Applicability of Interfaces to Network Security Functions to Network-Based Security Services
(draft-ietf-i2nsf-applicability-09)

IETF 104, Prague
March 26, 2019

Jaehoon Paul Jeong, Sangwon Hyun, Tae-Jin Ahn, Susan Hares, and Diego R. Lopez

Updates from the Previous Version

- The Previous Draft:
  - draft-ietf-i2nsf-applicability-08

- In this new version (-09), we revised the draft to address the comments from AD Eric Rescorla.

Updates for AD's Comments (1/3)

- **Comment 1**: It is insecure to allow the DMS for real-time management-level access to NSFs.
  - The role of the DMS is restricted to providing an I2NSF system with the software package/image for NSF execution.
  - The DMS is never allowed to access NSFs in online (or activated status) for the I2NSF system's security.
  - An access to running (online) NSFs is only allowed to the security controller.

Updates for AD's Comments (2/3)

- **Comment 2**: Show an XML example and the text summary of the security policy for the time-dependent web access control in Section 4.
  - We have added an example XML code for web filter and provided the text summary of the XML code.

Updates for AD's Comments (3/3)

- **Comment 3**: In Section 6, it is unclear how to tell if a given software element in NFV environments is an NSF or a virtualized switch.
  - NFV MANO includes a subsystem that maintains the descriptions of the capabilities each VNF can offer.
    - e.g., VNF onboarding system
  - Based on the capability descriptions, this subsystem can determine whether a given software element (VNF instance) is an NSF or a virtualized SDN switch.

Next Steps

- Submission to IESG
  - It is necessary for WG chairs to discuss our revision with AD to move this draft forward.