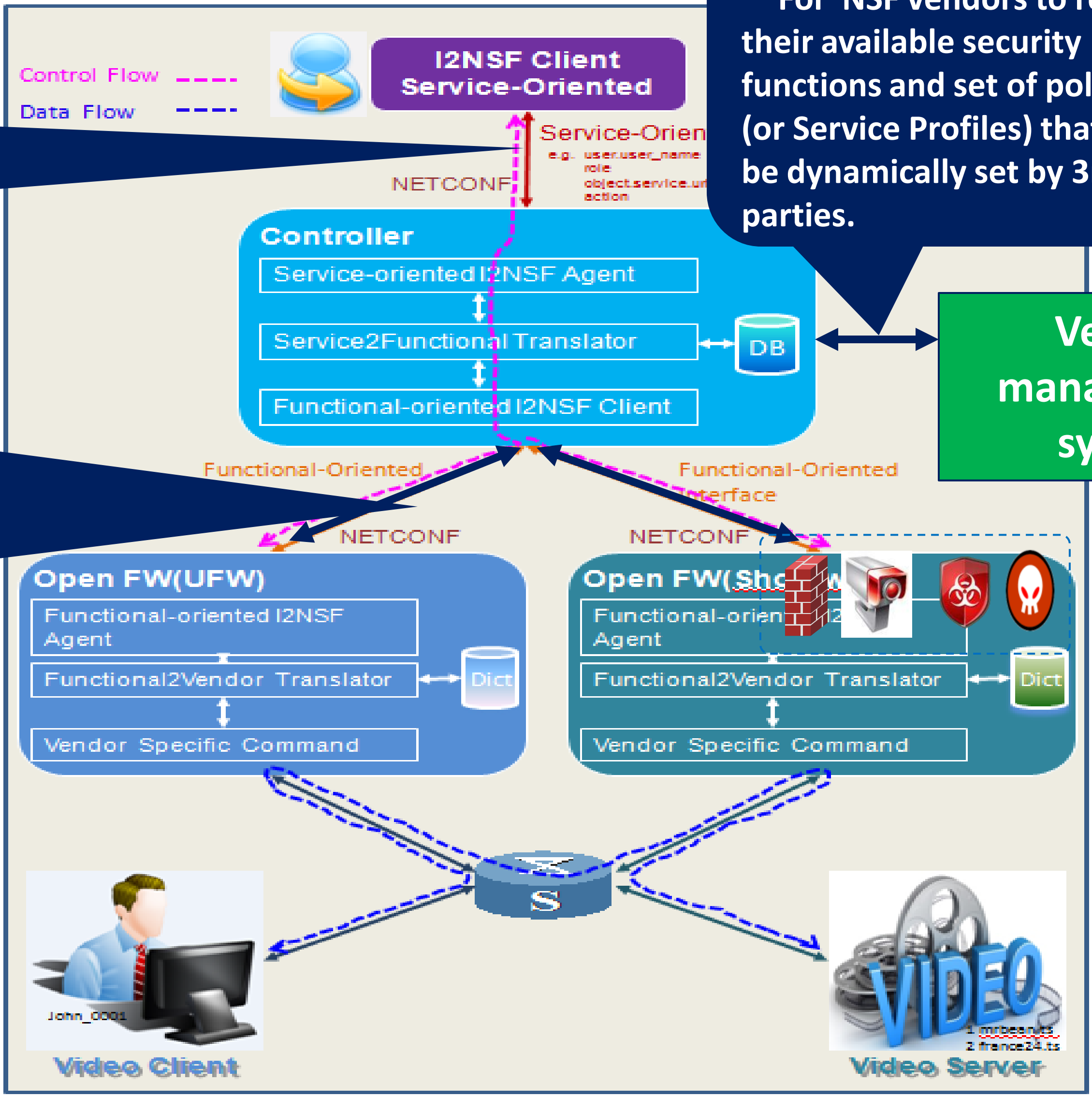
An Information Model for the Monitoring of Network Security Functions (NSF)

draft-zhang-i2nsf-info-model-monitoring-02

DaCheng Zhang	Huawei
Yi Wu	Alibaba
Liang Xia	Huawei
Rakesh Kumar	Juniper
Anil Lohiya	Juniper

November 2016 Seoul

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

Mailing List Discussion

- Does I2NSF need the work of NSF monitoring part? Yes
- Is producing a information model useful? Yes
- If we produce a YANG module, do we still need to publish the information model?
  Not yet decided
- What do you think of the content of the draft? Nobody dislike it, some people say it is a good start, others say it is a key part and very useful😊
- Improvement comments from Robert Moskowitz, Diego R. Lopez, Susan Hares, John Strassner, ...: will consider, many thanks!

Updates

- New contents for clearly describing:
  - use cases for NSF monitoring data;
  - classification way of NSF monitoring data;
  - the way to export NSF monitoring data;
  - basic Information model for all monitoring data

- Restructure the existing NSF monitoring data into suitable classification respectively

- Update and improvement on the detailed NSF monitoring data information model

- New co-authors from Juniper

Overall Introductory Contents for NSF Monitoring Data

- Use cases
- Classification
  - System Alarms, System Events, System Logs, System Counters
  - NSF Events, NSF Logs, NSF Counters
- The way to export
  - Pull-Push model, subscription method
  - Export frequency
  - Authentication
  - Transport method, data transfer mode

Basic Information Model

- The general information is included in each message as meta data information:
  - Message_version
  - Message_type
  - Time_stamp
  - vendor_name
  - NSF_name
  - NSF_type: firewall, WAF, IPS
  - NSF_version

NSF Monitoring Data IM Specification

- System Alarm
  - Memory Alarm
  - CPU Alarm
  - Disk Alarm
  - Hardware Alarm
  - Interface Alarm
- System Event
  - Access Violation
  - Configuration Change

- event_name: ’IFNET_STATE_ALARM’
- interface_Name: The name of interface
- interface_state: ’UP’, ’DOWN’, ’CONGESTED’
- threshold: The threshold triggering the event
- severity: The severity of the alarm such as critical, high, medium, low
- message: ’Current interface state’

- event_name: ’ACCESS_DENIED’
- user: Name of a user
- group: Group to which a user belongs
- login_ip_address: Login IP address of a user
- authentication_mode: User authentication mode. e.g., Local Authentication, Third-Party Server Authentication, Authentication Exemption, SSO Authentication
- message: ’access denied’

NSF Monitoring Data IM Specification

- System Log
  - Access Logs
  - Resource Utilization Log
  - User Activity Log

  - **user: Name of a user**
  - group: Group to which a user belongs
  - login_ip_address: Login IP address of a user
  - authentication_mode: User authentication mode. e.g., Local Authentication, Third-Party Server Authentication, Authentication Exemption, SSO Authentication
  - access_mode: User access mode. e.g., PPP, SVN, LOCAL
  - online_duration: Online duration
  - lockout_duration: Lockout duration
  - type: User activities. e.g., Successful User Login, Failed Login attempts, User Logout, Successful User Password Change, Failed User Password Change, User Lockout, User Unlocking, Unknown
  - cause: Cause of a failed user activity

- System Counter
  - Interface counter

  - **interface_name: Network interface name configured in NSF**
  - **in_total_traffic_pkts: Total inbound packets**
  - **out_total_traffic_pkts: Total outbound packets**
  - **in_total_traffic_bytes: Total inbound bytes**
  - **out_total_traffic_bytes: Total outbound bytes**
  - **in_drop_traffic_pkts: Total inbound drop packets**
  - **out_drop_traffic_pkts: Total outbound drop packets**
  - **in_drop_traffic_bytes: Total inbound drop bytes**
  - **out_drop_traffic_bytes: Total outbound drop bytes**
  - **in_traffic_ave_rate: Inbound traffic average rate in pps**
  - **in_traffic_peak_rate: Inbound traffic peak rate in pps**
  - **in_traffic_ave_speed: Inbound traffic average speed in bps**
  - **in_traffic_peak_speed: Inbound traffic peak speed in bps**
  - **out_traffic_ave_rate: Outbound traffic average rate in pps**
  - **out_traffic_peak_rate: Outbound traffic peak rate in pps**
  - **out_traffic_ave_speed: Outbound traffic average speed in bps**
  - **out_traffic_peak_speed: Outbound traffic peak speed in bps.**

NSF Monitoring Data IM Specification

- NSF Event
  - DDoS Event
  - Session Table Event
  - Virus Event
  - Intrusion Event
  - Botnet Event
  - Web Attack Event
- NSF Log
  - DDoS Log
  - Virus Log
  - Intrusion Log
  - Botnet Log
  - DPI Log
  - Vulnerability Scanning Log
  - Web Attack Logs
- NSF Counter
  - Firewall counter
  - Policy Hit Counter

o event_name: the name of event: ’SEC_EVENT_WebAttack’
o sub_attack_type: Concret web attack type, e.g., sql injection, command injection, XSS, CSRF
o src_ip: The source IP address of the packet
o dst_ip: The destination IP address of the packet
o src_port: The source port number of the packet
o dst_port: The destination port number of the packet
o src_zone: The source security zone of the packet
o dst_zone: The destination security zone of the packet
o req_method: The method of requirement. For instance, ’PUT’ or ’GET’ in HTTP
o req_url: Requested URL
o url_category: Matched URL category
o filtering_type: URL filtering type, e.g., Blacklist, Whitelist, User-Defined, Predefined, Malicious Category, Unknown
o rule_id: The ID of the rule being triggered
o rule_name: The name of the rule being triggered
o profile: Security profile that traffic matches.

o attack_type: Web Attack
o rsp_code: Response code
o req_clientapp: The client application
o req_cookies: Cookies
o req_host: The domain name of the requested host
o raw_info: The information describing the packet triggering the event.

o src_zone: Source security zone of traffic
o dst_zone: Destination security zone of traffic
o src_region: Source region of the traffic
o dst_region: Destination region of the traffic
o src_ip: Source IP address of traffic
o src_user: User who generates traffic
o dst_ip: Destination IP address of traffic
o src_port: Source port of traffic
o dst_port: Destination port of traffic
o protocol: Protocol type of traffic
o app: Application type of traffic
o policy_id: Security policy id that traffic matches
o policy_name: Security policy name that traffic matches
o hit_times: The hit times that the security policy matches the specified traffic.

Next Step

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

Thanks!

Liang Xia (Frank)