CHECK POINT + L7 DEFENSE
DDOS ATTACK MITIGATION

Benefits

- Automatic real time detection and mitigation of applicative DDoS threats
- Auto discovery of web systems and full transparency
- No need for updates as applications are updated (auto training)
- Highly scalable for mitigation of IoT-enabled DDoS attacks

INSIGHTS

In today's threat landscape, Denial of Service (DoS) attacks are increasing in number, speed and complexity. Denial of Service and Distributed Denial of Service (DDoS) attacks are relatively easy to carry out, and can cause serious damage to companies who rely on web services to operate.

L7 DEFENSE ADVANTAGE

L7 Defense Ammune® contains a state of the art algorithm that is inspired by the immune system model and enhanced by several "mini" Machine Learning models. No prior knowledge of the attack method or its parameters is required. This enables us to detect unknown application DDoS attack vectors. Attacks within encrypted traffic are also detected.

Ammune operates autonomously, without the need for operator supervision or intervention, defending web systems and maintaining normal performance level Service Level Agreements (SLA). Ammune has been tested at several data centers. Advanced DDoS attacks that were skipped by existing defense systems were identified by Ammune, with very low rates of false positive and false negatives.

Ammune is a virtual server based system that is deployed either on-premises or in the cloud. The system introduces no latency and scales easily and economically with the customer's own network. When deployed, Ammune performs automatic discovery of the protected web systems and servers, requiring minimal effort even for large scale customers.

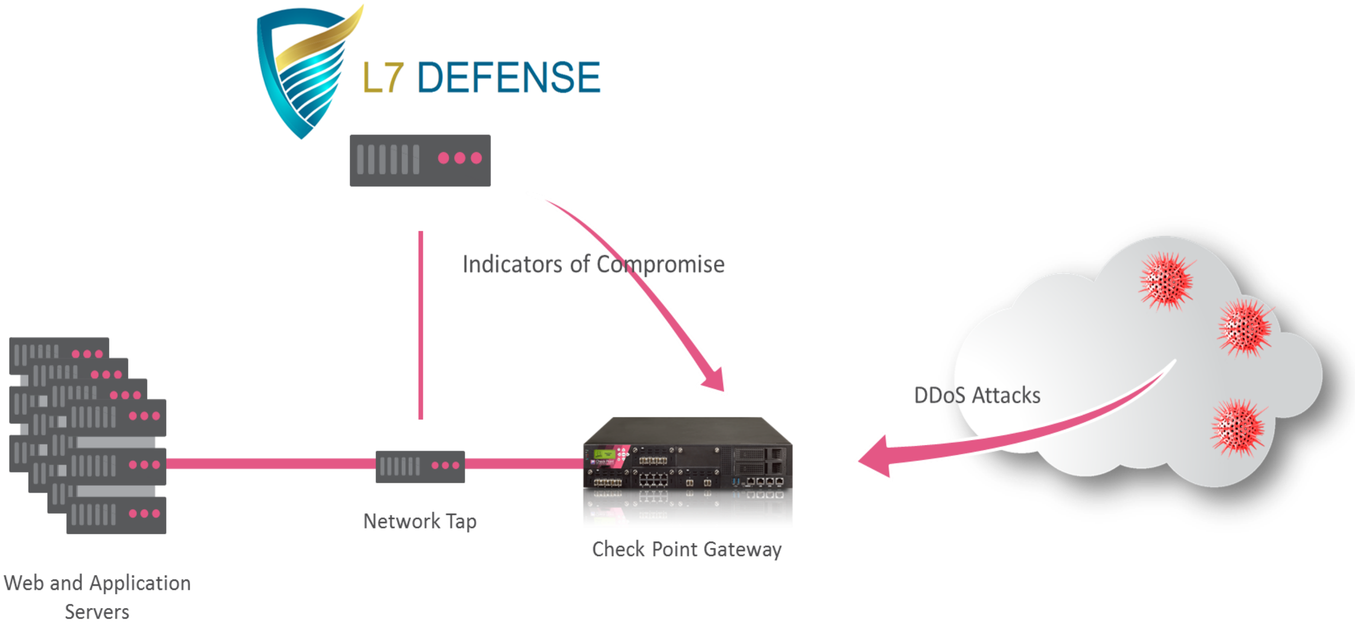
JOINT SOLUTION

Ammune is installed between Check Point Next Generation Threat Prevention appliances and web servers in either inline reverse proxy mode or monitoring mode with a network tap. During a DDoS attack, Ammune generates and manages a set of attack sources (IP addresses) and creates an optimal set of patterns to block. We strive to capture as much attack traffic as is possible with a minimal false positive rate. Ammune adds these Indicators of Compromise (IoC) to the Check Point gateways and updates them every few seconds to block the attack.

Ammune® detects and orchestrates the mitigation of attacks, while the mitigation itself happens on the Check Point gateway. Ammune® status updates and alerts are visible directly within Check Point SmartLog and SmartEvent. Our joint solution is available both on premise and in cloud environments.

A BETTER APPROACH TO MITIGATE DDOS ATTACKS

- Ammune is among the first commercially available "Natural Intelligence" cyber security systems. Just like the natural immune system that are capable of detecting variations in the antigen patterns of attacking viruses and bacteria without destroying the host cells, Ammune is capable of identifying DDoS attack vectors patterns with high precision and accuracy. We do this automatically with almost no mistakes even at extreme traffic and attacks scenarios, avoiding "auto-immune" responses.
- A critical issue for clients is that the system adapts itself automatically to frequent changes at the applicative systems under protection. Auto-updating is scheduled automatically to take place every few seconds, just after the full auto-discovery process (which is set for 1-hour) is finalized. There is no need to prepare for new web application versions uploaded to production, as Ammune® will just incorporate this into its baseline and move on.



Check Point and L7 Defense DDoS Attack Mitigation

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest network cyber security vendor globally, providing industry-leading solutions and protecting customers from cyberattacks with an unmatched catch rate of malware and other types of threats. Check Point offers a complete security architecture defending enterprises – from networks to mobile devices – in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes.

ABOUT L7 DEFENSE

L7 Defense developed a breakthrough technology named Ammune® for mitigating Advanced Distributed Denial of Service (DDoS) Attacks, automatically and in real time. Ammune® contains state of the art algorithm, inspired by the immune model and enhanced with several "mini" Machine Learning models. It does not require any prior knowledge of the attack method or any of its parameters and hence can cope automatically with unknown applicative DDoS attack vectors. More information is available at www.l7defense.com.