

Network Working Group  
Internet-Draft  
Intended status: Experimental  
Expires: January 2, 2017

D. Zhang  
Y. Wu  
Aliababa Group  
L. Xia  
Huawei  
July 1, 2016

An Information Model for the Monitoring of Network Security Functions  
(NSF)  
draft-zhang-i2nsf-info-model-monitoring-01

Abstract

The Network Security Functions (NSF) Capability interface exists between the Service Provider's management system (or Security Controller) and the NSFs to enforce the rule provisioning and monitoring on the NSFs in the functional implementation level. This document focuses on the monitoring part of it and proposes the information model for it.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 2, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	3
2.1. Key Words . . . . .	3
2.2. Definition of Terms . . . . .	3
3. Common Information . . . . .	4
4. Alarm . . . . .	4
4.1. System Alarm . . . . .	4
4.1.1. Memory Alarm . . . . .	4
4.1.2. CPU Alarm . . . . .	5
4.1.3. DISK Alarm . . . . .	5
4.1.4. Session Table Alarm . . . . .	5
4.1.5. Interface Alarm . . . . .	5
4.2. Security Event Alarm . . . . .	6
4.2.1. DDoS Alarm . . . . .	6
4.2.2. Virus Alarm . . . . .	6
4.2.3. Intrusion Alarm . . . . .	7
4.2.4. Botnet Alarm . . . . .	8
4.2.5. Web Attack Alarm . . . . .	9
5. Reports . . . . .	10
5.1. Attack Report . . . . .	10
5.1.1. DDoS Report . . . . .	10
5.1.2. Virus Report . . . . .	10
5.1.3. Intrusion Report . . . . .	11
5.1.4. Botnet Report . . . . .	11
5.1.5. Web Attack Report . . . . .	12
5.2. Service Report . . . . .	12
5.2.1. Traffic Report . . . . .	12
5.2.2. Policy HIT Report . . . . .	13
5.2.3. DPI Report . . . . .	14
5.2.4. Vulnerability Scanning Report . . . . .	15
5.2.5. User Activity Report . . . . .	15
5.3. System Report . . . . .	16
5.3.1. Operation Report . . . . .	16
5.3.2. Running Report . . . . .	16
6. IANA Considerations . . . . .	17
7. Security Considerations . . . . .	17
8. Acknowledgements . . . . .	17
9. References . . . . .	17
9.1. Normative References . . . . .	17
9.2. Informative References . . . . .	17
Authors' Addresses . . . . .	18

## 1. Introduction

According to [I-D.ietf-i2nsf-framework], the interface provided by a NSF (e.g., FW, AAA, IPS, Anti-DDOS, or Anti-Virus) for other network entities (e.g., NMS, security controller) to enforce the rule provisioning and monitoring on the NSF is referred to as a 'capability interface'. The monitoring part of the capability interface is meant to monitor the network events and the execution status of the NSFs, then aggregate and analyze them to learn what is happening and send a report to the administrator. Regarding to monitoring, the NSF can communicate with the security controller though the capability interface in either a 'push' or a 'pull' way. The NSF can send out a report about its status or about certain network event proactively or send out message as a reply to security controller who control or monitor it. This document will not go into the design details of capability interface. Instead, this draft is focused on specifying the information that a NSF needs to provide in the monitoring part of the capability interface, as well as its information model. Besides, [I-D.draft-xia-i2nsf-capability-interface-im] specifies the information model for the rule provisioning part of the capability interface.

In this document, the following types of security information that a NSF needs to provide are considered:

- o The alarm triggered by a certain status in NSF
- o The alarm triggered by a certain security event
- o The report about the security events occurred in a certain period
- o The report about the status of NSF in a certain period

## 2. Terminology

### 2.1. Key Words

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

### 2.2. Definition of Terms

This document uses the terms defined in [I-D.draft-ietf-i2nsf-terminology].

### 3. Common Information

Some general information should be provided in each message sent from a NSF to the security controller who monitor it.

- o time\_stamp: Indicate the time when the message is generated
- o vendor\_name: The name of the NSF vendor
- o NSF\_name: The name (or IP) of the device generation the message
- o NSF\_type: Indicate what type the NSF is (e.g., firewall, WAF, IPS)
- o NSF\_version: The software version of the NSF
- o module\_name: Indicate the module for outputting alarms or reports
- o version: Indicate the version of the log format and is a two-digit decimal numeral starting from 01
- o log\_type: Alarm, periodical report, etc
- o severity: Indicates the level of the logs. There are total eight levels, from 0 to 7. The smaller the numeral is, the higher the severity is. The details is: 0 - Emergency; 1 - Alert; 2 - Critical; 3 - Error; 4 - Warning; 5 - Notification; 6 - Informational; 7 - Debugging.

### 4. Alarm

An alarm is the message generated by a NSF. An alarm could be 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).

#### 4.1. System Alarm

##### 4.1.1. Memory Alarm

The following information should be included in a Memory Alarm:

- o event\_name: 'MEM\_USAGE\_HIGH'
- o usage: The usage rate of memory
- o threshold: The threshold triggering the event
- o message: 'The memory usage exceeded the threshold'

#### 4.1.2. CPU Alarm

The following information should be included in a CPU Alarm:

- o event\_name: 'CPU\_USAGE\_HIGH'
- o usage: The usage rate of CPU
- o threshold: The threshold triggering the event
- o message: 'The CPU usage exceeded the threshold'

#### 4.1.3. DISK Alarm

The following information should be included in a Disk Alarm:

- o event\_name: 'DISK\_USAGE\_HIGH'
- o usage: The usage rate of disk
- o threshold: The threshold triggering the event
- o message: 'The disk usage exceeded the threshold'

#### 4.1.4. Session Table Alarm

The following information should be included in a Session Table Alarm:

- o event\_name: 'SESSION\_USAGE\_HIGH'
- o current: The number of concurrent sessions
- o max: The maximum number of sessions that the session table can support
- o threshold: The threshold triggering the event
- o message: 'The number of session table exceeded the threshold'

#### 4.1.5. Interface Alarm

The following information should be included in a Interface Alarm:

- o event\_name: 'IFNET\_STATE'
- o interface\_Name: The name of interface

- o state: 'UP' or 'DOWN'
- o message: 'Current interface state'

#### 4.2. Security Event Alarm

##### 4.2.1. DDoS Alarm

The following information should be included in a DDoS Alarm:

- o event\_name: 'SEC\_EVENT\_DDoS'
- o 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.
- o dst\_ip: The IP address of a victim under attack
- o dst\_port: The port numbers that the attack traffic aims at.
- o start\_time: The time stamp indicating when the attack started
- o 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.
- o attack\_rate: The PPS of attack traffic
- o attack\_speed: the bps of attack traffic
- 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.

##### 4.2.2. Virus Alarm

The following information should be included in a Virus Alarm:

- o event\_Name: 'SEC\_EVENT\_Virus'
- o virus\_type: Type of the virus, e.g., trojan, worm, macro Virus type
- o virus\_name

- o dst\_ip: The destination IP address of the packet where the virus is found
- o src\_ip: The source IP address of the packet where the virus is found
- o src\_port: The source port of the packet where the virus is found
- o dst\_port: The destination port of the packet where the virus is found
- o src\_zone: The source security zone of the packet where the virus is found
- o dst\_zone: The destination security zone of the packet where the virus is found
- o file\_type: The type of the file where the virus is hided within
- o file\_name: The name of the file where the virus is hided within
- o virus\_info: The brief introduction of virus
- o raw\_info: The information describing the packet triggering the event.
- 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.

#### 4.2.3. Intrusion Alarm

The following information should be included in a Intrustion Alarm:

- o event\_name: The name of event: 'SEC\_EVENT\_Intrusion'
- o sub\_attack\_type: Attack type, e.g., brutal force, buffer overflow
- 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 protocol: The employed transport layer protocol, e.g., TCP, UDP
- o app: The employed application layer protocol, e.g., HTTP, FTP
- 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 intrusion\_info: Simple description of intrusion
- o raw\_info: The information describing the packet triggering the event.

#### 4.2.4. Botnet Alarm

The following information should be included in a Botnet Alarm:

- o event\_name: the name of event: 'SEC\_EVENT\_Botnet'
- o botnet\_name: The name of the detected botnet
- 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 protocol: The employed transport layer protocol, e.g., TCP, UDP
- o app: The employed application layer protocol, e.g., HTTP, FTP
- o role: The role of the communicating parties within the botnet:
  - 1. the packet from zombie host to the attacker
  - 2. The packet from the attacker to the zombie host

3. The packet from the IRC/WEB server to the zombie host
  4. The packet from the zombie host to the IRC/WEB server
  5. The packet from the attacker to the IRC/WEB server
  6. The packet from the IRC/WEB server to the attacker
  7. The packet from the zombie host to the victim
- o botnet\_info: Simple description of Botnet
  - 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 raw\_info: The information describing the packet triggering the event.

#### 4.2.5. Web Attack Alarm

The following information should be included in a Web Attack Alarm:

- 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.

## 5. Reports

Different from Alarms, a report normally triggered by a timer or a request from the NE monitoring the device. So compared to alarms, a report contains more statical information.

### 5.1. Attack Report

#### 5.1.1. DDoS Report

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

- o `attack_type`: DDoS
- o `attack_ave_rate`: The average pps of the attack traffic within the recorded time
- o `attack_ave_speed`: The average bps of the attack traffic within the recorded time
- o `attack_pkt_num`: The number attack packets within the recorded time
- o `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.
- o `action`: Actions against DDoS attacks, e.g., Allow, Alert, Block, Discard, Declare, Block-ip, Block-service.

#### 5.1.2. Virus Report

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

- o `attack_type`: Virus
- o `protocol`: The transport layer protocol

- o app: The name of the application layer protocol
- o times: The time of detecting the virus
- o action: The actions dealing with the virus, e.g., alert, block
- o os: The OS that the virus will affect, e.g., all, android, ios, unix, windows

#### 5.1.3. Intrusion Report

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

- o attack\_type: Intrusion
- o times: The times of intrusions happened in the recorded time
- o os: The OS that the intrusion will affect, e.g., all, android, ios, unix, windows
- o action: The actions dealing with the intrusions, e.g., e.g., Allow, Alert, Block, Discard, Declare, Block-ip, Block-service
- o attack\_rate: NUM the pps of attack traffic
- o attack\_speed: NUM the bps of attack traffic

#### 5.1.4. Botnet Report

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

- o attack\_type: Botnet
- o botnet\_pkt\_num: The number of the packets sent to or from the detected botnet
- o action: The actions dealing with the detected packets, e.g., Allow, Alert, Block, Discard, Declare, Block-ip, Block-service, etc
- o os: The OS that the attack aiming at, e.g., all, android, ios, unix, windows, etc.

#### 5.1.5. Web Attack Report

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

- 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.

#### 5.2. Service Report

##### 5.2.1. Traffic Report

Traffic reports provide visibility into traffic signatures, bandwidth usage, and how the configured security and bandwidth policies have been applied.

- 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 in\_interface: Inbound interface of traffic
- o out\_interface: Outbound interface of traffic
- o total\_traffic: Total traffic volume
- o in\_traffic\_ave\_rate: Inbound traffic average rate in pps
- o in\_traffic\_peak\_rate: Inbound traffic peak rate in pps
- o in\_traffic\_ave\_speed: Inbound traffic average speed in bps
- o in\_traffic\_peak\_speed: Inbound traffic peak speed in bps
- o out\_traffic\_ave\_rate: Outbound traffic average rate in pps
- o out\_traffic\_peak\_rate: Outbound traffic peak rate in pps
- o out\_traffic\_ave\_speed: Outbound traffic average speed in bps
- o out\_traffic\_peak\_speed: Outbound traffic peak speed in bps.

#### 5.2.2. Policy HIT Report

Policy HIT reports record the security policy that traffic matches and its hit count. It can check if policy configurations are correct.

- 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.

#### 5.2.3. DPI Report

DPI reports provide statistics on uploaded and downloaded files and data, sent and received emails, and alert and block records on websites. It's helpful to learn risky user behaviors and why access to some URLs is blocked or allowed with an alert record.

- o type: DPI action types. e.g., File Blocking, Data Filtering, Application Behavior Control
- o file\_name: The file name
- o file\_type: The file type
- 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 action: Action defined in the file blocking rule, data filtering rule, or application behavior control rule that traffic matches.

#### 5.2.4. Vulnerability Scanning Report

Vulnerability scanning reports record the victim host and its related vulnerability information that should to be fixed. the following information should be included in the report:

- o victim\_ip: IP address of the victim host which has vulnerabilities
- o vulnerability\_id: The vulnerability id
- o vulnerability\_level: The vulnerability level. e.g., high, middle, low
- o OS: The operating system of the victim host
- o service: The service which has vulnerability in the victim host
- o protocol: The protocol type. e.g., TCP, UDP
- o port: The port number
- o vulnerability\_info: The information about the vulnerability
- o fix\_suggestion: The fix suggestion to the vulnerability.

#### 5.2.5. User Activity Report

User activity reports provide visibility into users' online records (such as login time, online/lockout duration, and login IP addresses) and the actions users perform. User activity reports are helpful to identify exceptions during user login and network access activities.

- o user: Name of a user
- o group: Group to which a user belongs
- o login\_ip\_address: Login IP address of a user
- o authentication\_mode: User authentication mode. e.g., Local Authentication, Third-Party Server Authentication, Authentication Exemption, SSO Authentication

- o access\_mode: User access mode. e.g., PPP, SVN, LOCAL
- o online\_duration: Online duration
- o logout\_duration: Lockout duration
- o type: User activities. e.g., Succeeded User Login, Failed User Login, User Logout, Succeeded User Password Change, Failed User Password Change, User Lockout, User Unlocking, Unknown
- o cause: Cause of a failed user activity

### 5.3. System Report

#### 5.3.1. Operation 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:

- o Administrator: Administrator that operates on the device
- o login\_ip\_address: IP address used by an administrator to log in
- o login\_mode: Mode in which an administrator logs in
- o operation\_type: The operation type that the administrator execute, e.g., login, logout, configuration, etc
- o result: Command execution result
- o content: Operation performed by an administrator after login.

#### 5.3.2. Running Report

Running reports record the device system's running status, which is useful for device monitoring. The following information should be included in running report:

- o system\_status: The current system's running status
- o CPU\_usage: The usage rate of CPU
- o memory\_usage: The usage rate of memory
- o disk\_usage: The usage rate of disk

- o disk\_left: The left space of disk
- o session\_number: The concurrent sessions' number
- o process\_number: The number of system process
- o in\_traffic\_rate: The total inbound traffic rate in pps
- o out\_traffic\_rate: The total outbound traffic rate in pps
- o in\_traffic\_speed: The total inbound traffic speed in bps
- o out\_traffic\_speed: The total outbound traffic speed in bps

## 6. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

## 7. Security Considerations

TBD

## 8. Acknowledgements

## 9. References

### 9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

### 9.2. Informative References

- [I-D.ietf-i2nsf-framework] elopez@fortinet.com, e., Lopez, D., Dunbar, L., Strassner, J., Zhuang, X., Parrott, J., Krishnan, R., and S. Durbha, "Framework for Interface to Network Security Functions", draft-ietf-i2nsf-framework-01 (work in progress), June 2016.

[I-D.xia-i2nsf-capability-interface-im]

Xia, L., Zhang, D., elopez@fortinet.com, e., Bouthors, N.,  
and L. Fang, "Information Model of Interface to Network  
Security Functions Capability Interface", draft-xia-i2nsf-  
capability-interface-im-05 (work in progress), March 2016.

Authors' Addresses

Dacheng Zhang  
Aliababa Group

Email: dacheng.zdc@alibaba-inc.com

Yi Wu  
Aliababa Group

Email: anren.wy@alibaba-inc.com

Liang Xia  
Huawei

Email: frank.xialiang@huawei.com