Network Device Interpretation # 201827

ND cPP Certifications of Cloud Deployments

Status: ☒ *Active* □ *Inactive*

Date: *13-Mar-2019*

End of proposed Transition Period (to be updated after TR2TD process): *13-Mar-2019*

Type of Change: ☒ Immediate application □ Minor change □ Major change

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

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

Affected Document(s): *ND cPP v2.0e; ND cPP v2.1*

Affected Section(s): *None*

Superseded Interpretation(s): *None*

Issue:

References

[cPPND] collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018

Background

Many vendors of products seeking evaluation against [cPPND] include virtual network devices (vNDs) in their product offerings. The [cPPND] provides for the evaluation of vNDs that can meet all the requirements and assumptions of a physical ND as specified in [cPPND]. As stated in Section 1.2 of [cPPND], this means:

The virtualization layer (or hypervisor or Virtual Machine Manager (VMM)) is considered part of the vND's software stack, and thus is part of the TOE and must satisfy the relevant SFRs. Virtual NDs 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. Virtual NDs 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.

The physical hardware supporting the cloud platform is likewise included in the TOE. Virtual NDs 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.

A cloud provider that offers subscribers the ability to reserve a physical computer dedicated for their exclusive use (known to be offered by AWS and Azure) would seem to satisfy the first two requirements, while the third and fourth requirements are controlled by the TOE user when deploying the vND. If the TOE vendor can provide this environment to the evaluation team for the purposes of testing, then it appears the evaluation team ought to be able to test the TOE with the same level of control on the operational environment as the end user will have when deploying and operating the TOE for themselves.

So, given the above conditions, can a product being evaluated against [cPPND] include cloud platforms in the evaluated configuration?

Response by NIAP:

This specifice use-case hasn't (to the TRRTs knowledge) been discussed and addressed by the TC. The TRRT may only provide an interpretation to clarify cPP Security Functional Requirements (SFRs) and Evaluation Activities (EAs) in the context of a specific product evaluation and specifically its ability to meet the cPP requirements. Your request for interpretation will be sent to the Network Device Interpretations Team (NIT) which has been established by the iTC to address issues. We highly recommend your participation in the iTC to bring this to closure.

Resolution:

Cloud platforms may not be included in CC certifications at this time.

It is expected that cloud platforms could be certified once the virtualization changes are included in a future version of NDcPP.

Rationale:

Per RFI#201623, the HW and platform a VM is being run on must be included as part of the TOE. This creates several problems in a cloud environment.

- *Non-TOE administrators can make changes to the TOE.*
- *Chances are high that the TOE version is subject to frequent changes due to continuous maintenance of the different TOE components – a customer is most likely not running the CC certified configuration. See also:*
  https://aws.amazon.com/maintenance-help/
  https://docs.microsoft.com/en-us/azure/virtual-machines/windows/maintenance-and-updates
- *To demonstrate that the underlying cloud platforms (e.g. AWS, Azure, Google cloud) would be able to meet the SFRs related to the underlying cloud platforms (e.g. FIA or FAU SFRs), documentation would be necessary that is not publicly available. This would require either*

collaboration with cloud platform providers or some form of composition of certifications or similar. This level of complexity is not covered in the current versions of NDcPP.

- *It's not clear how SFRs like FPT_TST_EXT and FPT_TST_TUD would be met, or tested, for the platform.*

In short. It is not obvious that the reviewed platforms would meet the SFR requirements related to the underlying cloud platform and the NDcPP in its current form is not covering the level of complexity that would be required to properly cover this.

Further Action:

None

Action by Network iTC:

None