Hi,

I had little time to complete the process, but here a start

A. Discovery Phase

 1. Discovery of accelerators devices and their capabilities by VIM, this includes NFVI vSwitch or vRouter inventory on compute nodes.

B. Network Service Bring up time

 1. Selection of compute nodes by VIM to bring up the various vNF that make up the service based on the selected Deployment Flavor (see MANO 6.2.1.3 & 6.3.1.1).

 2. Create a Network Forwarding Path (see MANO 7.5) for the Network Service Descriptor (see MANO 6.5 & 6.2)

 3. Instantiate the VNFs

 4. VIM Network Controller setup the Forwarding Path, including settting up NFVI vSwitchvRouter in compute nodes

 5. Assignment of virtual accelerators to the vNFs on all compute nodes.

C. Run time

 1. Communication between vNF and virtual accelerators.

 2. Communication between NFVI vSwitchvRouter and virtual accelerators.

D. vNF Closing phase (Graceful and Non-Graceful)

 1. Non Graceful

 a. Recovery of virtual accelerators from vNF and NFVI vSwitchvRtouter by compute node.

 b. Recovery of virtual accelerators by VIM.

 2. Graceful

 a. Orchestrator requesting VIM to bring down vNF.

 b. Unassignment of virtual accelerators by compute node.

 C. VIM updating its local accelerator database

Each VNF has Connection Points that can be linked by a Network Forwarding Path (computed by the VIM). They are generic end points such as simple IP or the end of a VPN Tunnel (see MANO 6.3.1.2.1.2).

So a Small Cell PNFVNF IPSec Connection Point can be connected to a Signaling Gateway IPSec connection point through the Forwarding Graph described in the Network Service Descriptor.

VIM will compute a Network Forwarding Path and its Network Controllers (Neutron, SDN...) will program whatever hardware or software need to be updated.

This means that in the NFVI vRouter case, the vRouter will terminate IPSec and deal with IPSec events such as re-keying. It has full visibility of the hardware and can accelerate its functions.