YANG Data Model for Monitoring I2NSF Network Security Functions
draft-hong-i2nsf-nsf-monitoring-data-model-01

Dongjin Hong
Jaehoon Paul Jeong
Jinyong Tim Kim
Susan Hares
Liang Xia

SKKU
SKKU
SKKU
Huawei
Huawei

IETF-100, Singapore
11/14/2017
Agenda

• Updates from draft-hong-i2nsf-nsf-monitoring-data-model-00

• YANG Data Model Design based on Information Model

• Next steps and plans
Updates from -00 version

• The following updates from draft-hong-i2nsf-nsf-monitoring-data-model-00:

  ✓ The YANG data model is defined in more detail based on the information model for monitoring NSFs.
  ✓ Typos and grammatical errors are corrected.
Basic Information Model for All Monitoring Data
draft-zhang-i2nsf-info-model-monitoring-04
Data Model for All Monitoring Data

Monitoring Information

- message_id
- message_version
- message_type
- time_stamp
- Severity

message

- Event
- Log
- Counter
- Alarm (Alert)
Event

• event-name

• event-type
  ✓ **system-event**: “access-violation” or “config-change”
  ✓ **nsf-event**: “ddos-event”, “session-table-event”, “virus-event”, “intrusion-event”, “botnet-event”, or “web-attack-event”
Log

• log-type
  ✓ **system-log**: “access-logs”, “resource-utilize-logs”, or “user-activity-logs”
Counters

• counter-type
  ✓ system-counter: "interface-counters"
  ✓ nsf-counter: "firewall-counters"
  ✓ policy-hit-counters: "policy-hit-counters"
Next steps and plans

• Revise draft
  ✓ Synchronize with draft-zhang-i2nsf-info-model-monitoring

• Verify YANG data model by implementing prototype.
Thank you