Applicability of Interfaces to Network Security Functions to Networked Security Services
(draft-jeong-i2nsf-applicability-01)

IETF 99, Prague, Czech
July 18, 2017

Jaehoon (Paul) Jeong*, Sangwon Hyun, Tae-Jin Ahn,
Susan Hares, and Diego Lopez

Motivation of This Draft

- I2NSF Applicability
  - I2NSF Chartered Working Item
  - This draft explains how I2NSF framework and interfaces can be used for real network services.
- Contents
  - An I2NSF Framework with Software-Defined Networking (SDN)
  - Use Cases
    - Firewall
    - Deep Packet Inspection
    - Attack Mitigation

Why the Combination of I2NSF and SDN?

- Accelerated Security Service
  - SDN switch can perform simple firewall services.
  - SDN's flow table is good at basic security actions (e.g., forward, drop, and mirror).
  - Complicated security services (e.g., session-based firewall) can be performed at a close or remote NSF.
- I2NSF Policy Rule Enforcement
  - I2NSF User's firewall policies (according to the Capability Information Model) can be set up in both an NSF and SDN Switches via SDN Switch Control.
  - NSF-Facing Interface can be used for this configuration setup.

I2NSF Framework with SDN

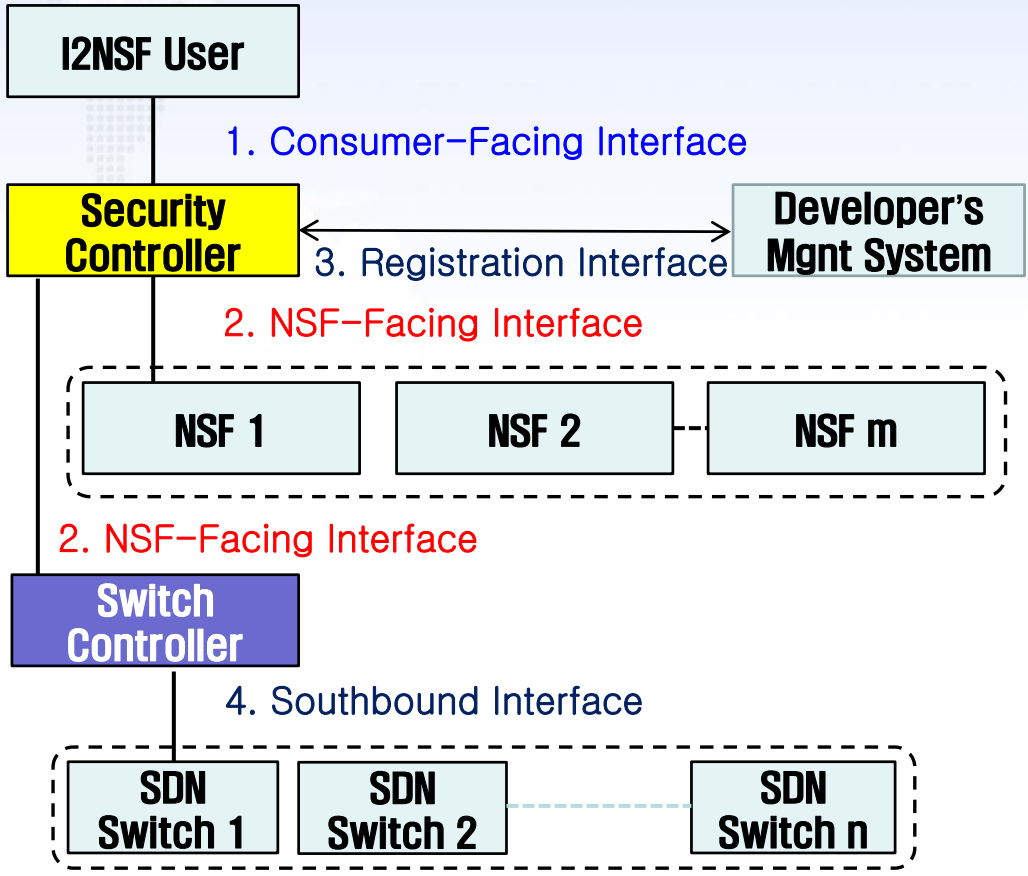
An I2NSF Framework with SDN for Efficient Security Services

1. **I2NSF User** asks for security services with high-level security policies to **Security Controller** via **Consumer-Facing Interface.**

2. **Security Controller** delivers low-level security policies to **NSFs** and **Switch Controller** via **NSF-Facing Interface.**

3. **Network Security Function** configures such low-level security policies into its local system.

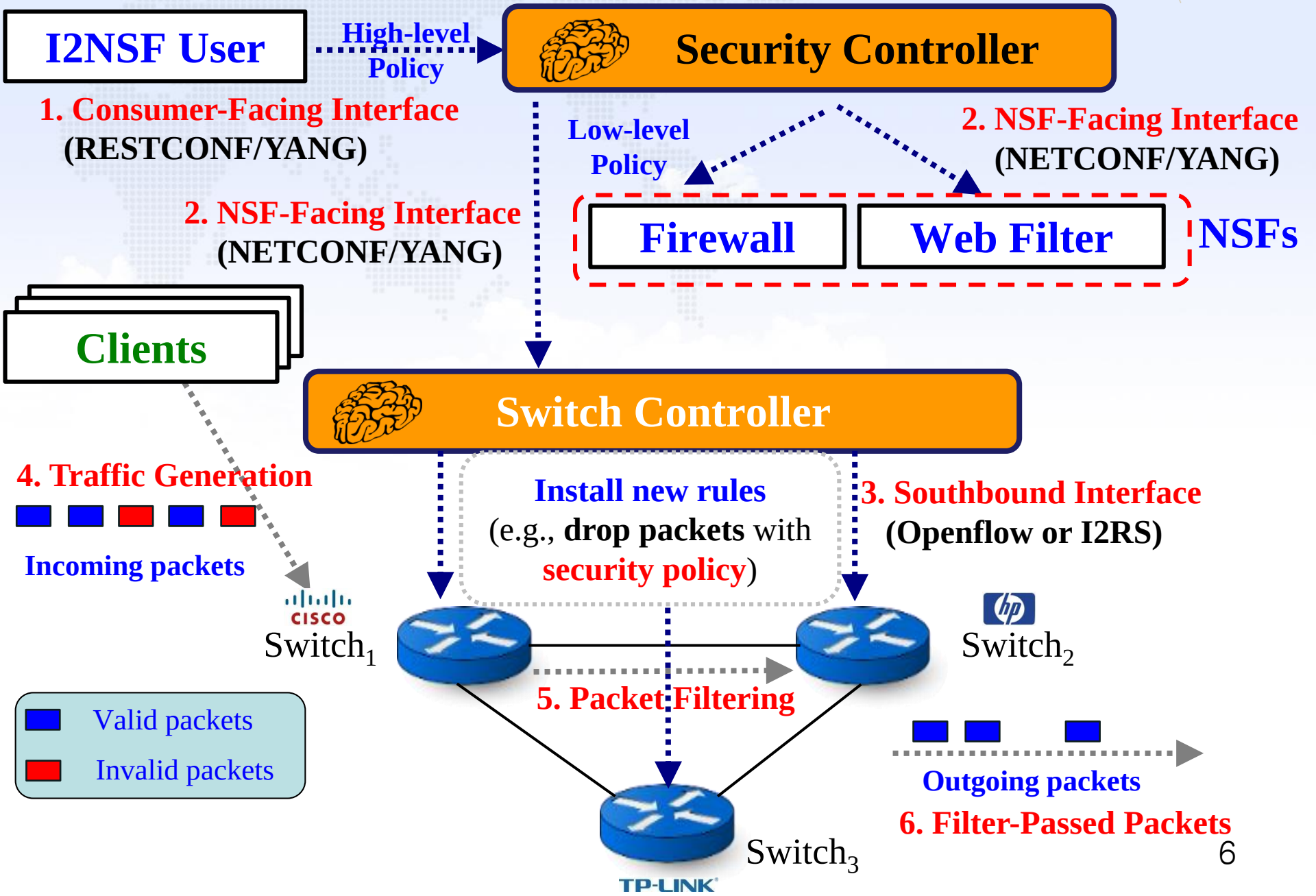
4. **Switch Controller** sets up filtering rules for the low-level policies on Switches via **Southbound Interface**.



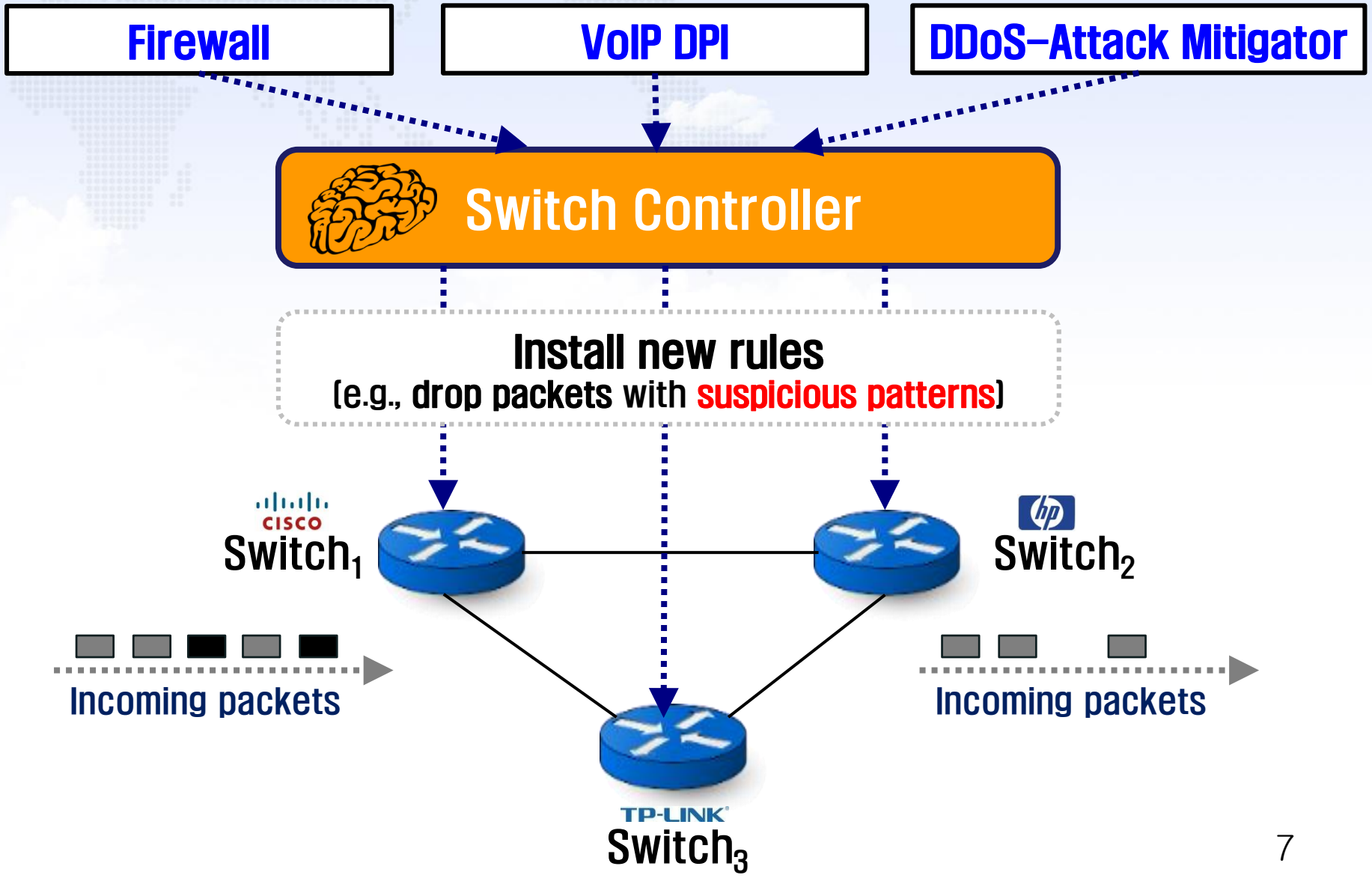
Information and Data Models for I2NSF

- Consumer-Facing Interface
  - Information Model
    - draft-kumar-i2nsf-client-facing-interface-im-03
  - Data Model
    - draft-jeong-i2nsf-consumer-facing-interface-dm-02
- NSF-Facing Interface
  - Information Model
    - draft-xibassnez-i2nsf-capability-02
  - Data Model
    - draft-kim-i2nsf-nsf-facing-interface-data-model-02
- Registration Interface
  - Information Model
    - draft-hyun-i2nsf-registration-interface-im-02
  - Data Model
    - draft-hyun-i2nsf-registration-interface-dm-01

Security Service Procedure in I2NSF Framework



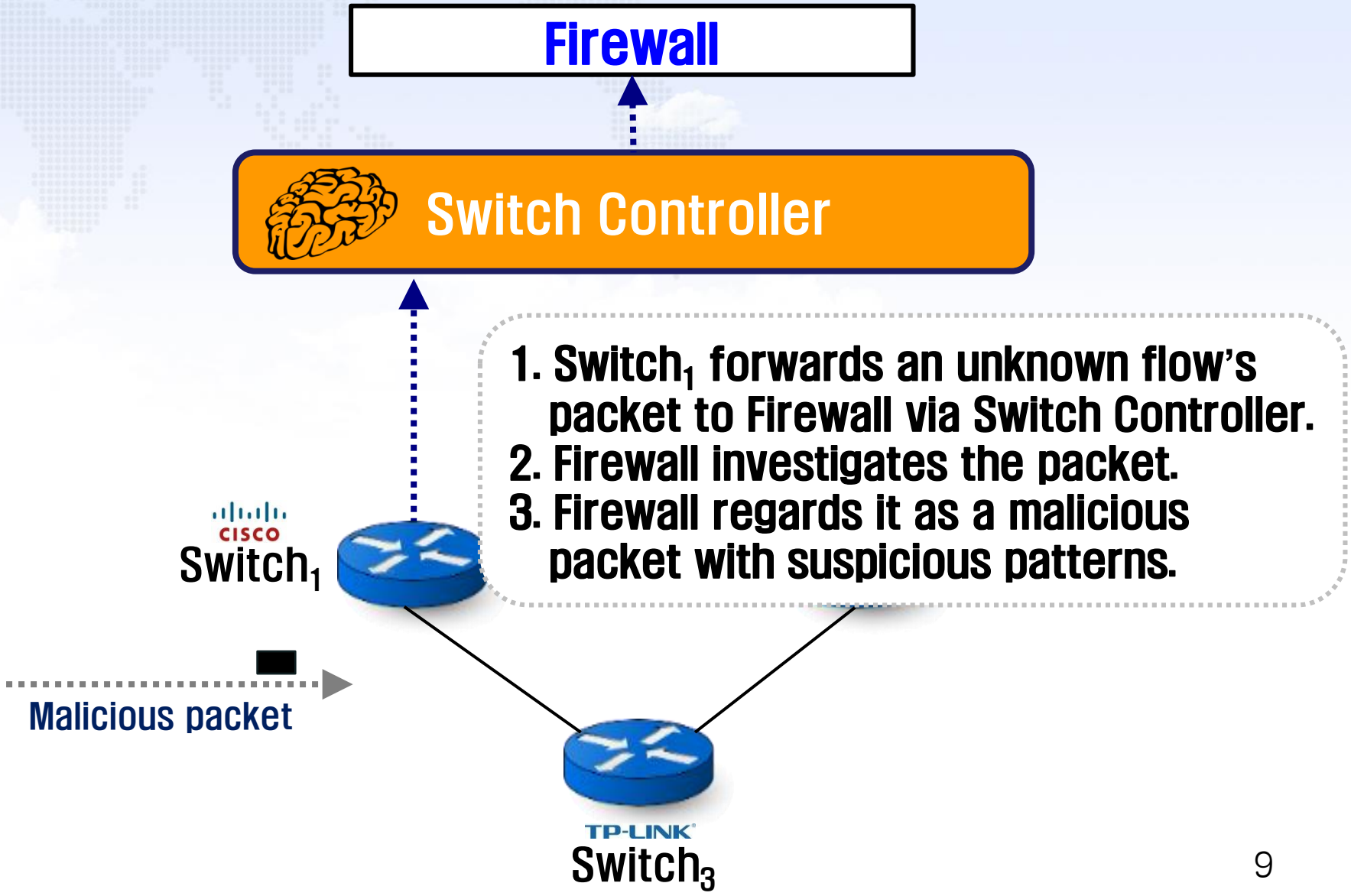
I2NSF Security Services with SDN



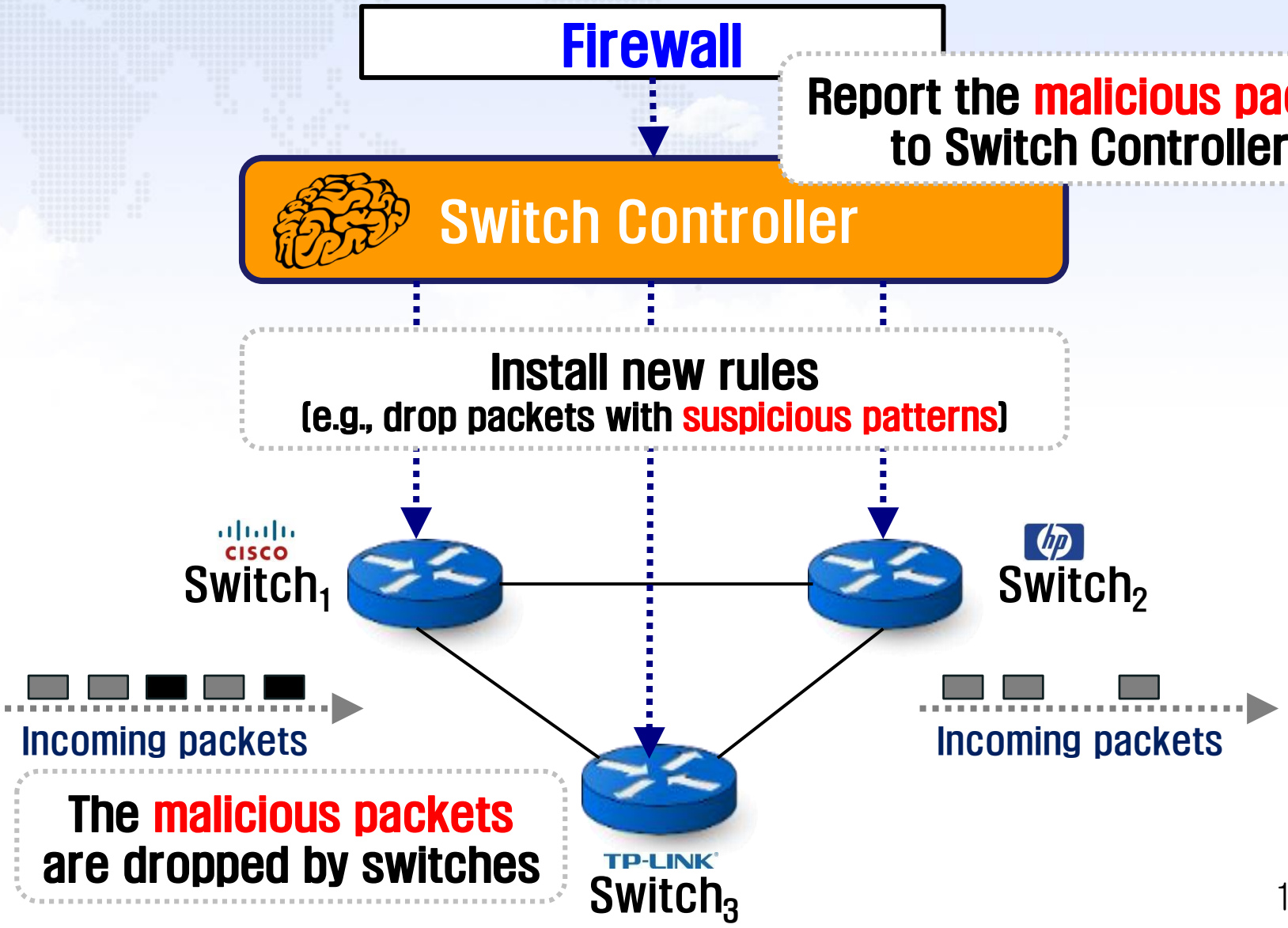
Use Cases

- Centralized Firewall System
  - This is for malicious packets.
- Centralized VoIP/VoLTE Security System
  - This is for Hacker's invalid voice call packets.
- Centralized DDoS-Attack Mitigator
  - This is for DDoS-attack packets.

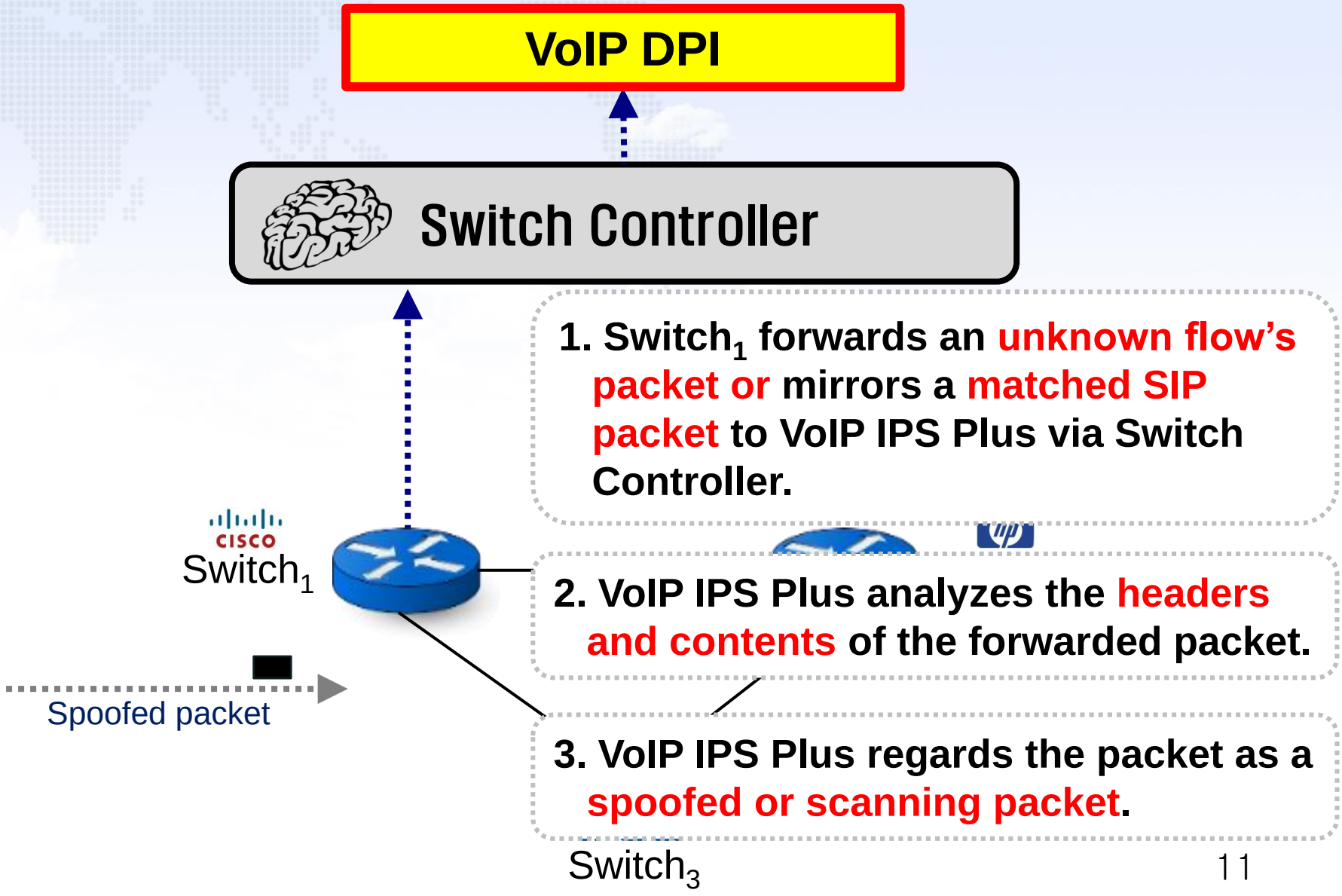
Centralized Firewall System (1/2)



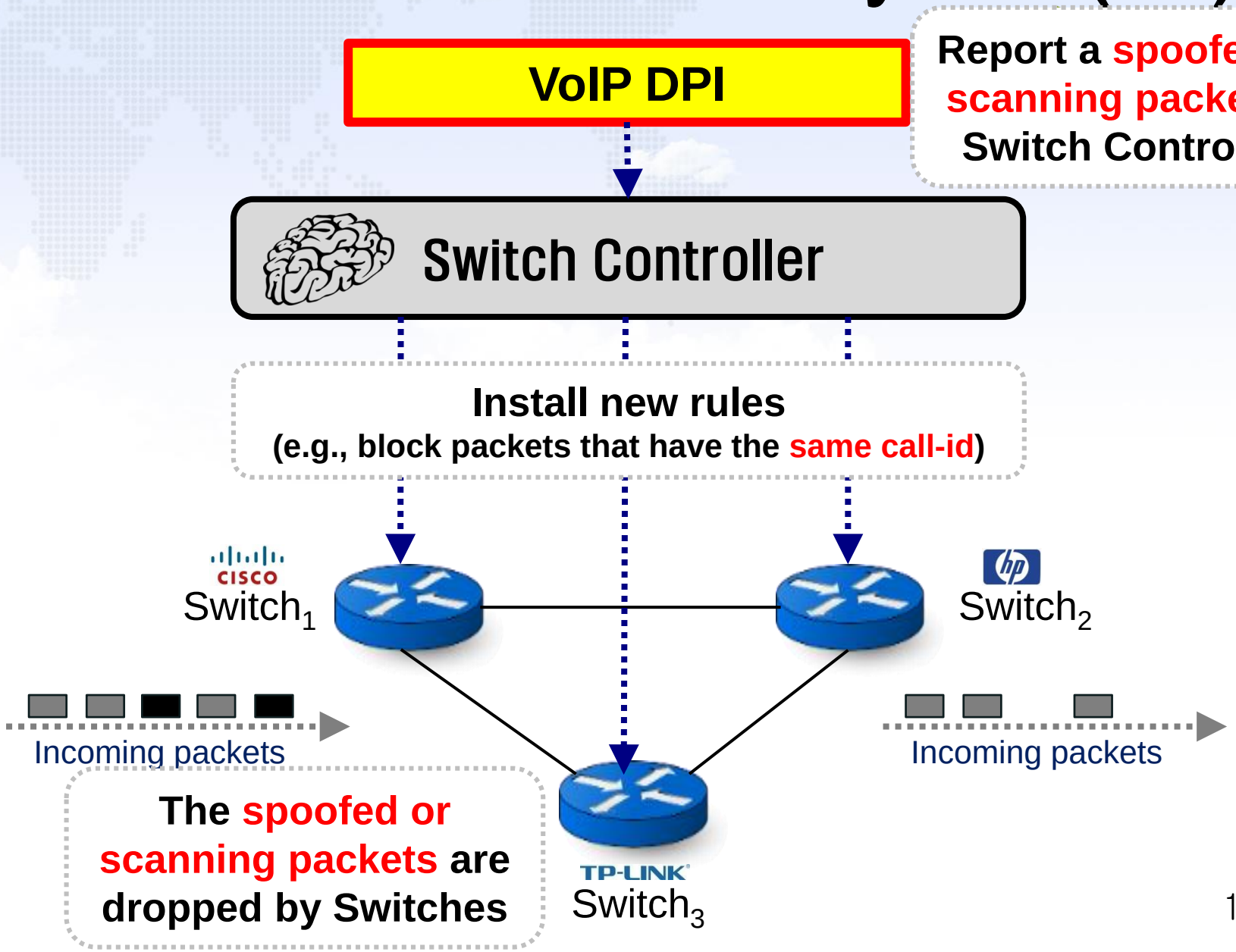
Centralized Firewall System (2/2)



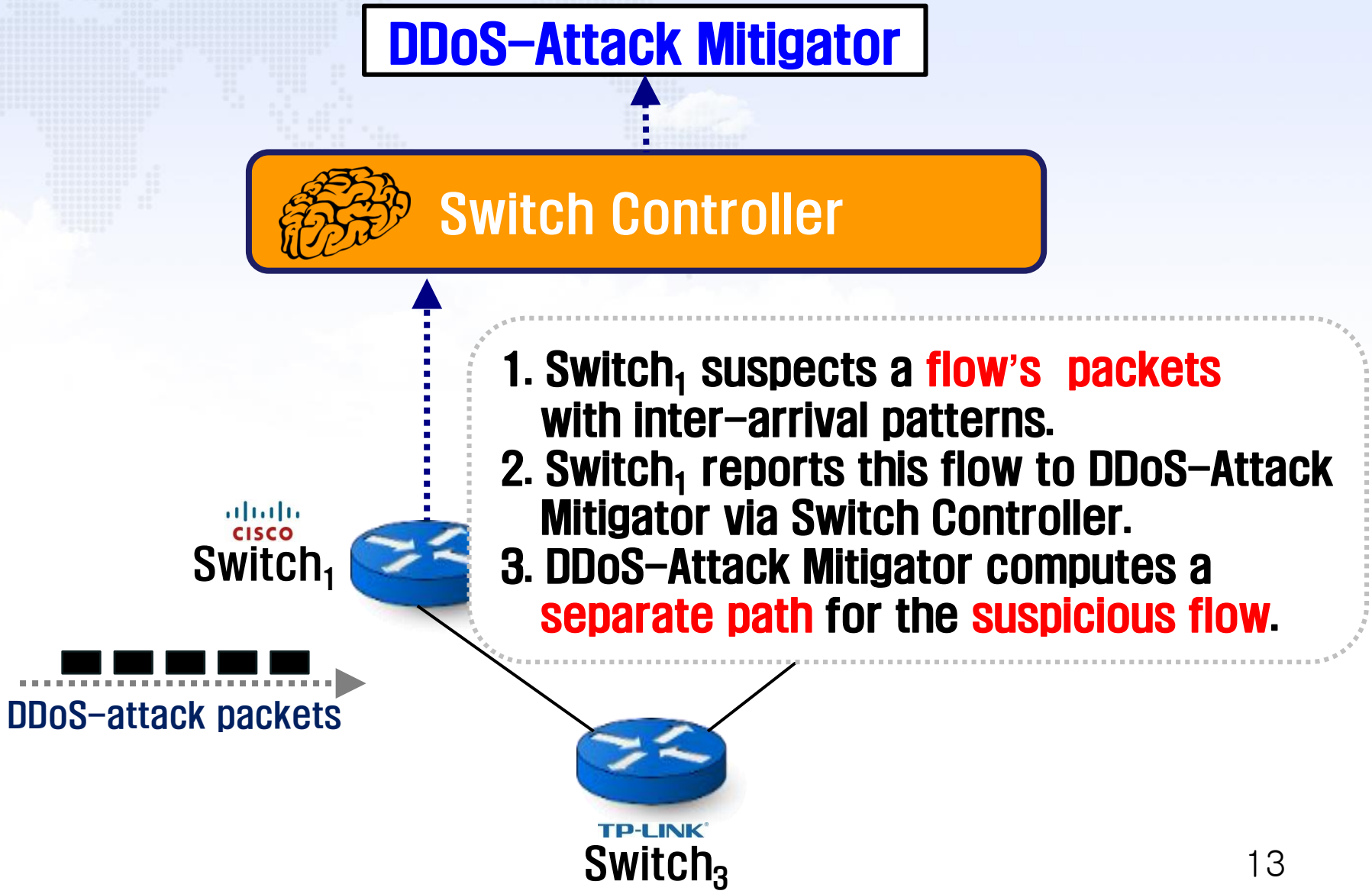
Centralized VoIP/VoLTE System (1/2)



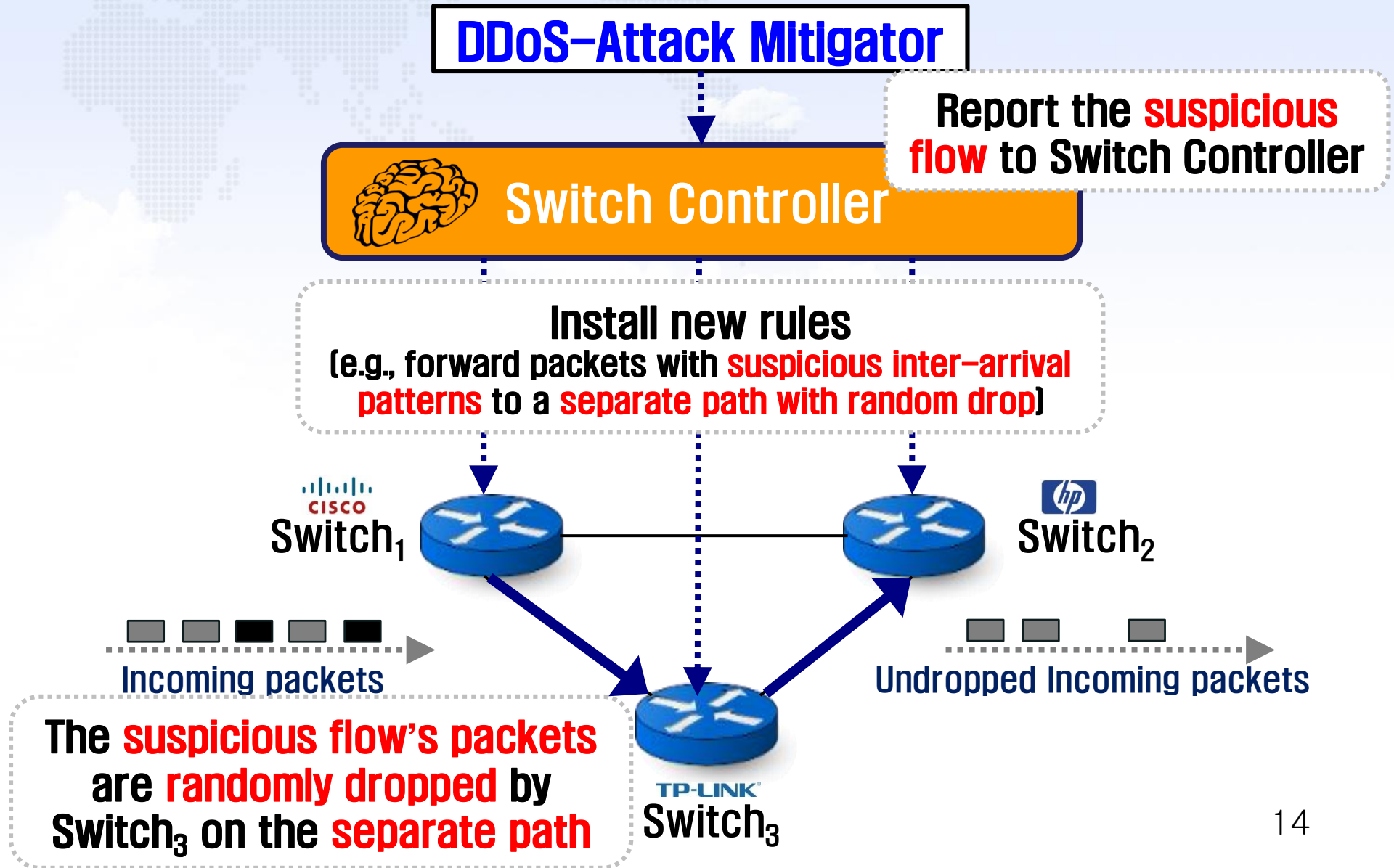
Centralized VoIP/VoLTE System (2/2)



Centralized DDoS-Attack Mitigator (1/2)



Centralized DDoS-Attack Mitigator (2/2)



Next Steps

- Use Cases for SFC-based Security Function Chaining will be added.
  - Firewall and Web Filter
  - Firewall and DDoS-Attack Mitigator
- Reflection of I2NSF Hackathon Experience
  - This draft will be described in more detail with the experience and lessons from IETF I2NSF Hackathon Project.
- Can this draft be adopted as a WG document?
- Welcome your Feedback!