Requirements for Security Services based on Software-Defined Networking

draft-jeong-i2nsf-sdn-security-services-00

IETF 91, Honolulu, HI,
November 13, 2014

Jaehoon (Paul) Jeong, Hyoungshick Kim, and Jung-Soo Park
Sungkyunkwan University & ETRI

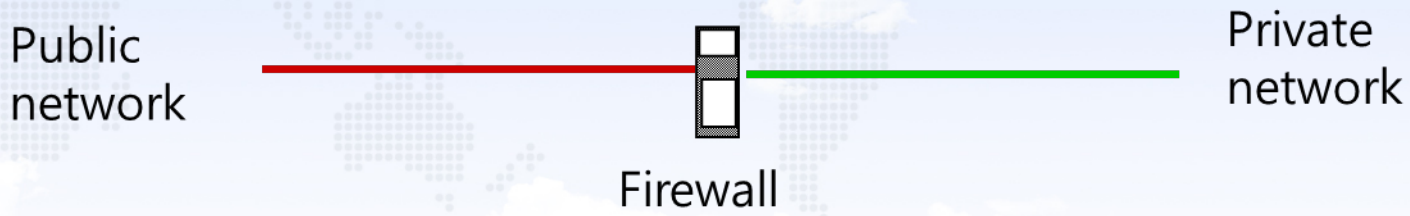
Contents

Standardization Status in ITU-T

- Working Item in Study Group 17 (SG 17), Question 6 (Q.6) in ITU-T
  - Our proposal for“**Requirements for Security Services based on Soft ware-Defined Networking**”was accepted as a **working item** in Septe mber Meeting in 2014.
- Scope of the Draft in SG 17.
  - Classify the network resources for SDN-based security services.
  - Define the requirements for SDN-based security services.
  - Define the enhanced framework to support SDN-based security service s.
  - Define use cases for security services based on SDN.

Motivation

Legacy Firewall



- Firewall inspects packets that attempt to cross a network boundary.

- Firewall rejects any illegal packets such as
  - Incoming requests to open illegal TCP connections,
  - Packets of other illegal types (e.g., UDP and ICMP), and
  - IP datagrams with illegal IP addresses (or ports).

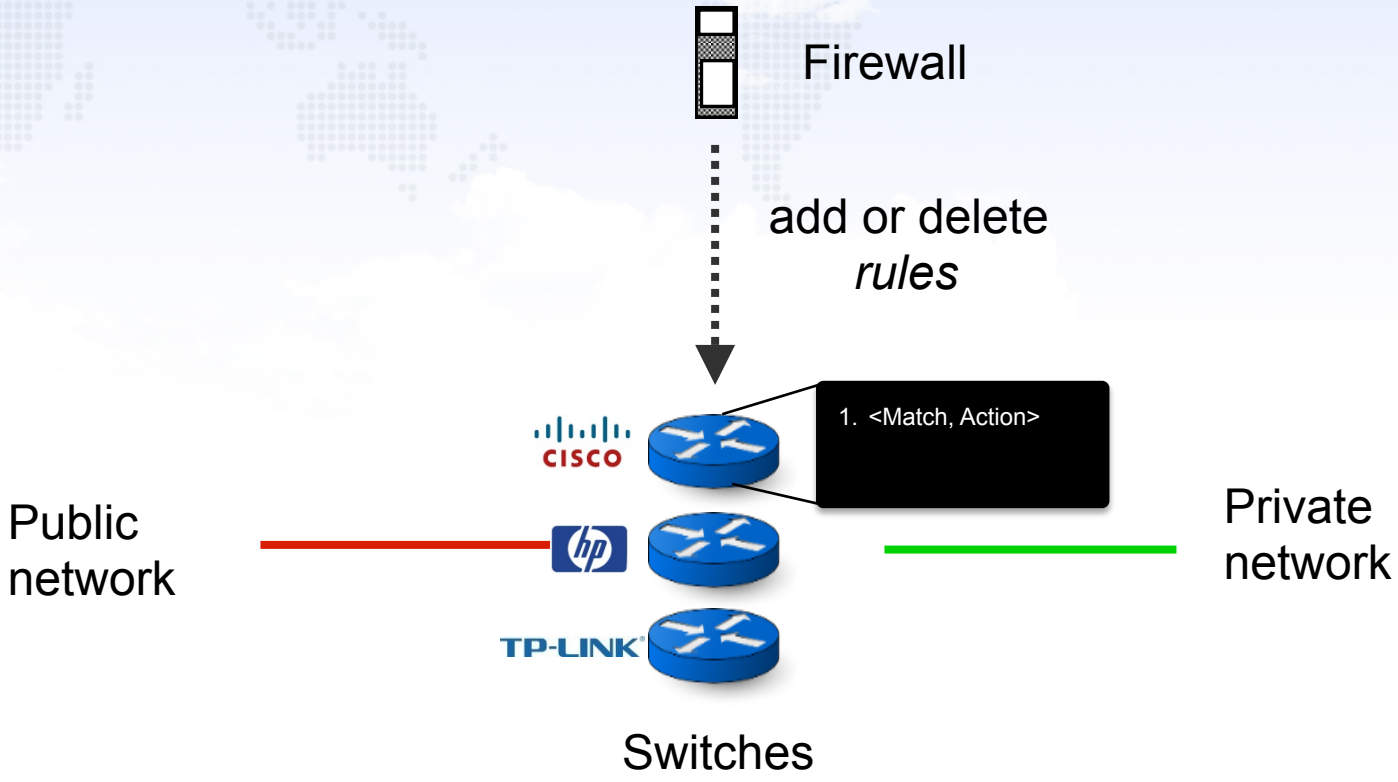
- Firewall provides security at the loss of flexibility and the cost of network administration.

Challenges in Firewall

- Cost
  - The cost of adding firewalls to routers is substantial.
- Performance
  - Firewalls are often slower than the link speed of their network interfaces .
- Management
  - Managing access control dynamically across hundreds of network elem ents is a challenge.
- Policy
  - It is difficult to describe what are permitted and denied flows within the s pecific organization.
- Binding
  - Packet-based access mechanism is not enough in practice since the ba sic unit of access control is usually user or application.
    - e.g., Skype connections for specific users are open.

Centralized Network Firewall based on Software-Defined Networking (SDN)

- Centralized Network Firewall

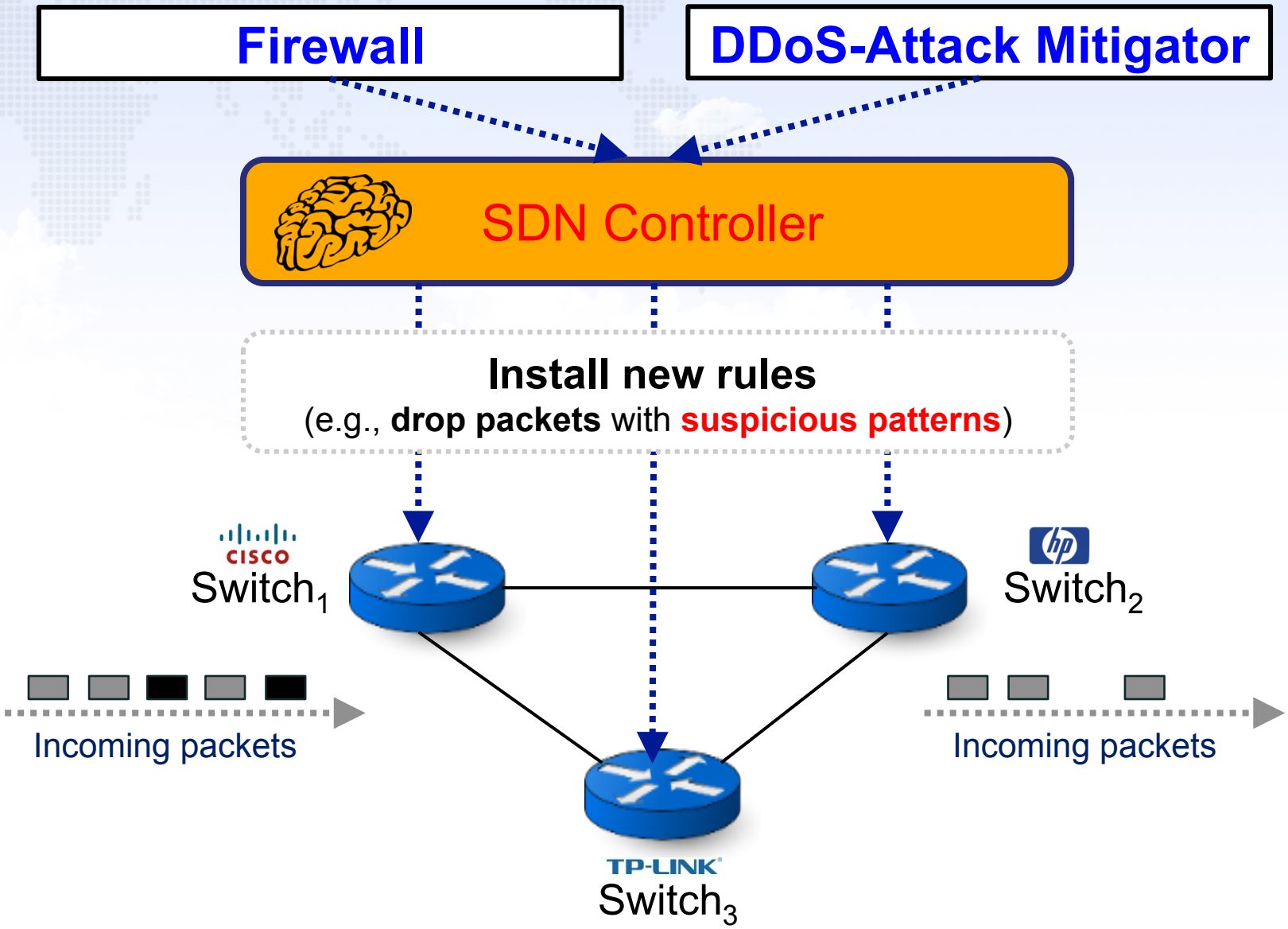


- Firewall rules can be managed flexibly by a centralized server.
- SDN protocols can be used for a standard interface between firewall applications and switches.

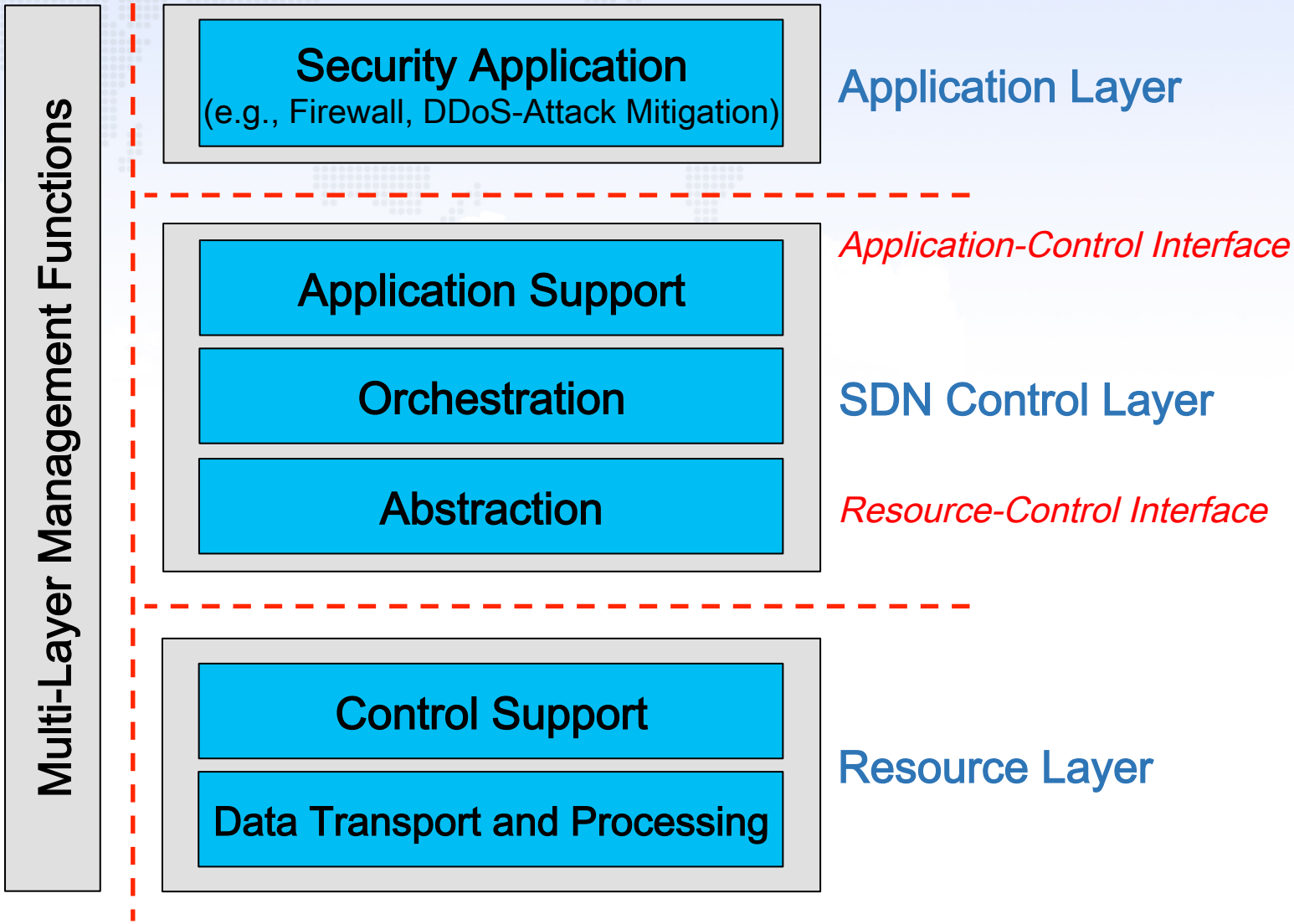
Expectations for SDN-Based Firewall

- Cost
  - Ideally, one single firewall is enough.
- Performance
  - Firewalls can adaptively be deployed depending on network conditions .
- Management
  - Firewall rules can dynamically be added with new attacks.
- Policy
  - Centralized view might be helpful to determine security policies.
- Binding
  - Application level rules can be defined by software.

SDN-Based Security Services



High-Level Architecture for SDN-Based Security Services



Objectives

- Prompt reaction to new network attacks
  - SDN-based security services allow private networks to defend themsel ves against new sophisticated network attacks.

- Autonomous defense from network attacks
  - SDN-based security services identify the category of network attack (e. g., worms and DDoS attacks).
  - They take counteraction for the defense without the intervention of net work administrators.

- Network-load-aware resource allocation
  - SDN-based security services measure the overhead of resources for s ecurity services.
  - They dynamically select resources considering load balance for the ma ximum network performance.

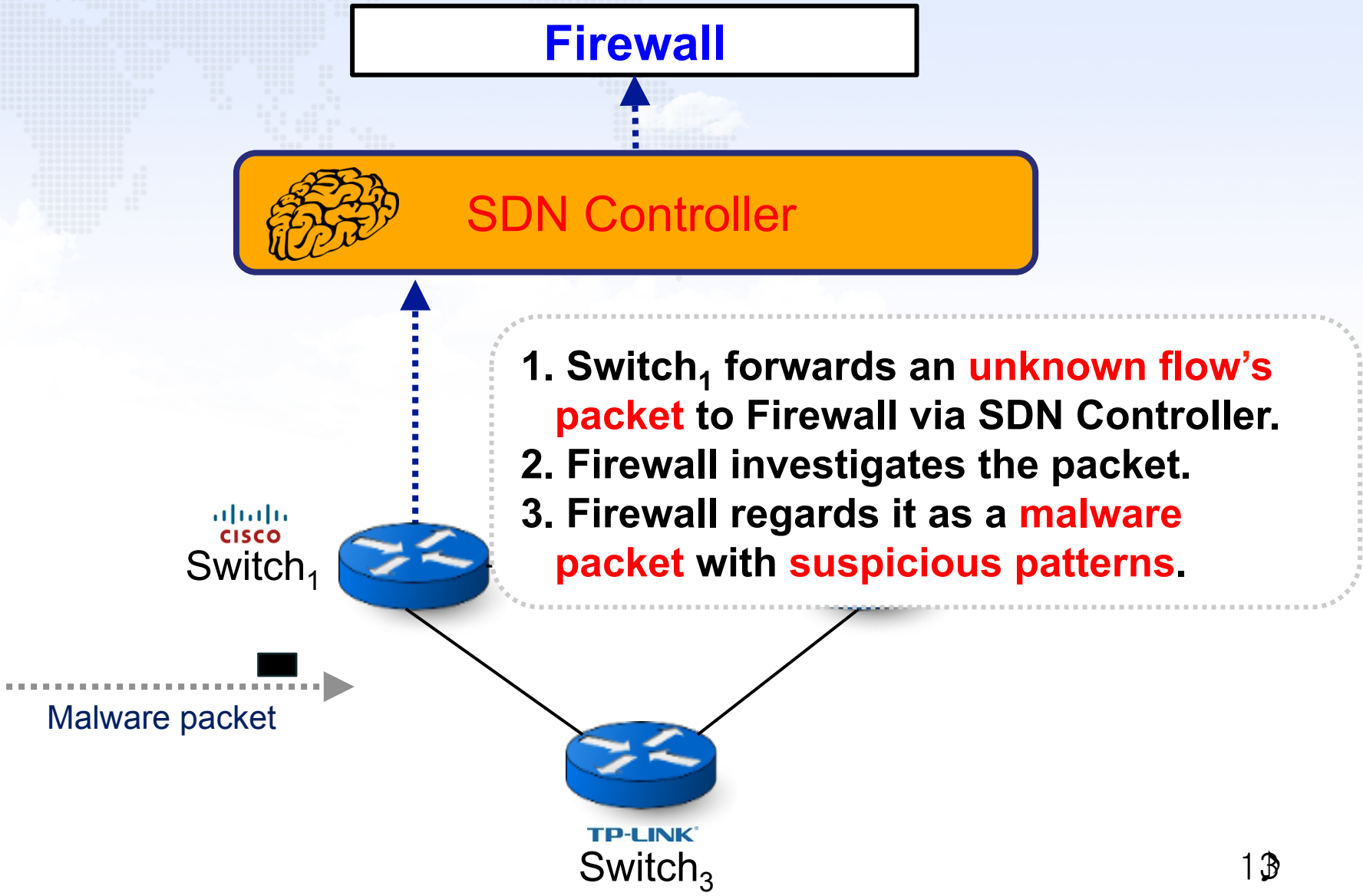
Requirements

- The support of the programmability of network resources to mitigate network attacks.
- The support of an application interface allowing the management of access control policies in an autonomous and prompt manner.
- The support of a resource-control interface for control of network resources to mitigate network attacks.
- The support of logically centralized control of network resources to mitigate network attacks.

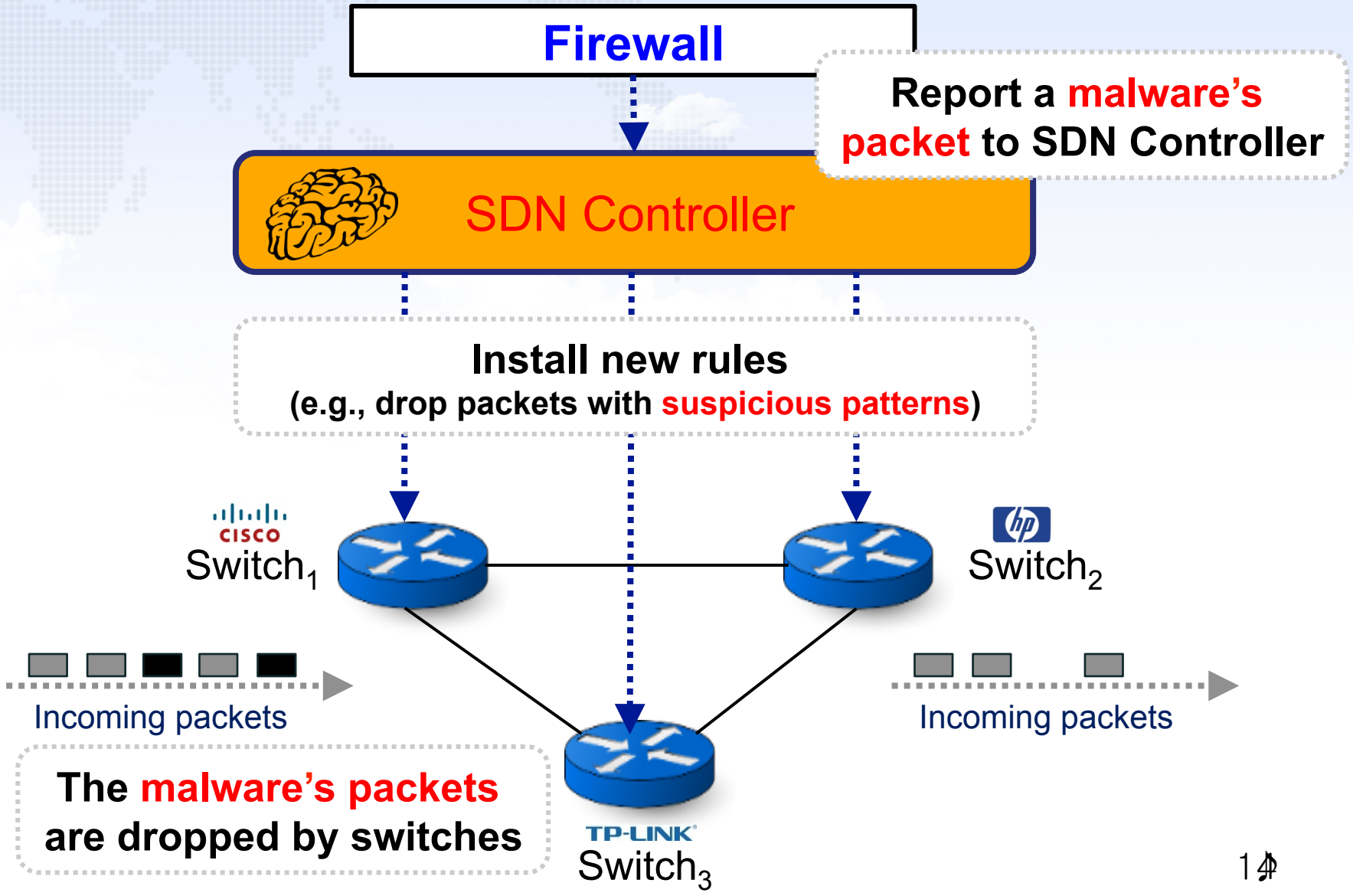
Use Cases

- Centralized Firewall System
  - This is for malware packets.
- Centralized DDoS-Attack Mitigator
  - This is for DDoS-attack packets.

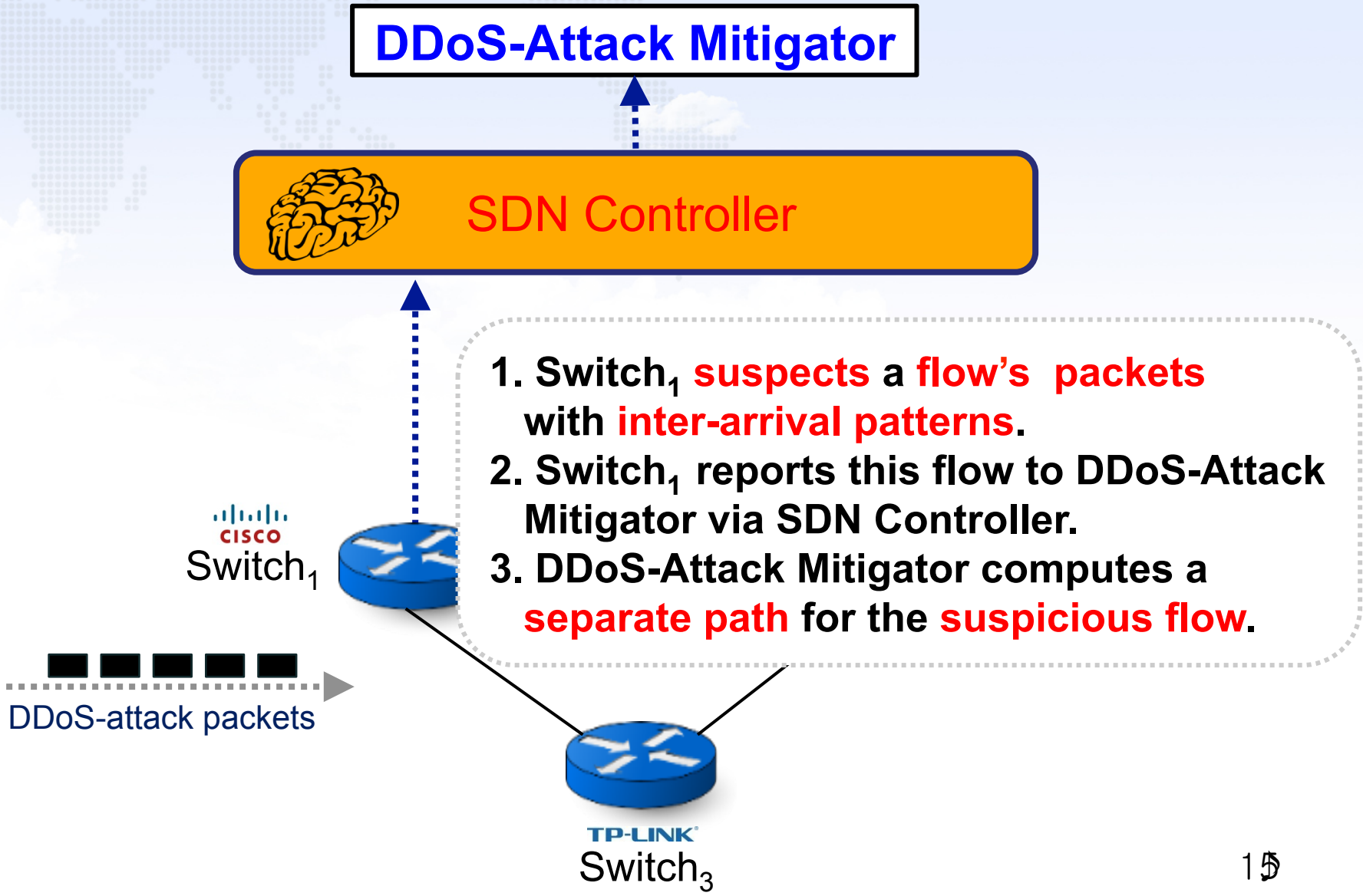
Centralized Firewall System (1/2)



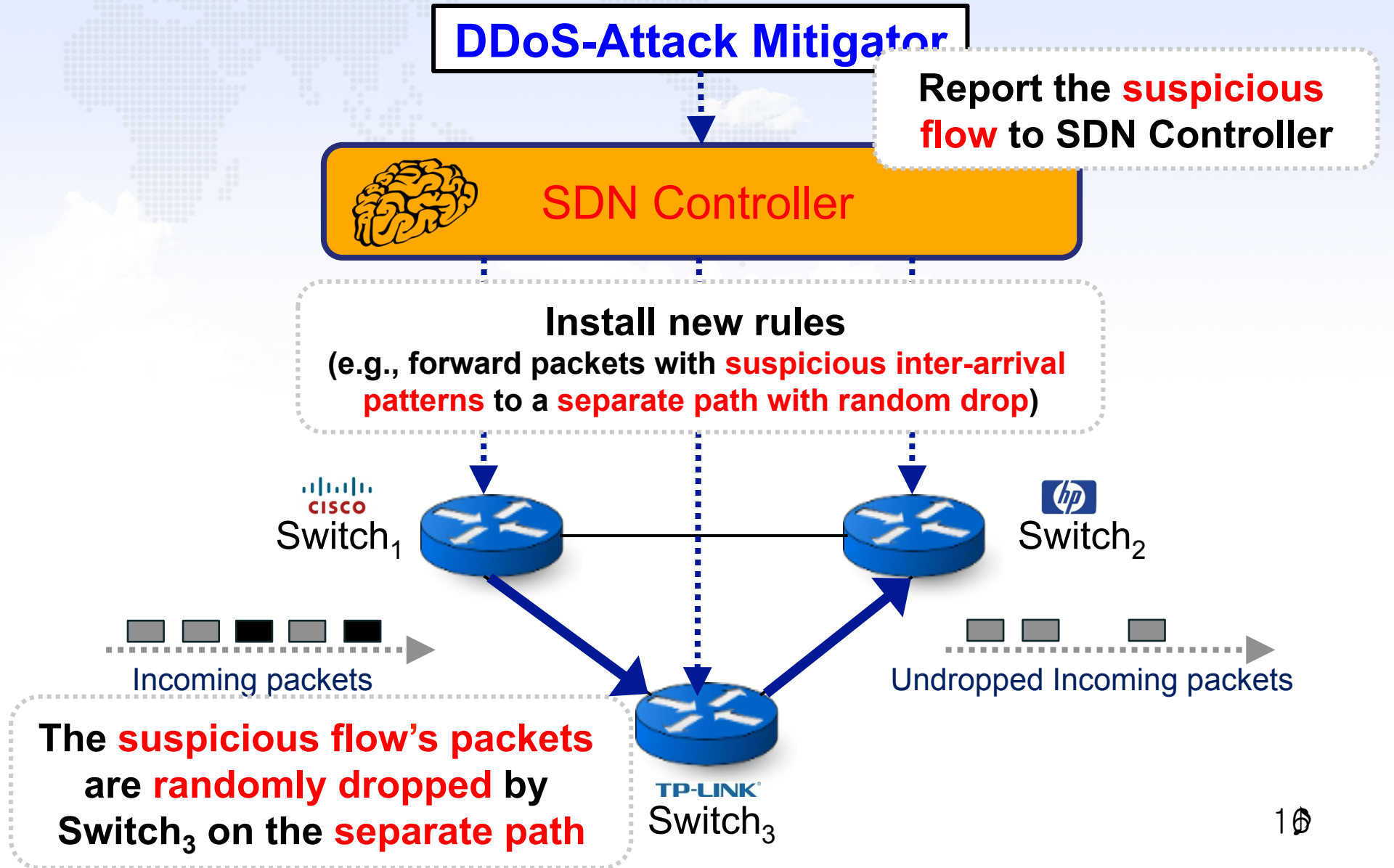
Centralized Firewall System (2/2)



Centralized DDoS-Attack Mitigator (1/2)



Centralized DDoS-Attack Mitigator (2/2)



Discussion

- Direction of This Draft
  - Develop **SDN-based Security Services** (e.g., Firewall and DDoS-Attack Mitigator) including API.
  - Include **other Security Services**, such as **Preventing the leakage of internal traffic into the outside networks**.

- Direction of our ITU-T SG 17 Draft
  - Develop **Security Scenarios and Requirements** for ITU-T Y.3300 (Framework of Software-Defined Networking).

- Thanks for your attention.

- Any Comments or Questions?