SUPA WG:
I2NSF Client Facing Interface Requirements

Rakesh Kumar
Anil Lohiya
Agenda

- Security Controller Architecture
- I2NSF framework for Security Controller
- I2NSF Client Facing Interface requirements
- Leverage SUPA Policy driven framework for client interfaces
- Draft proposal
Security Controller Architecture

- Interface (Policy Driven User-Intent) (Independent of Network topology, NSF location)
- RESTful API SUPA Leveraged or I2NSF defined Client Interface
- Southbound Security Function Interface (Independent of individual NSFs, devices, & vendors)
- I2NSF's NSF-Facing Interface

NSFs (Virtual & Physical)

I2NSF Agent

I2NSF Agent

I2NSF Agent

I2NSF Agent
I2NSF Framework for Security Controller

- Security Controller — I2NSF Client Interface
  - Security Controller’s interface to the client
    - GUI Portal, RESTful 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
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