SOLUTION BRIEF

Performance as a Key Attribute of Fortinet Virtual Next-Generation Firewalls

Executive Overview

Virtual firewalls are commonly used to protect virtualized environments in software-defined data centers and multi-cloud environments on the basis that they are the least expensive and the most portable, enabling users to easily move a virtual firewall from cloud to cloud. One disadvantage of most virtual firewalls is that they deliver significantly lower network throughput as compared with physical firewalls, creating bottlenecks throughout the network and reducing business agility and performance.

FortiGate virtual firewalls (FortiGate-VM), featuring advanced virtual security processing units (vSPUs), overcome the throughput barrier to provide top performance in private and public clouds. With FortiGate-VM, organizations can securely migrate any application and support a variety of use cases, including highly available large-scale virtual private networks (VPNs) in the cloud.

Fortinet Sets the Performance Standard for Enterprise-Grade Virtual Firewalls:

- vSPU (DPDK and vNP offloading)
- SR-IOV and PCI pass-through
- Intel QAT support
- Higher throughput than other leading firewalls with comparable licenses

The Real Cost of Lightweight, Low-Priced Firewalls

Physical firewalls have built-in hardware to handle heavy traffic loads, enabling them to perform their security functions with minimal delay to network traffic. Typical virtual firewalls lack such hardware, so they can deliver only a fraction of the network throughput of their physical counterparts. The delay that virtual firewalls introduce can ripple across the network, slowing business processes, downgrading user experience, and inhibiting business agility. Network engineering and operations leaders and security architects may even consider turning off some security processing features in order to meet performance service-level agreements.

The apparent cost advantage of virtual firewalls presents another difficult trade-off. Although each virtual firewall costs less than a physical device, the cost of purchasing and deploying a large number of virtual firewalls may still be significant. Further, managing a large number of firewalls—whether virtual or physical—can pose challenges in areas ranging from deployment, to end-to-end visibility, to propagation of threat response.

Bringing Hardware Expertise to the Software World

FortiGate next-generation firewalls (NGFWs) use the NP6 and NP6lite network processors to provide fast-path acceleration by offloading communication sessions from the FortiGate CPU. This hardware expertise translates to FortiGate-VM (virtual machine) NGFWs with vSPU/vNP technology for enhanced performance.

FortiGate-VM removes the cost-performance barriers to adopting virtual NGFWs, with several industry-leading features:

- The FortiGate-VM vSPU is a unique technology that enhances performance by offloading part of packet processing to user space, while using a kernel bypass solution within the operating system. With vSPU enabled, FortiGate-VM can achieve more than triple the throughput for a UDP firewall rule.
- Support for Intel QuickAssist Technology (Intel QAT), working on the latest QuickAssist Adapters, accelerates traffic processing through site-to-site IPSec VPNs. With QAT enabled, FortiGate-VM can achieve two to three times throughput improvements depending on the packet frame size.
- Fortinet is the first NGFW vendor to support AWS C5n instances, which enables organizations to use a virtual firewall to secure compute-heavy applications in the cloud.

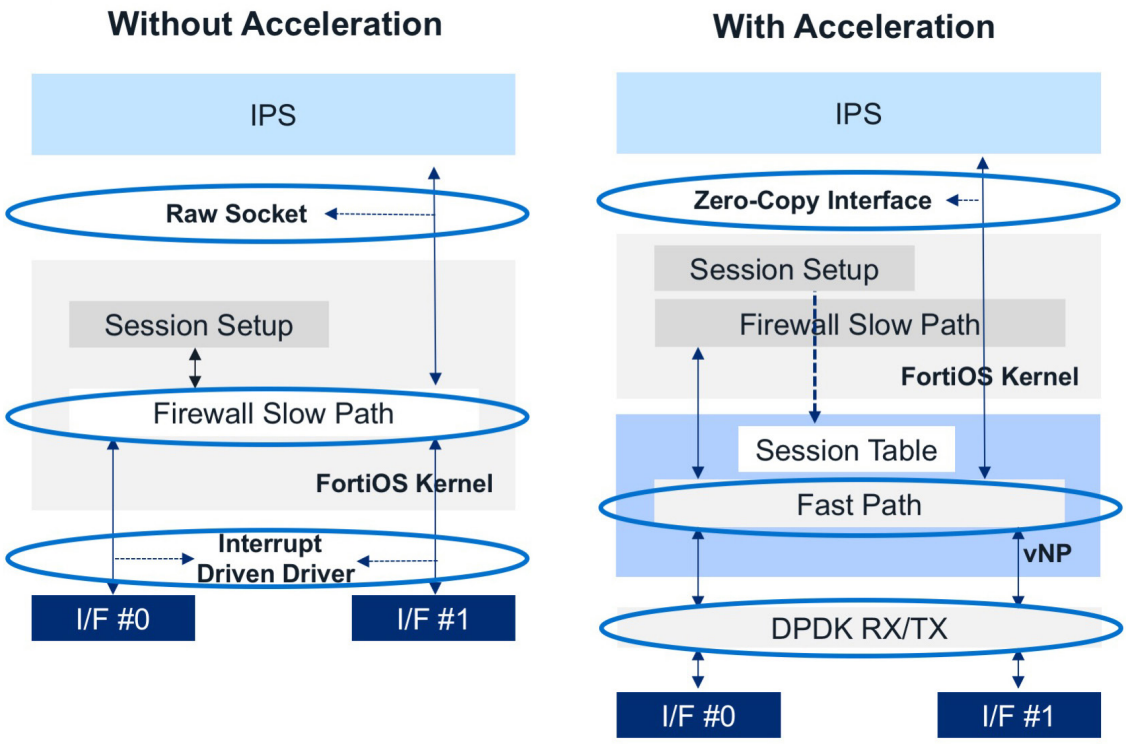

Figure 1: Packet flow comparison without and with virtual SPU acceleration.

A Virtual Firewall with Real Advantages

FortiGate-VM features one of the smallest footprints among leading NGFW vendors, and the smallest virtual network function (VNF) footprint available for virtual mobile infrastructure. It boots within seconds and offers highly efficient storage efficiencies, both of which maximize performance. Available in multiple sizes, FortiGate virtual firewalls help security architects optimize throughput and performance, scaling out or up as the needs of the organization change.

For highly mobile applications in multi-cloud networks, FortiGate virtual firewalls with advanced vSPU technology offer cost-effective, flexible security without performance compromises.

April 5, 2019 11:32 AM

381122-0-0-EN

Macintosh HD:Users:bhoulihan:Documents:_Projects:Solution Brief:sb-performance-as-key-attribute-for-virtual-firewalls Folder:sb-performance-as-key-attribute-for-virtual-firewalls