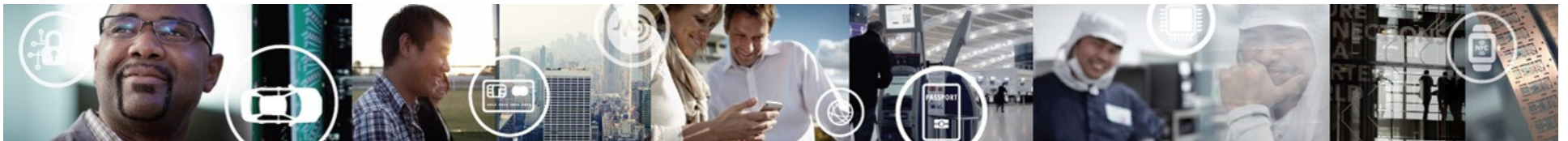


# VORTIQA INTELLIGENT VIRTUALIZATION ACCELERATION SOFTWARE (IVAS)

PRASAD GORJA  
22 MARCH 2016



SECURE CONNECTIONS  
FOR A SMARTER WORLD

# Agenda

- Introduction to VortiQa IVAS
- Features and Benefits
- VortiQa IVAS Architecture
  - Overview of various functional blocks
- Use Cases and Packet Flow
- Question and Answer

# VortiQa IVAS: Introduction

VortiQa IVAS (Intelligent Virtualization Acceleration Software) is an accelerated NFVI (Network Functions Virtualization Infrastructure) software to deploy virtual networks and network services in VNFs.

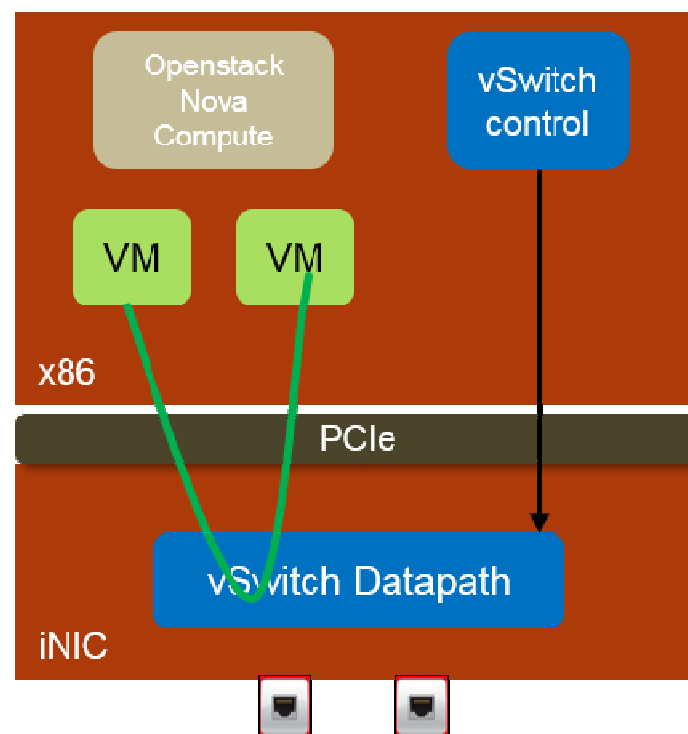
It leverages both SDN and NFV technologies to deploy and manage virtualized networks and services.

VortiQa IVAS implements and accelerates the following four key elements of NFVI

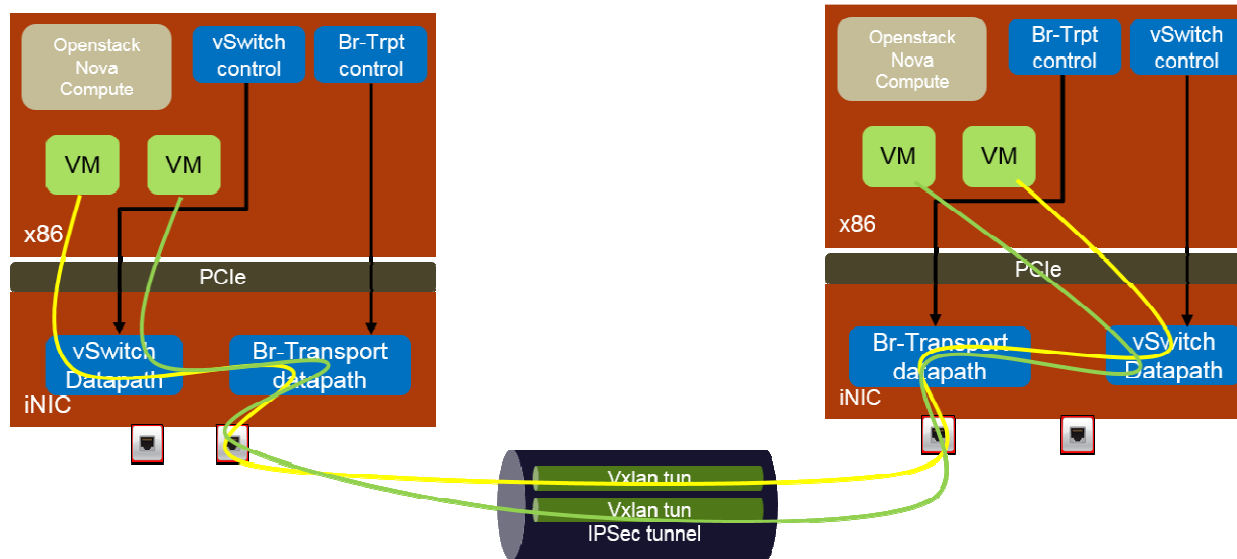
- Virtual Network Switch
- Secure Virtualized Networks
- VNF acceleration
- OpenStack Orchestrations

# VortiQa IVAS: Virtual Network Switch

- VortiQa IVAS accelerates Open vSwitch datapath.
- Leverages NXP Open Network Switch (ONSW), an OpenFlow based datapath to offload vSwitch data path functionality to a PCIe based iNIC.
- Integrated with OVS using OVSDDB
  - NXP OVS Relay Agent (OVSRA) listens to events from OVSDDB and configures the datapaths
  - Enables use of standard OVS utilities to configure the vSwitch datapath.



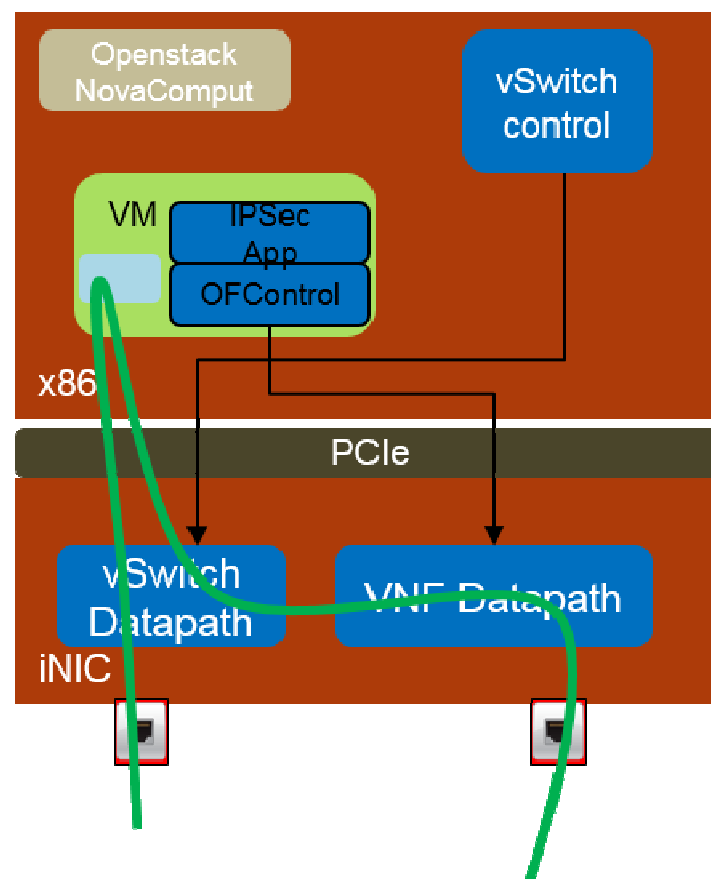
# VortiQa IVAS: Secured Virtualized Networks



- VortiQa IVAS provides Infrastructure for creating virtualized L2 networks between VMs across different compute nodes over the existing L3 Networks.
- Enables virtual networking with OpenFlow based VXLAN tunneling protocol.
- Provides security on virtual networks with VXLAN over IPsec.
- VXLAN and IPsec are implemented in OpenFlow compliant Br-Transport datapath.

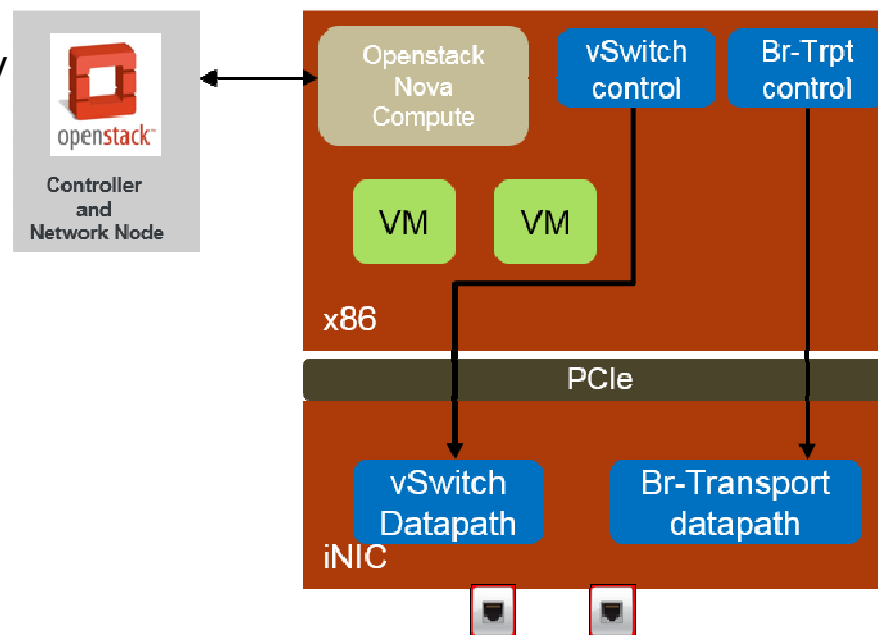
# VortiQa IVAS: VNF Acceleration

- VortiQa IVAS enables acceleration of network applications running in VMs.
- The VNF applications such as IPsec can be offloaded to its corresponding OpenFlow datapath in iNIC.
- Each VNF runs its own OpenFlow based control module to configure and control its OpenFlow datapath in iNIC.
- VortiQa IVAS provides an integration module with Linux network applications (IPsec, routing etc.) and required OF Control module for VMs.
- Slated for release in 2016.



# VortiQa IVAS: OpenStack Orchestration

- VortiQa IVAS deployment does not need any changes to OpenStack controller for its orchestration.
- NXP iNIC driver plugin in OpenStack Nova compute facilitates orchestration in following ways.
  - Enables OpenStack Integration for iNIC.
  - Support detection of VFs
  - PF/VF Management
  - FSL-INIC Driver allocates Virtual Functions of iNIC to VM.
  - Adds ports to the iNIC Switch, which are mapped to VM using ovs-vsctl commands.
  - Sets Mac-addresses to the VM interfaces assigned by OpenStack Neutron.
  - Facilitates detection of iNIC card.
  - Ability to use iNIC or local host based virtual switching.
  - The administrator will use the standard OpenStack dashboard APIs REST interface for the management.
  - Support for ONSW ports, VXLAN Tunnel Ports.



# VortiQa IVAS: Features and Benefits

- VortiQa IVAS is a commercial-grade performance optimized software along with comprehensive host software modules for NFVI.
- VortiQa IVAS endpoint software runs on subsystems based on best in class NXP processors QorIQ T2080
  - Leverages T2080's unique acceleration capabilities, HW Crypto & DPAA
  - Leverages NXP Open Network Switch for High performance datapath forwarding.
  - Compliant with OpenFlow v 1.3 based system.
  - Implements L2 switching, VXLAN, IPSec, Routing, ARP etc., in OpenFlow based datapaths.
  - OVS acceleration using OVSDDB based integration.
  - Integrated with Linux networking applications, e.g. StrongSwan
  - OpenFlow datapath based VNF acceleration
- Familiar Linux based SDK base framework with virtualization support.
- OpenStack Orchestration with FSL host virtual interface function.

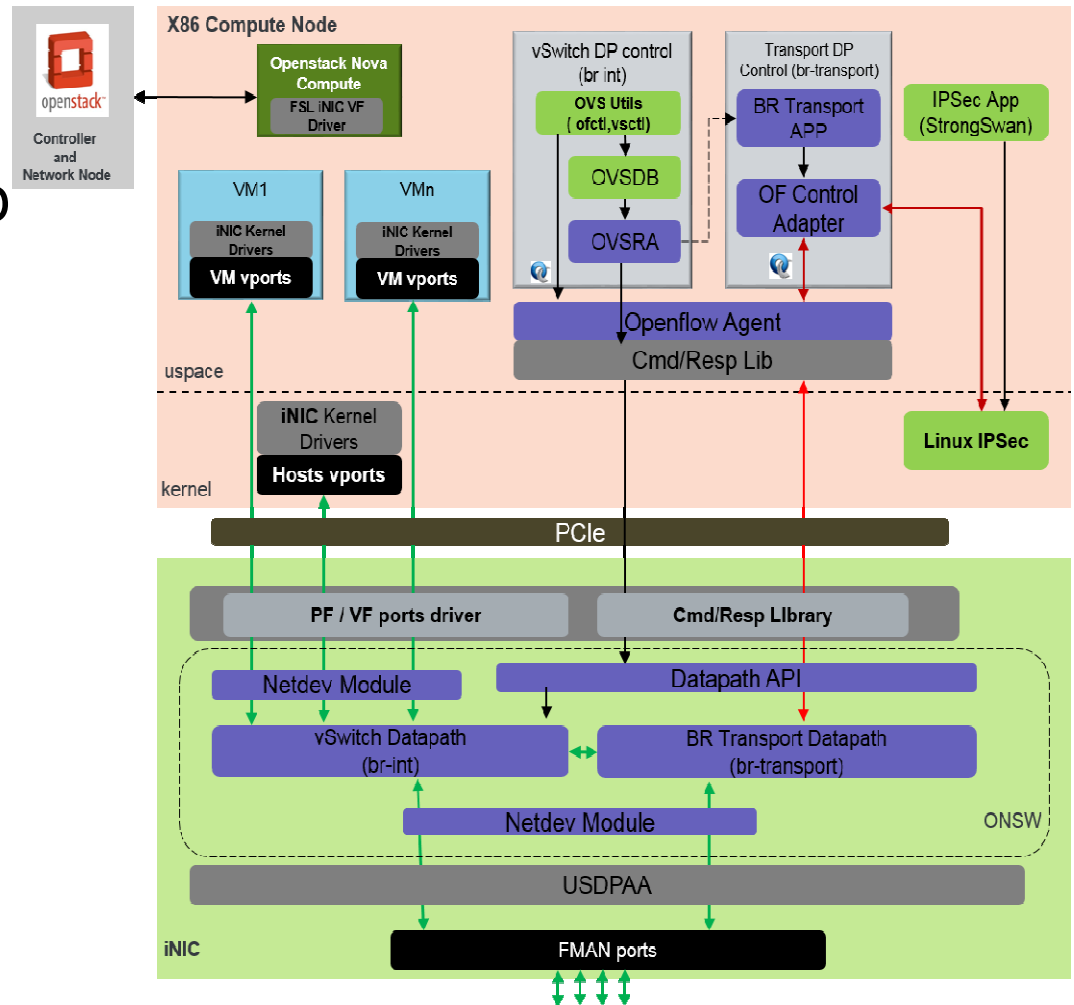


# VortiQa IVAS: Architecture

The VortiQa IVAS software is partitioned into control and data planes.

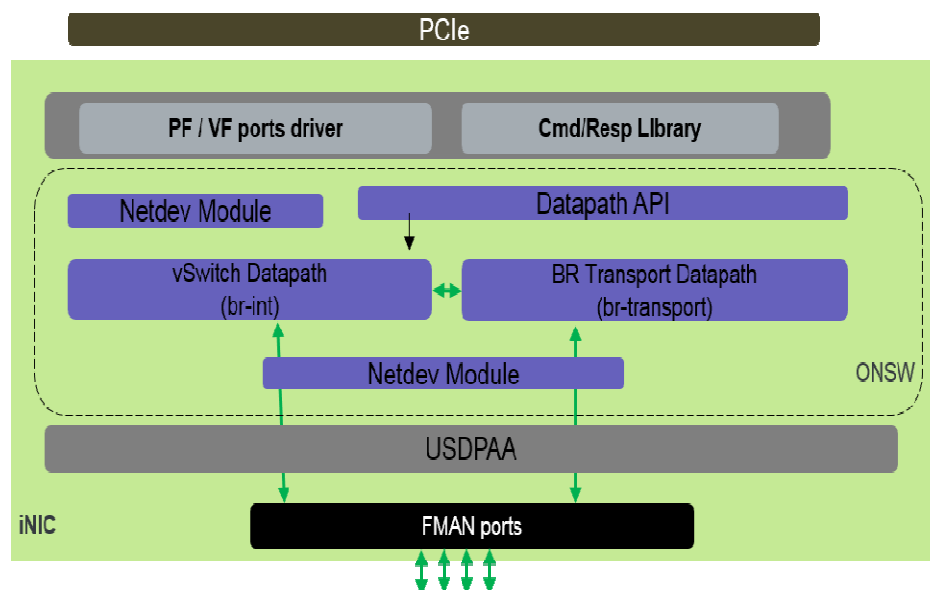
- The control portion of the software runs on the X86 compute host.
- The data plane runs on the FSL iNIC.

This architecture leverages both the SDN and NFV technologies.



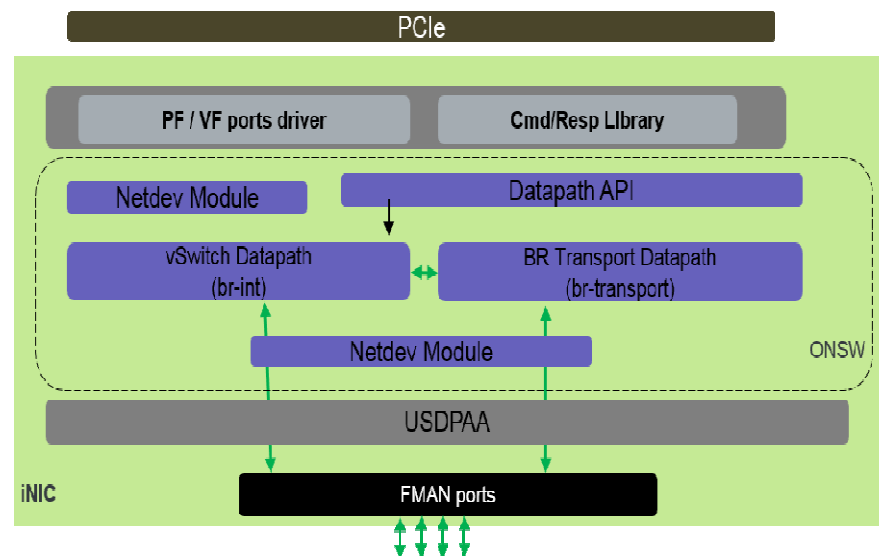
# VortiQa IVAS : Data Plane

- OpenFlow based datapath implementation.
- Implemented in iNIC subsystem
- User space Implementation based on top of NXP USDPAA infrastructure.
- Leverages the following acceleration capabilities of iNIC platform.
  - HW Crypto Engine for IPsec protocol processing
  - DPAA packet classification and distribution
  - Decorated Storage for statistics.
  - CEETM for QoS ( future )

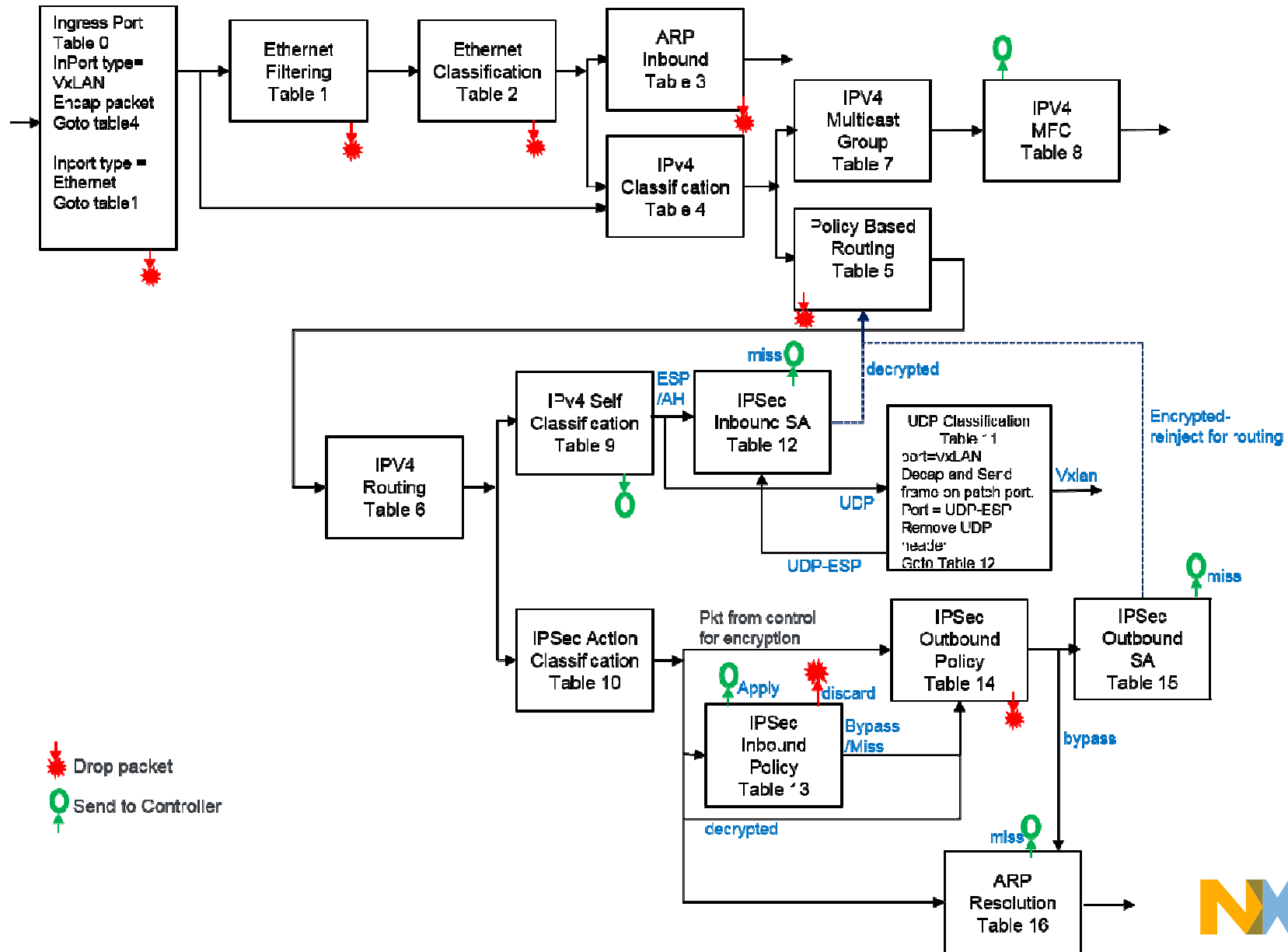


# VortiQa IVAS : Data Plane

- **Netdev Module:**
  - Device discovery.
  - Device database and management
  - Receive/Transmit Hooks.
- **Datapath API**
  - Openflow based APIs
  - Translation of OF messages
  - Configures datapaths.
- **Cmd/Resp Library**
  - Command transport mechanism
- **vSwitch datapath:**
  - Accelerates vSwitch datapath
  - Created from ovs vsctl.
  - Enables virtual switching
- **Br-Transport datapath:**
  - Datapath for based VXLAN and IPsec.
  - Enables virtualized networks.
  - Created when VXLAN port is added to vSwitch datapath.



# VortiQa IVAS: Data Plane Br Transport Pipeline

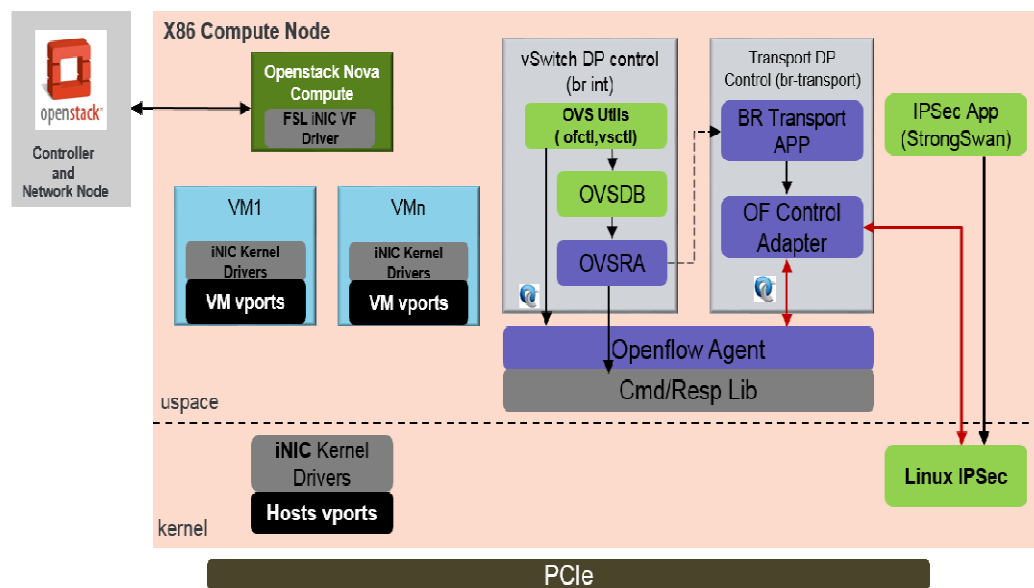


# VortiQa IVAS : Data Plane Features

- Flow Indexing Table.
  - High performance forwarding
  - Generic, can be leveraged by any application ex IPSec, Firewall etc.
- OF extensions for IPSec, VXLAN, IP Reassembly/Fragmentation,
  - Provides Infrastructure for adding new extensions.
- Integrated with SEC (hardware cryptographic) engine.
- Multiple logical datapaths
  - Datapaths doing different functions
  - patch port support to connect them,
- Supports LPM and Exact match tables other than ACL tables.
  
- Following features are currently not being used in VortiQa IVAS.
  - OF Extensions for Policy Based Routing and ARP Response.
  - Queue objects support for QoS.
  - Integrated with CEETM HW block and Linux qdisc for QoS.
  - Support OVS acceleration based on OVS DPFIF integration.

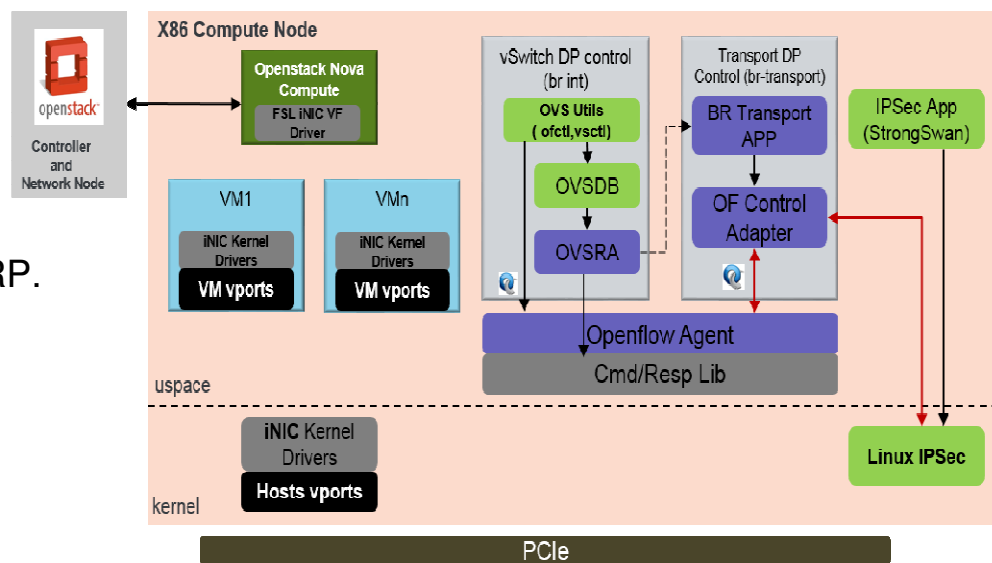
# VortiQa IVAS: Control Plane

- OpenFlow based control to drive the OF datapaths on iNIC.
- Implemented in user space on X86 compute node.
- Has following major blocks
  - vSwitch DP Control
  - Br-Transport DP Control
  - OpenFlow Agent
- vSwitch DP Control:
  - Controls vSwitch datapath in iNIC.
  - Replaces vSwitchd.
  - OVSRA:
    - Interface layer between OVSDDB and datapaths,
    - Translates the events from OVSDDB to datapath APIs to configure datapaths.



# VortiQa IVAS : Control Plane ..Contd

- Transport DP control:
  - Controls and configures the Br-Transport datapath on iNIC
  - Br Transport App:
    - Instantiates Br-Transport datapath on iNIC when VXLAN port is added to vSwitch datapath.
  - OF Control Adapter: It has three functional blocks
    - Linux integration layer
      - Integrates with Linux IPsec/Routing/ARP.
    - Br-Transport TTP
    - OpenFlow Controller Driver.
- OF Agent
  - NXP OpenFlow protocol implementation for switch.
  - Translates OF messages and invokes datapath APIs.
  - De-Multiplexes commands to multiple datapaths.



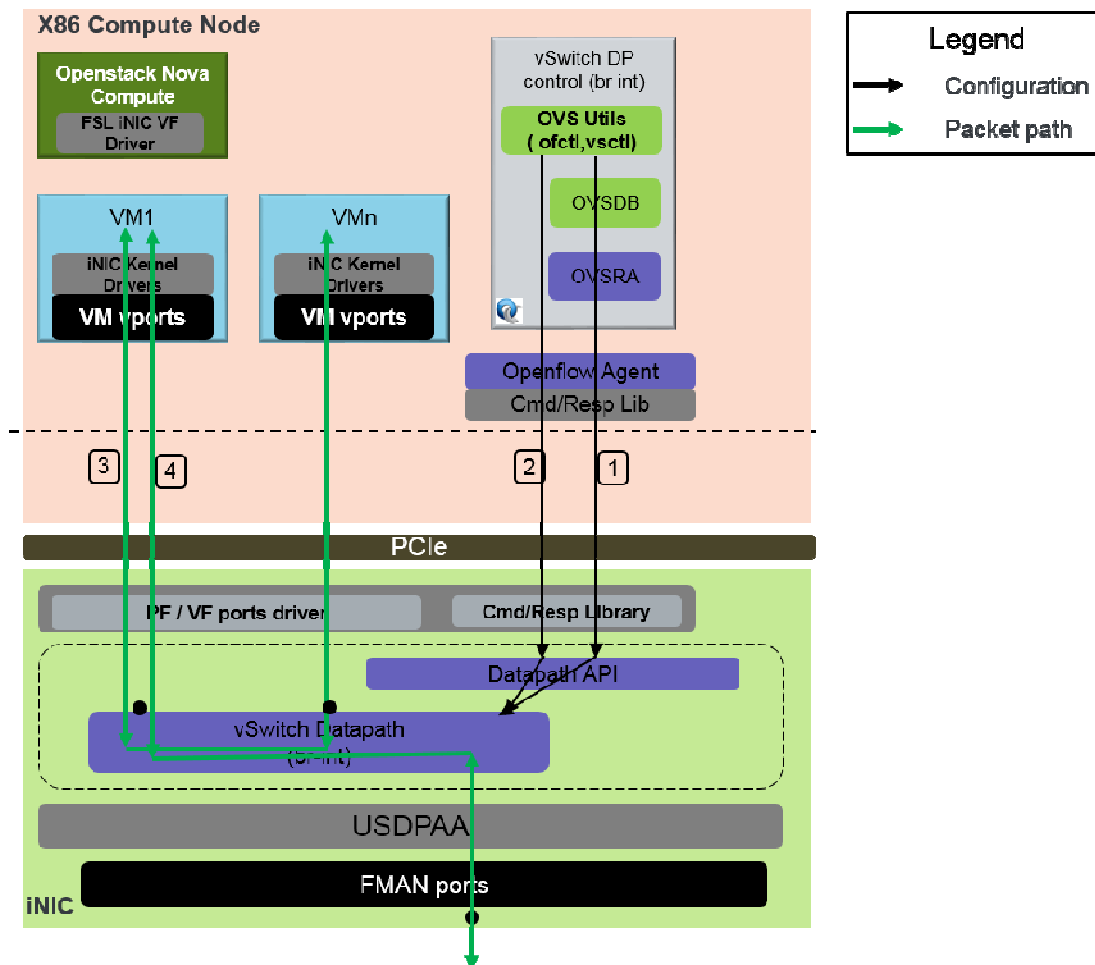
# VortiQa IVAS : Use Cases and Packet flow

- Virtual Switching
- Virtualized Networks with VXLAN
- Secure Virtualized Networks with VXLAN over IPSec.



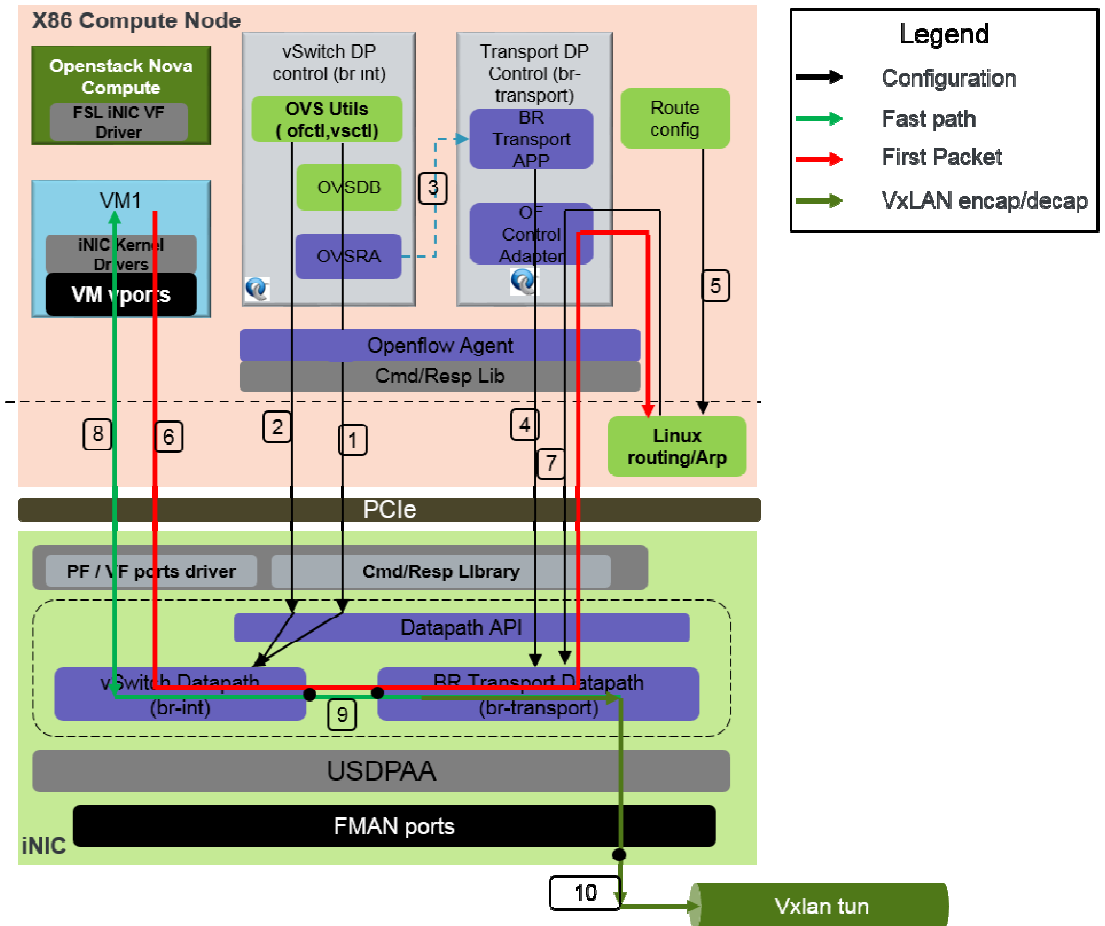
# VortiQa IVAS : Virtual Switching

- The vSwitch datapath creation and provisioning of ports in iNIC is done using the standard OVS utilities from the X86 host, as shown in step 1 and 2 in above picture
- The vSwitch datapath in this use case is basically configured with flows to do L2 switching from one VM to other or from one VM to external work, as shown in paths 3 and 4 in picture.

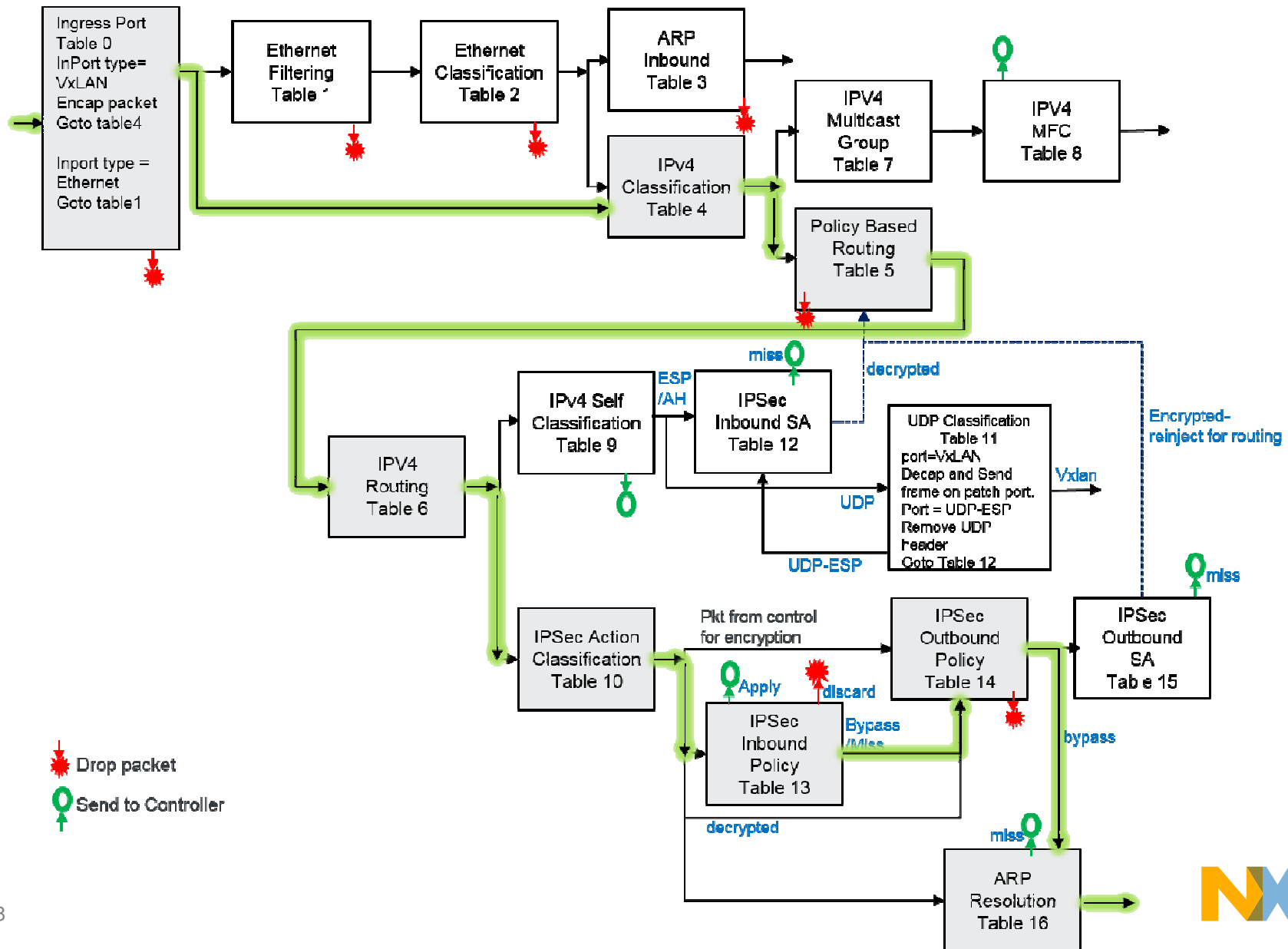


# VortiQa IVAS : Virtual Networks with VXLAN

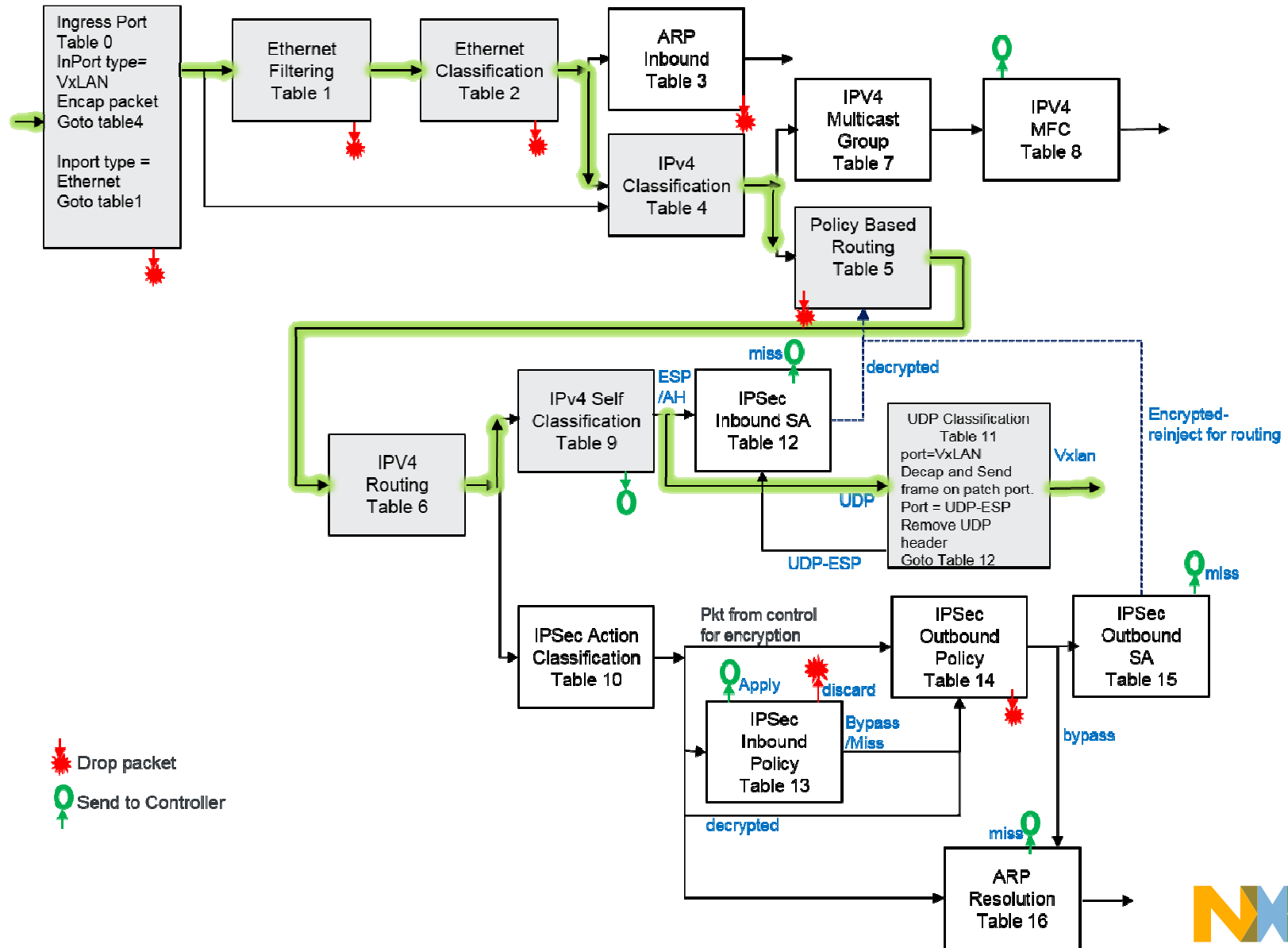
- The VXLAN tunneling is achieved by the combination of vSwitch datapath and Br-transport datapath on iNIC controlled by respective control blocks on the X86 compute host.
- The VXLAN encap and decap is done using OpenFlow extensions in BR-Transport datapath, the flows with actions for VXLAN encap and decap are configured from Transport DP control block from X86.
- When VXLAN port is created with required parameters and added to the vSwitch datapath, this triggers the Br-Transport App and all the VXLAN parameters that are configured as part of VXLAN port creation are passed in this event, as shown in path 3.
- The Br-Transport App initiates creation of BR-Transport datapath in iNIC and patch ports to attach vSwitch datapath and Br-Transport datapath; shown in path 4.
- The flow with VXLAN Encap and Decap parameters are programmed into InPort table and UDP classification tables.



# VortiQa IVAS : VXLAN packet flow for Encap

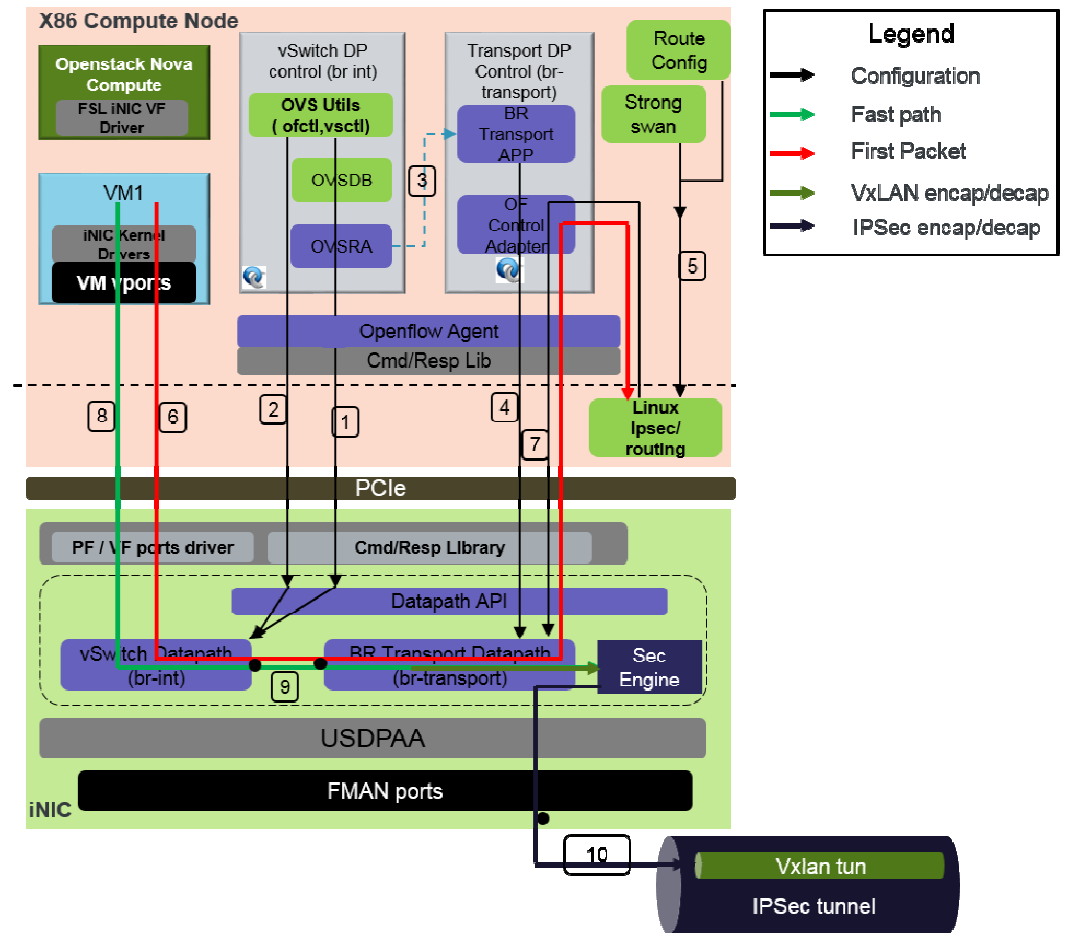


# VortiQa IVAS : VXLAN packet flow for Decap

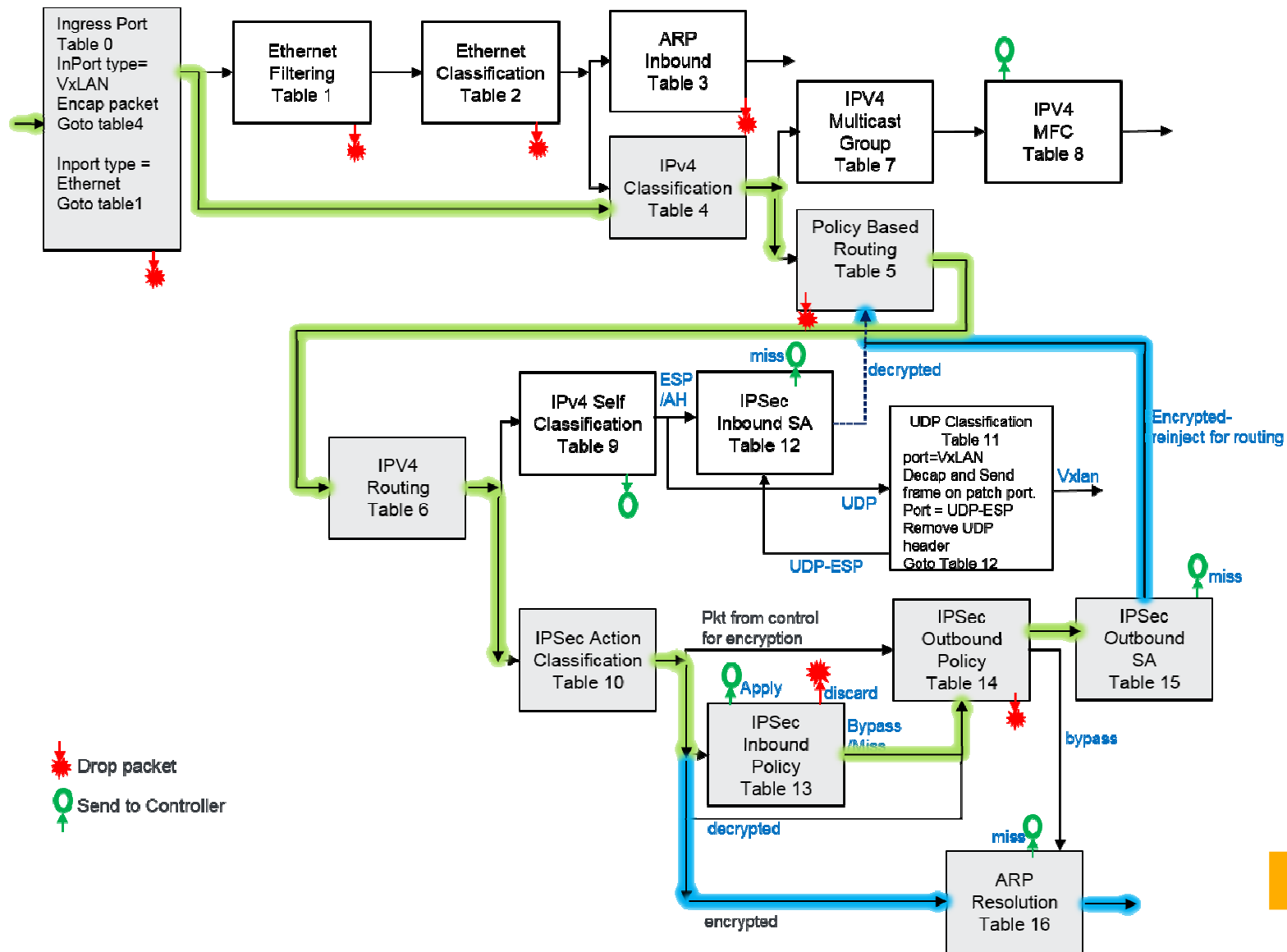


# VortiQa IVAS : Secure Virtual Networks with VXLAN over IPsec

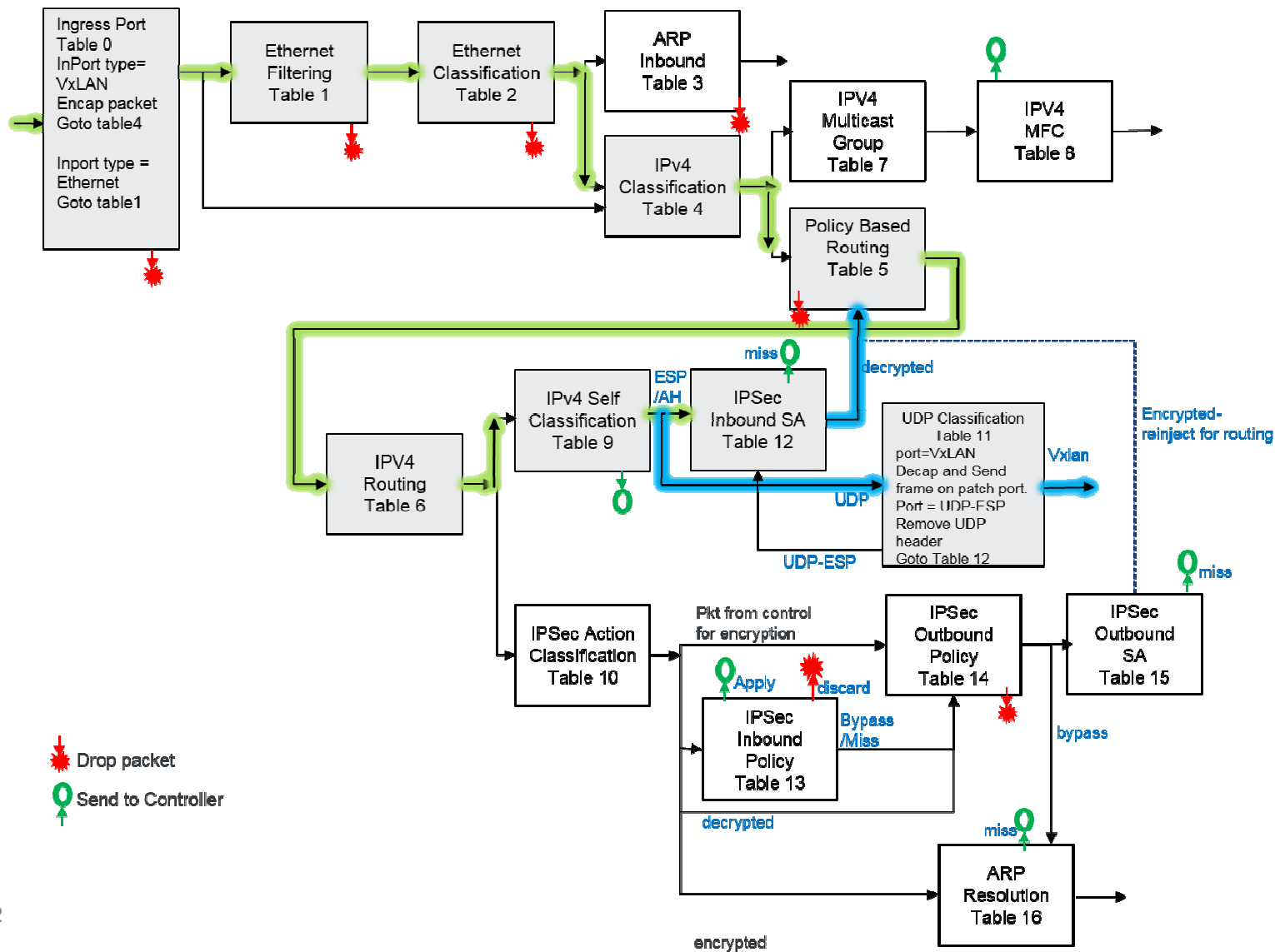
- Here IPsec is applied to the VXLAN tunneled packets.
- The Linux StrongSwan IPsec application running on the X86 compute hosts does the key exchanges and pushes the SAs in Linux Kernel IPsec module. The SA addition events are listened to by the OFControl Adapter and these SAs are pushed to br-transport datapath in respective IPsec tables.
- Br-transport uses the Crypto engine to perform IPsec encap and decap operations.
- First packet in br-transport does not match any SAs in outbound SA table and that packet is sent to Linux kernel IPsec to trigger SA creation.
- After SAs are pushed to br-transport datapath, subsequent packets are handled in iNIC itself.
- ARP for peer security gateway is resolved by Linux running on X86 host and is pushed as flow to br-transport datapath.



# VortiQa IVAS : VXLAN over IPsec packet flow for Encap



# VortiQa IVAS : VXLAN over IPSec packet flow for Decap



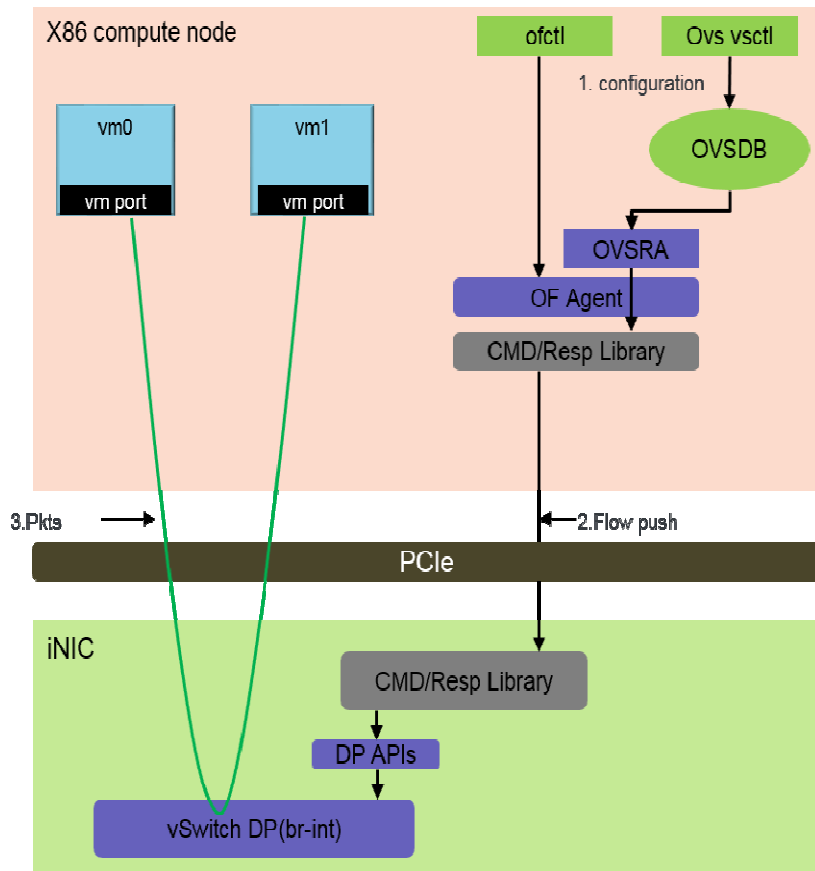
# VortiQa IVAS : Comparison with DPDK OVS

VortiQa IVAS	DPDK OVS
VortiQa IVAS essentially accelerates the OVS by implementing OpenFlow based datapath in iNIC subsystem, it completely replaces the vswitch daemon and the kernel datapath of OVS in the host system with a high performance OF based datapath in iNIC subsystem, keeping the user interface (ovsctl, ofctl etc.) intact.	DPDK OVS accelerates the OVS by offloading certain functions of OVS datapath in vswitch to datapath running in iNIC subsystem, any functionality that DPDK OVS cannot handle in iNIC is given as exception to vswitch datapath for normal processing.
The flow configuration done through ofctl is pushed directly to vSwitch DP, thereby avoiding any exceptions packets going to host for non stateful flows. The OVSRA is the glue logic with OVS-DB server to listen to the configuration events and push them to ONSW DP.	Here the flow configuration is not pushed directly DPDK OVS DP in iNIC, the first packet goes as exception to vswitch which forms the flow and pushes it to DPDK OVS DP, thereby generating quite an amount traffic between host and iNIC subsystem.
Additionally the ONSW DP implements the VXLAN and IPsec tunneling as OpenFlow extensions.	DPDK OVS does not have VXLAN implementation until 2.3 version, it is only available in 2.4, IPsec tunneling is not present even in 2.4.
ONSW DP implements flow indexing to mitigate the performance bottlenecks that comes with an OpenFlow based implementation of datapaths.	No such implementation available in DPDK OVS.
It is a fully OpenFlow based solution providing greater extensibility and scalability, any new function added to datapath automatically gets the performance benefit though FIT.	The transport functions such as VXLAN and IPsec are done in legacy method and each has to be optimized independently for performance.

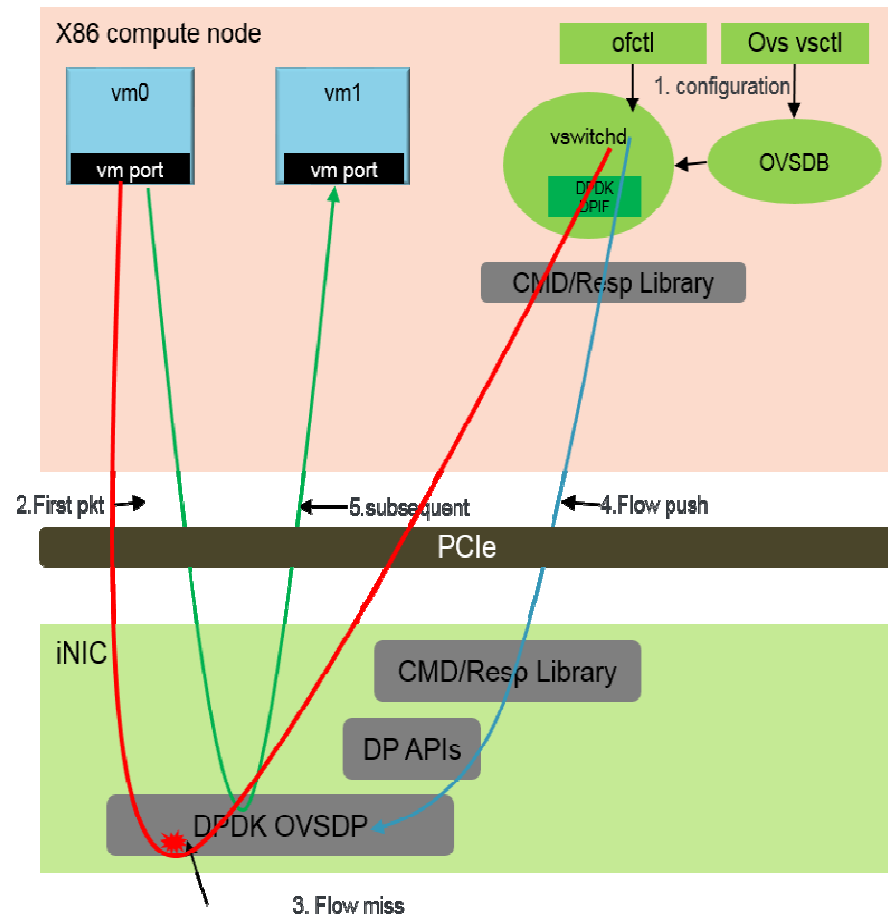


# VortiQa IVAS : Packet flow Comparison with DPDK OVS

## VortiQa IVAS switching



## DPDK OVS switching





SECURE CONNECTIONS  
FOR A SMARTER WORLD