MAZEBOLT

The Essential Guide to Optimizing your DDoS Protection

What you need to know, and what can go wrong

Table of Contents

Executive Summary

The DDoS attack landscape presents a growing challenge to enterprises today. As networks and online services become more complex, DDoS attacks adapt, getting more sophisticated and malicious. The dynamic nature of cloud environments and their associated applications provides threat actors with a growing attack surface to inflict damaging interruption to services. Industry research reveals that, on average, 60% of enterprises get hit by a DDoS attack they experience losses exceeding $120,000 due to downtime. Moreover, 15% of organizations impacted by DDoS attacks suffer losses surpassing $1 million, with some even experiencing extensive reputational damage and dramatic drops in market capitalization For example, following a DDoS attack in 2021, Bandwidth.com stock dropped dramatically from $2.4 Billion to less than $0.4 Billion in market capitalization. Twelve months later the market CAP was still less than $0.4 Billion.

The ramifications of DDoS attacks extend beyond the targeted organization. A successful attack will also affect their customers, partners, and stakeholders. When successful, these attacks can persist for hours, days, and in extreme cases, weeks. Notably, the "popularity" of DDoS attacks among global threat actors has spurred their evolution into ransomware attacks, which seek to extort money from compromised organizations. Attackers exploit these attacks, causing substantial downtime that disrupts business continuity and the availability of services to their customers. In recent years, DDoS attacks have also been utilized as diversions, enabling security breaches aimed at accessing sensitive data while attention is diverted elsewhere.

Many organizations grapple with a lack of time and technical resources to ensure comprehensive DDoS security. The lack of updates and maintenance leads to serious misconfigurations leaving organizations vulnerable. This eBook will address these issues and explain why a proactive approach is needed to DDoS security. We will explore common DDoS mitigation services, explain common misconfigurations, and propose a set of best practices to help significantly reduce the risk of damaging DDoS attacks.

Losses to DDoS Attacks

60% of businesses lose at least **$120K**

15% of businesses lose at least **$1 Million**

Elements of DDoS Mitigation

No matter what mitigation system or provider you choose to work with, DDoS mitigation typically comprises three primary categories: cloud-based, on-premises, and hybrid solutions.

DDoS mitigation policies are typically established for each IP address, FQDN or network, guaranteeing that only legitimate traffic reaches essential services for external users. Once the initial configurations for DDoS mitigation are in place, establishing a routine for updates, configurations, and tests becomes crucial.

When evaluating the most suitable DDoS mitigation strategy for your organization, there are several important considerations:

1 **Mitigation Type**
An "always-on" approach is required and should be consistently active. How many layers of DDoS protection do you require? E.g. Scrubbing, CDN, WAF etc..

2 **IT Infrastructure**
Understand your existing infrastructure capacity and anticipate its growth to align with a mitigation solution(s) that can scale.

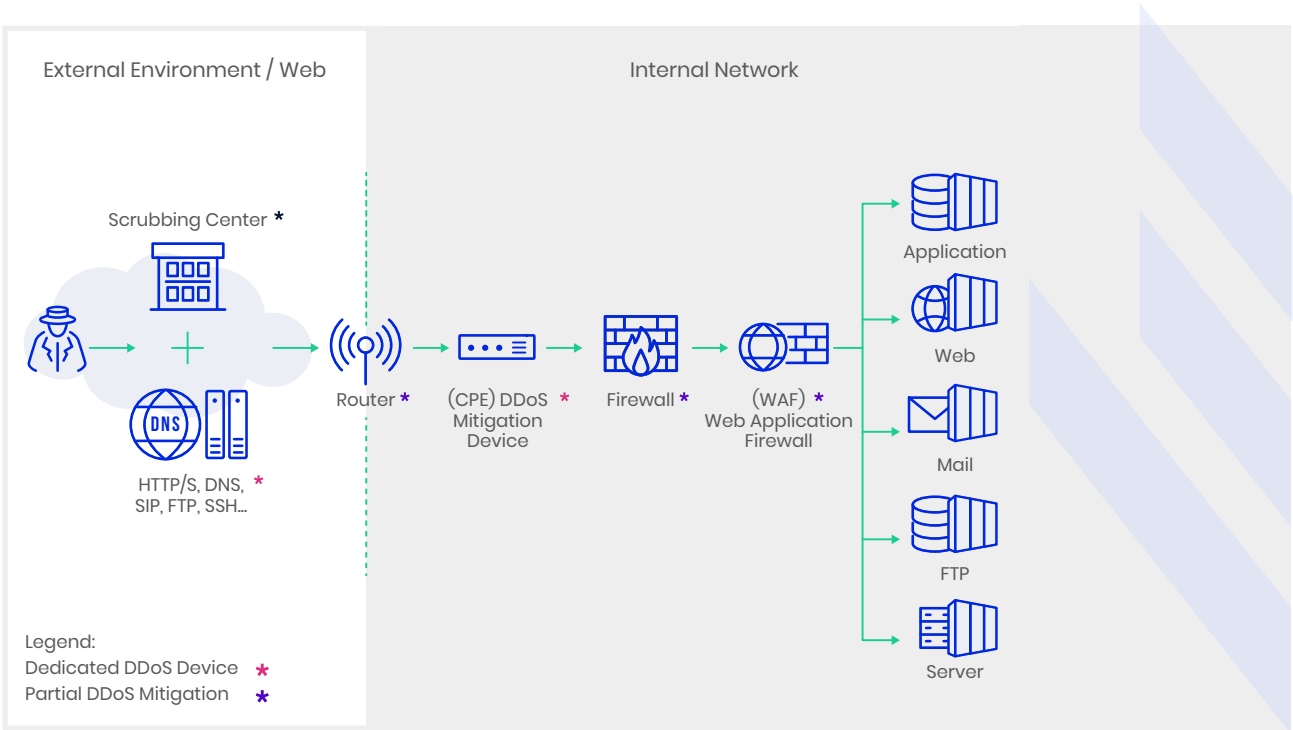
3 **Adaptability and Flexibility**
Assess your network's adaptive capabilities and flexibility, ensuring the mitigation solution can adjust to evolving threats and network changes.

4 **IT Infrastructure and Blind Spots**
Consider the size of your IT infrastructure eg. networks, cloud regions, etc. Anticipate potential blind spots, and account for anticipated network expansion to create a comprehensive mitigation plan.

Potential Vulnerabilities

Production networks and services frequently change, posing potential new vulnerabilities in DDoS mitigation policies. Keeping pace with these changes presents a major challenge for any network security team. Therefore, staying vigilant in updating and continuously testing to identify and remediate vulnerabilities becomes paramount to maintaining an effective DDoS mitigation strategy.

Hybrid DDoS Mitigation Architecture



Scrubbing Center

Deployment Location	Functional Role	DDoS Mitigation Capabilities
Cloud-Based	Scalable Data Cleanser	Layers 3 & 4 - Strong Layer 7 – Weak and conditional on SSL Visibility

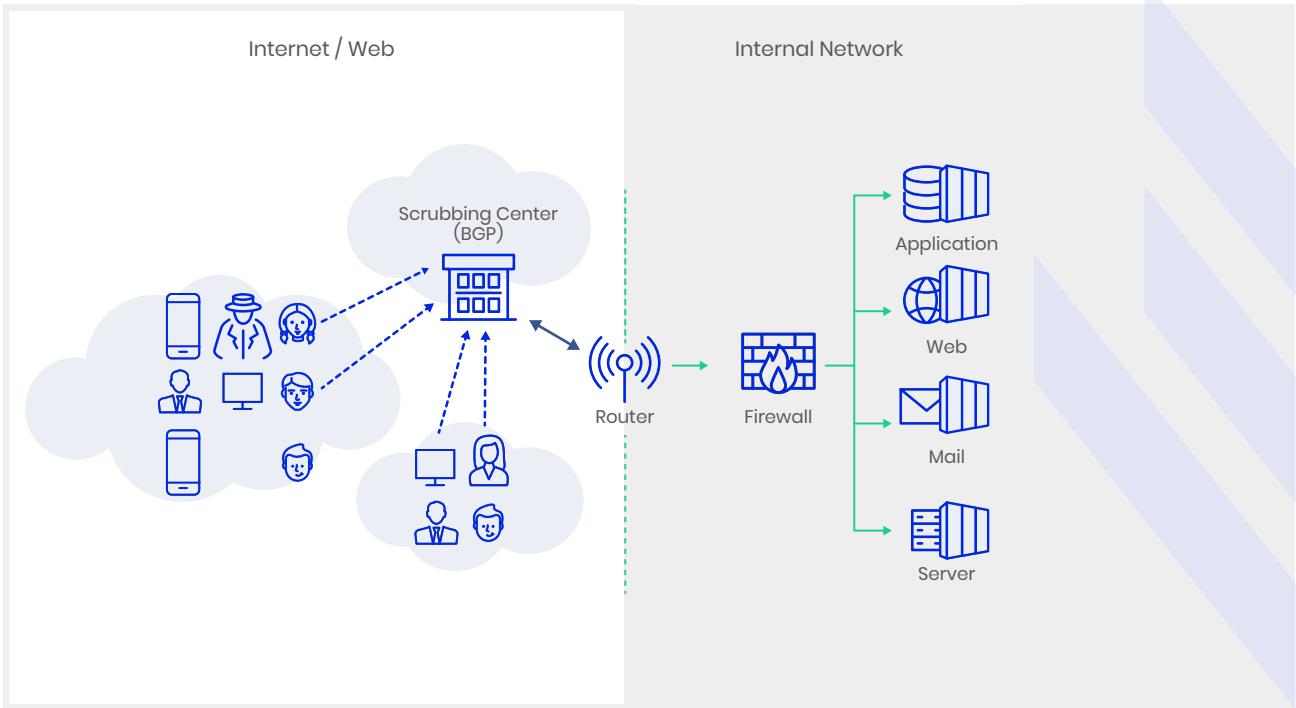
The frontline defense against DDoS attacks is the scrubbing center. These upstream centers are responsible for scrutinizing and filtering attack traffic and are distributed across high capacity networks. Their efficiency primarily lies in blocking volumetric DDoS attacks at layers 3 and 4.

Their scalability is a defining feature, capable of handling even the largest floods that exceed 10Tbps. Functioning as "data cleansers," scrubbing centers meticulously examine incoming traffic, removing malicious packets identified as attack traffic and letting through the "clean" good traffic. Utilizing the Border Gateway Protocol (BGP), most scrubbing centers offer network-wide protection.

Potential Vulnerabilities

BGP shields against DDoS attackers targeting your direct IP or DNS names. However, at the application layer (layer 7), traffic is often encrypted. The ability of scrubbing centers to effectively counter malicious application layer attacks rely on possessing the necessary decryption keys - for "SSL visibility", which is often impractical to provide. Therefore, other solutions are usually required to mitigate Layer 7 threats (CDN, WAF, or CPE).

A Cloud Scrubbing Service



Content Delivery Network (CDN)

Deployment Location	Functional Role	DDoS Mitigation Capabilities
Cloud-Based	Content Delivery & Security	Good – Layer 7 only, by design

CDNs leverage the DNS protocol to direct traffic through the provider's system. They are primarily used to enhance customer access to website content by caching certain and delivering content as close to the requesting user as possible.

CDNs specifically handle Layer 7 traffic while refraining from forwarding traffic at Layers 3 and 4 to the organization's IT infrastructure. This approach shields the organization against volumetric attacks by design.

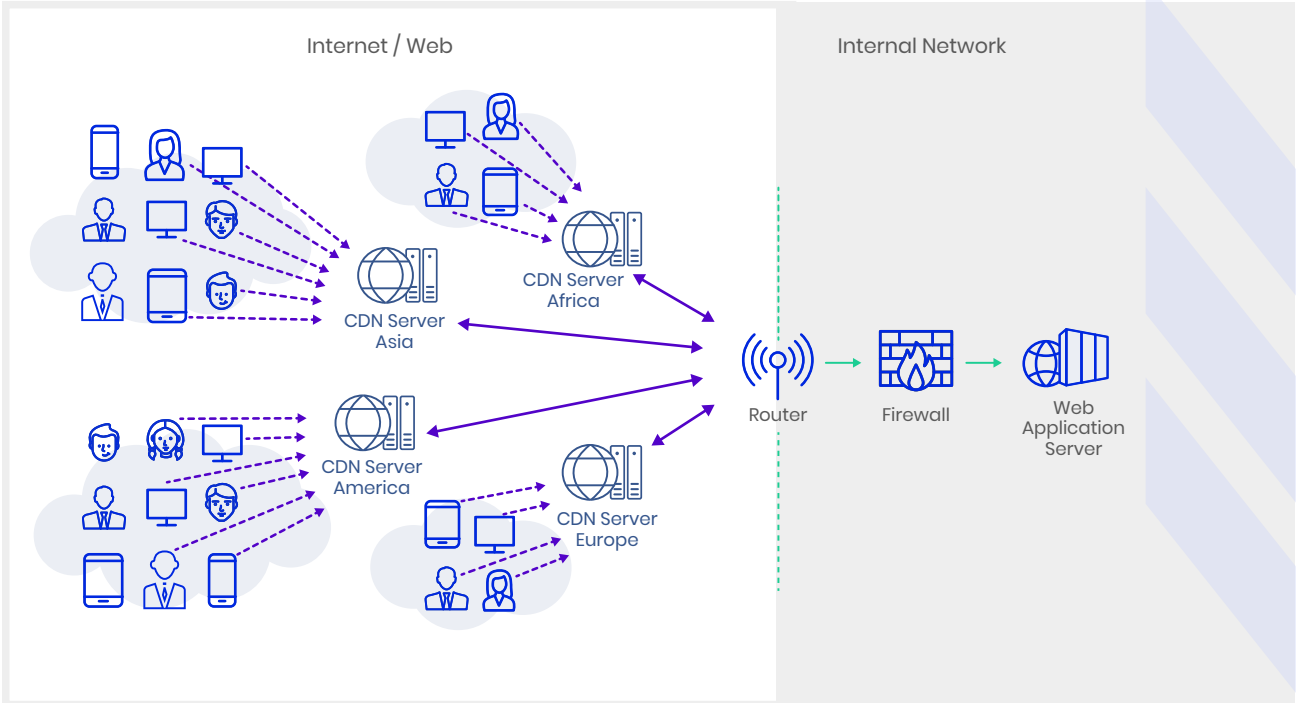
CDNs are designed to manage significant traffic surges, which can be expected during legitimate high-traffic events. However, attackers understand how to ensure their malicious requests go through the CDN servers and to the originating "origin" server responsible for providing the CDN its content. This then makes the server the CDN relies upon (the "origin") server unavailable.

To prevent this, CDN DDoS protection policies need to be in place and configured correctly.

Potential Vulnerabilities

It's critical to understand that a CDN is only one component of an overall DDoS mitigation system and only for Layer 7 traffic that was directed by DNS to go through it. The CDN's DDoS protection primarily revolves around DNS redirection. Sophisticated DDoS threat actors may identify and directly target the website's source IP, bypassing the CDN's protective measures together and rendering it ineffective in such scenarios, for that you need to have a scrubbing center.

Content Distribution Network (CDN):



Customer Premises Equipment (CPE)

Deployment Location	Functional Role	DDoS Mitigation Capabilities
On-premises	DDoS Mitigation and Protection	Strong Layer 3, 4, and 7 (will not protect bandwidth upstream)

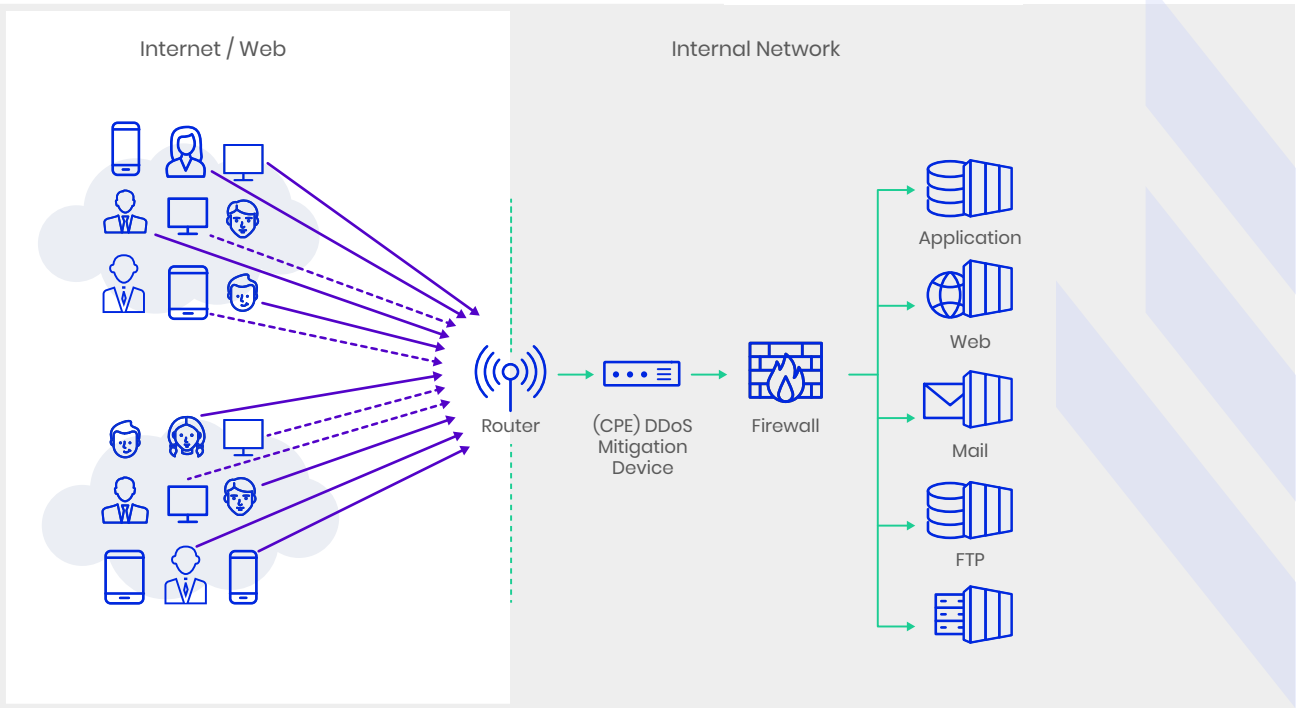
CPE appliances encompass a range of technologies designed to identify and block DDoS attacks. Positioned at the outer edge of an organization's network infrastructure, the CPE resides after (downstream) the router but before (upstream) accessing the internal network infrastructure, including firewalls and load balancers.

These CPE devices offer in-depth traffic analysis, bandwidth monitoring, and performance reporting capabilities with secure SSL visibility (since the appliance is hosted by the organization itself). They facilitate better network traffic management and enable detailed analysis of DDoS attacks. Post-attack reports provide crucial insights and action items, aiding in refining systems for future attacks.

Potential Vulnerabilities

CPE equipment, without a scrubbing center, will not adequately protect against large-scale volumetric attacks, even with optimal configuration. Manual adjustments and continual infrastructure management are inherent to protecting CPE devices, so continual validation of security settings and fine-tuning is a requirement. In the face of internet pipe saturation, CPEs may prove insufficient in protecting the network against substantial threats.

Dedicated on-Premises DDoS Mitigation Equipment



Intrusion Prevention Systems (IPS)

Deployment Location	Functional Role	DDoS Mitigation Capabilities
On-premises or Cloud-based	Detecting and Stopping Cyber Attacks	Poor

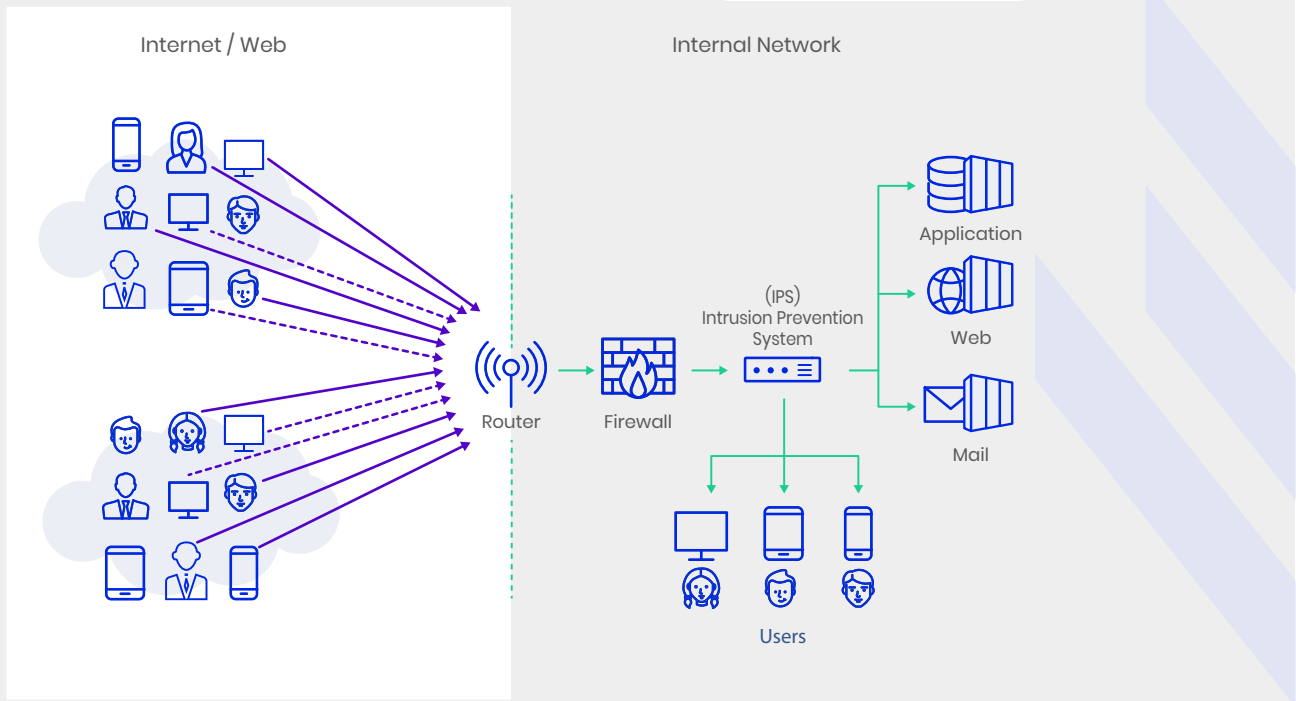
Intrusion Prevention Systems (IPSs) serve the critical role of monitoring suspicious activities within a network. These systems may function as part of firewalls or alone. An IPS meticulously inspects and scans packets, relying on pre-existing settings, signatures, protocol status, or anomaly detection to generate alerts and potentially block potential cyberattacks.

However, an IPS is primarily designed to block malware, web attacks, or other known exploitation attempts and is not designed to stop DDoS attacks. While they possess some capabilities across layers 3, 4, and 7, DDoS attacks often surpass the mitigation capacity of IPS systems. Resorting to an IPS to counter a DDoS attack typically suggests that the targeted organization is experiencing an exceptionally advanced DDoS attack campaign. This situation arises when CPEs and/or scrubbing and/or CDN services fail to mitigate attacks effectively.

Potential Vulnerabilities

IPS is vulnerable to DDoS attack, since it is a stateful appliance and will likely go into a "fail open" or "fail closed" state. Scrubbing Centers, CDNs and CPE should be configured upstream to prevent having to rely on IPS systems for DDoS mitigation.

Intrusion Prevention System (IPS)



Web Application Firewall (WAF)

Deployment Location	Functional Role	DDoS Mitigation Capabilities
On-premises or Cloud-based	Protection against layer 7 Application Attacks	Layer 3,4 - Very Poor Layer 7 - Good

Web application firewalls (WAFs) are specialized firewalls that primarily inspect web-based traffic.

WAFs excel at analyzing application traffic, distinguishing between potential risks and legitimate usage, and controlling access to applications and services by applying rules to incoming HTTP traffic. Employing deep-packet inspection, they identify, categorize, reroute, or block packets containing specific data or code payloads; Legitimate user traffic is permitted, while suspicious traffic is either redirected for further scrutiny or blocked outright.

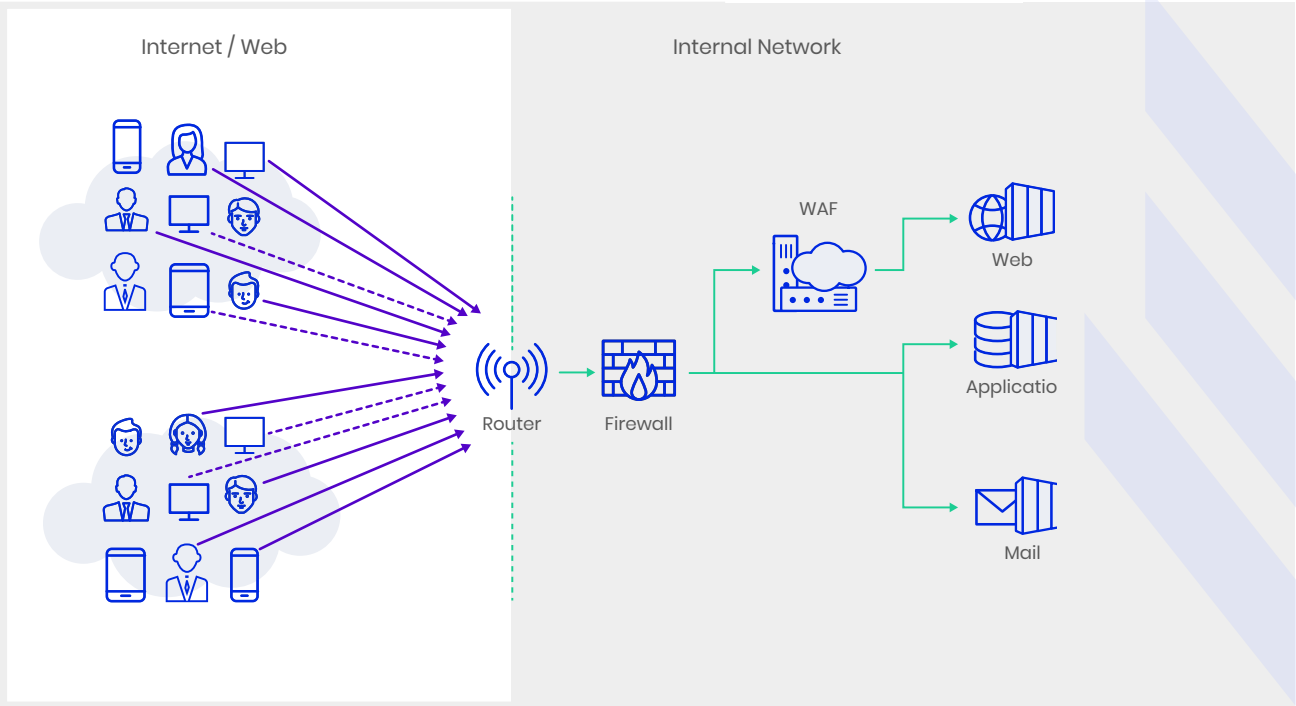
WAFs are effective against layer 7 attacks that directly impact applications. However, the inspection process can introduce latency and impact user experience, emphasizing the importance of efficiency.

WAFs can be implemented as cloud-based services offered by service providers. While firewalls can mitigate certain DDoS attacks, they are vulnerable targets that, when overwhelmed, can contribute to the disruption of online services. WAFs, due to their bot detection and DPI (deep packet inspection) capabilities, are integrated into the DDoS protection layers of many organizations for Layer 7, assuming volumetric attacks are taken care of upstream.

Potential Vulnerabilities

WAFs are not specifically designed to counter DDoS attacks but are often utilized to do so. WAF should only be utilized to mitigate Layer 7 attacks that cannot be mitigated by CDN, CPE capabilities. It is the last line of defense against a DDoS attack.

Web Application Firewall (WAF)



Load Balancer

Deployment Location	Functional Role	DDoS Mitigation Capabilities
On-premises	Distributing Incoming Traffic	Poor

Load balancers serve as intermediaries, receiving traffic from multiple clients and evenly distributing it across various similar application servers. Clients connect to the load balancer, which then establishes a connection to an application server on the client's behalf. Given their stateful nature, load balancers must monitor and manage the state of each connection, making them susceptible to saturation DDoS attacks like HTTP and SYN floods.

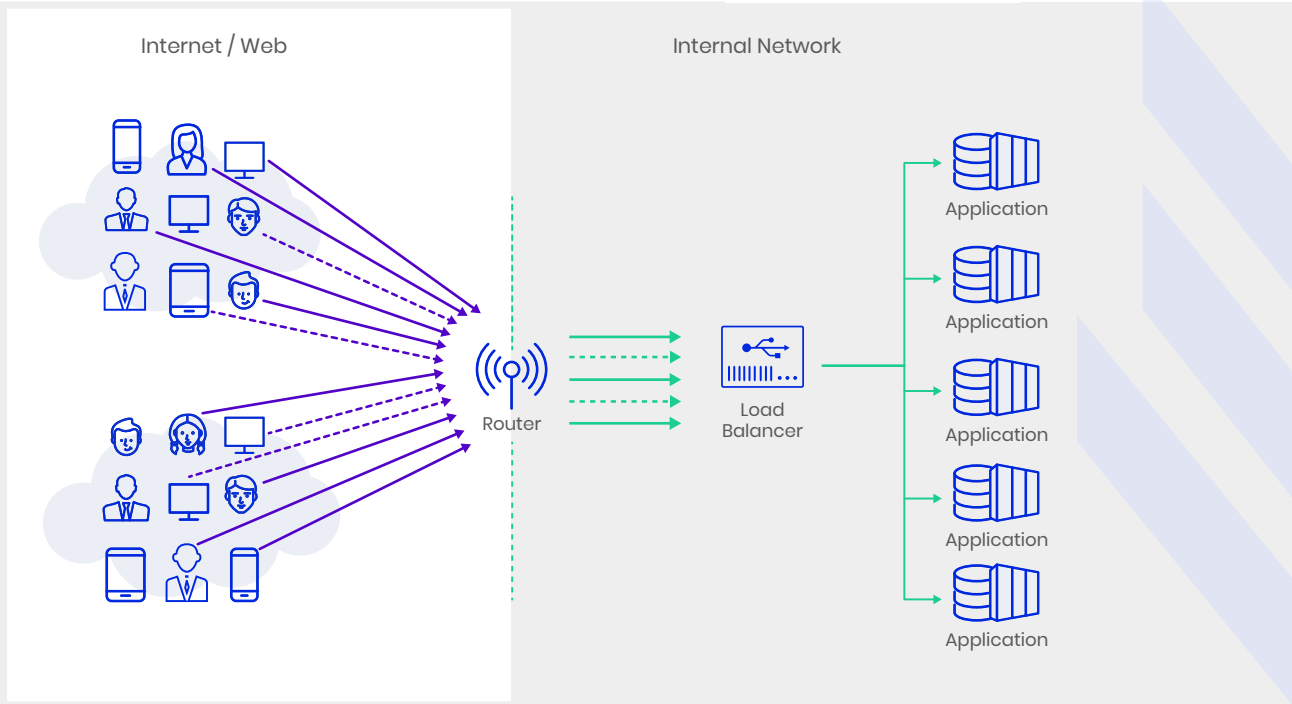
Stateful devices, including load balancers, often fall first during a DDoS attack. Stateful devices require high amounts of processing power and memory to function, which is not good in a DDoS scenario.

Load balancers play a role in mitigating DDoS attacks by dispersing malicious traffic among different application servers. However, in the absence of a suitable upstream DDoS mitigation component designed to filter out the majority of the attack traffic, will likely have no effect, relying solely on load balancers will not suffice to prevent service disruption under attack, in fact the load balancer itself has a high chance of failure.

Potential Vulnerabilities

Without the proper DDoS mitigation component located upstream in the pipeline, designated to filter out most of the attack traffic, a load balancer will not be enough to stop your services from being disrupted and will fail quickly as load balancers are stateful appliances.

Load Balancer



Firewall

Deployment Location	Functional Role	DDoS Mitigation Capabilities
On-premises	Rule-based Traffic Filtering	Poor

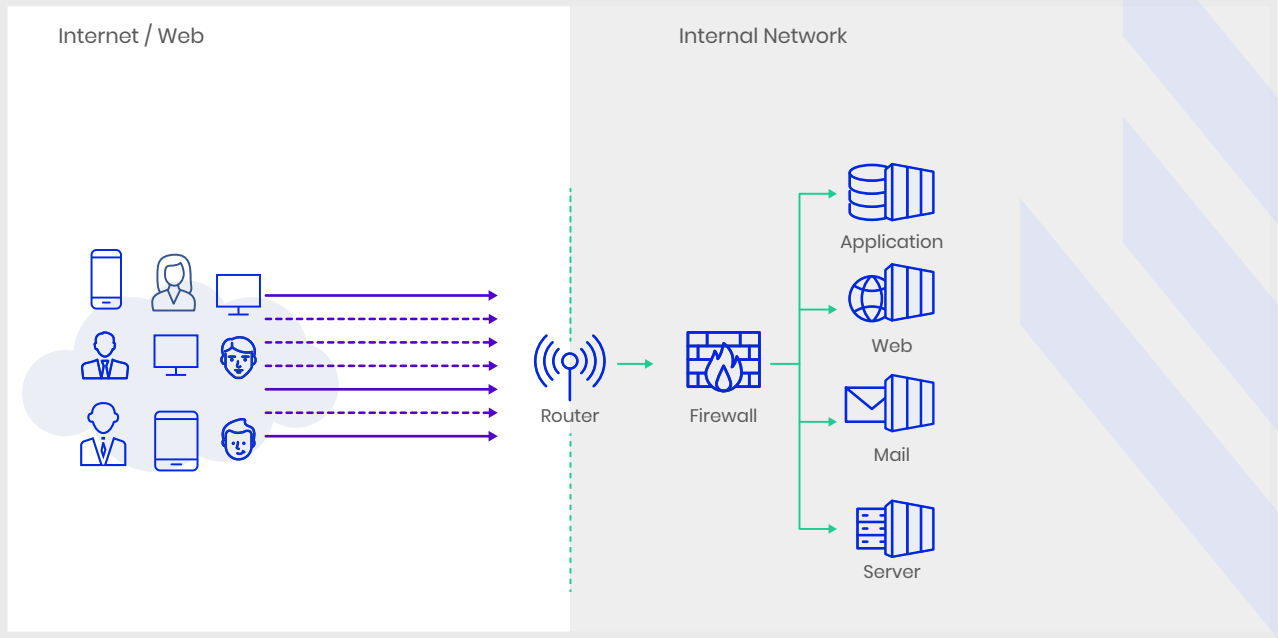
Firewalls act as the gatekeepers of your internal network, controlling and filtering incoming packets or requests based on predefined rules. Configured with specific rulesets, the firewall scrutinizes and manages traffic based on allowed packet types and connection states. A firewall keeps a record of every connection opened between external clients and the internal servers and uses those records to filter out any out-of-state packets.

This qualifies the firewall as a stateful device, and like many other stateful devices, the firewall is vulnerable to saturation DDoS attacks such as HTTP attacks and SYN floods. While the firewall can sift through packets related to a DDoS attack, it's generally not optimized to handle the sheer volume of incoming packets that accompany such attacks. This results in the firewall quickly becoming overwhelmed, leading it to "fail closed" state, which leads to downtime.

Potential Vulnerabilities

Relying on a firewall for DDoS protection is insufficient. Organizations should employ a multi-layered approach incorporating specialized DDoS mitigation components and strategies upstream to protect the firewall and other stateful devices from DDoS attack damage.

Firewall



Key Takeaways

1 **Thorough Research is Crucial**
Invest time and resources in understanding your network's specific requirements, growth projections, types of services, and capabilities. Select the best DDoS mitigation solution for your architecture.

2 **Mitigation Selection Based on Capabilities**
Choosing the right combination of mitigation capabilities with an in-depth understanding of how each of the capabilities align with your environment's needs.

3 **Regular Updates and Testing**
Define a routine for updates, configurations, and ongoing testing after implementing DDoS mitigation. Constant changes in production networks and services will create new vulnerabilities in the DDoS mitigation setup that have to be identified and eliminated through policy updates.

4 **Scrubbing Centers**
First Line of Defense - Scrubbing Centers provide good mitigation capabilities for Layers 3 and 4, serving as the initial defense against DDoS attacks.

5 **Content Delivery Networks (CDNs)**
CDNs are pivotal for first line Layer 7 DDoS mitigation but should be part of an overall DDoS mitigation system, taking into account direct attacks.

6 **Customer Premises Equipment (CPEs)**
CPEs are critical for organizations that have their own IT infrastructure and possess strong DDoS mitigation capabilities. However they will fail to protect the network from Internet pipe saturation.

7 **Intrusion Prevention Systems (IPSs)**
IPSs are unreliable for DDoS mitigation. If you try to mitigate a DDoS attack using only an IPS, you will likely fail.

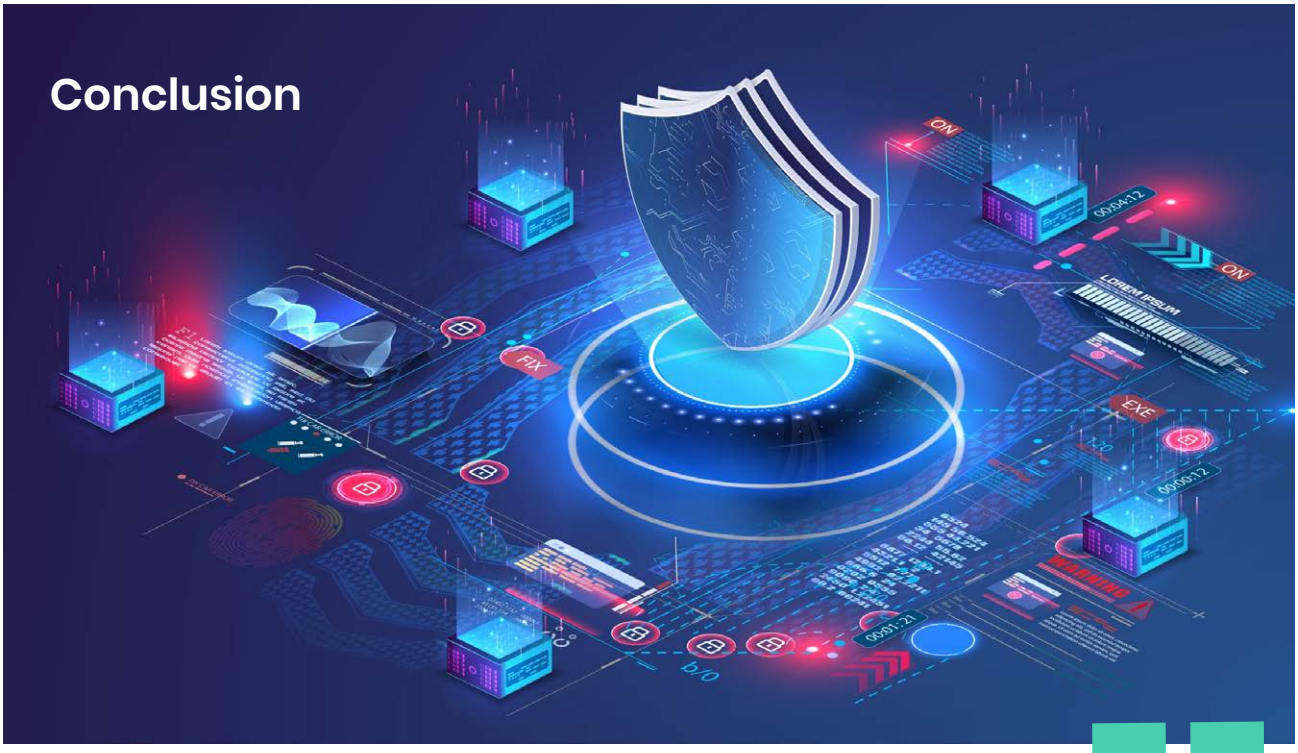
8 **Web Application Firewalls (WAFs)**
WAFs, although popular, should be used for Layer 7 attacks that could not be mitigated upstream, they are the last line of defense for Layer 7.

9 **Load Balancers**
Load balancers are not sufficient to mitigate DDoS attacks.

10 **Firewall**
Firewalls are not sufficient to mitigate DDoS attacks.

11 **Continuous DDoS testing**
Even with the best DDoS mitigation solution in place, organizations can still face up to 75% exposure to DDoS vulnerabilities. Continuous and proactive DDoS testing is critical to identify and remediate vulnerabilities in the DDoS security solutions deployed.

Conclusion



DDoS protection providers rely heavily on reactive rather than a proactive strategy, configuring their defenses based on a static approach geared towards addressing common threats at a point in time, with a deploy and forget attitude. Consequently, these protections often miss even well known DDoS attacks and organizations are unnecessarily damaged. As network complexities increase, so does the sophistication of DDoS threats, posing a greater challenge. The inherent static nature of DDoS protection services, and a complete lack of continual insight to the effectiveness of protection configurations for a specific production environment, create significant configurations.

These DDoS protection misconfigurations create vulnerabilities in an organizations protection, paving the way for disruptive attacks that necessitate emergency responses that rely on manual intervention and SLAs. This leaves organizations operating under a false sense of security, and even with the best "automated" DDoS protection solutions in place, but without continuous testing and remediation, wil suffer from between 30% to 75% vulnerability levels in their deployed protections.

With the best DDoS protection solutions in place, organizations still suffer from

30%

to

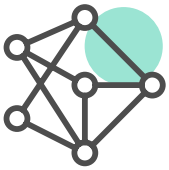
75%

exposure to their online services and security posture

By visualizing the entire online services posture and getting accurate vulnerability data on all DDoS attack vectors that evade DDoS protections, an organization can achieve key proactive goals:

Identify vulnerabilities by OSI Layer

Fully automated DDoS protections with zero down-time



Prioritize and manage remediation

Maximize ROI on DDoS protection investments

Validate the fixes

Checking these boxes will ensure that your organization solved the critical challenge of DDoS security - proactively identify & eliminate DDoS vulnerabilities by prioritizing and managing vulnerability remediation.

About MazeBolt

MazeBolt is pioneering a new approach in DDoS security. MazeBolt RADAR™ is the only solution that identifies and enables the elimination of DDoS vulnerabilities in every layer of DDoS protection, by continuously testing every attack vector across online services, with zero operational downtime.

Using RADAR's patented vulnerability testing technology, enterprises have unparalleled visibility into their DDoS protection solutions so they can be confident that damaging DDoS attacks can be prevented - before they happen.

Visit www.mazebolt.com to learn more.