Trends in Data Center Security

IP Traffic Inside the Data Center Creates a Security Risk

According to the Cisco Cloud Index report, over 90% of IP traffic is now within the data center if you include rack-local traffic, and it’s expected to grow 26% per year through 2020. For IT organizations, that means the security risk with the biggest impact is a breach “inside” the data center.

The Hyperscale Solution: Hardware Server Firewalls

With millions of servers inside their data centers, hyperscale cloud service providers need a security solution they can trust, that is affordable, and which can scale. The answer for major cloud service providers like Google is to instrument thousands of servers with their own security chips delivering line-speed packet inspection, that cannot be hacked with root access to the server OS, and which allow network engineers to define application-specific firewall policies down to a single server.

Secure Boot Stack and Machine Identity

“...The components are all Google-controlled, built, and hardened. With each new generation of hardware we strive to continually improve security: for example, depending on the generation of server design, we root the trust of the boot chain in either a lockable firmware chip, a microcontroller running Google-written security code, or the above mentioned Google-designed security chip.”

https://cloud.google.com/security/security-design/
SolarSecure: Hardware Server Firewalls for the Masses

Solarflare brings server firewalls to the masses with SolarSecure, a NIC-based security application. Firewalls are shipped with every XtremeScale™ 8000 Series Solarflare NIC. Once enabled by the SolarSecure Manager, the firewalls discover normal traffic flows between servers, monitor every packet, and are set to send alerts and/or “lock” the server by dropping out of policy packets when they’re detected.

SolarSecure represents a trend which will soon be a best practice for Enterprise IT: fast, cost-effective, scalable and trusted NIC-based server firewalls on every server.

Summary of Features and Benefits

**An Important New Best Practice** — Driven by hyperscale CSPs, the deployment of server firewalls is a new best practice for securing traffic inside the data center.

**Secure Every Server** — Because SolarSecure resides on a NIC that’s in every server, it’s time to think in terms of firewalling every server in the data center with its own monitoring, alerting and locking policy.

**Tamper-Resistant** — The hardware based solution requires no software on the application servers, making SolarSecure highly tamper resistant, even to hackers with server and switch OS root permissions.

**Packet-Level Security Analytics** — The XtremePacket Engine inside Solarflare NIC ASICs inspects every packet in real-time, and the network flow data is used by SolarSecure and third party software for packet-level security analytics.

**Ultra Low Latency** — Inspecting every packet adds less than 250ns of latency, 10x faster than firewall appliances. SolarSecure is also interoperable with Solarflare Onload™ kernel bypass software for application acceleration.

**Highly Scalable** — Scales to thousands of servers by simply enabling firewalls on your Solarflare NICs.

**Open Architecture** — Use SolarSecure management and analytics, or integrate with your framework of choice.
SolarSecure Specifications

Firewall Capability

- Implement unique whitelist or blacklist filters per local IP address.
- Filter millions of headers every second, deciding whether to allow or drop each packet.
- Filter for IP address, port number, IP protocol and Ethernet protocol.
- Filter on IP address subnets.
- Supports 5,000 filters and 1,000 counters.
- Low latency data path – filtering adds less than 250ns.
- Allows separate filtering for TCP client and TCP server applications (to support “Established” firewall rule semantics).
- Isolate a server by switching quickly to an alternative rule set.

Management Capabilities

- Manage security policies for the network, breaking down policies into individual firewall rules.
- New application flows are discovered and reported.
- Secure binding of NIC cards to ServerLock Manager establishes an encrypted control channel.
- User alerts.
- Security event management.

Configurations Supported

- Bare-metal, containers and virtualization configurations supported.
- Driver support for Linux, Windows, VMware, KVM and Hyper-V.
- Compatible with other Solarflare products, including Onload, TCP Direct, and Precision Timing Protocol software.
- Runs on SFN8000 series NICs, and beyond.

SolarSecure Manager is a clustered server application for configuring Solarflare XtremeScale NICs and for monitoring their security. The network flow information from the NICs can be accessed from the SolarSecure Manager GUI, a CLI, or through third party analytics software using the API.