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

I. Introduction
II. SDN-Based Security Services
III. Objectives
IV. Requirements
V. Use Cases
VI. Discussion
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 Software-Defined Networking" was accepted as a working item in September 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 services.
  - 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 elements is a challenge.

❖ Policy
- It is difficult to describe what are permitted and denied flows within the specific organization.

❖ Binding
- Packet-based access mechanism is not enough in practice since the basic 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)

- 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

Firewall

DDoS-Attack Mitigator

SDN Controller

Install new rules
(e.g., drop packets with suspicious patterns)

Switch 1

Switch 2

Switch 3

Incoming packets

Incoming packets
High-Level Architecture for SDN-Based Security Services

Application Layer
- Security Application (e.g., Firewall, DDoS-Attack Mitigation)

SDN Control Layer
- Application Support
- Orchestration
- Abstraction

Resource Layer
- Control Support
- Data Transport and Processing
Objectives

- **Prompt reaction to new network attacks**
  - SDN-based security services allow private networks to defend themselves 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 network administrators.

- **Network-load-aware resource allocation**
  - SDN-based security services measure the overhead of resources for security services.
  - They dynamically select resources considering load balance for the maximum 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.
1. Switch$_1$ forwards an unknown flow’s packet to Firewall via SDN Controller.
2. Firewall investigates the packet.
3. Firewall regards it as a malware packet with suspicious patterns.
Centralized Firewall System (2/2)

Firewall

SDN Controller

Install new rules (e.g., drop packets with suspicious patterns)

Report a malware’s packet to SDN Controller

The malware’s packets are dropped by switches
1. Switch₁ suspects a flow’s packets with inter-arrival patterns.
2. Switch₁ reports this flow to DDoS-Attack Mitigator via SDN Controller.
3. DDoS-Attack Mitigator computes a separate path for the suspicious flow.
The suspicious flow's packets are randomly dropped by Switch\textsubscript{3} on the separate path.
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?**