Use cases and Gap Analysis Hares (editor)

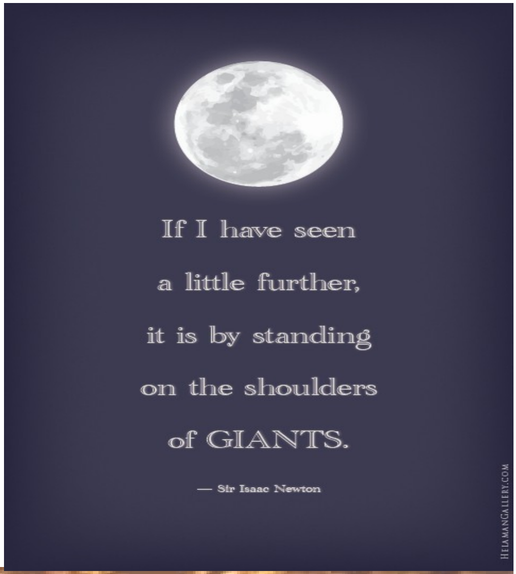
draft-hares-i2nsf-use-gap-analysis-00.txt

Sue Hares

Use Cases and Requirements for an Interface to Network Security Functions

(draft-pastor-i2nsf-merged-use-cases-00)

- Antonio Pastor (antonio.pastorperales@telefonica.com0O
- Diego Lopez (diego.r.lopez@telefonica.com)
- Ke Wang (wangkeyj@chinamobile.com)
- Xiaojun Zhuang (zhuangxiaojun@chinamobile.com)
- Minpeng Qi (quiminpeng@chinamobile.com)
- Myo Zarny (myo.zarny@gs.com)
- Sumandra Majee (lal2ghar@gmail.com)
- Nic Leymann Deutsche Telekom (n.leymann@telekom.de)
- Linda Dunbar Huawei
- M. Georgiades PrimeTel June 26, 201



Analysis of Existing work for I2NSF

- Susan Hares (shares@ndzh.com)
- Dacheng Zhang (dacheng.zdc@aliabab-inc.co
- Robert Moskowitz (rgm@labs.htt-consult.com)
- H. Rafiee (ietf@rozanak.com)
- Linda Dunbar (linda.dunbar@huawei.com)

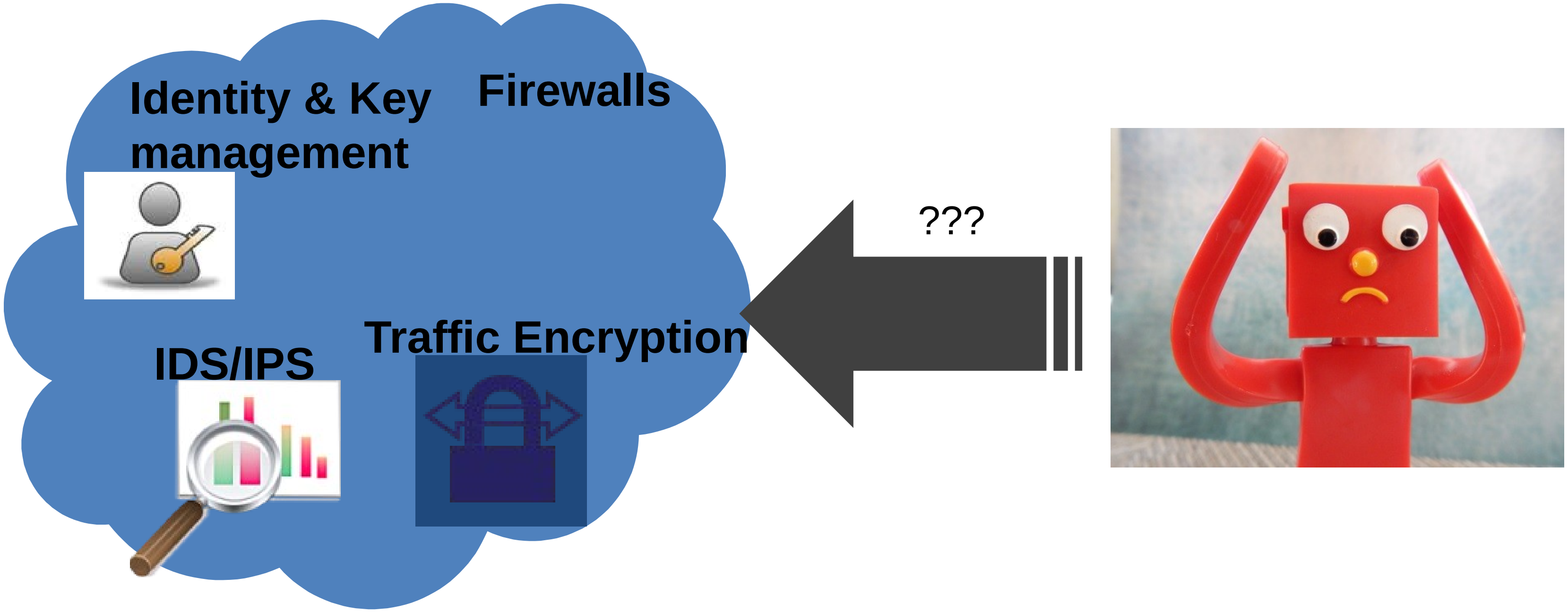
Combined Use Cases

Where the Story Begins…

- We need to close the gap between customers and security vendors or service providers
  - Customer security services are being offloaded to network or cloud based infrastructures
  - There is a demand for management interfaces of these delegated
- Draft contains use cases and requirements for a common interface to Network Security Functions (NSF). It considers several use cases, organized in two basic scenarios:

  - Access Networks

  - Data Centers



Identity & Key management

Firewalls

IDS/IPS

Traffic Encryption

???

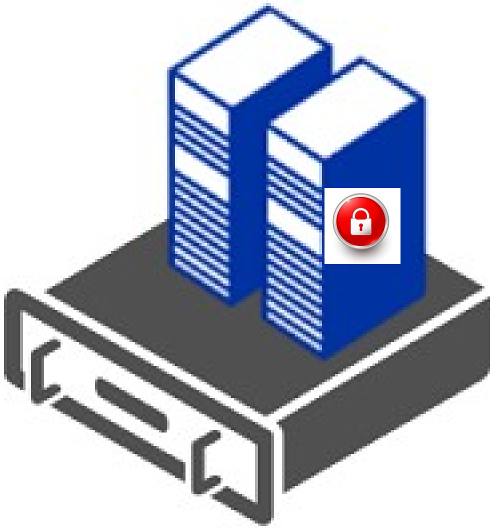
Terminology: A Couple of Basic Definitions

NSF

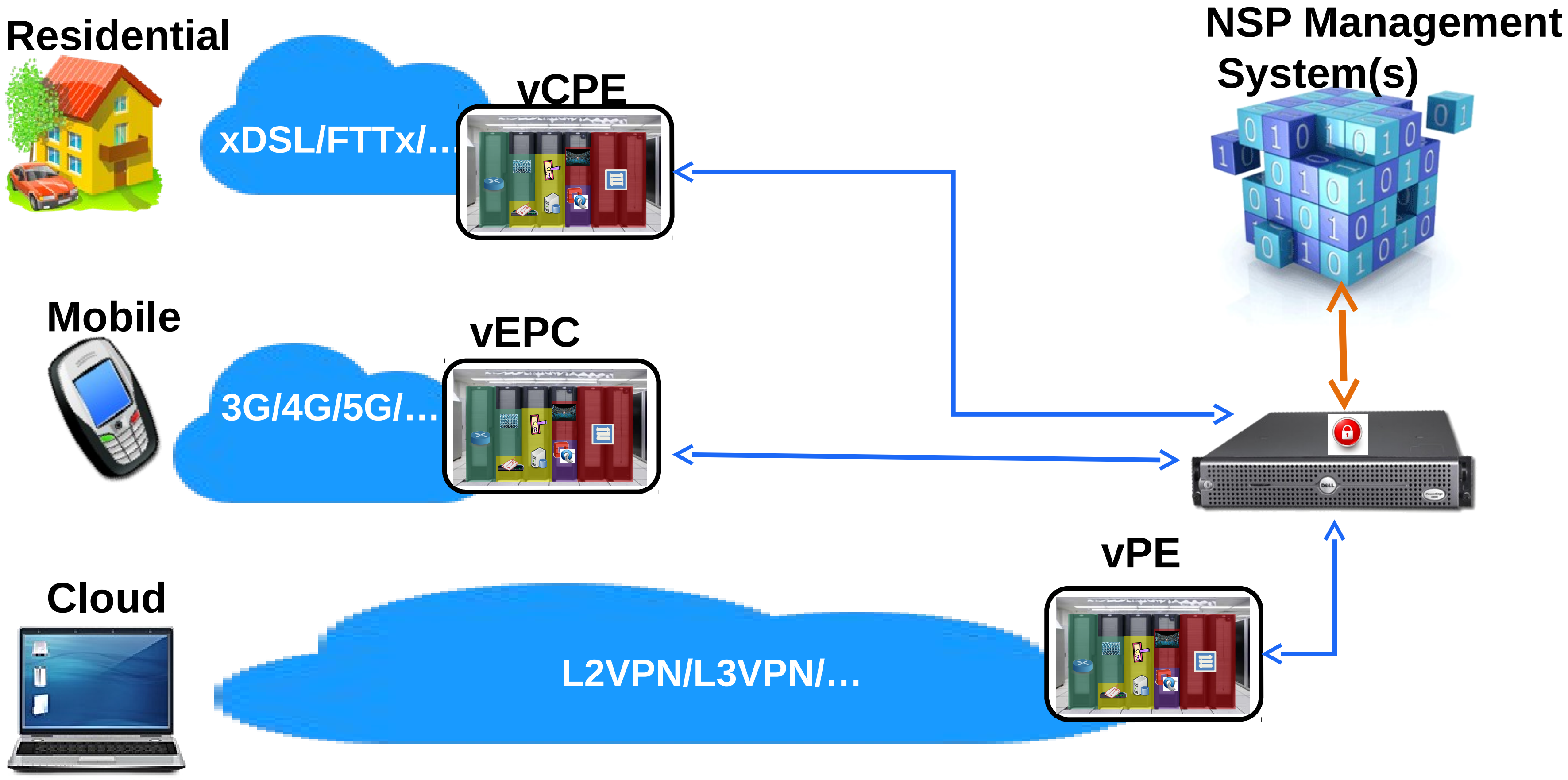
Network Security Function (NSF): A functional block within a network infrastructure to ensure integrity, confidentiality and availability of network communications, to detect unwanted activity, and to deter and block this unwanted activity or at least mitigate its effects on the network

vNSF

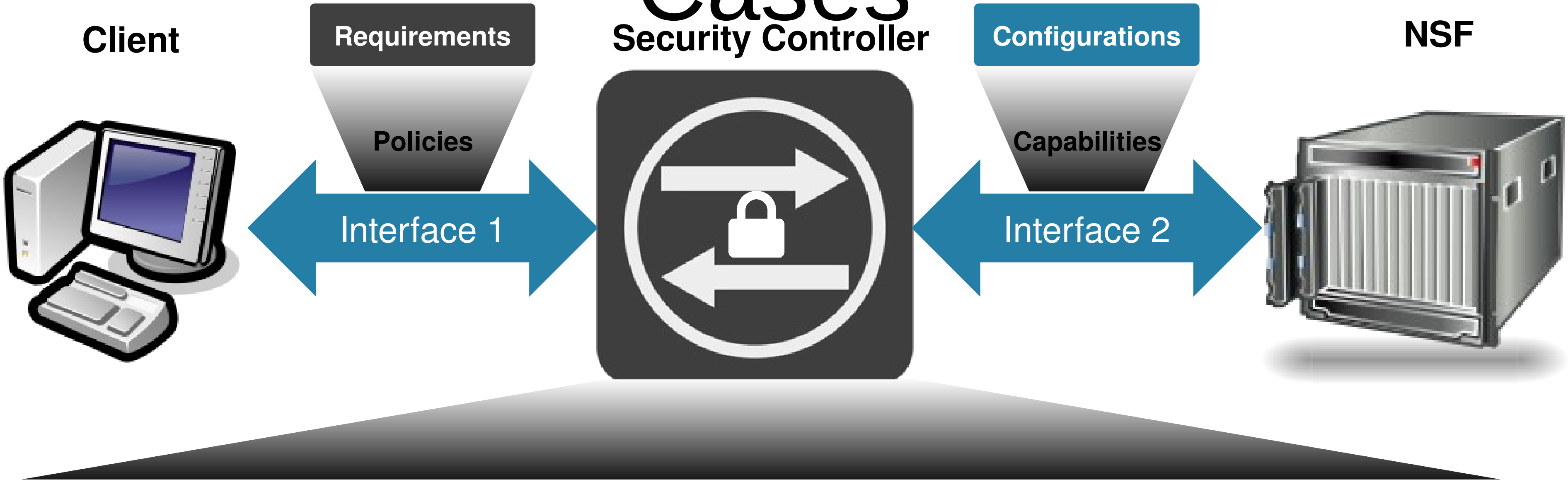
Virtual Network Security Function: A network security function that runs as a software image on a virtualized infrastructure, and can be requested by one domain but may be owned o managed by another domain



The Scenarios. A Global View



The Scenarios. Common Use Cases



Instantiation and Configuration	Updating	Collecting Status	Validation
Client sends security requirements through interface 1 to the security controller, which instantiates and configure the NSF through Interface 2	The client requires the update of security service functions, including adding or deleting a security function, and updating configurations	When users want to get the executing status of security functions they can request statistics information	Users may require to validate NSF availability, provenance, and/or its correct execution

The Two Scenarios at Play

Cloud Datacenter

The on-demand, dynamic nature of datacenter deployment essentially requires that the network security "devices" be in software or virtual form factors

On-demand vFirewall

- A service provider needs the ability to dynamically deploy virtual firewalls for each client's set of servers based on established security policies and underlying network topologies.
- Simplify the highly complex process, by the automation of firewall policy

Access Network

Customers (enterprise user, network administrator, residential user...) that request and manage security services hosted in the network service provider (NSP) infrastructure

vNSF deployment

- Instantiate a security service as one or the combination of several vNSF(s)
- Make it available for provisioning

vNSF customer provisioning

- Customer enrollment and cancellation to a vNSF
- Configuration of the vNSF, based on specific configurations, or derived from common security policies
- Retrieve and list of the vNSF functionalities, extracted from a manifest or a descriptor

And a Few Essential Requirements

Key Requirements

The I2NSF framework should provide a set of standard **interfaces** that **facilitate**:

- **Dynamic** creation, enablement, disablement, and removal of network security functions;
- **Policy-driven** placement of new function instances in the right administrative domain;
- Attachment of appropriate security and **traffic policies** to the function instances
- **Management** of deployed instances in terms of fault monitoring, event logging, inventory, etc.
- Single and **multi-tenant** environments and traffic policies.
- **Premise-agnostic**
- **Translation** of security policies into functional tasks and into vendor-specific configurations

Security Considerations

- **Relationship** between different actors must be associated with **administrative domains**
  - Closed environments with one administrative domain
  - Open environments where some NSFs can be hosted in different administrative domains
    - More restrictive security controls
    - Co osure ac
- **Attestation** e clients

Gap analysis

Interfaces for Virtual Security Functions Manager

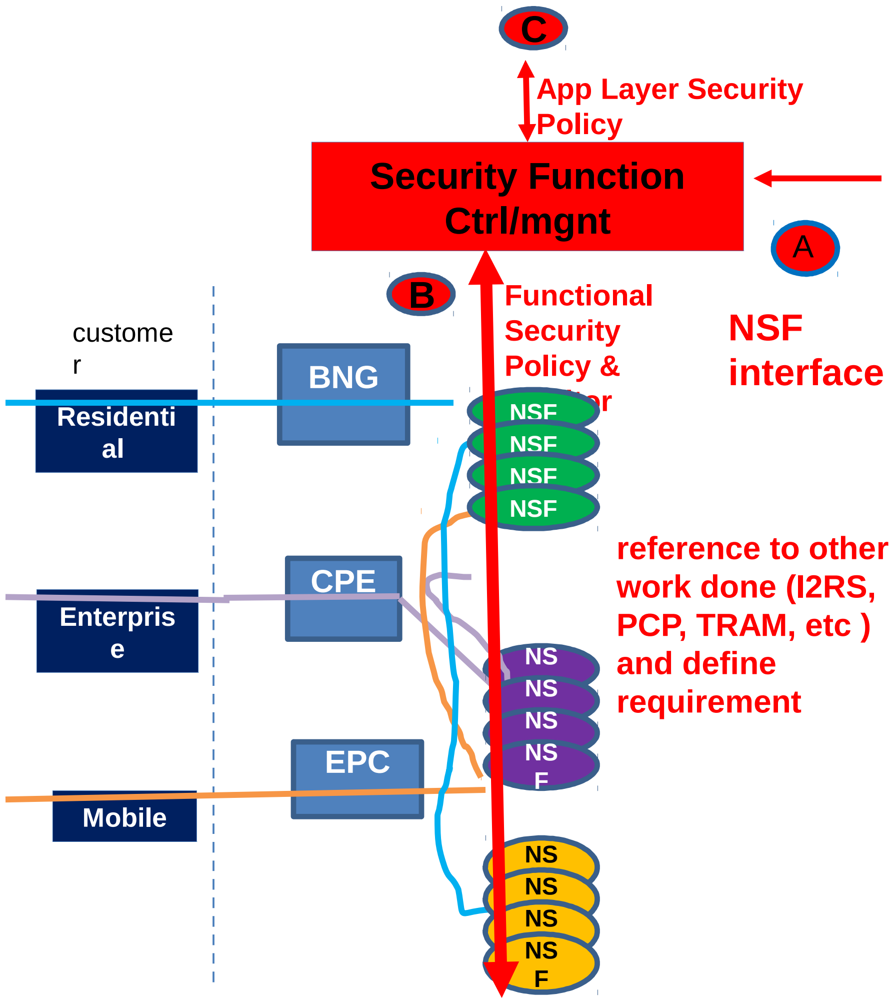
Interface: A

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

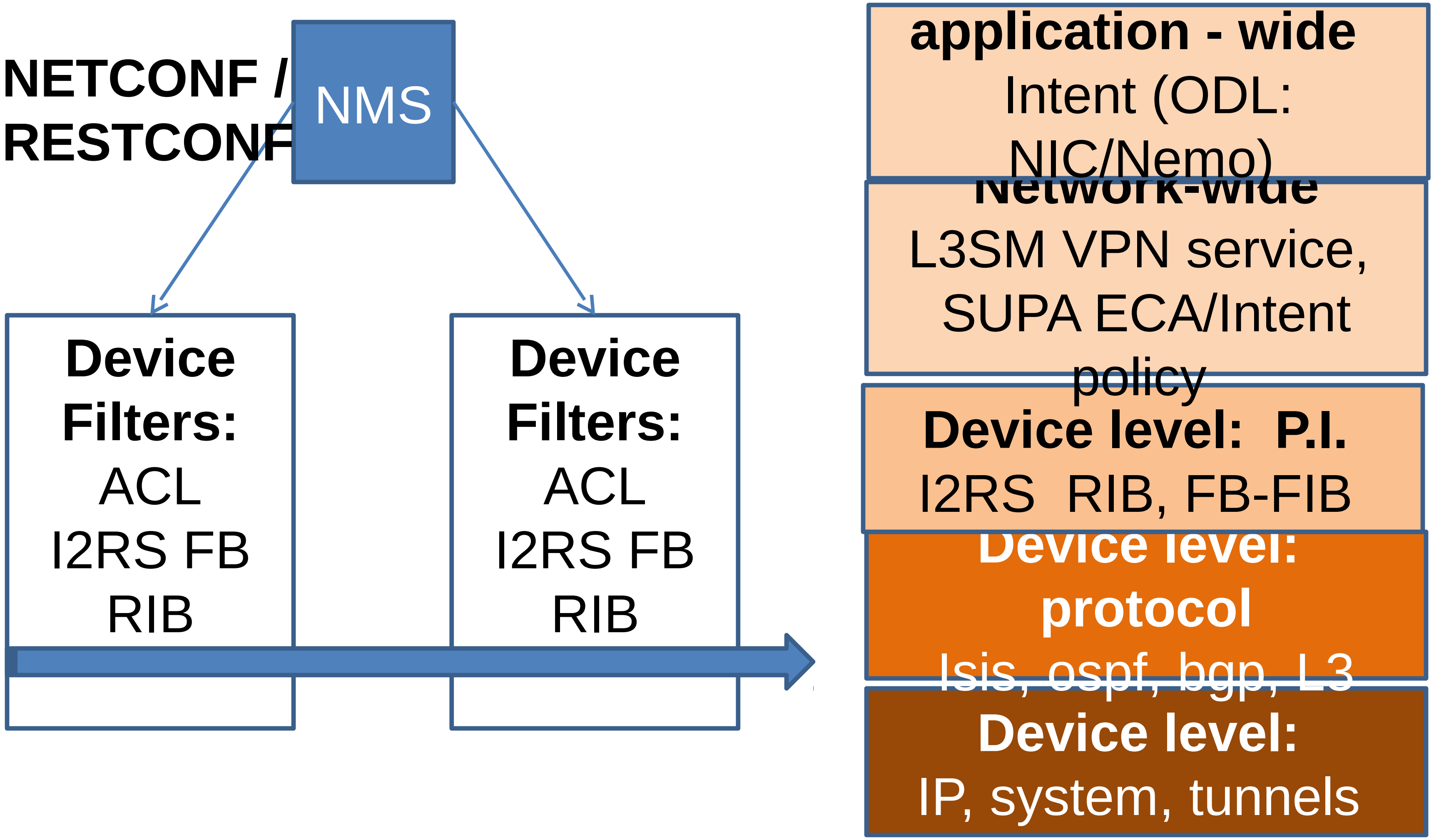
Interface: B & C

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



reference to other work done (I2RS, PCP, TRAM, etc) and define requirement

Filters



NETCONF / RESTCONF

NMS

Device Filters:
ACL
I2RS FB
RIB

Device Filters:
ACL
I2RS FB
RIB

application - wide
Intent (ODL: NIC/Nemo)

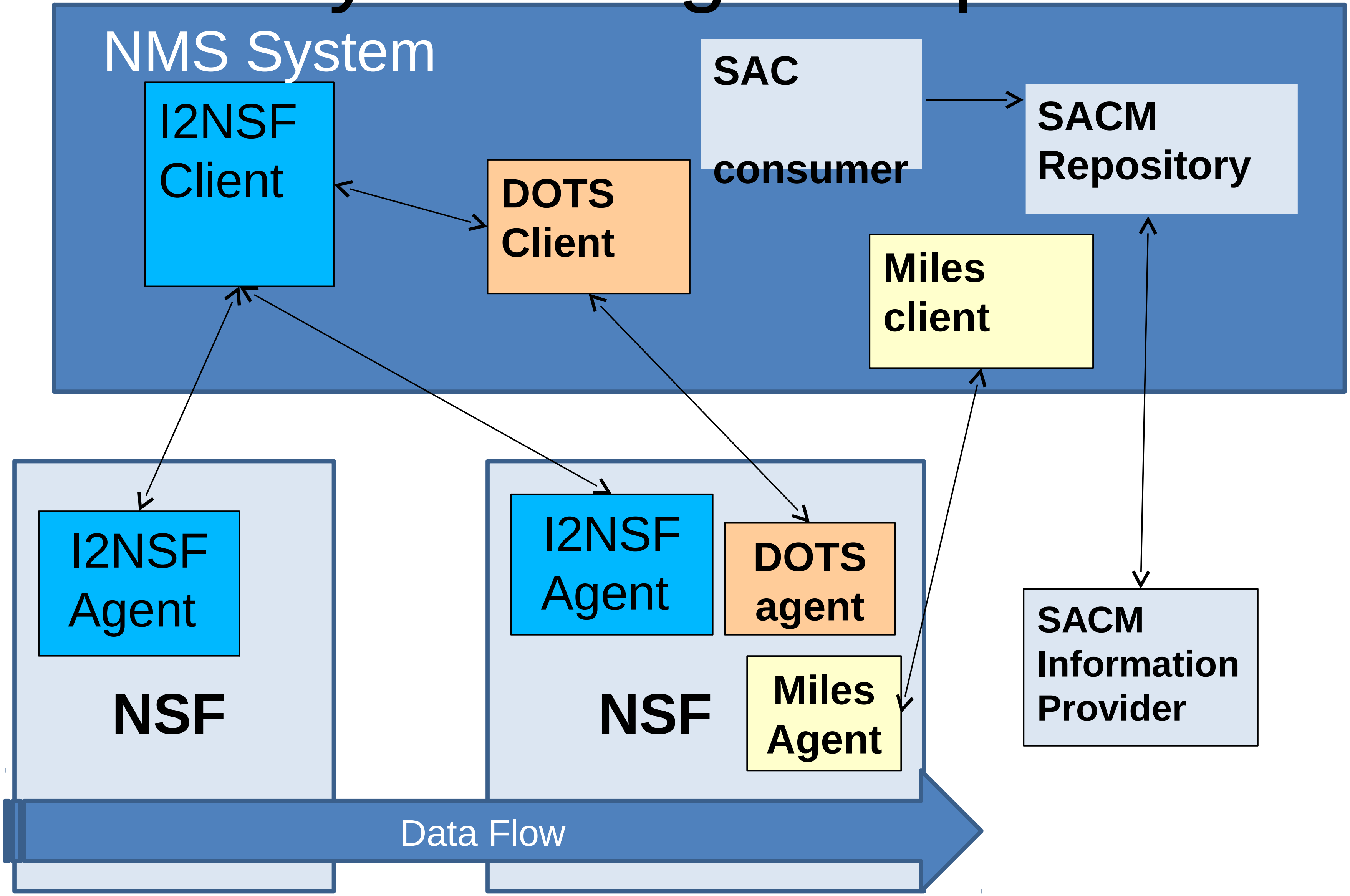
Network-wide
L3SM VPN service, SUPA ECA/Intent policy

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

Device level: protocol
Isis, ospf, bgp, L3

Device level:
IP, system, tunnels

Security Working Groups



NMS System

I2NSF Client

DOTS Client

SAC consumer

SACM Repository

Miles client

I2NSF Agent

NSF

I2NSF Agent

DOTS agent

Miles Agent

NSF

SACM Information Provider

Data Flow

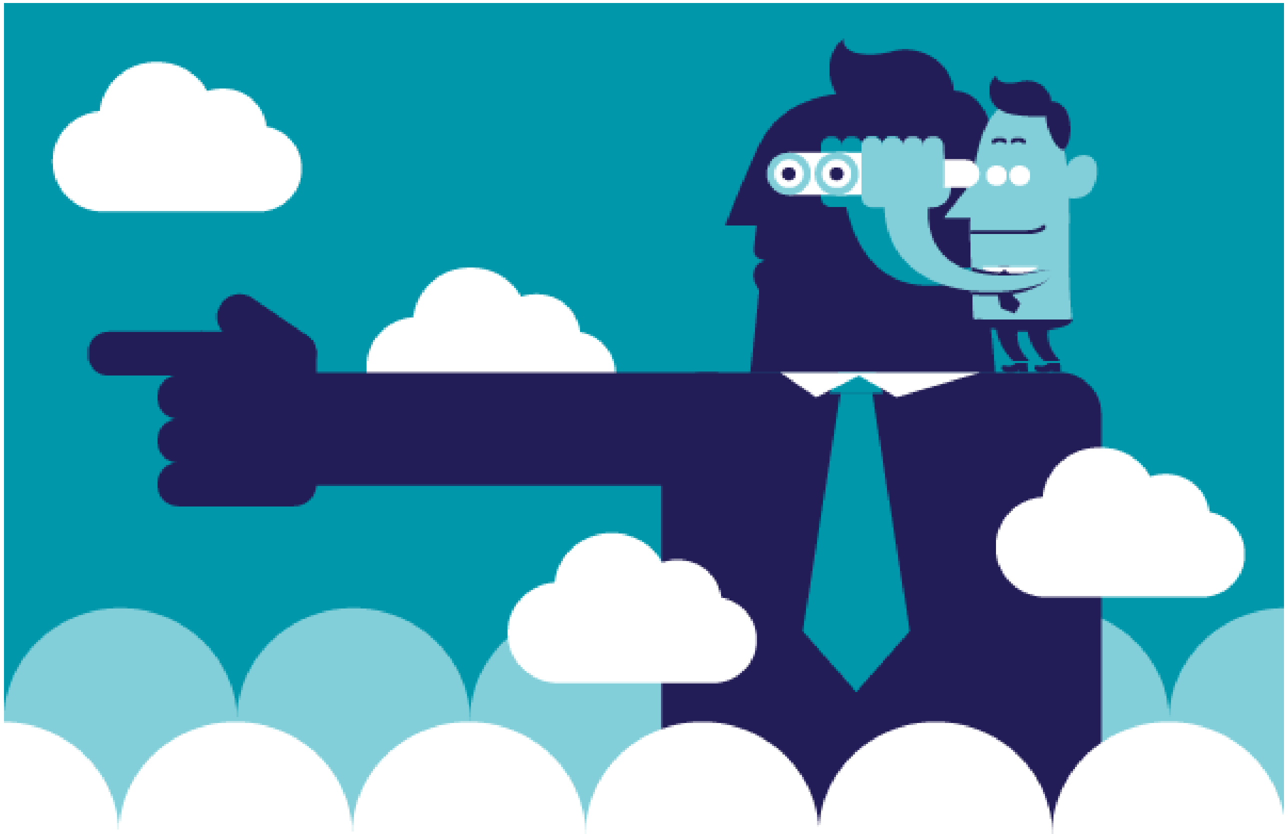
Other Areas

- 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

Call for Help



Security experts to help review and guide these documents