An Information Model for the Monitoring of Network Security Functions (NSF)

draft-zhang-i2nsf-info-model-monitoring-01

DaCheng Zhang	Alibaba
Yi Wu	Alibaba
Liang Xia	Huawei

July 2016 Berlin

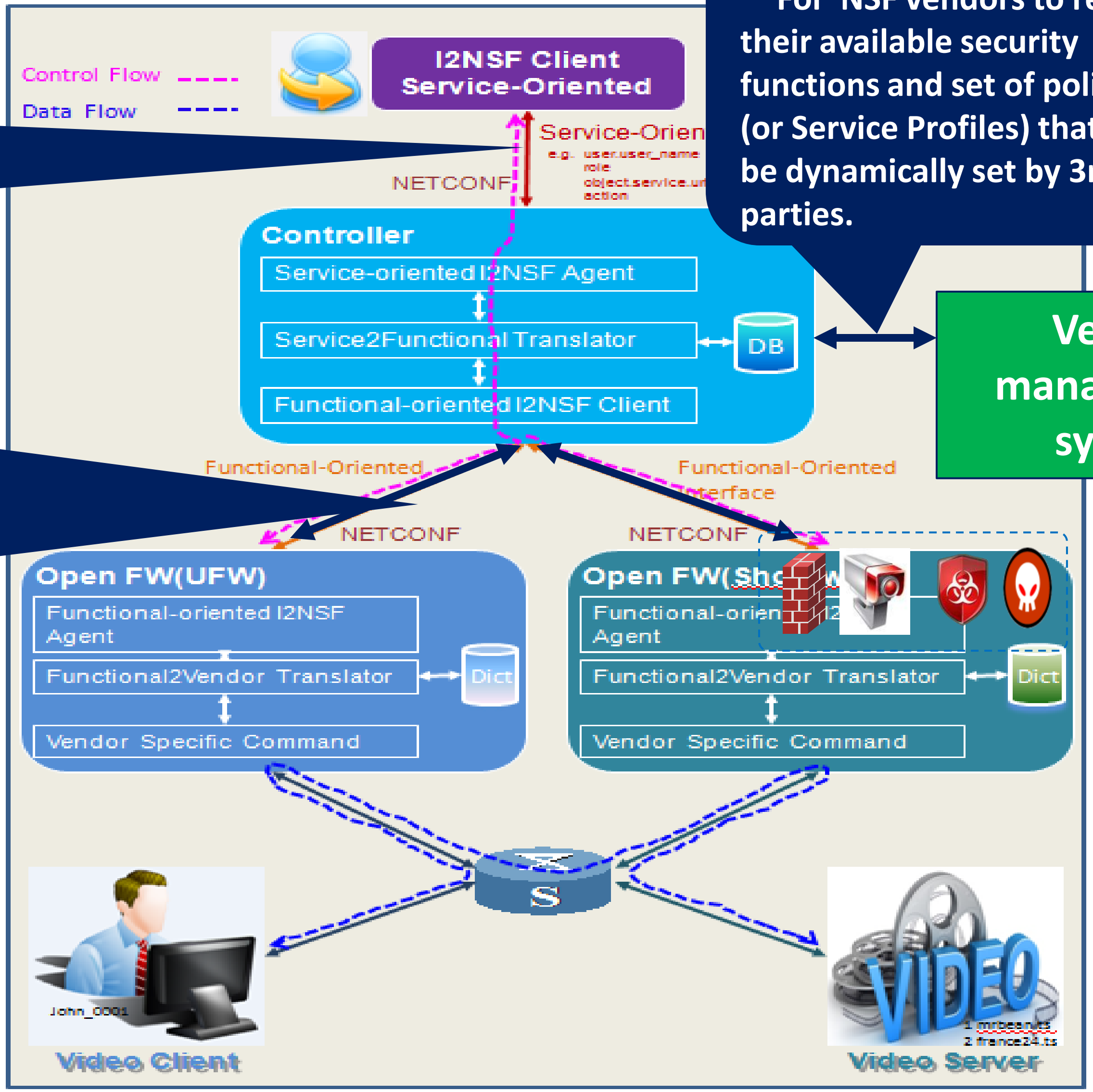
Monitoring Part of I2NSF Architecture

Service Interface

For clients or App Gateway to express and monitor security policies for their specific flows

NSF Registration

For NSF vendors to register their available security functions and set of policies (or Service Profiles) that can be dynamically set by 3rd parties.



Vendor management system

Capability Interface

For controller to define explicit rules for individual NSFs to treat packets, as well as methods to monitor the execution status of those functions

Objectives

- Specify the information model for the monitoring part of capability interface:
  - ✓ Which information should be provided: security related status and event from NSFs, others (traffic statistics, policy execution, operation related, etc);
  - ✓ The standard information model for the monitoring information: alarms vs reports (distinguished by the real time vs periodically, NSF status vs security events, etc.).

Information Model Design

- Monitoring message types:
  - Alarm: the message triggered by certain abnormal conditions occurred in a NSF (referred to as a System Alarm) or a detected network abnormal conditions (referred to as a Security Event Alarm)
  - Report: the message triggered by a timer or a request from the NE which monitors the NSFs. A report contains more statistical information comparing to alarm.

From -00 to -01

- Add new kinds of report:
  - Service Report
    - Traffic Report
    - Policy Hit Report
    - DPI Report
    - Vulnerability Scanning Report
    - User Activity Report
  - System Report
    - Operation Report
    - Running Report
- Update the attributes of most of the Alarms and Reports
- Editorial changes

Common Information

- The common information that should be included in all the alarm or report messages:
  - timestamp
  - vendor_name
  - NSF_name
  - NSF_type: firewall, WAF, IPS
  - NSF_version
  - module_name
  - version
  - log_type: Alarm, report, etc
  - severity: 0 - Emergency; 1 - Alert; 2 - Critical; 3 - Error; 4 - Warning; 5 - Notification; 6 - Informational; 7 - Debugging

Alarm Specification

- System Alarm
  - Memory Alarm
  - CPU Alarm
  - DISK Alarm
  - Session Table Alarm
  - Interface Alarm
- Security Event Alarm
  - DDoS Alarm
  - Virus Alarm
  - Intrusion Alarm
  - Botnet Alarm
  - Web Attack Alarm

- event_name: 'SESSION_USAGE_HIGH'
- current: The number of concurrent sessions
- max: The maximum number of sessions that the session table can support
- threshold: Yhe threshold triggering the event
- message: 'The number of session table exceeded the threshold'

- event_name: 'SEC_EVENT_DDoS'
- sub_attack_type: Any one of Syn flood, ACK flood, SYN-ACK flood, FIN/RST flood, TCP Connection flood, UDP flood, icmp flood, HTTPS flood, HTTP flood, DNS query flood, DNS reply flood, SIP flood, and etc.
- dst_ip: The IP address of a victim under attack
- dst_port: The port numbers that the attack traffic aims at.
- start_time: The time stamp indicating when the attack started
- end_time: The time stamp indicating when the attack ended. If the attack is still undergoing when sending out the alarm, this field can be empty.
- attack_rate: The PPS of attack traffic
- attack_speed: The bps of attack traffic
- rule_id: The ID of the rule being triggered
- rule_name: The name of the rule being triggered
- profile: Security profile that traffic matches.

Report Specification

- Attack Report
  - DDoS Report
  - Virus Report
  - Intrusion Report
  - Botnet Report
  - Web Attack Report

Besides the fields in an DDoS Alarm, the following information should be included in a DDoS Report:

- attack_type: DDoS
- attack_ave_rate: The average pps of the attack traffic within the recorded time
- attack_ave_speed: The average bps of the attack traffic within the recorded time
- attack_pkt_ num: The number attack packets within the recorded time
- attack_src_ip: The source IP addresses of attack traffics. If there are a large amount of IP addresses, then pick a certain number of resources according to different rules
- action: Actions against DDoS attacks, e.g., Allow, Alert, Block, Discard, Declare, Block-ip, Block-service.

- Service Report
  - Traffic Report
  - Policy Hit Report
  - DPI Report
  - Vulnerability Scanning Report
  - User Activity Report
- System Report
  - Operation Report
  - Running Report

Operation reports record administrators' login, logout, and operations on the device. By analyzing them, security vulnerabilities can be identified. The following information should be included in operation report:

- *Administrator: Administrator that operates on the device*
- *login_ip_address: IP address used by an administrator to log in*
- *login_mode: Mode in which an administrator logs in*
- *operation_type: The operation type that the administrator execute, e.g., login, logout, configuration, etc*
- *result: Command execution result*
- *content: Operation performed by an administrator after login.*

Next Step

- Comments are welcome!
- Be aligned with I2NSF framework and terminology drafts
- Keep on improving...

Thanks!

Liang Xia (Frank)