CASE STUDY

Army Cyber School Leverages FD.io to Achieve Superior Network Performance and Scale

Use case enables training programs and cloud infrastructure to support a growing user base

Business

The US Army Cyber Center of Excellence was started in October, 2015. As cyberspace is now one of the key defense domains along with land, sea and air, the center has the important task of training army soldiers in cyber technologies. The school takes the standards provided by the U.S. Cyber Command and the U.S. Army as key inputs for formulating learning outcomes. The objectives are to equip the students with sufficient hands-on cybersecurity knowledge so they become adept in cyber warfare, both in cyber defense as well as offensive campaigns. While the standards dictate the learning objectives, the school creates the content and delivery mechanisms that are timely and relevant in the context of a rapidly evolving cyber domain. The school follows an agile process for creating, updating and delivering training content spanning documents, scripts, system resources provisioning (target systems, attacker nodes and defending nodes [VMs/containers]), using an automated revision control approach or "training-as-code". The formal name for the solution is "Broadband Handrail" to denote the ongoing support to students and alumni get through their cybersecurity learning.

The school trains more than 500 students annually. The students come from a range of educational levels, from high school graduates to college graduates with different majors. The school also provides the alumni access to the school training systems and resources as long as they are in the service--allowing them to refresh their knowledge and continue contributing to the knowledge base. Currently, the number of total active users is more than 8,000 and growing.

Challenges

With the ongoing proliferation of always-on cloud-connected communication devices, computing equipment and the Internet of Things (IOT), cyber attack vectors and trends are evolving at a rapid pace. The school recognizes the need for high performance, low-cost, open standards-based agile cloud-based environment to develop, deliver and update relevant training courses. Despite being a part of a highly structured operating environment, the school has been able to deliver an innovative and agile model for the cloud using already available hardware infrastructure, e.g. servers; internet connectivity, e.g. LTE; and facilities. The private cloud is used for both hosting hands-on lab exercises and ad-hoc experiments.

The school prefers open source solutions for transparency, community-driven innovation, increased agility, and the ability to run on high volume, commodity hardware. It selected solutions such as Linux and OpenStack for compute and storage software needs. Until recently, the school had been using pfSense® open-source network connectivity and security solution for its cloud networking and security software needs. pfSense is a widely used open-source secure routing and firewall solution.

Some of the upcoming performance and scale needs of the private cloud are to support:

- 8,000 and growing user user base using thousands of tenant networks
- 100 Gbps line rate east-west traffic with routing, network address translation (NAT), port forwarding, and firewall with policy enforcement
- Several thousand route configurations in the network security solution
- IPSec and Layer 7 security functions such as threat detection/protection, Anti-X[1] without materially degrading performance
- API based dynamic configuration and control
- Various CPU architectures such as Intel, arm, MIPS, and Power[2]

As the school's east-west network traffic needs have been growing progressively, the pfSense-based solution had become a bottleneck in terms of performance, scale and agility needs. The school wanted not only to overcome the bottlenecks in terms of current needs, but also to "future provision" the capacity for next few years to streamline the infrastructure procurement approval process. For example, the network may need to support experiments such as spinning up 10,000 containers acting as BGP routers. The entire learning environment needs to be enabled via self-service automated user portal.

In summary the school needs a high performance, scalable, robust, low cost open, programmable, source network forwarding and security solution that can efficiently run on commodity hardware already available.

[1] A combination of anti-virus, anti-spam, anti-spyware, anti-theft etc.

[2] The various trademarks belong to the rightful owners.

Solution

To solve the east-west network performance and scale problem, the school considered several alternatives to pfSense, including commercial software, proprietary integrated hardware and software, and TNSR from Netgate. TNSR is an open source advanced router, firewall and VPN networking solution with enterprise grade quality, high-performance and programmable management capabilities. At the core of the TNSR solution are two highly efficient open source packet processing functions, FD.io project and DPDK. These packet processing projects are both part of the Linux Foundation, as is the Free Range Routing (FRR) project with the product's control plane. The school ultimately chose TNSR based on FD.io and DPDK. The TNSR block diagram is illustrated in Figure 1.

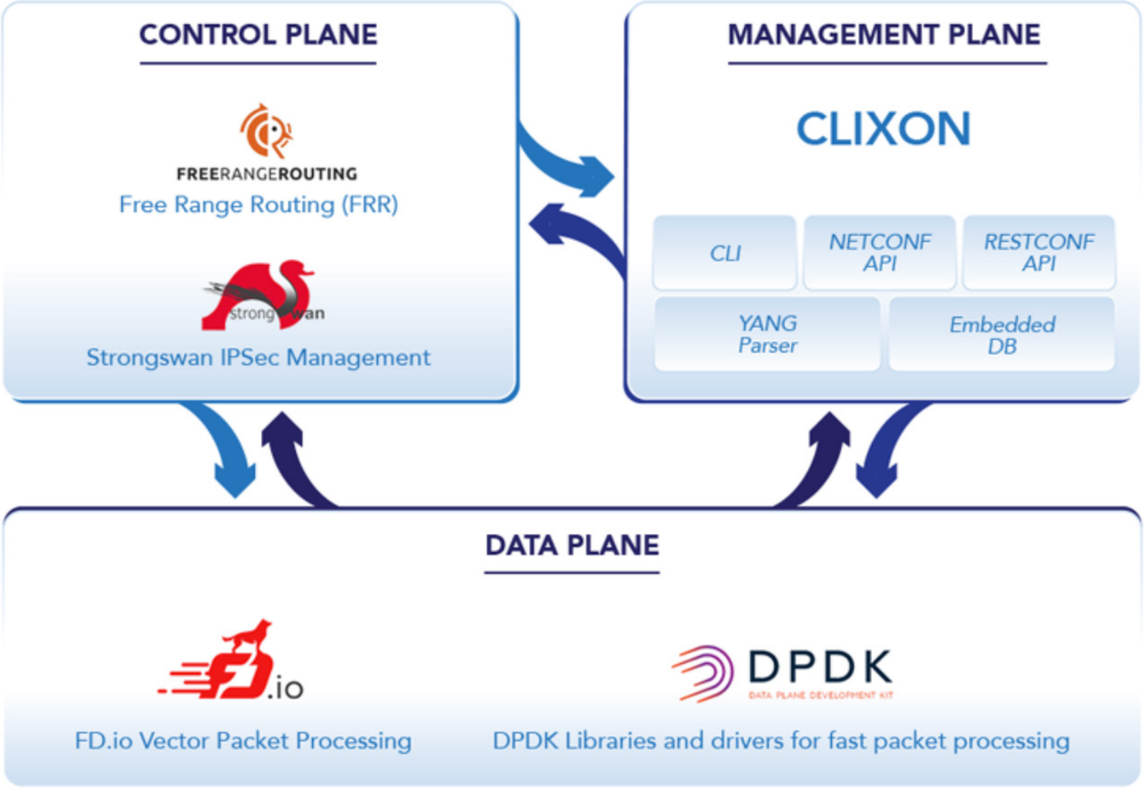
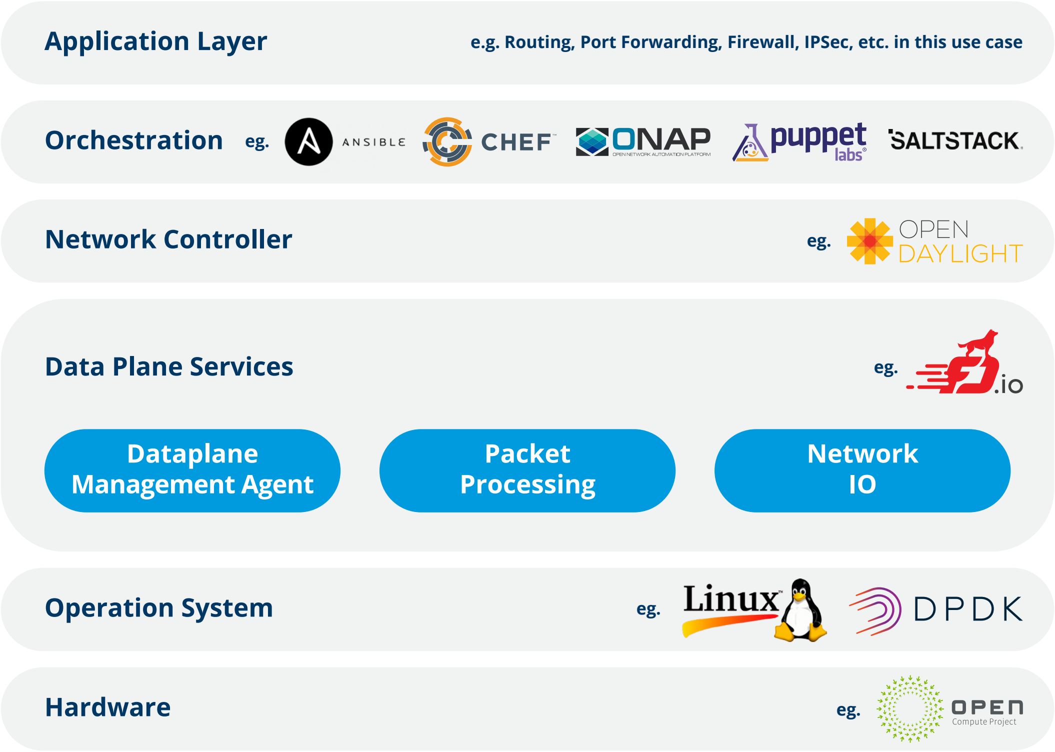


Figure 1 TNSR Block Diagram

FD.io (Fast data – Input/Output) is a set of Linux Foundation projects and libraries that support robust, flexible, programmable and composable services on commodity hardware platforms. FD.io offers software-based high-performance, low-latency and resource-efficient networking packet processing solutions for bare metal, VM and Cloud Native(container) in a combination of deployment environments.

A key component of FD.io is the Vector Packet Processing (VPP) library. VPP is a highly modular, flexible software packet processing block allowing for new packet processing functions to be easily “plugged in” without changes to the underlying code base. The main innovation in VPP is that it processes a number of packets in parallel instead of one at a time. This spreads the overhead of lookups and instruction cache code fetches across an entire set of packets - contributing to a dramatic improvement in efficiency. Hence, the performance scales linearly in proportion with deployed CPU/thread count in a deterministic manner, and with low latency. FD.io supports developer friendly features such as runtime counters (for throughput, IPC, errors, etc.), pipeline tracing facilities, multi-language API bindings and VPP command line introspection. This efficiency and flexibility gives developers and integrators the potential to easily build a variety of packet processing solutions ranging from layer 2 all the way up to layer 7 applications. Fd.io VPP readily supports widely used network functions such as layer 2 - layer 4 stack, IPSec and more. When combined with DPDK, VPP processing can occur in user mode using a polling driver instead of being interrupt driven. This further contributes to its performance and scale benefits.

Figure 2 below describes how FD.io fits in the broader ecosystem of open source networking and computing initiatives.



Application Layer — e.g. Routing, Port Forwarding, Firewall, IPSec, etc. in this use case

Orchestration — eg.

Network Controller — eg.

Data Plane Services — eg.

Dataplane Management Agent

Packet Processing

Network IO

Operation System — eg.

Hardware — eg.

Figure 2 FD.io in the overall cloud stack

The school chose the FD.io-based TNSR solution since it fit the school's above-listed networking needs in terms of being open-source, high performance, scalable, capable of running on commodity hardware, programmable and cost efficient. The performance and scale were achieved on existing hardware without any additional capital expenditures. The programmable management capability aligned with the school's agile continuous integration (CI), and continuous delivery (CD) methodology of rolling out the Broadband Handrail program.

Results

TNSR, with FD.io VPP and DPDK at its core, delivers high-performance packet processing with low latency for routing, NAT, port forwarding, firewall functionality—all running on commodity hardware. The FD.io engine also provides greater scalability across a number of metrics.

The following table summarizes the school's experience with a pfSense solution versus the TNSR solution.

Aspect	Before FD.io	After FD.io
Solution	pfSense (hybrid — Kernel & Userspace) packet processing	Fd.io (userspace VPP & DPDK) packet processing
Problem	Inefficient use of hardware, low performance, manual configuration	Efficient utilization of hardware, Line-rate 100 Gbps performance, automation
User experience	Slow and manual	Fast and automated

Table 1: Before and After Migration to Fd.io based solution

Next Steps and Conclusion

The school plans to exercise the IPSec functionality of the solution in the near future to secure the traffic between its training network and its Microsoft Azure based virtual private cloud network. Once encryption enters the picture, TNSR is expected to far outperform pfSense performance, making the upgrade even more valuable. The school also plans to open source the cybersecurity tools and templates to make them accessible to a wider community at no cost.

With a FD.io-based TNSR solution, The US Army Cyber School is successfully addressing the evolving networking and security needs of their training cloud infrastructure for openness, high performance, scale, programmability and cost.[3]

References

https://www.youtube.com/watch?v=fRRiQVxbQ1g

https://www.youtube.com/watch?v=UQ0gcqKEAGs

https://www.youtube.com/watch?v=f5MRdaM-E0g&t=4s

https://fd.io/

https://www.dpdk.org/

https://www.tnsr.com

https://www.netgate.com/solutions/pfsense/

https://www.pfsense.org/

https://www.cio.com/article/3195771/how-the-us-army-is-using-openstack-to-train-cyber-soldiers.html

[3] Participation in this case study is in no way to be considered an endorsement of a product by the Department of Defense, nor can it be indicated in any product advertisement that such an endorsement exists.