An Information Model for the Monitoring of Network Security Functions (NSF)
draft-zhang-i2nsf-info-model-monitoring-00

DaCheng Zhang    Alibaba
Yi Wu            Alibaba
Liang Xia        Huawei

April 2016   Buenos Ayres
Monitoring Part of I2NSF Architecture

**Service Layer**
For clients or App Gateway to express and monitor security policies for their specific flows.

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

**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**
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, 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.
Common Information

• The common information that should be included in all the alarm or report messages:
  – Time Stamp
  – NSF name
  – Vendor name
  – Type of NSF: firewall, WAF, IPS
  – NSF model
  – Interface Version
  – NSF Version
  – Type of report: Alarm, report, etc
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: the 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
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
- rule_id: The ID of the rule being triggered
- rule_name: The name of the rule being triggered
- 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.
Next Step

• Solicit comments

• Keep on improvement, including:
  – incorporate contents from draft-zhou-i2nsf-capability-interface-monitoring-00
  – supplement missing contents
Thanks!

Liang Xia (Frank)