NETRONOME

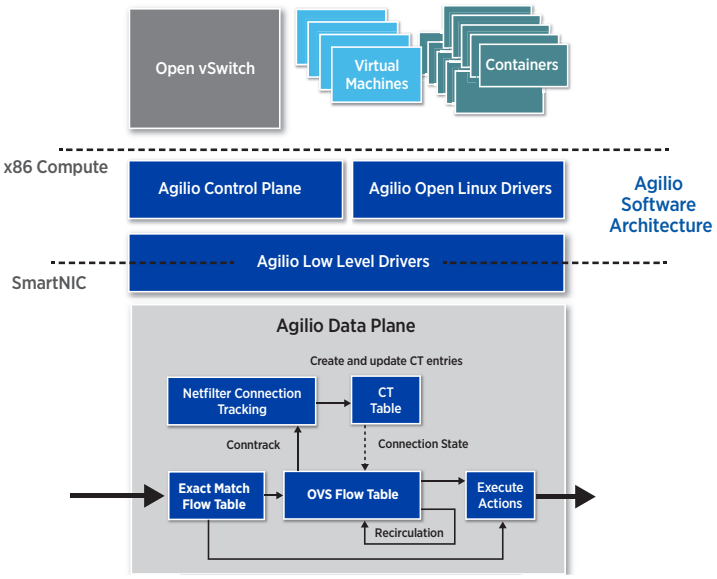
PRODUCT BRIEF

Agilio® OVS Firewall Software

OFFLOAD AND ACCELERATE SERVER-BASED STATEFUL FIREWALL PROCESSING

With the rise of east-west traffic in the data center, traditional perimeter-based firewall security is being replaced with zero-trust defense inside the data center where each VM and application within a VM needs appropriate level of trust or privilege. The Linux firewall feature based on Connection Tracking (Conntrack) is now supported in Open vSwitch (OVS) and is designed to enable zero-trust stateful security in data centers using OpenStack-based automation. Agilio OVS Firewall Software, combined with Agilio SmartNICs, enables zero-trust security while significantly improving server-based networking performance. Agilio OVS Firewall Software restores valuable CPU cores by offloading OVS and Conntrack to Netronome's SmartNICs. This gives users the ability to define more intelligent filtering policies, security groups, access control lists and stateful firewall applications.

Agilio OVS Firewall Software offloads the complete OVS datapath including Conntrack to the network flow processor (NFP) boosting performance dramatically. Performing this connection tracking in the NFP, in addition to standard OVS match-action profiles, accelerates the enforcement of the most comprehensive policies, eliminating the bottlenecks associated with implementing zero-trust security within a server. The solution is a drop-in accelerator for OVS, making it compatible with existing network tools, controllers and orchestration software.



KEY FEATURES

- Full offload of OVS datapath to Agilio SmartNIC
- Full offload of Linux Netfilter Connection Tracking (Conntrack)
- Connectivity to VMs over SR-IOV and Express Virtio (XVIO)
- Accelerated term/orig of VXLAN, VXLAN-GPE, GTP, NVGRE and NSH tunnels
- Standard host interfaces through Linux netdev and DPDK
- Configuration through standard OVS tools (ovsctl) and protocols (OVSDB, OpenFlow)
- Integration with OpenStack cloud orchestration
- Offload for millions of microflows
- Networking offloads for overlay and underlay packets

BENEFITS

- 5X improvement in vSwitch performance
- 4X improvement to Conntrack performance
- Low CPU consumption: one CPU core for control plane
- Improved VM density and application performance
- High scale for tunnel capacity and security policies
- Leverage pre-existing networking software and automation tools

VERSION 2.6.A FEATURES AND SPECIFICATIONS

Open vSwitch Offload	• OVS version 2.6.1 • Offload kernel datapath • Acceleration via Exact Match Flow Cache • Offload Connection Tracking (Conntrack) • Fastpath forwarding of traffic between specified vSwitch vPorts • Transparent offload via OVS fallback and datapath hooks • OVSDB, OpenFlow, OVS CLI (for configuration) • Optional Local Flow API • Stand-alone or controller modes • OVS statistics • Match-action offload • NVGRE tunnel encap/decap • VXLAN, VXLAN-GPE tunnel encap/decap
Advanced Features	• Load Balancing for up to 32 OF groups to host and to ports • Link Aggregation with LACP • Traffic mirroring at ingress and egress • VM QoS: Rate limiting and network bandwidth guarantees • PXE Boot • OpenStack integration / OOO • OPNFV support • Flow-based egress queue selection • Flow-based traffic metering
Networking I/O	• 60 Datapath VFs • 60 netdevs, or 60 DPDK PMD instances • SR-IOV • Express Virtio (XVIO) • VM live migration • L3/L4 RX and TX checksum offloads (inner and outer headers) • NIC stats via Ethtool • Jumbo frame support
Operating Systems	Ubuntu 14.04/16.04, CentOS/RHEL 7.1, Linux Kernels 3.13 – 3.19
Supported Platforms	• Agilio CX dual-port 10GbE SmartNIC • Agilio CX dual-port 25GbE SmartNIC • Agilio CX single/dual-port 40GbE SmartNIC • Agilio LX dual-port 40GbE SmartNIC • Agilio LX single-port 100GbE SmartNIC • PCIe expansion for each of the Agilio LX SmartNICs • 4x10GbE and 10x10GbE breakout cables for 40/100GbE ports

OVS Match Fields

- Tunnel ID
- Tunnel IPv4 Source
- Tunnel IPv4 Destination
- Tunnel Flags
- Tunnel IPv4 TOS
- Tunnel IPv4 TTL
- Input port
- Ethernet source address
- Ethernet destination address
- Ethernet TCI
- Ethernet Type
- MPLS top label stack entry
- IPv4 source address
- IPv4 destination address
- IPv6 source address
- IPv6 destination address
- IPv6 flow label
- IP protocol
- IP TOS
- IP TTL
- IP Fragmentation
- Transport layer SRC
- Transport layer DST
- Transport layer flags
- Conntrack State
- Conntrack Zone
- Conntrack Mark
- Conntrack Label
- Conntrack Recirculation ID

OVS Actions

- Output to port
- Fallback to user space
- Set tunnel header
  - tun_id, ipv4_src, ipv4_dst, tun_flags, ipv4_tos and ipv4_ttl
- Set ethernet header
  - eth_src and eth_dst
- Set IPv4 header
  - ipv4_src, ipv4_dst, ip_tos and ip_ttl
- Set IPv6 header
  - ipv6_src, ipv6_dst, ip_tos and ip_ttl
- Set TCP header
  - tcp_src and tcp_dst
- Set UDP header
  - udp_src and udp_dst
- Set MPLS header
  - Sets MPLS top label stack entry
- Push VLAN header
- Pop VLAN header
- Push MPLS header
- Pop MPLS header
- Conntrack Set Mark
- Conntrack Set Label
- Conntrack Set Table
- Conntrack Set Zone
- Conntrack Set Algorithm

NETRONOME

Netronome Systems, Inc.
2903 Bunker Hill Lane, Suite 150
Santa Clara, CA 95054
Tel: 408.496.0022 | Fax: 408.586.0002
www.netronome.com

PB-AGILIO-FW-SW-7/18