haltdos

Why Firewalls and Intrusion Prevention System fail to mitigate **DDoS** Attacks?

Whitepaper

CONNECT WITH US:

www.haltdos.com

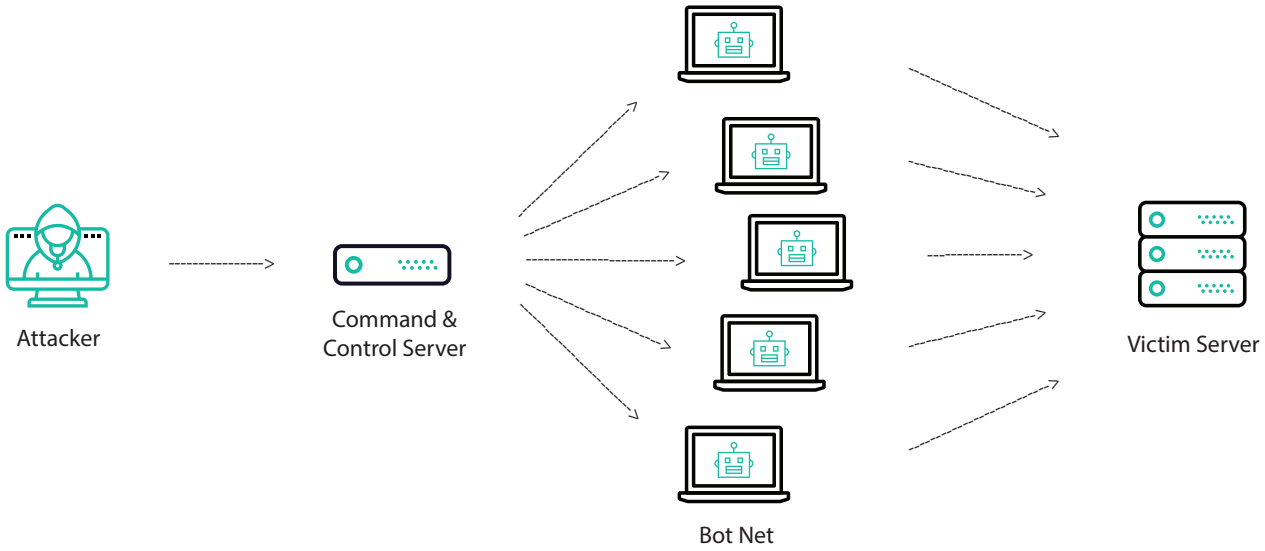
EXECUTIVE SUMMARY

This white paper is written to help organizations understand why Firewalls and Intrusion Prevention System fail to mitigate DDoS Attacks? Confidentiality, integrity, and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. In order to secure their assets, organization's security team rely on firewall, intrusion prevention system (IPS) and application firewall (WAF) to prevent a breach of the CIA triad. Firewalls are a policy enforcer that prevents unauthorized access to data and services whereas IPS block break-in attempts aimed at data theft and corruption. While these security controls are essential elements to a sound security strategy, contrary to common belief, they are ill-equipped to mitigate modern day DDoS attacks. Why? Because they were never designed to mitigate the loss of network/service availability.

Connect with us on facebook, twitter, linkedIn or through email (info@haltdos.com) to know more about how HaltDos can protect your infrastructure.

It's in their Design

DDoS attacks are aimed to disrupt the normal functioning of a system by depleting its resources till it is unable to serve its users resulting in downtime or loss of availability. As inline stateful devices, firewalls and IPS track all connections for inspection and store them in a connection table. Every packet is matched against the connection table to verify that it was transmitted over an established, legitimate connection. The typical connection table can store tens of thousands of active connections, which is sufficient for normal network activity. However, a DDoS attack may include thousands of packets per second. As a result, even before your servers give in to DDoS, it is likely that the firewall or IPS are already toast.



What about the big picture?

Firewalls and IPS only examine individual sessions. DDoS attacks such as HTTP floods are composed of millions of legitimate sessions. Each session on its own is legitimate and it cannot be marked as a threat by firewalls and IPS. For instance, Sockstress is a DDoS attack tool that opens multiple TCP Sessions and does not send any data over them. How will firewalls and IPS mark them as a threat if no data is exchanged between the client and the server?

Firewalls and IPS do not start inspecting the request until the request is complete. Low and Slow DDoS attack such as Slowloris and R.U.D.Y. opens long running sessions with the web server that never complete their HTTP request. When too many such requests bypass them, web servers stop taking in more requests – causing DDoS.

Fill the white spaces with HaltDos

HaltDos focusses exclusively on availability threats such as **DDoS** attacks. It does not replace your firewall and IPS but augments them so that they can do their work without worrying about getting overwhelmed. Data centers and enterprises can deploy HaltDos in front of their firewall and IPS devices to also stop other application specific attacks and botnet communications and ensure continuity of service with zero downtime.

HaltDos On-Premises DDoS Protection

With the rise of botnets and DDoS attacks globally, it is important for every online business to have a DDoS protection in place to mitigate service outages risks. The DDoS attacks create massive business risks for any enterprise small or large. HaltDos's DDoS Mitigation Solution provide the highest level of network protection and proper mitigation techniques to prevent a variety of DDoS attacks from ever reaching the enterprise network and ensure 24*7*365 uptime of the online business operations.

HaltDos On-Premises DDoS Mitigation Solution Deployment:

- At deployment location, HaltDos mitigation appliances will be installed between the router (edge or aggregate) and the downstream switch / firewall.
- HaltDos mitigation appliances will provide bi-directional DDoS detection and mitigation supporting both SM mode optical fiber or copper connectivity.