its absence**, the **internet pipe** is very likely to be easily **saturated**, even if the attack traffic does not penetrate the internal network.

However, 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.

In October 2019, a major DDoS attack, roughly eight hours long struck Amazon Web Services (AWS), making it impossible for users to connect because AWS miscategorized their legitimate customer queries as malicious.

FIGURE 1: ILLUSTRATION OF A TYPICAL HYBRID DDoS MITIGATION POSTURE



Approaches to Mitigation Activity

DDoS mitigation generally follows one of two approaches:

- **Proactive**, ‘always on’ – goes into effect **automatically**. All traffic is inspected, and suspicious traffic is separated before it reaches the infrastructure, preventing it from going down.
- **Reactive**, “on demand” – Also known as **Monitoring Mode** does not block suspicious traffic automatically but monitors and waits for a block order. This is not always automated, which means by the time the mitigation provider discovers the problem – often reported via a client calling the customer service line – it is usually too late to prevent downtime.

Cloud Based Solutions

Scrubbing Center

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

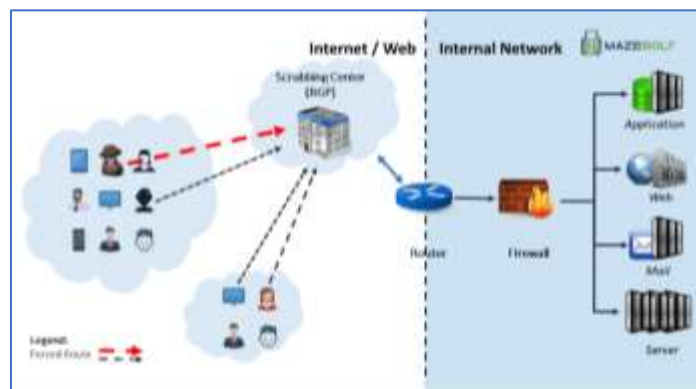
Introduction to Scrubbing Center

Scrubbing centers are essentially data cleansers – they **review traffic** going through them and **remove packets** that **do not adhere to the rules** and guidelines defined. Scrubbing centers are often cloud-based. They are the first source of **defense** for [volumetric attacks](#), which send an enormous number of packets in an attempt to overwhelm existing network resources and saturate bandwidth.

DDoS vulnerabilities are generated all the time. Mainly because the production network that DDoS Mitigation protects undergo changes all the time. Only when a [Proactive Feedback](#) is built on the DDoS Mitigation, these vulnerabilities are identified and eliminated.

In a recent article titled [‘How traffic scrubbing can guard against DDoS attacks’](#), [ComputerWeekly](#) says, “Although most scrubbing services can help fend off distributed denial of service attacks, a more comprehensive mitigation strategy is required to remain unscathed”.

FIGURE 2: ILLUSTRATION OF A CLOUD SCRUBBING SERVICE



Advantages of Cloud Scrubbing

- **Ability to scale and match:** The reason cloud scrubbing is used against large volumetric attacks is because of the **ability to scale and match** even some of the **largest floods** exceeding 10Tbps.
- **Uses BGP:** Scrubbing centers generally use the **Border Gateway Protocol (BGP)**. BGP routes traffic according to **rulesets, 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.

- **DNS or IP Target protection:** Scrubbing centers **protect** organizations against attackers **targeting** the name (**DNS name**) of the organization or the **numerical IP address**.

Disadvantages of Scrubbing Centers:

- **Application Layer Attack:** A scrubbing center's advantage is analyzing large volumes of traffic however are generally less able to **recognize application-layer attacks**. This is because most Application Layer (Layer 7) traffic is **encrypted, as well as scrubbing centers being cautious of applying incorrect settings resulting in false positives**. 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"**. and professional services engagement.
- **Expensive:** Scrubbing centers can have **expensive subscription fees, especially with regards to always on scrubbing**.
- **Sophisticated Attacks:** Sophisticated **multi-layer attacks** require a **granular capability for detecting and blocking attacks** which scrubbing centers are **not always efficient at adapting to**.

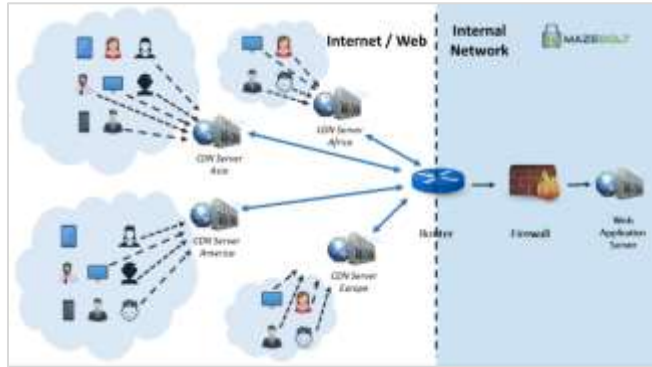
Content Delivery Network (CDN)

| | | |
|----------------|-------------------------------|-------------------------------|
| Component Case | Deployment Location: | Cloud-based |
| | Functional Role: | Static Content Serving |
| | DDoS Mitigation Capabilities: | Good - Situational |

Introduction to Content Delivery Networks

Content Delivery Networks (CDNs) use the DNS (Domain Name System) protocol to **route traffic** through the **CDN provider's** system. Distributed Denial of Service (DDoS) attacks are a serious threat to a content delivery network. Remote **malware** can **overwhelm a network**, making it unavailable or very slow to users. CDN's primary role is to ensure that **content** is **delivered** to end customers **without delay**. A **DDoS attack** can result in **latency** which can lead to loss of reputation, and revenue.

FIGURE 3: ILLUSTRATION OF A CONTENT DISTRIBUTION NETWORK (CDN)



Advantages of CDN to mitigate DDoS

- **Access to website:** In its most basic form, a Content Deliver Network is used to improve customers’ access to a website’s content. CDNs often offer a full security service and have the capability to perform real-time analysis of ongoing attacks.
- **Volumetric attacks:** They by design block Layer 3 and 4 attacks.
- **Realtime visibility:** They may monitor and provide real-time visibility into security events. They offer NOC services to continually monitor traffic to ensure that they can react on time.

Disadvantages of CDN:

- **IP addresses not protected:** CDNs 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 – **the site is not protected because the CDN provider never even sees the attack.**
- **CDN can be circumvented:** 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-Premise-based Solutions

Vendor Appliances (Customer Premises Equipment - CPE)

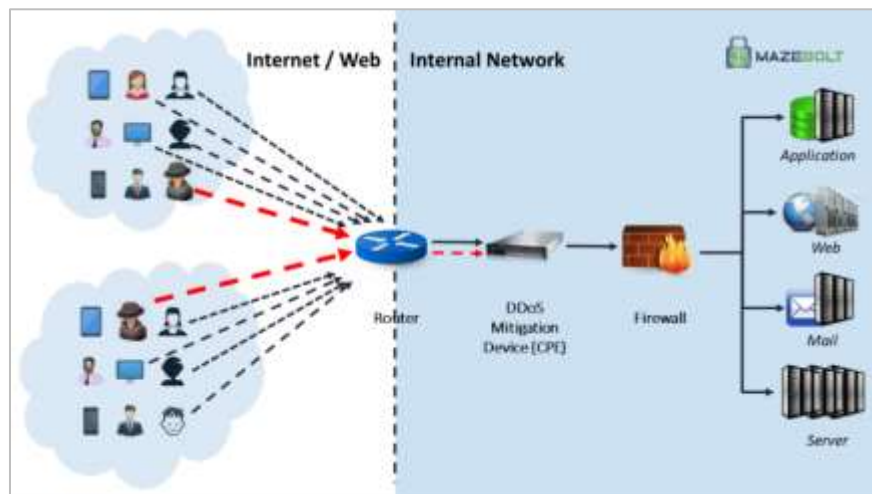
| | | |
|----------------|-------------------------------|---------------------------------------|
| Component Case | Deployment Location: | On-Prem. |
| | Functional Role: | DDoS Mitigation and Protection |
| | DDoS Mitigation Capabilities: | Strong |

Introduction to Vendor Appliances

Vendor appliances contain a variety of proprietary technologies, but, at their **core**, they are all **tuned** to **detect** and **stop DDoS attacks**. The appliances vary from being a combination of other components – to be a completely proprietary device consisting of highly specialized software and hardware fine-tuned to protect against 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



Advantages of CPE:

- **Network traffic planning and analysis:** Many of the devices deliver in-depth traffic analysis, bandwidth monitoring, and anomaly reports, allowing for **better network traffic planning** and DDoS attack analysis.
- **Improvisation from 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**.
- **AI based intelligence:** 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.

Disadvantages of CPE:

- **Standalone CPE has limitations:** CPE equipment without a scrubbing center will not protect against large volumetric attacks, even if the CPE equipment is well configured. The CPE will not provide protection against **internet pipe saturation**.
- **Requires manual fine tuning:** On-premise equipment requires manual fine tuning as well as ongoing costs related to infrastructure management making it expensive and often undependable.

Intrusion Prevention Systems (IPS)

| | | |
|----------------|-------------------------------|---|
| Component Case | Deployment Location: | On-Prem. |
| | Functional Role: | Detecting and Stopping Cyber Attacks |
| | DDoS Mitigation Capabilities: | Poor |

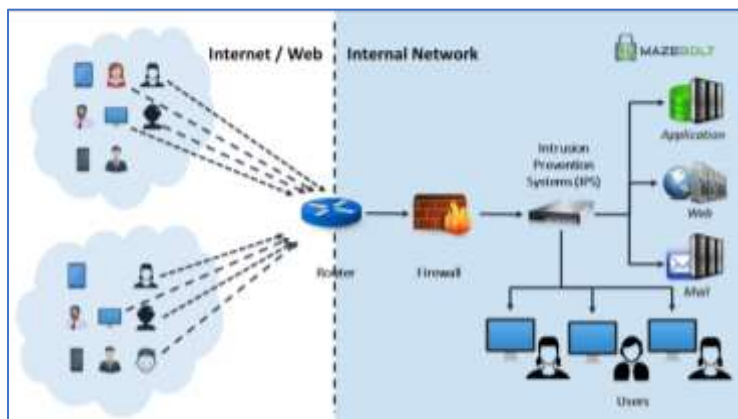
Introduction to IPS:

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**.

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.

Generally, most DDoS attacks cannot be mitigated using IPS systems. 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.

FIGURE 5: ILLUSTRATION OF AN INTRUSION PREVENTION SYSTEM (IPS)



Advantages of IPS

- **Custom filters in place:** IPS inspects incoming traffic to weed out malicious requests by using advanced filters. Also customized filters may be created on the fly.
- **Additional threat blocking:** IPS does block additional cyber threats in fact, IPS is not thought of as a DDoS mitigation mechanism/component.

Disadvantages of IPS:

- **Inability to stop initial DDoS attack:** 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.
- **Can create false alarms:** IPS is beneficial when the all is configured and works as expected. If the IPS is not well configured, it can result in a false alarm, causing wasted time and effort to identify its source.
- **Gap in security:** Encrypted packets can **remain undiscovered by IPS** leaving a gap in security.

Web Application Firewalls (WAFs)

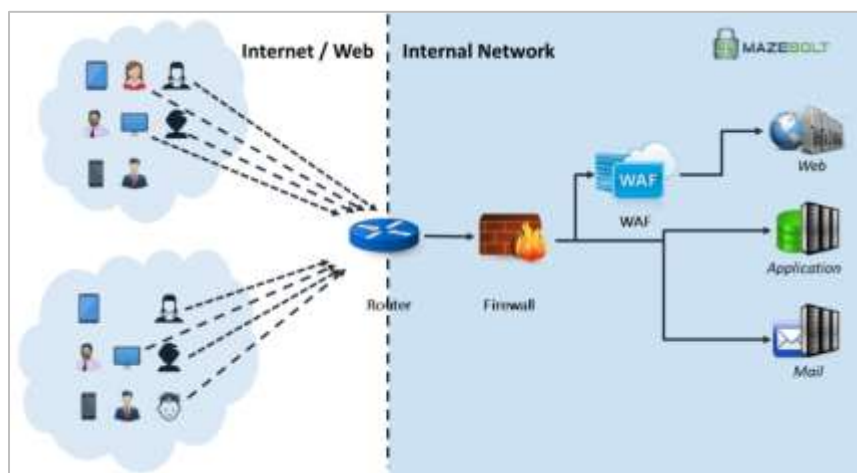
| | | |
|----------------|-------------------------------|---|
| Component Case | Deployment Location: | On-Prem./Cloud-based |
| | Functional Role: | Protection against Layer 7 Application Attacks |
| | DDoS Mitigation Capabilities: | Mild to negligible |

Introduction to Web Application Firewalls

WAFs perform multiple functions – **intrusion detection and web based analytics**. 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.

“The variety of cyber threats today – as well as the vulnerabilities they target – are so diverse that organizations can only hope to fend them off by deploying multiple layers of defenses.” Says CSO Online in the article, ‘Enhancing DDoS Defences with a Web Application Firewall.’

FIGURE 6: ILLUSTRATION OF A WEB APPLICATION FIREWALL (WAF)



Advantages of Web Application Firewalls

- **Listings control:** 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.
- **Customization possible:** 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.
- **Can be cloud-based:** 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.

Disadvantages of Web Application Firewalls:

- **Protocol vulnerability:** Application firewalls require proxy applications for each protocol. This is cumbersome and difficult to create and manage. Proxy agents are often used to **support undefined protocols and applications**, but the fact that they are undefined makes them a vulnerability.
- **Manual intervention:** Firewalls require **manual intervention for installation, configuration** and **ongoing maintenance** creating budget escalations.
- **Network reconfiguration:** All WAF network security solutions require **network re-configuration**, and all require **tuning** as they attempt to “**learn**” the applications they are protecting.

Load Balancer

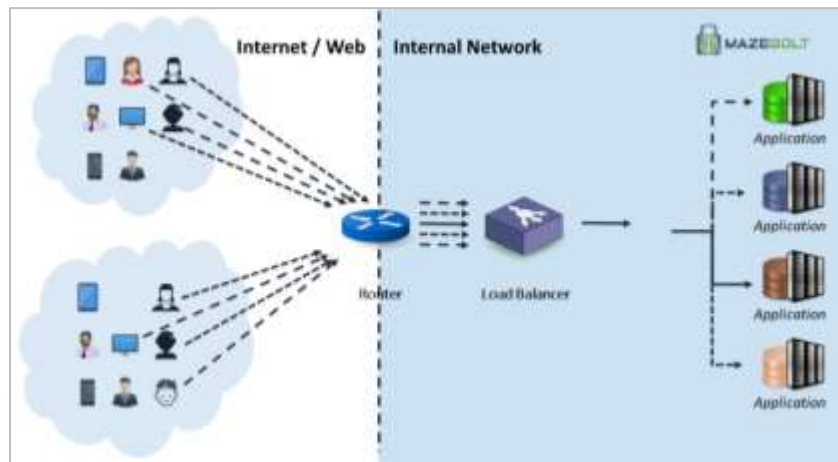
| | | |
|----------------|-------------------------------|--------------------------------------|
| Component Case | Deployment Location: | On-Prem. |
| | Functional Role: | Distributing Incoming Traffic |
| | DDoS Mitigation Capabilities: | Poor |

Introduction to Load Balancers:

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**.

FIGURE 7: ILLUSTRATION OF A LOAD BALANCER



Advantages of Load Balancers:

- **Agility:** They provide agility to deploy **high performance load balance** to align with business requirements.
- **Prevent overload:** By evenly **distributing traffic** they help to **prevent failure from overload**. As a result there is a **predictable performance** and **availability** of applications and **websites**.
- **Traffic reroute when required:** Load balancers while spreading workloads, add **resiliency** by **rerouting traffic** from **one server to another** if it falls prey to DDoS attacks.

Disadvantages of Load Balancers:

- **Vulnerability to state-table attacks:** Like many other stateful devices, the load balancer is vulnerable to state-table saturation attacks e.g. HTTP attacks and a SYN flood.
- **Can be overwhelmed:** 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 a site** from being **overwhelmed**.
- **Interception possible:** Attackers can directly send **volumetric DDoS traffic** to the **custom TCP and UDP communication protocols** used for custom gaming protocols, remote server access (SSH), secure file transfer services (SFTP), and email (SMTP). They can also use these ports to **intercept unencrypted data** in transit. Defending these ports and protocols without compromising performance requires additional resources. Be sure your **load balancer supports protection against layers 3 and 4 DDoS attacks**, along with TLS/SSL protection to encrypt customer data.

With [Proactive Feedback](#) working together with current DDoS Mitigation, DDoS Vulnerabilities are cut down from 48% to under 2% ongoing, 24x7.

Firewalls

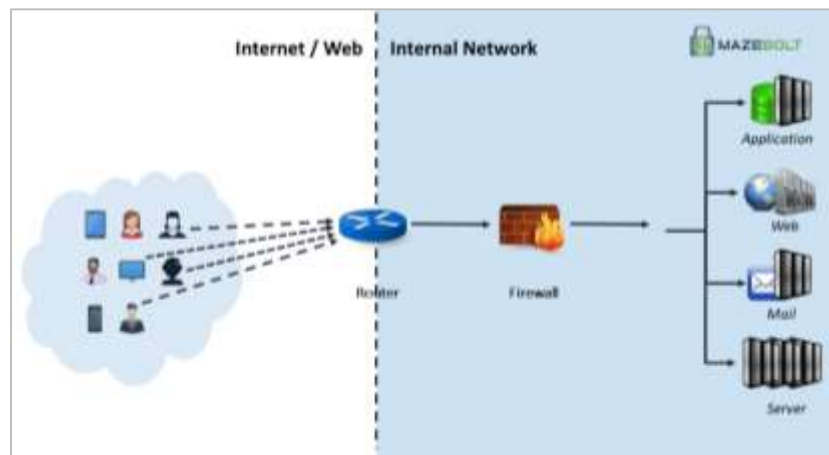
| | | |
|----------------|-------------------------------|-------------------------------------|
| Component Case | Deployment Location: | On-Prem. |
| | Functional Role: | Rule-based Traffic Filtering |
| | DDoS Mitigation Capabilities: | Mild |

Introduction to Firewalls:

The Firewall **guards** the **entrance** to the **internal network**, **preventing** certain types of **packets** or requests from reaching the **servers**. It does so by using **rules** defined at **setup time**, and mostly filters according to allow packet types and the connection states. A recent survey by Gartner estimates that through the year 2023, “99% of firewall breaches will be caused by misconfigurations, not firewalls.”

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**.

FIGURE 8: ILLUSTRATION OF A FIREWALL



Advantages of Firewalls:

- **Protection against layer attacks:** Firewalls offer protection against application-layer attacks in HTTP and HTTPS traffic
- **Request restriction:** They enable restriction of requests for certain geographical regions increasing security
- **Limit violations:** Controls can be pre-defined, **configured to address and limit violations** and protect against application-layer DDoS and other volumetric attacks.

Disadvantages of Firewalls:

- **Vulnerable to state table attacks:** Like many other stateful devices, the firewall is vulnerable to state-table saturation attacks e.g. HTTP attacks and a SYN flood.
- **Results in downtime:** 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.**
- **Volumetric traffic can exploit firewalls:** Firewalls work well to protect internal assets but may be overwhelmed on a perimeter network which is shared with third party platforms. Volumetric traffic can exploit firewalls and their limited bandwidth since most average **DDoS attacks exceed 6 Gbps.**

You have DDoS Mitigation in place but still experience disruption intermittently. Then, there are [Techniques to build a strong DDoS mitigation defense.](#)

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

From the above analysis it is obvious that no single DDoS Mitigation Posture is comprehensive. In order to build strong DDoS defenses, enterprises need to understand their business needs and adapt a mix and match approach when selecting the DDoS mitigation posture and components.

Experience indicates that even with a combination of different DDoS mitigations postures, network vulnerability remains at around 48%, as the underlying network is continuously changing and is dynamic in nature. This is because DDoS Mitigation postures are based on the mechanism of analyzing legitimate incoming traffic and passing it on to the requested destination IP (Internet protocol address). Nevertheless, hackers have several ways to sneak through these postures. What makes DDoS defense stronger is when there are no vulnerabilities exposed in the underlying network to exploit.

Today's DDoS mitigation is missing this critical functionality, to be able to continuously identify and fix vulnerabilities generated due to the underlying network changes.

[MazeBolt's DDoS Radar®](#) is the only product that advances **any DDoS mitigation posture** by bringing visibility into the DDoS vulnerabilities real-time 24x7 without disrupting the production environment. DDoS Radar enables Proactive Feedback layer by identifying DDoS vulnerabilities, giving feedback to

threat intelligence to take corrective actions and once the vulnerabilities are closed, it revalidates the closures. The process cuts DDoS Risks from ongoing 48% to under 2% ongoing.

Benefits of DDoS Radar®

- Anticipates DDoS Exposures Real-Time Before Getting Exploited

It proactively identifies and closes DDoS vulnerabilities in real-time **to strengthen existing DDoS Mitigation defenses.**

- Keeps DDoS Risk Continuously and in Real-Time Under 2% Ongoing

Through dashboards and reports. It provides a clear understanding of DDoS vulnerabilities from the initial validation, how they **were brought to under 2%**, and how they are continuously kept under 2%.

- Clear and Concise Dashboards and Reporting

Enterprises get **a clear report that show the percentage of vulnerabilities open** in the underlying network. Percentage of detected vulnerabilities vs. percentage closed vulnerabilities. KPIs of monthly improvement and one dashboard that shows vulnerabilities open and fixed, across all data center sub-divisions or subsidiaries across the networks globally.

- Empowers In-House Security Staff & Mitigation Vendors

In-house security staff can view exactly where the vulnerabilities are open in the network and can easily communicate with their **DDoS Mitigation Vendor to immediately close the gap.** Once the Mitigation vendor submits a report of closing the gap, with the help of DDoS Radar® the customer or vendor can re-validate immediately to ensure the vulnerability is closed

- Ensures that your Network Is Resilient to the Latest, Smart and Sneakiest DDoS Attacks

[DDoS Radar™](#) has a library of DDoS Attack vectors and it is updated weekly as per the knowledge of new attack vectors that constantly evolve. This makes sure that the all the networks across the **global centers are validated against latest DDoS Attack vectors.**

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.ijss.org/ijss/index.php/ijss2/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
9. <https://www.darkreading.com/cloud/eight-hour-ddos-attack-struck-aws-customers/d/d-id/1336165https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-building-resilience-to-denial-of-service-attacks.pdf>
10. <https://www.csoonline.com/article/3234529/enhancing-ddos-defenses-with-a-web-application-firewall.html>
11. <https://www.computerweekly.com/news/252456702/How-traffic-scrubbing-can-guard-against-DDoS-attacks>