ACL Digital
an ALTEN group company

DPI BASED VIRTUAL FIREWALL

Deep Packet Inspection (DPI) is playing an increasingly important role in modern networks, becoming more and more of a service enabler for quality of experience(QoE), virtual CPE services, network and subscriber analytics, data center and network security and more. With advancements in Network Function Virtualization (NFV) and Software Defined Networking (SDN), the way DPI isused at various network deployments will vary according to the needs.

The changes in network communications and applications has brought changes in the threat management and mitigation as well. The next gen firewall, deeply integrated with ACL Digital DPI framework creates strong security framework. This framework addresses a need for security tools to prevent increasingly sophisticated attacks, with sufficient intelligence and automation to take the guesswork out of attack prevention and resolution. The solution is an optimized and balanced combination of Access Control Lists, stateful Firewall, Intrusion Detection/Prevention system, Application QoS and Application Visibility & Control.

Solution Overview

This security framework is developed to run on any DPDK (Data Plane Development Kit) supported platforms, using DPDK's Software Development Kit (SDK). Software and Hardware architecture of vFirewall allows achieving high performances over the solutions from Traditional Network Equipment Manufacturers.

DPDK is a set of libraries and drivers for fast packet processing. It was designed to run on any processors. The first supported CPU was Intel x86 and it is now extended to IBM Power 8, EZchip TILE-Gx and ARM. It runs mostly in Linux userland. A FreeBSD port is available for a subset of DPDK features.

DPDK is an Open Source BSD licensed project.

Features:

- DPDK based optimized packet handling for high performance
- Linearly scalable architecture for higher throughputs
- IPv6 Support
- Tunnel decoding
- TCP session tracking & stream reassembly
- File identification, extraction and logging
- Network stack visibility
- Stateful HTTP parsing
- IP reputation
- Malware/botnet/DoS/DDoS protection
- Signature/rule management with Emerging Threats
- User friendly GUI with comprehensive analytics
- GeoIP lookup
- Application QoS
- NIC level software based packet distribution control
- Detection of thousands of protocols & applications including some of the most widely used applications worldwide like facebook, twitter, whatsApp, World of Warcraft, Lync, Skype, Youtube, Webex etc using industry leading DPI libraries

Platform Support

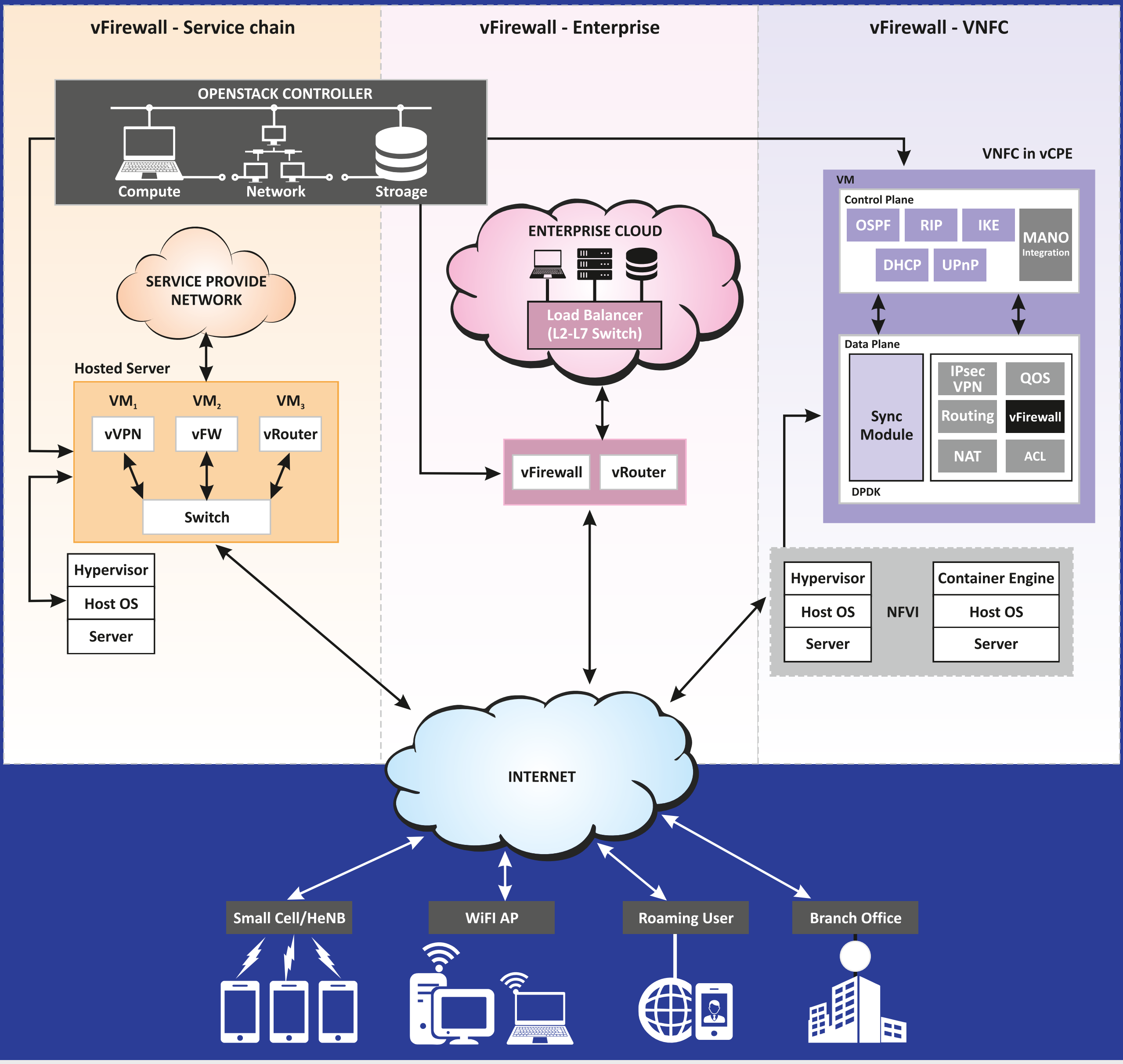
Support for different virtual environments (KVM/Xen)

- Deployable on a VM or bare metal using any DPDK supported COTS platform
- IO-Virtualizations: VirtIO, SR-IOV

Deployment Models

Service Chaining:

The deployment scenario presents the orchestration of vFirewall on Server (bare-metal) or VM mode using various virtualization methods/technologies. The orchestration can be carried out using several free/open-source software management platforms like Openstack, Docker and also with cloud platforms like Google Cloud Platform and Amazon Web Services. This deployment scenario provides user friendly interface for managing cluster of instances of vFirewall, which acts as backbone to achieve high availability and reduce the downtime.



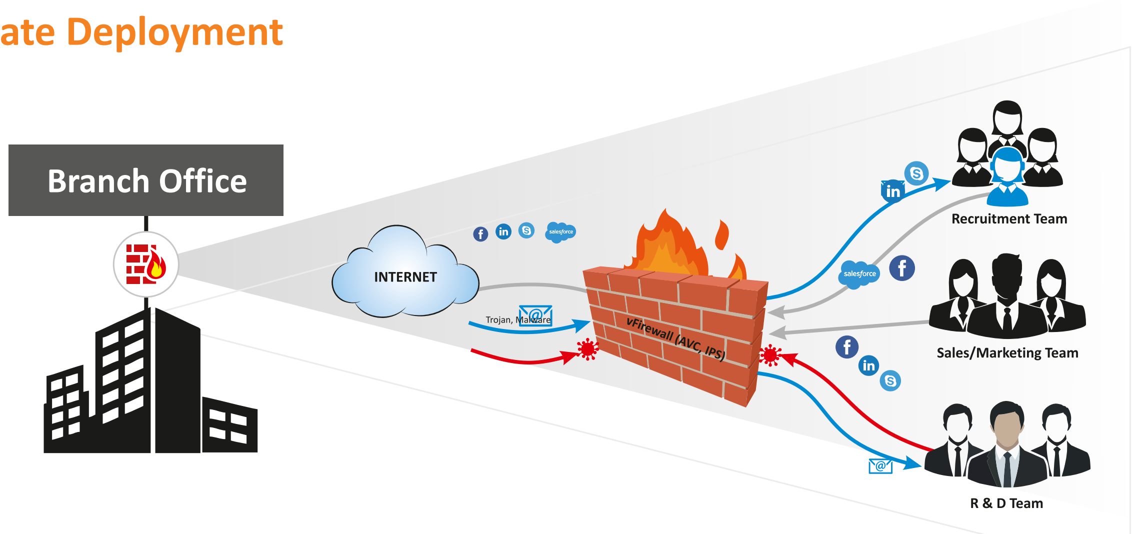
Enterprise Solution

This deployment scenario reflects ACL Digital vFireall solution providing security to brach & head offices. In Enterprise security is essential both from external world as well as LAN network. Threat safety from external world via IDS/IPS and application control from LAN side via AVC is desired. Also using Orchestration methods, service providers can centralize all resources for administration of critical resources at Data Centers.

as VNF Component

This deployment scenario represents ACL Digital vFirewall as VNF component which is integrated with third party solution, in the packet processing pipeline. vFirewall as an independent solution can be integrated in to a solution for deployment scenarios like Subscriber analytics, content caching, application security and QoS.

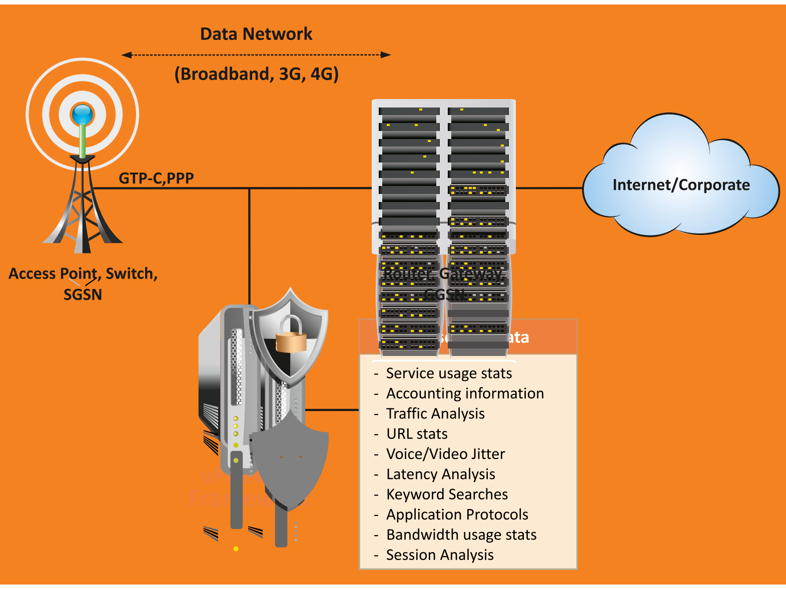
Corporate Deployment



In a corporate branch or head office security plays an important role. Securing the private network from outsiders and filtering the traffic going out to internet based on IT policies. IT policies could be different for different departments of the organization based on the nature of work.

Telecom Deployment

In telecom domain, subscriber's information is crucial for business. Understanding subscriber application preferences and usage patterns can help the service provider to optimize his network bandwidth for better service with cost efficiency. vFirewall can provide this important subscriber data in a desired format through various communication methods. vFirewall's framework is flexible enough to gather different type of information based on placement of vFirewall in telecom's data network.



- Service usage stats
- Accounting information
- Traffic Analysis
- URL stats
- Voice/Video Jitter
- Latency Analysis
- Keyword Searches
- Application Protocols
- Bandwidth usage stats
- Session Analysis

Scalability & Performance

- High performance detection engine
- 6.5Gbps of packet inspection processing per CPU core with 18K+ rules loaded
- Performance can linearly scale with compute processing as more CPU cores are added, providing unparalleled performance in a compact form factors.

ACL Digital is a design-led Digital Experience, Product Innovation, Engineering and Enterprise IT offerings leader. From strategy, to design, implementation and management we help accelerate innovation and transform businesses. ACL Digital is a part of ALTEN group, a leader in technology consulting and engineering services.

business@acldigital.com | www.acldigital.com

USA | UK | France | India