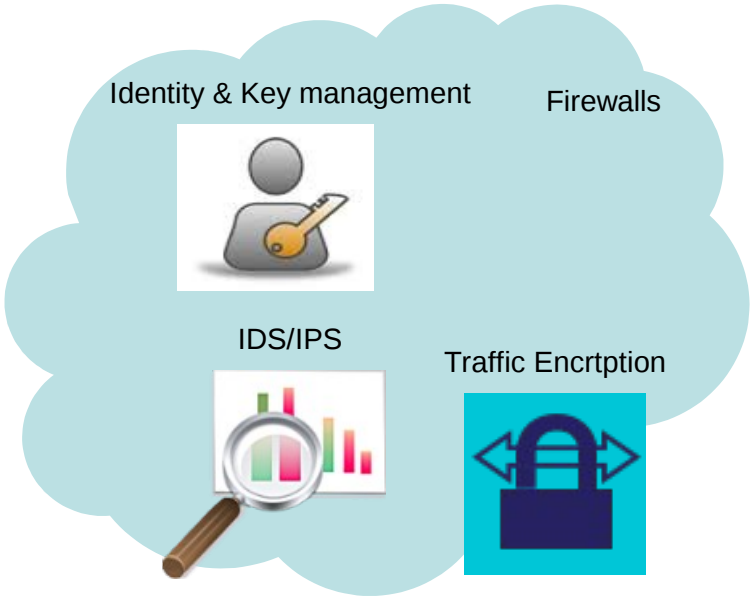
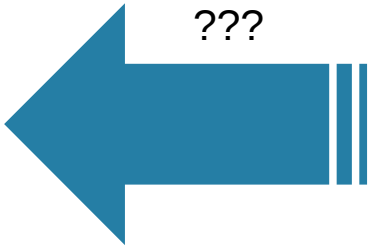
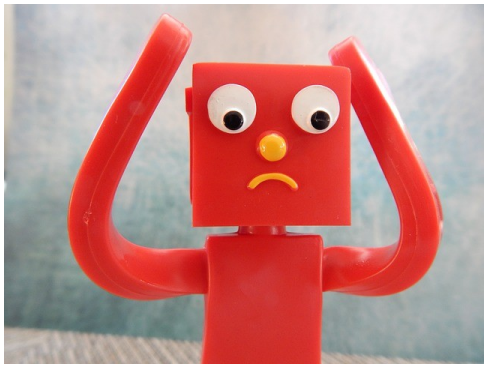

Telefónica
Use Cases and Requirements for I2NSF_
draft-pastor-i2nsf-merged-use-cases
BE MORE_

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
- The current draft describes 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
  - Datacenters







Terminology: A Couple of Basic Definitions

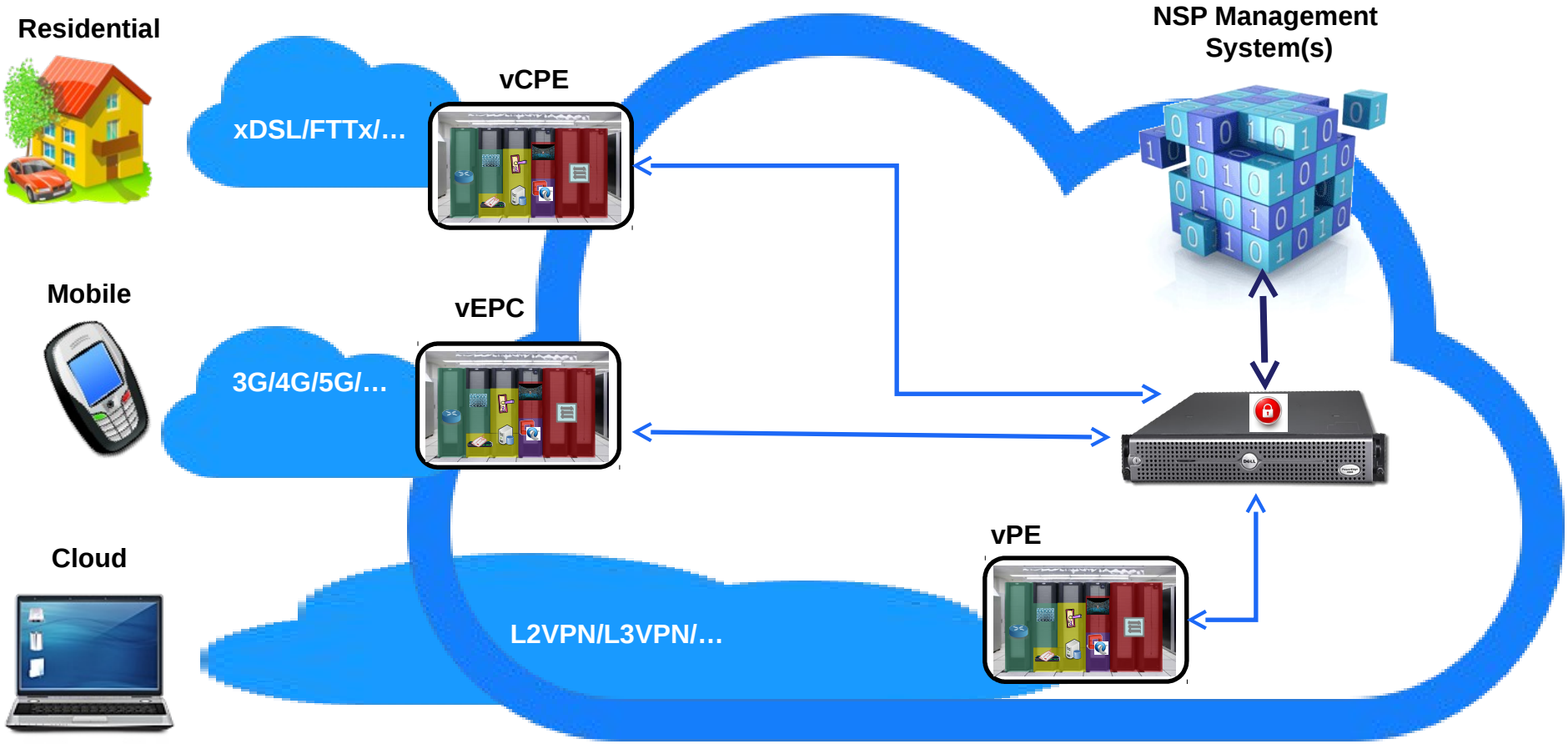
NSF

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

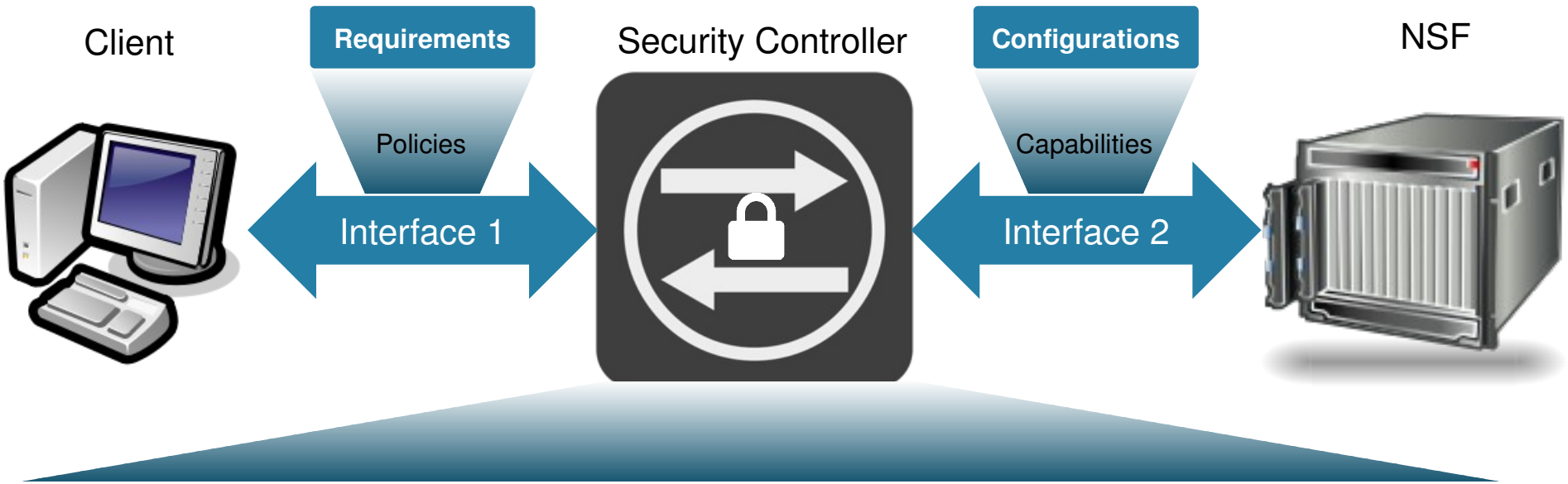
vNSF

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

Client sends security requirements through interface 1 to the security controller, which instantiates and configure the NSF through Interface 2

Updating

The client requires the update of security service functions, including adding or deleting a security function, and updating configurations

Collecting Status

When users want to get the executing status of security functions they can request statistics information

Validation

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 deployment

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
  - Control on policy disclosure across domains

Attestation of the vNSF by the clients