Gap analysis

Draft-hares-i2nsf-gap-analysis-00.txt
Interfaces for Virtual Security Functions Manager

**Interface: A**

For Service Function Vendors to register their available service functions & instances, and a set of policies (or policy profiles) that can be dynamically set by 3rd party security controller or management system (e.g. Operator’s OSS or management system).

- common mechanism to inform the Network Operator Mgmt Sys what they offer and what attributes can be dynamically configurable or monitored

**Interface: B & C**

For Clients dynamically set the policies (or profiles) to the VNFs that are supported, monitor & verify the execution & performance.
Filters

NETCONF / RESTCONF

Device Filters:
ACL
I2RS FB RIB

Device Filters:
ACL
I2RS FB RIB

NMS

application - wide
Intent (IB-Nemo)

Network-wide
L3SM VPN service,
SUPA ECA/Intent policy

Device level: P.I.
I2RS RIB, FB-FIB

Device level: protocol
Isis, ospf, bgp, L3

Device level:
IP, system, tunnels
Other Areas

• ETSI-NFV - EMS to VNF interface
  – Defines interface between EMS (element management system) and VNF
  – This matches I2NSF work

• OPNFV Moon project – An interface between EMS-VNF
  – Problems: NO dynamic control, only 1 definition, no room for existing vendor, no fine grain authentication, no allowance for central control

• CSA – 1 definition, 10 implementation agreements
  – All are concerned about the NMS-NSF interface