MAZEBOLT

www.mazebolt.com

A Simple Guide to DDoS Mitigation

TABLE OF CONTENTS

TABLE OF FIGURES

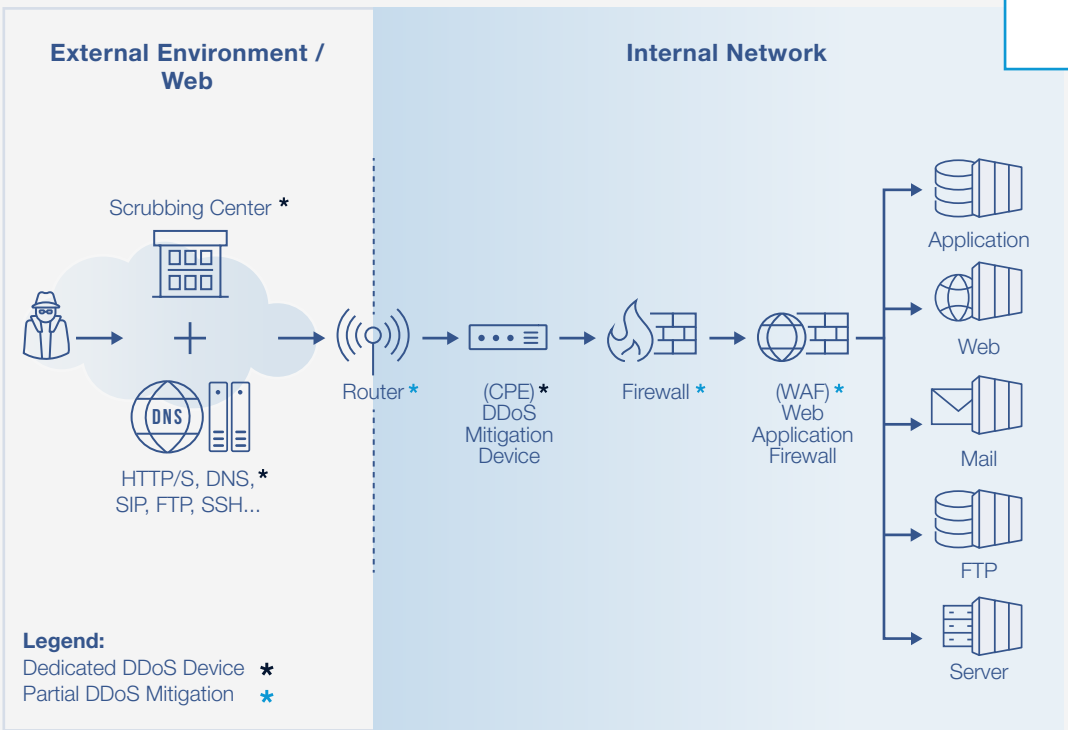
EXECUTIVE SUMMARY

The more complex the mitigation system, the more likely failure will be due to configuration issues as most enterprise IT organizations do not 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. 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.

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.

Figure 1: Illustration of a Typical Hybrid DDoS Mitigation Posture



Cloud-Based Solutions

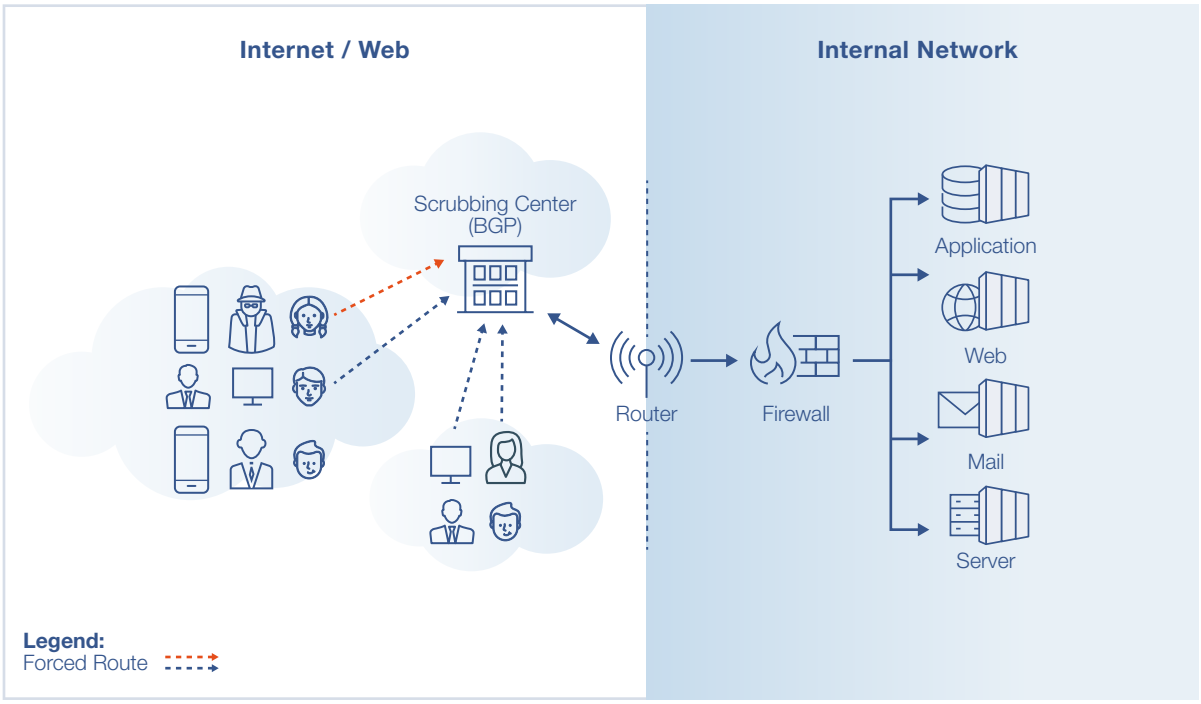
Scrubbing Center

Deployment Location	Functional Role	DDoS Mitigation Capabilities
Cloud-Based	Scalable Data Cleanser	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 network resources and saturate bandwidth. 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. As data cleansers, they review traffic going through them and remove packets that don't adhere to the rules and guidelines defined.

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



Content Delivery Network (CDN)

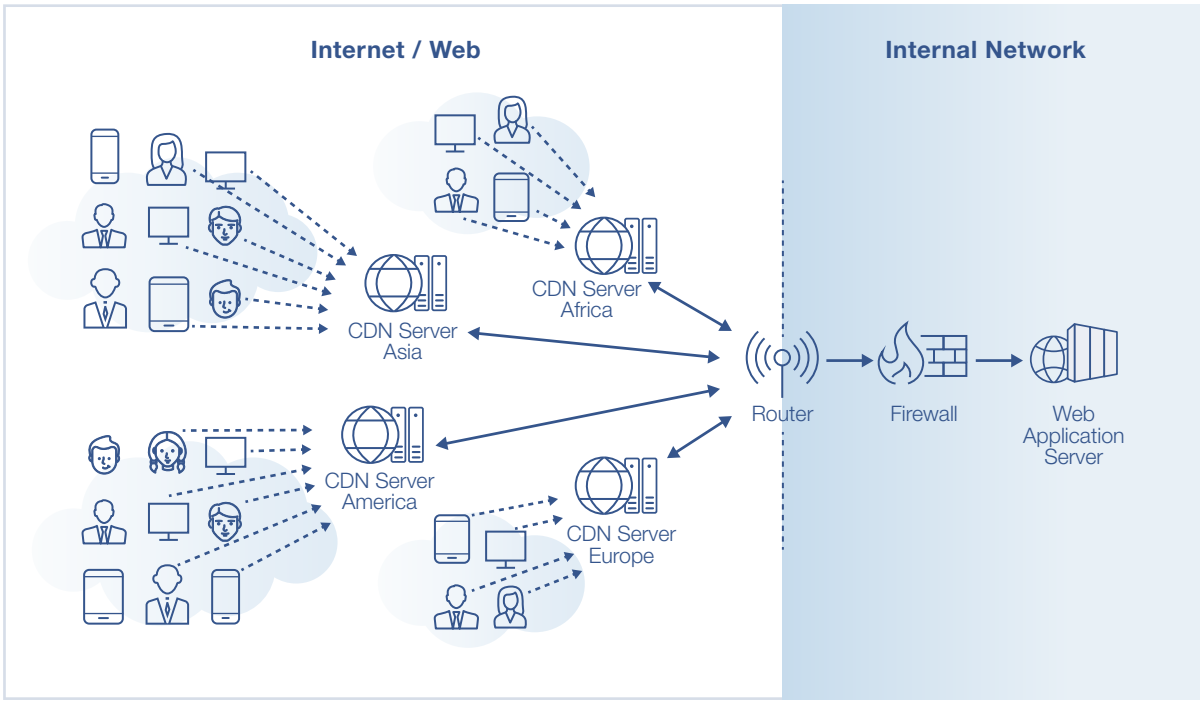
Deployment Location	Functional Role	DDoS Mitigation Capabilities
Cloud-Based	Static Content Serving	Good - Situational

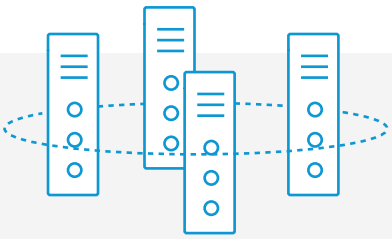
Content Delivery Networks (CDNs) use the DNS (Domain Name System) protocol to route traffic through the CDN provider's system.

CDNs are used to improve customers' access to website 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.

CDNs will only protect organizations against attacks that use the DNS names as their target. 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.

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





On-Prem. Based Solutions

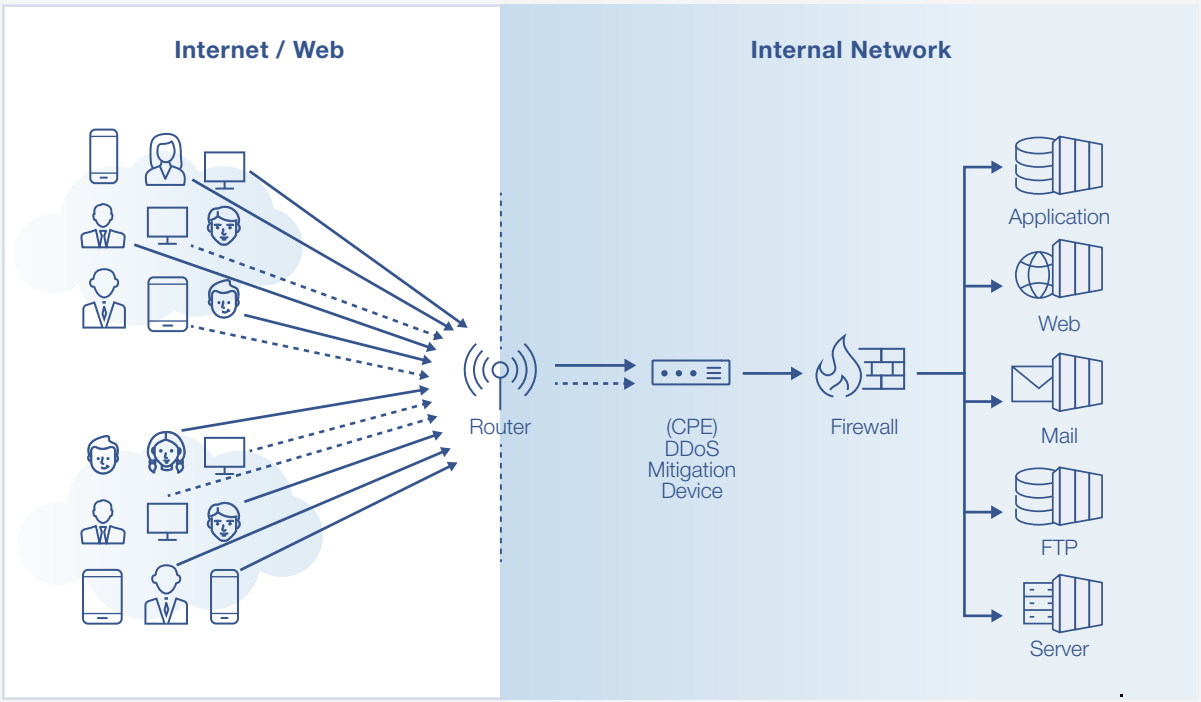
Vendor Appliances (Customer Premises Equipment - CPE)

Deployment Location	Functional Role	DDoS Mitigation Capabilities
On-Prem.	DDoS Mitigation and Protection	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 organization's network, after the router but before reaching the internal network infrastructure, E.g. Firewalls, Load Balancers etc.
Many of the devices deliver in-depth traffic analysis, bandwidth monitoring, and anomaly reports, allowing for better network traffic planning and DDoS attack analysis. Post-attack forensics may provide lessons learned, so the systems can be better tuned for mitigation of future attacks.

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.

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



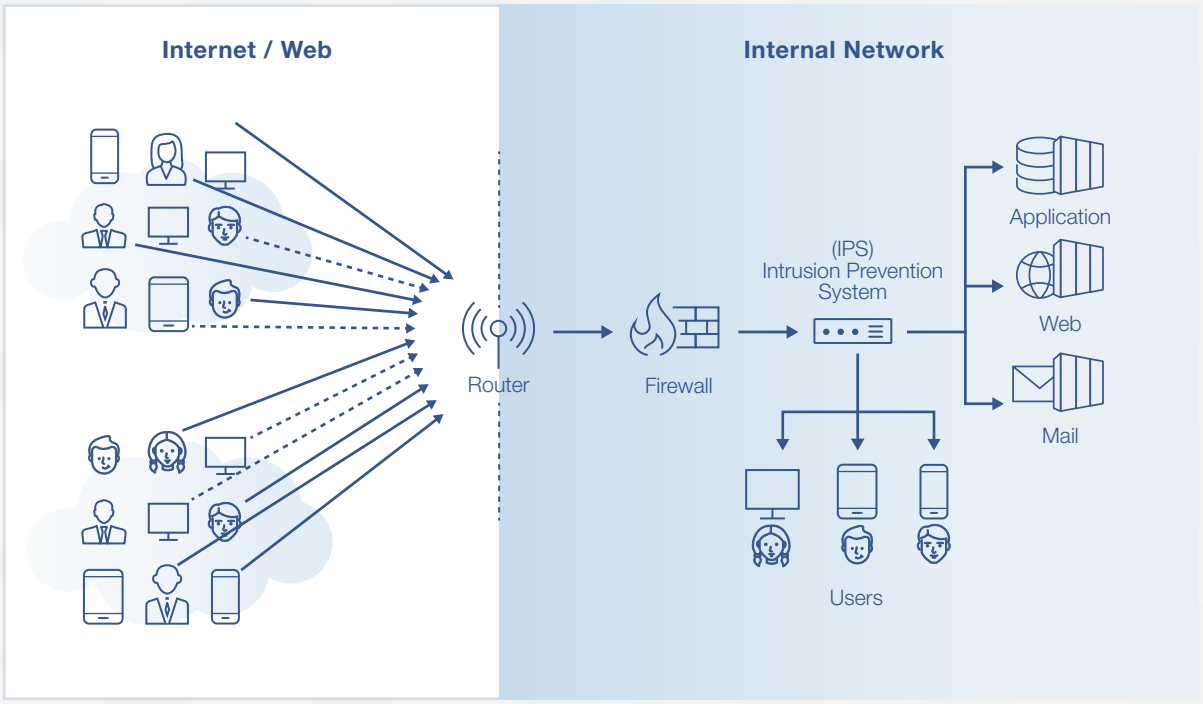
Intrusion Prevention Systems (IPS)

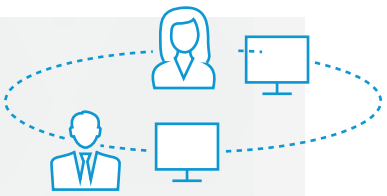
Deployment Location	Functional Role	DDoS Mitigation Capabilities
On-Prem.	Detecting and Stopping Cyber Attacks	Poor

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. 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.

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.

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





Web Application Firewalls (WAFs)

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

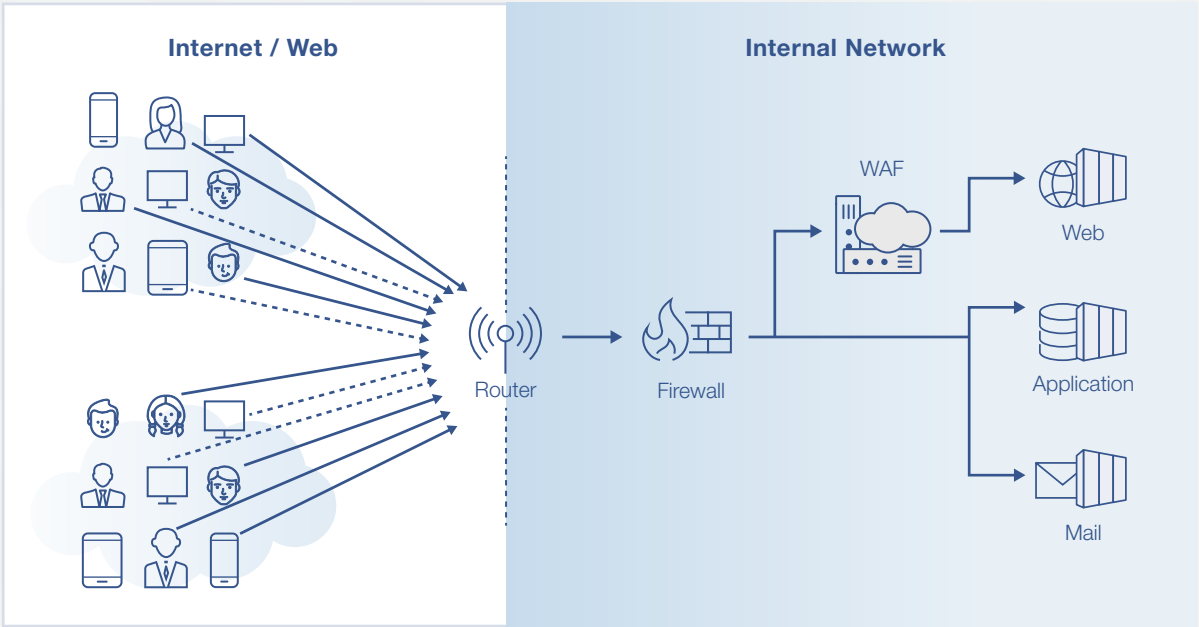
WAFs perform multiple functions – intrusion detection, DDoS attack detection and prevention. They analyze application traffic, distinguish potential risks from legitimate usage, control access to applications and services by applying a set of rules to the incoming HTTP traffic. They perform deep-packet inspections by locating, identifying, classifying, rerouting and/or blocking packets with specific data or code payloads. 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. Apparently, it does not protect against volumetric attacks on layers 3 and 4 that target network availability.

WAFs depend on white-listing and black-listing, which means they must be updated continuously.

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



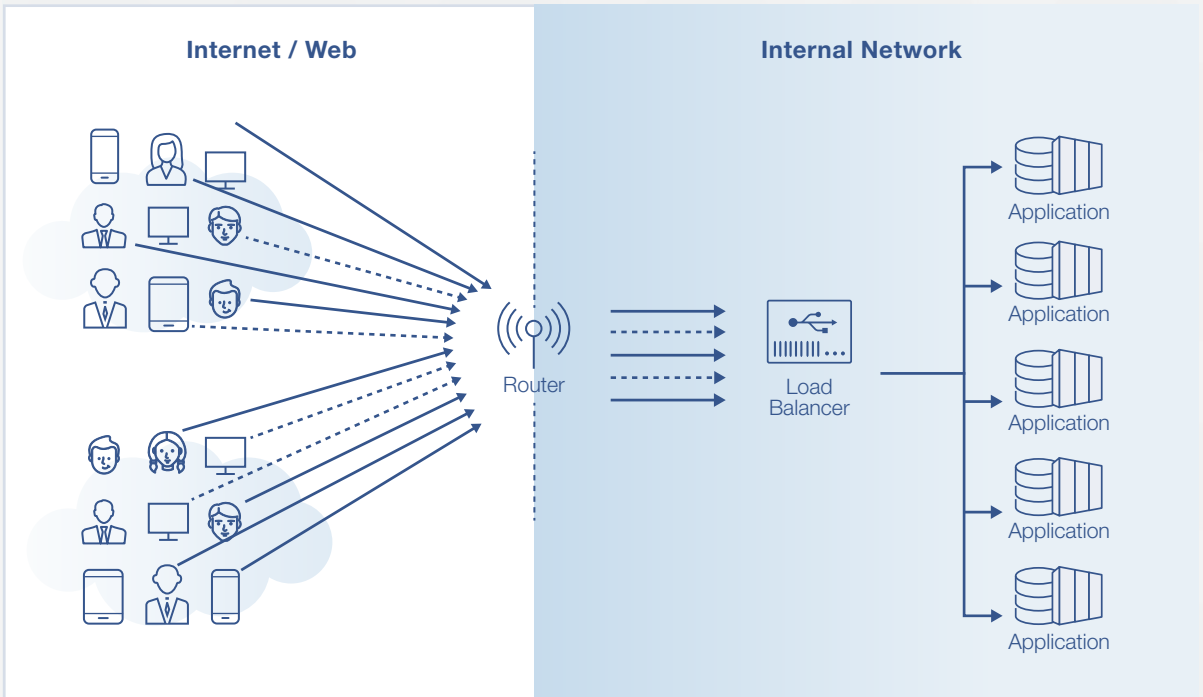
Load Balancer

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

A Load Balancer receives traffic from many clients and distributes that traffic evenly between multiple application servers of the same type. It 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. A Load Balancer can help offset DDoS Attacks by distributing the malicious traffic between the application servers. Unfortunately, without a robust 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.

Figure 7: Illustration of a Load Balancer



Firewall

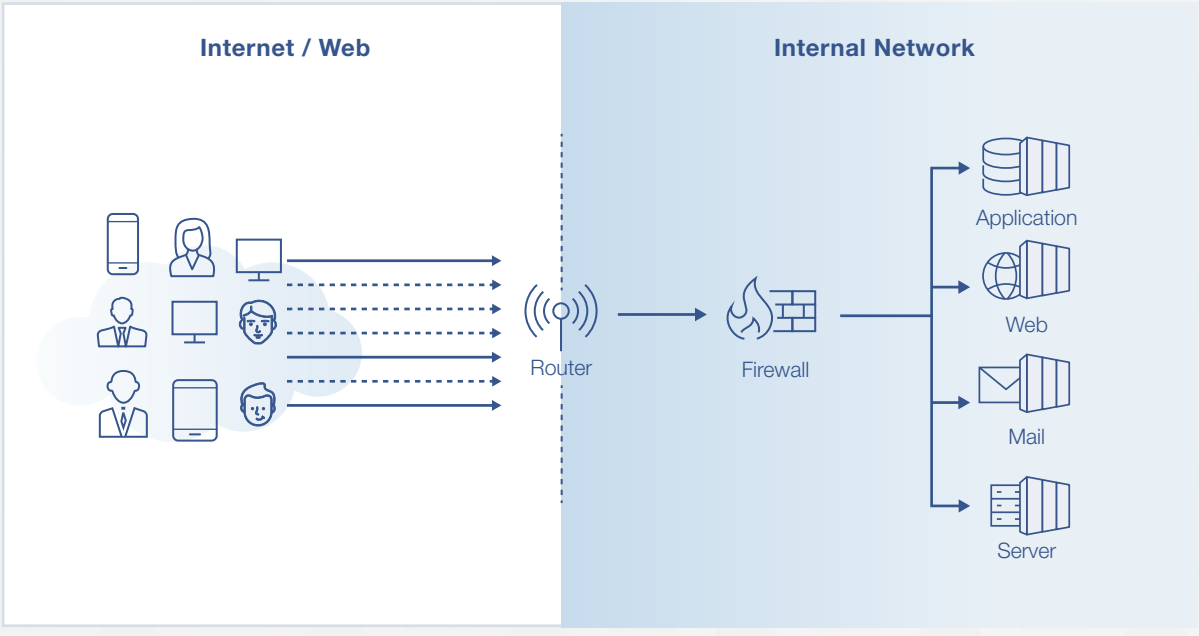
Deployment Location	Functional Role	DDoS Mitigation Capabilities
On-Prem.	Rule-Based Traffic Filtering	Mild

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 the setup time, and filters according to the allowed packet types and the connection states. 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. Seemingly, 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 number 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.

Figure 8: Illustration of a Firewall



CONCLUSION

Choosing the right combination of mitigation devices requires an understanding of how each devices' capabilities match your environment's 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.

RADAR™, MazeBolt's new patented technology solution is part of the MazeBolt security platform. RADAR™ simulates DDoS attacks continuously and non-disruptively. Delivering advanced intelligence through straightforward reports on how to remediate the detected DDoS vulnerabilities found. With RADAR™ organizations can achieve, maintain, and verify the continuous closing of their DDoS vulnerability gaps. Reducing and maintaining the vulnerability level of a damaging DDoS attack from an average of 48% to under 2% ongoing.

RESOURCES

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

About MazeBolt

MazeBolt is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and elimination and working with any mitigation system to provide end to end full coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before an attack happens.