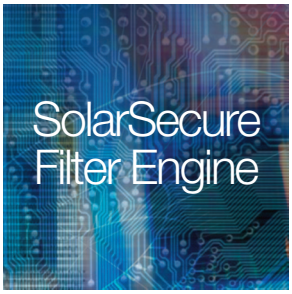


SolarSecure Filter Engine

SolarSecure™ is the first distributed, active security solution that is implemented within network servers – the prime targets of cyber attacks. SolarSecure equips servers to precisely record, capture, filter and block malicious traffic before it penetrates the server. SolarSecure Filter Engine, a high performance packet filter engine, can selectively rate-limit or even block traffic from network sources perceived or identified as potentially harmful, thus avoiding interruptions to business critical systems and avoiding suspension of service.

Solarflare SolarSecure

SolarSecure is a first-of-its-kind set of applications that empower the network with the technological sophistication necessary to effectively capture, identify and block malicious traffic before it penetrates the operating system or applications on network servers and enforce security policies, all without requiring any additional hardware.

The SolarSecure active security layer is built on Solarflare's industry-leading Flareon™ SFN7000 series 10/40GbE network adapters. SolarSecure provides a new level of protection across the network, delivering integrated, real-time, active protection of targeted assets. Today, these capabilities include time synchronization, packet capture, packet filtering and rate limiting for distributed denial of service (DDoS) protection.

DoS/DDoS

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 system or network resources. One common method of attack involves saturating the 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 Filter Engine

At the core of Solarflare's DDoS attack prevention you'll find the SolarSecure Filter Engine – a high performance packet filter engine. The SolarSecure Filter Engine uses a pseudo-microcode instruction set to configure the filter engine to selectively accept, reject or rate-limit packets based on packet headers and packet contents. The microcode used for filtering is under user control. So, the filtering behavior is highly configurable and can be customized for particular customer use cases.

The SolarSecure Filter Engine enables "bad" traffic to be detected very early in the network stack, so DDOS attacks can be absorbed without degradation of "good" traffic. The filter engine provides the ability to efficiently block or rate limit packets based on their contents. It is designed to work on large address sets and can scale to configurations with lookups against millions of IP addresses. In addition to network level address matching with associated blocking or rate limiting, the filtering engine supports request-level deep packet inspection. For example, HTTP requests can be inspected and connections aborted dependent on the contents of the HTTP headers.

Instruction Set

SolarSecure Filter Engine instructions, defined using the pseudo-microcode instruction set, enable the filter engine to inspect and test individual header fields or payload data from received packets.

SolarflareFilterEngine

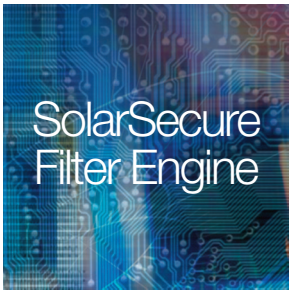
sales@solarflare.com

US 1.949.581.6830 x2930

UK +44 (0)1223 477171

HK +852 2624-8868

www.solarflare.com



SolarflareFilterEngine

Instructions exist for specific operations such as isolating the packet source IP address before checking against a lookup table or checking flags set in TCP packets. Other instructions give the user complete flexibility to select any multi-byte sections from a packet.

Command Line Interface

The command line interface is used to initiate a filter engine instance for selected Solarflare adapter interfaces. All packets received at the interface are then subject to the microcode filter instructions and lookup tables. Commands are available to load IP lookup tables, enable additional interfaces to use a filter engine or to switch an interface to another filter engine instance. Commands can be invoked from the command line or can be placed directly into the header section of the configuration file.

Configuration File

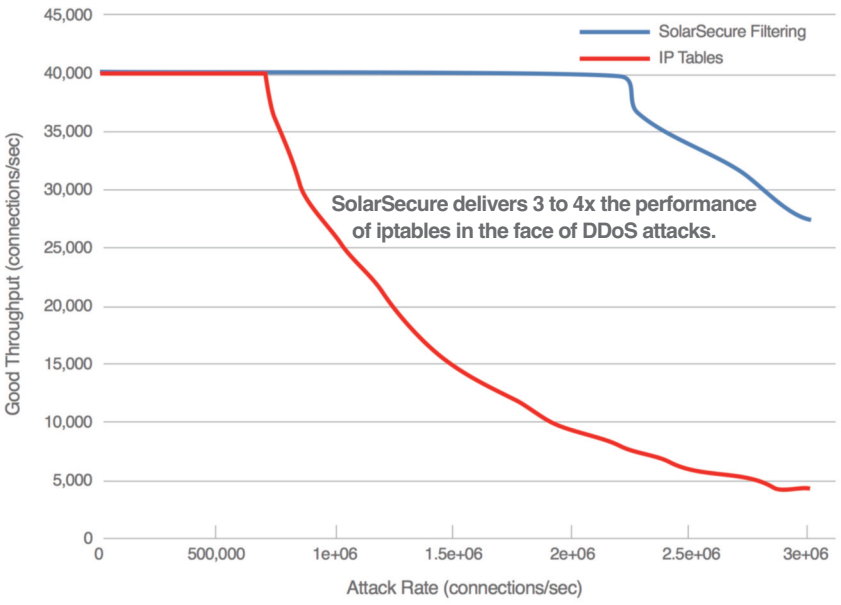
The configuration file is used to define the pseudo-microcode instructions which the filter engine will apply to incoming packets. A single configuration file can be loaded into a filter engine instance and consists of:

- configuration commands
- pseudo-microcode instructions
- IP lookup tables

Lookup Tables

The user can define and populate multiple lookup tables of IP addresses. Each address entry in a lookup table has an associated action which decides how a packet directed to the lookup table is processed. Lookup tables can be defined and populated directly in the configuration file or can be loaded into the filter engine from files. Additional entries can be added to existing tables and entries can be removed from tables without interruption to the filter engine operation.

Packet-Level Filtering – A 3 to 4x Improvement in Headroom



In benchmark testing, a SolarSecure Filter Engine enabled server shows a 3 to 4x improvement in packet-level filtering server headroom over iptables. Server headroom refers to the server's ability to continue to serve "good" traffic while withstanding a DDOS attack.

SOLARFLARE®

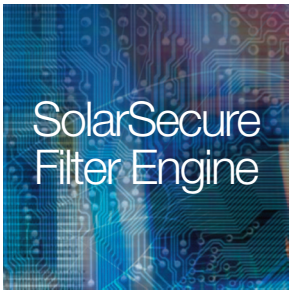
sales@solarflare.com

US 1.949.581.6830 x2930

UK +44 (0)1223 477171

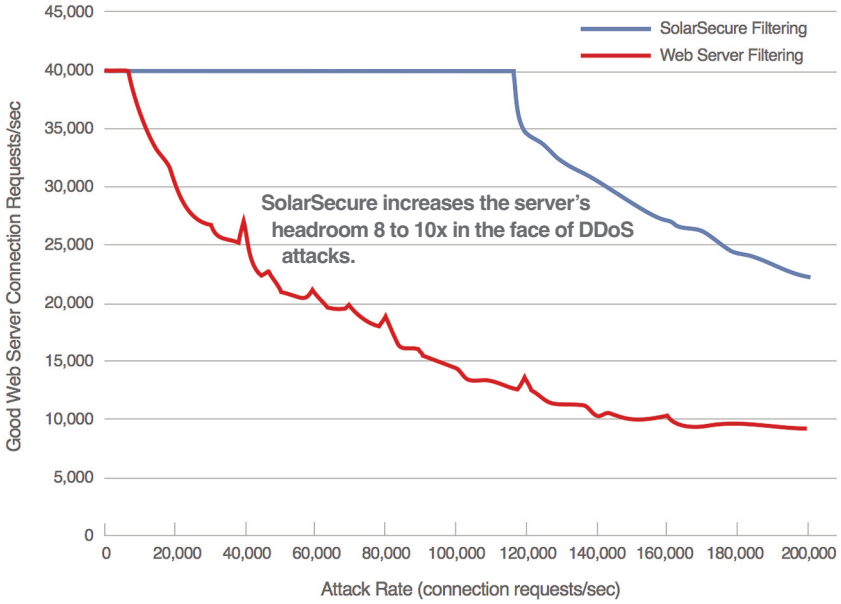
HK +852 2624-8868

www.solarflare.com



SolarflareFilterEngine

Request-Level Filtering – An 8 to 10x Improvement in Headroom



With request-level filtering, the SolarSecure Filter Engine shows an 8 to 10x improvement in server headroom over performing request-level filtering within the webserver. Figures show "good" customer traffic throughput in connections per second, and the degradation in the ability to service this traffic relative to a synthetic DDoS attack for packet-level filtering and request-level filtering.

Performance

Because the filter engine works in conjunction with the driver and the network adapter, it is highly efficient and has minimal performance load for normal traffic. It also provides a very low overhead packet discard path which allows it to excel at system defense when under DDoS attack. 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.

Hardware Requirements

- SolarSecure Filter Engine is supported on Solarflare Flareon™ SFN7000 series adapters which have the SolarSecure Filter Engine license installed

Software Requirements

- Solarflare SolarSecure compatible driver
- Red Hat Enterprise Linux 6 and 7
- SUSE Linux Enterprise Server 11and 12

Order Information

SFS-SSFE SolarSecure Filter Engine License plus one year maintenance

SOLARFLARE®

sales@solarflare.com

US 1.949.581.6830 x2930

UK +44 (0)1223 477171

HK +852 2624-8868

www.solarflare.com

SF-112758-CD Issue 2
SFS-FE_PB_033116