**Summary**

OVS has already seamlessly supported userspace conntrack (dpif-netdev).

No performance downgrade should be expected with option #3: Openflow + conntrack-based (stateful) native OVS firewall driver.

No gap is identified between OVS agent (w/ native firewall driver) and userspace conntrack.

**Feature readiness status in OVS: latest**

===================== ============== ============== ========= =======

Feature Linux upstream Linux OVS tree Userspace Hyper-V

===================== ============== ============== ========= =======

NAT 4.6 YES Yes NO

Connection tracking 4.3 YES PARTIAL PARTIAL

Tunnel - LISP NO YES NO NO

Tunnel - STT NO YES NO YES

Tunnel - GRE 3.11 YES YES YES

Tunnel - VXLAN 3.12 YES YES YES

Tunnel - Geneve 3.18 YES YES YES

Tunnel - GRE-IPv6 NO NO YES NO

Tunnel - VXLAN-IPv6 4.3 YES YES NO

Tunnel - Geneve-IPv6 4.4 YES YES NO

QoS - Policing YES YES YES NO

QoS - Shaping YES YES NO NO

sFlow YES YES YES NO

IPFIX 3.10 YES YES NO

Set action YES YES YES PARTIAL

NIC Bonding YES YES YES YES

Multiple VTEPs YES YES YES YES

Meters 4.15 YES YES NO

Conntrack zone limit 4.18 YES NO NO

===================== ============== ============== ========= =======

Initial patch: Basic connection tracking for the userspace datapath (no ALG, fragmentation or NAT support yet). Later, ALG, NAT etc. have been supported by the follow-up patches.

**Detailed commit information related w/ userspace conntrack in OVS**

**Userspace conntrack in OVS**

a489b16854b590004e3234573721fd0f676b3295

 conntrack: New userspace connection tracker.

 This commit adds the conntrack module.

 It is a connection tracker that resides entirely in userspace. Its

 primary user will be the dpif-netdev datapath.

 The module main goal is to provide conntrack\_execute(), which offers a

 convenient interface to implement the datapath ct() action.

 The conntrack module uses two submodules to deal with the l4 protocol

 details (conntrack-other for UDP and ICMP, conntrack-tcp for TCP).

 The conntrack-tcp submodule implementation is adapted from FreeBSD's pf

 subsystem, therefore it's BSD licensed. It has been slightly altered to

 match the OVS coding style and to allow the pickup of already

 established connections.

 Signed-off-by: Daniele Di Proietto <diproiettod@vmware.com>

 Acked-by: Antonio Fischetti <antonio.fischetti@intel.com>

 Acked-by: Joe Stringer <joe@ovn.org>

**Enable conntrack in dpif-netdev**

5cf3edb311ffe6bc4df93cd7b759801c6932d81f

 dpif-netdev: Execute conntrack action.

 This commit implements the OVS\_ACTION\_ATTR\_CT action in dpif-netdev.

 To allow ofproto-dpif to detect the conntrack feature, flow\_put will not

 discard anymore flows with ct\_\* fields set. We still shouldn't allow

 flows with NAT bits set, since there is no support for NAT.

 Signed-off-by: Daniele Di Proietto <diproiettod@vmware.com>

 Acked-by: Flavio Leitner <fbl@sysclose.org>

 Acked-by: Antonio Fischetti <antonio.fischetti@intel.com>

**Add NAT, ALG, TFTP etc. support**

7be77cb0d3378a71a18b0d1d0f3513da16f071c6

 Userspace Datapath: Add TFTP support.

 Both ipv4 and ipv6 are supported. Also, NAT support is included.

 Signed-off-by: Darrell Ball <dlu998@gmail.com>

 Signed-off-by: Ben Pfaff <blp@ovn.org>

bd5e81a0e596dd012d11824cce69b7c80ae107c5

 Userspace Datapath: Add ALG infra and FTP.

 ALG infra and FTP (both V4 and V6) support is added to the userspace

 datapath. Also, NAT support is included.

 Signed-off-by: Darrell Ball <dlu998@gmail.com>

 Signed-off-by: Ben Pfaff <blp@ovn.org>

5ed7a0b402879e604d6986e8ca4bf08bb5307773

 Userspace Datapath: Introduce conn\_key\_cmp().

 A new function conn\_key\_cmp() is introduced and used to replace

 memcmp of conn\_keys. Given that OVS runs on with many compilers and

 on many architectures, it seems prudent to avoid memcmp in case

 existing and future holes in conn\_key are not handled by a given

 compiler for a given architecture.

 Signed-off-by: Darrell Ball <dlu998@gmail.com>

 Suggested-by: Ben Pfaff <blp@ovn.org>

 Signed-off-by: Ben Pfaff <blp@ovn.org>

286de27299550d1c4b2b4abb8048a189669962ef

 dpdk: Userspace Datapath: Introduce NAT Support.

 This patch introduces NAT support for the userspace datapath.

 Most conntrack module changes are in this patch, with the

 exception of icmp related handling and recent orig tuple

 support.

 The per packet scope of lookups for NAT and un\_NAT is at

 the bucket level rather than global. One hash table is

 introduced to support create/delete handling. The create/delete

 events may be further optimized, if the need becomes clear.

 Some NAT options with limited utility (persistent, random) are

 not supported yet, but will be supported in a later patch.

 Signed-off-by: Darrell Ball <dlu998@gmail.com>

 Acked-by: Flavio Leitner <fbl@sysclose.org>

 Acked-by: Daniele Di Proietto <diproiettod@ovn.org>

 Signed-off-by: Ben Pfaff <blp@ovn.org>

**Native Open vSwitch firewall driver**

**CT states used/supported by native openvswitch\_firewall**

OF\_STATE\_NOT\_TRACKED = "-trk"

OF\_STATE\_TRACKED = "+trk"

OF\_STATE\_NEW\_NOT\_ESTABLISHED = "+new-est"

OF\_STATE\_NOT\_ESTABLISHED = "-est"

OF\_STATE\_ESTABLISHED = "+est"

OF\_STATE\_ESTABLISHED\_NOT\_REPLY = "+est-rel-rpl"

OF\_STATE\_ESTABLISHED\_REPLY = "+est-rel+rpl"

OF\_STATE\_RELATED = "-new-est+rel-inv"

OF\_STATE\_INVALID = "+trk+inv"

OF\_STATE\_NEW = "+new"

OF\_STATE\_NOT\_REPLY\_NOT\_NEW = "-new-rpl"

All states have already been supported by OVS-DPDK.

**Prerequisites**
The native OVS firewall implementation requires kernel and user space support for conntrack, thus requiring minimum versions of the Linux kernel and Open vSwitch. All cases require Open vSwitch version 2.5 or newer.

Kernel version 4.3 or newer includes conntrack support.
Kernel version 3.3, but less than 4.3, does not include conntrack support and requires building the OVS modules.

**Enable the native OVS firewall driver**
On nodes running the Open vSwitch agent, edit the openvswitch\_agent.ini file and enable the firewall driver.

[securitygroup]
firewall\_driver = openvswitch

**Backup**

There are 3 security group implementations in neutron OVS-DPDK agent.

1. Iptables based security group
	* The OVS agent and Compute service use a Linux bridge between each instance (VM) and the OVS integration bridge br-int to implement security groups. This implementation is stateful but cause scalability and performance problems.
2. Openflow based security group
	* This implementation is stateless and based in OpenFlow 'learn action', which uses a firewall driver in networking-ovs-dpdk project.
	* <https://github.com/openstack/networking-ovs-dpdk/blob/master/networking_ovs_dpdk/agent/ovs_dpdk_firewall.py>
3. Openflow + conntrack based security group
	* This implementation is stateful, which uses a native firewall driver.
	* <https://docs.openstack.org/newton/networking-guide/config-ovsfwdriver.html>
	* <http://docs.openvswitch.org/en/latest/tutorials/ovs-conntrack/>