Network Device Interpretation # 23

NDcPP and SIP Server with virtualization

Status: ☒ *Active* ☐ *Inactive*

Date: *28-Mar-2016*

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☐ *Network iTC*

Affected Document(s): *NDcPP V1.0*

Affected Section(s): *All*

Superseded Interpretation(s): *None.*

Issue:

My question is regarding the NDcPP (collaborative NDPP) and the Extended Package SIP Server v1.1 PP. The product serves as a SIP server as an appliance as well as a virtual server. The vendor would prefer to claim and use the virtual appliance as this is what they ship more of. Their solution is a bunch of servers and they are deployed using virtual machines.

Specifically, the product has a hardware platform solution they sell on which their virtual server(s) run. So, the virtual servers (SIP included) all run on a defined piece of hardware. It has come to my attention that this is acceptable by NIAP for the PCL when claiming conformance to the NDPP. In a recent (November 2015) certification the following was noted for the inclusion of the vendors virtual appliances:

"Note, the NDPP specifies requirements for a network device-a device composed of hardware and software that is connected to the network and has an infrastructure role on the network. Therefore, the VM-Series virtual appliances are considered to be in their evaluated configuration only when installed on the following specified hardware platforms and are not evaluated for deployment on any other platforms."

Is the NDcPP allowing for virtualization? Can I take the same approach as above and provide the details of the hardware they supply with their virtual appliance solution and conform to the cPP?

Resolution:

NIT supports the response provided by NIAP on that request:

vNDs are software implementations of network device functionality that run inside virtual machines. NDcPP v1 expressly excludes evaluation of vNDs, but our position is that vNDs can be evaluated against NDcPPv1 if the product meets all the requirements and assumptions of a physical ND as required in NDcPPv1.

This means:

-- The virtualization layer (or hypervisor or VMM) is considered part of the ND's software stack, and thus is part of the TOE. vNDs that can run on multiple VMMs must be tested on each claimed VMM unless the vendor can successfully argue equivalence.

-- The physical hardware is likewise included in the TOE (like in the example included above). vNDs must be tested for each claimed hardware platform unless the vendor can successfully argue equivalence.

-- There is only one vND instance for each physical hardware platform.

-- There are no other guest VMs on the physical platform providing non-network device functionality.

Rationale:

N/A

Further Action:

Add corresponding clarification to NDcPP.

Action by Network iTC: