I2NSF WG:
Client Facing Interface Requirements

Rakesh Kumar

Anil Lohiya

Xialiang (Frank)

Youjianjie (Jianjie)

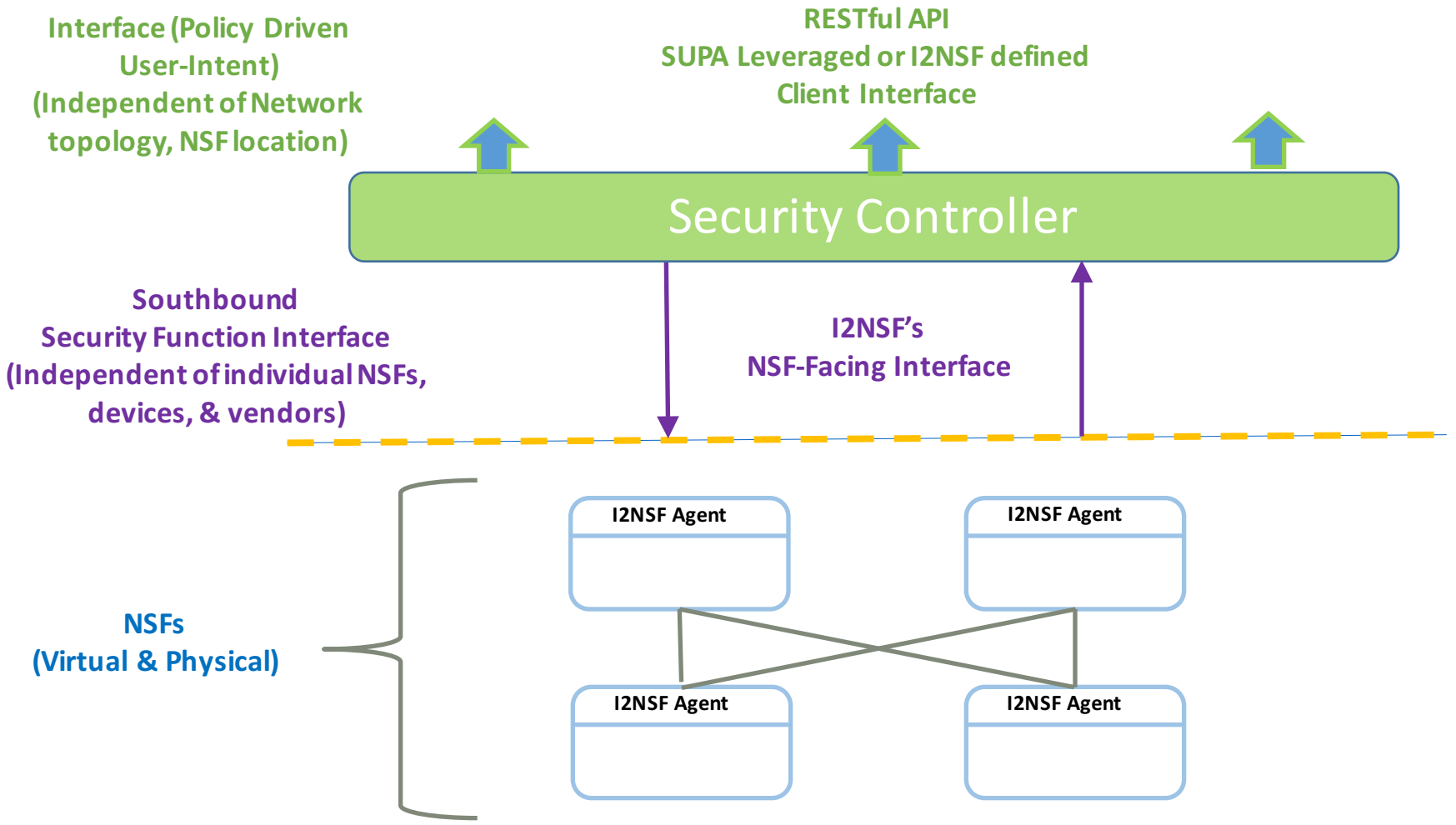
Version 1.0

Jul 21, 2016

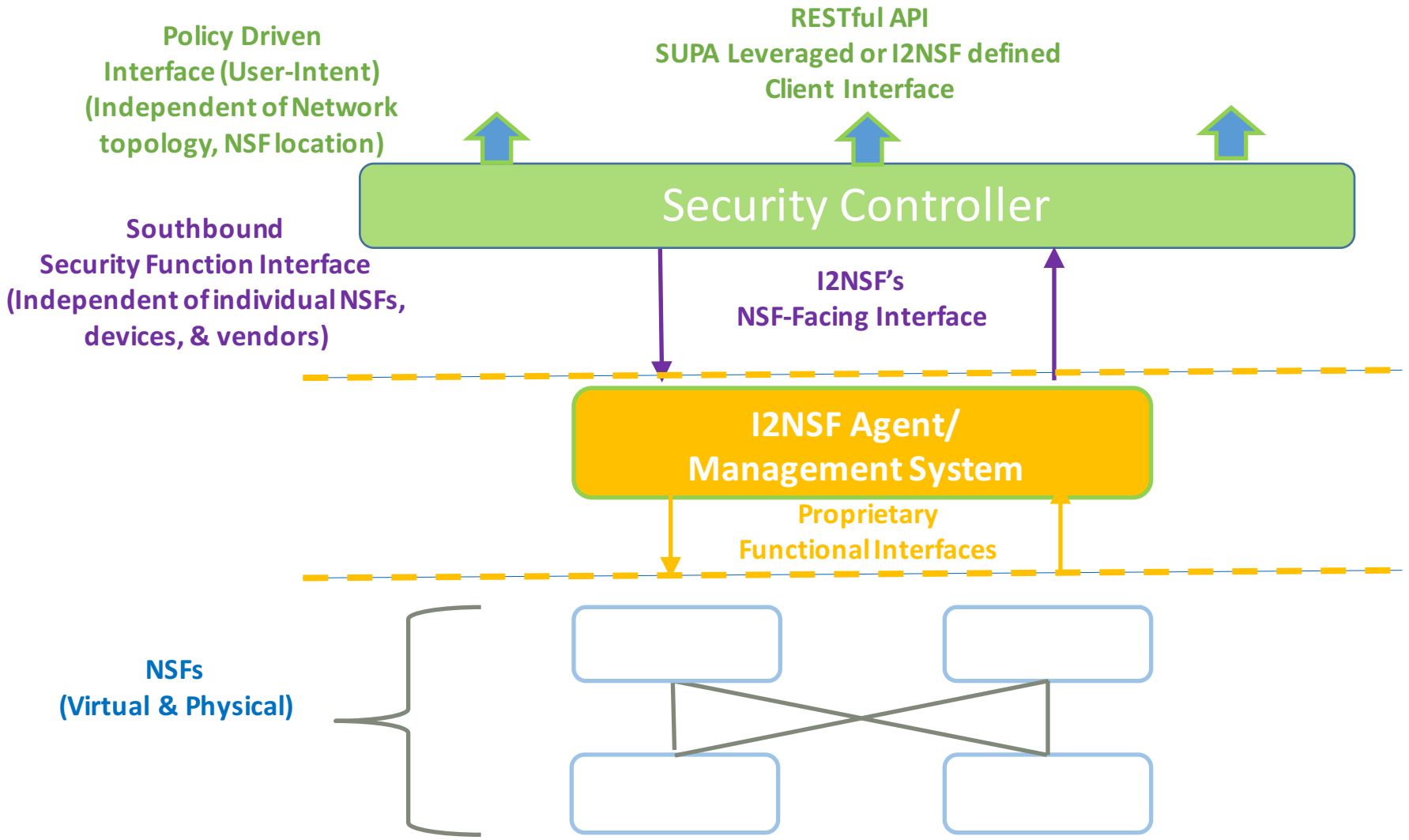
Agenda

- ❑ Security Controller Architecture
- ❑ I2NSF framework for Security Controller
- ❑ I2NSF Client Facing Interface requirements
- ❑ Leverage SUPA Policy driven framework for client interfaces
- ❑ Draft proposal
  - ➢ https://www.ietf.org/internet-drafts/draft-kumar-i2nsf-controller-northbound-framework-00.txt

Security Controller Architecture – Model-1



Security Controller Architecture – Model-2



I2NSF Framework for Security Controller

❑ Security Controller – I2NSF Client Interface

- ➢ Security Controller's interface to the client
  - GUI Portal, RESful API, Template Engine, Natural Language Parser (NLP)
- ➢ Agnostic of network topology and NSF location in the network
  - Declarative/Descriptive model instead of Imperative/Prescriptive model
    - How a user would like to see security policy instead of how it would be actually implemented
- ➢ Leverage SUPA policy interface, if possible
  - Client Interface can be modeled as a special case of SUPA's management policy

❑ Security Controller – I2NSF NSF Interface

- ➢ Security Controller's interface to NSF
  - Change and retrieve operational state related to security functions
- ➢ Agnostic of vendor, implementation and form-factor (physical, virtual)
  - Agnostic to how NSF is implemented and its hosting requirements
  - Agnostic to how NSF becomes operational
    - Network connectivity and other hosting requirements
  - Agnostic to NSF control plane implementation (if there is one)
    - E.g., cluster of NSF active as one unified service for scale and/or resilience
  - Agnostic to NSF data plane implementation
    - Encapsulation, Service function chains

I2NSF Client Interface Requirements …(1/3)

- User-Intent modeling requirements
  - Meta-data driven groups
    - User-group
      - e.g., HR-users, Finance-users
    - Device-group
      - e.g., Windows-devices, Lynix-devices
    - Application-group
      - e.g., Finance-apps, Legal-apps, HR-apps
    - Location-group
      - e.g., US-sites, EMEA-sites, APAC-sites
  - Group definition
    - Fixed definition
      - IP address
    - Dynamic mapping
      - LDAP, Active Directory, CMDB
- Policy modeling requirements
  - Policy lifecycle management
    - User-action based activation
    - Time-profile based activation
    - Event-profile based activation

I2NSF Client Interface Requirements …(2/3)

- Policy rules
  - Threat management
    - Botnet access
    - Malware handling
    - DDoS handling
    - Parental control (URL/domain filtering)
    - Application threats
  - Inter-group access
    - User-group, Application-group, Device-group, Location-group
  - Intra-group access
    - User-group, Application-group, Device-group, Location-group
- Policy actions
  - Permit, Deny
  - Metering, QoS profile
  - Quarantine/Redirect
  - Log, Monitor/Mirror

I2NSF Client Interface Requirements ...(3/3)

- Authentication requirements
  - Deployment and operational model governs the actual scheme
- Authorization requirements
  - Deployment model operational governs the actual scheme
- Operational requirements
  - Multi-tenancy
  - Telemetry
    - Threat visibility, Policy violations, Big-data analytics
  - Notification
    - Alarm, Event
  - Affinity
    - TPM
    - Other possible requirements
  - Capability discovery
    - Need further investigation
  - Test Interface
    - Test whether a client request can be implemented
    - Potential policy conflict assessment