SOLARFLARE®

Automating SolarSecure Filter Engine Configuration

Technology Brief

Application Note – Automating SolarSecure Filter Engine Configuration

Executive Summary

Solarflare SolarSecure is a distributed active security solution implemented at the endpoint. Central to SolarSecure - which includes SolarSecure Filter Engine (SSFE), SolarCapture Pro, Trusted Server Adapter, and Precision Time - is a high performance packet filter engine that can be configured to selectively accept, reject or rate-limit packets. To automate the configuration of SSFE across an enterprise or cloud, SSFE can be used in conjunction with IT automation frameworks including Puppet, Chef, Ansible, SaltStack and CFEngine. An open source Puppet Module for SSFE is available on the Puppet Forge as an example of how SSFE can be automatically and reliably configured within an IT automation framework. This application note also details the straightforward single line installation of the SSFE Puppet Module.

SolarSecure

SolarSecure is the first distributed, active security solution that is implemented within the prime target of cyber attacks - the endpoints. It is seamlessly deployed and works with Solarflare network adapters to provide a new level of server protection for business critical systems and networks against cyber security breaches. SolarSecure includes SolarSecure Filter Engine (SSFE), SolarCapture Pro, Precision Time and Trusted Server Adapter. The SSFE high performance packet filter engine enables precise recording, capturing, filtering and blocking of malicious traffic before it penetrates the server. SSFE also allows “bad” traffic to be detected, blocked or rate limited based on their content and is designed to work on large address sets, scaling to configurations with lookups against millions of IP addresses. The detection is performed very early in the network stack so DDoS attacks can be absorbed without degradation of “good” traffic. The result is that SSFE augments existing perimeter and network defenses and enables business critical systems to avoid interruptions or suspension of service.

SSFE Configuration

The SolarSecure Filter Engine configuration elements include a configuration file and a scriptable CLI to create filters that are used by the Filter Engine to incoming packets. The configuration file can be loaded into a Filter Engine instance and consists of the configuration commands, the instructions, and lookup tables of IP addresses. The configuration commands include “dynamic” filters including filters for protocols, ports, networks, IPs, and URI/URL for deep packet inspection, and blocking (SW) / filtering (HW) / rate limiting.

IT Automation

IT configuration management is used for tracking, recording and update of a company’s IT infrastructure including the hardware and software. To accelerate deployment and reduce

SolarflareTechnologyBrief

sales@solarflare.com

US 1.949.581.6830 x2930

UK +44 (0)1223 477171

HK +852 2624-8868

www.solarflare.com

Automating SolarSecure Filter Engine Configuration

SolarflareTechnologyBrief

downtime, automation and simplification of configuration management software have led to the wide-scale deployment of IT automation frameworks. When SSFE configuration is used in conjunction with IT automation frameworks – including Puppet, Chef, Ansible, SaltStack and CFEngine, the configuration management can be reliably automated across an enterprise or cloud.

Puppet and Puppet Modules

Puppet, from Puppet Labs, is an IT automation solution that gives the user the power to easily automate repetitive tasks, quickly deploy critical applications, and proactively manage infrastructure. It automates every step of the software delivery process, from provisioning of physical and virtual machines to orchestration and reporting. Using a model with a Puppet Master communicating with Puppet Agents at each device, Puppet is able to define the state of the computer, storage and networking devices, test configuration changes, enforce desired states, and report on actual and desired state differences.

Puppet modules are self-contained bundles of code and data that ideally manage a single piece of software from installation through setup, configuration, and service management. A SSFE Puppet Module will be executed by Puppet as a “re-usable infrastructure-as-code” that is defined once but can be applied to thousands of machines. It will be simulated before any deployment changes are made, automatically and reliably enforced, and reported if any discrepancies exist.

SSFE Puppet Module

Solarflare has developed a Puppet Module for the SolarSecure Filter Engine. The module is available on Puppet Forge at https://forge.puppetlabs.com/solarflare. The SSFE Puppet Module provides the following capabilities:

1) Checks to make sure that SSFE is installed.
2) Eases implementation of SSFE firewall rules.
3) Monitors that the firewall rules are actively enforced.
4) Reports any changes to the rules or breaches.

If Puppet is already running, then simply execute the command

```
puppet module install solarflare/ssfe
```

to install the SSFE Puppet Module. The result is that the SSFE Puppet Module is executed automatically and reliably across the enterprise using the Puppet framework.

SOLARFLARE®

SF-115742-TC Issue 1
Automating_SSFE_Config_TB_020516

sales@solarflare.com

US 1.949.581.6830 x2930

UK +44 (0)1223 477171

HK +852 2624-8868

www.solarflare.com