Nominee: SOLARFLARE

Nomination title: SolarSecure: Distributed, Active Security

According to Enterprise Strategy Group, there is a new class of server network I/O is enabling an application-centric paradigm by placing monitoring and capture at or in the server, in contrast to the traditional network-centric architecture that uses dedicated and relatively expensive capture and monitoring appliances on an overlay network.

Traditionally host systems have been left out of the network defense in depth paradigm due to the computational cost, and technology tradeoffs required to deploy robust security, and monitoring solutions on production systems. Solarflare helped address this problem by introducing SolarSecure, which enables high speed packet capture, filtering, bridging, and Denial of Service defenses within the host.

SolarSecure is the first distributed, active security solution that is implemented within network servers, the prime targets of cyber attacks. It is a first-of-its-kind security solution that empowers the enterprise with the technological sophistication necessary to effectively capture and enforce security policies to rate limit and block malicious traffic before it penetrates the operating system or applications on network servers, all without requiring any additional hardware.

SolarSecure adds security and monitoring capabilities to all servers in the enterprise network, including Distributed Denial of Service (DDoS), Packet Capture, Time Synchronization and Time Stamping, providing active protection throughout an organization. SolarSecure also provides a fully compatible interface with other network security and monitoring tools, and security, information, and event management (SIEM) systems.

Denial of service (DoS) or Distributed Denial of Service (DDoS) attacks represent a growing trend in network security, and succeed by making a machine, service, or network resource unavailable to its intended users by exhausting network resources. One common method of attack involves saturating a target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.

SolarSecure DDoS introduces an extra layer of security at the host server that adds protection against DoS and DDoS attacks not available in operating systems, and works in conjunction with routers, firewalls and the host operating systems. SolarSecure DDoS Linux kernel driver features SYN cookies, blocking, filtering, rate limiting and an API that enables connectors to rules sets or threat intelligence data services for advanced threat detection.

At the core of Solarflare's DDoS attack prevention is the SolarSecure Filter Engine, which is integrated with the network adapter and blocks attacks before they penetrate the OS or impact the application running on the server. It filters and blocks, rate limits and alerts on bad traffic and includes APIs that enable connectors to customers' policies and rule sets, plus third-party threat intelligence data services. The Filter Engine detects bad traffic much earlier, absorbs attacks longer without degradation of good traffic and scales as you add servers. It also increases headroom and responsiveness in the face of DDoS attacks. In fact, tests utilizing the Filter Engine showed an 8X improvement in server headroom – the ability to continue to serve good traffic while withstanding the onslaught of malicious traffic.

In benchmark testing, a SolarSecure enabled web server was able to withstand an attack rate of 120,000 connections/second without degradation in performance versus a rate of only 15,000 connections/second on a web server operating without SolarSecure. Also, in SYN flood tests, the SolarSecure Filter Engine performed 180% better than the competition. Solarflare hardware and software delivered 16 million packets per second – at 60 bytes per packet – compared to the next best alternative, which delivered just 9 million packets per second.

The SolarSecure security layer is deployed with Solarflare's industry-leading Flareon™ 10/40GbE network adapters to seamlessly deploy a new level of protection across the enterprise, delivering integrated, real-time, active protection of targeted corporate assets.

Why nominee should win

- Solarflare's SolarSecure Filter Engine equips the server to block malicious attacks before they penetrate the server operating system.

- The SolarSecure-enabled Web server is able to withstand an attack rate of 120,000 connections/second. The Web server without SolarSecure is only able to withstand an attack rate of less than 15,000 connections/second.

- SolarSecure can increase a server's headroom 8 to 10X in the face of DDoS attack (attached)

- CloudFlare reports that the Solarflare SFN5122F server adapters run circles around other offerings in the market. In flood tests, they performed 180% better than the competition. (attached)