

NAT Logging

draft-ietf-behave-ipfix-nat-logging-00

Senthil Sivakumar <ssenthil@cisco.com>

Reinaldo Penno <repenno@cisco.com>

draft-ietf-behave-syslog-nat-logging-02

Zhonghua Chen <18918588897@189.cn>

Cathy Zhou <cathy.zhou@huawei.com>

Tina Tsou <tina.tsou.zouting@huawei.com>

Tom Taylor <tom.taylor.stds@gmail.com>

Summary

- .Both IPFIX and SYSLOG drafts were adopted as WG documents in Orlando
- .Incorporated the comments received during WG meeting in Orlando
- .SYSLOG document subsequently updated based on list comments. IPFIX document has comments outstanding.

Goals

.Both documents to have:

- same events reported
- consistent representation of the parameters

.End user should not know the difference if the export was done by syslog or ipfix

NATx4 Session Cr/Del Events

IPFIX

timeStamp
vlanID/ingressVRFID
sourceIPvXAddress
postNATSourceIPv4Address
protocolIdentifier
sourceTransportPort
postNAPTsourceTransportPort
destinationIPv4Address
postNATDestinationIPv4Address
destinationTransportPort
postNAPTdestinationTransportPort
natOriginatingAddressRealm
natEvent
-- no (not needed) --
-- no --

SYSLOG

-- yes --
} Subscriber site identifier
-- yes --
-- yes --
-- yes --
-- yes --
-- no --
-- no --
-- no --
-- no --
-- yes --
-- yes --
Device identifier
Device type

Subscriber site identifier is an implementation- / deployment-dependent human-readable string.

Issue 1 - Destination Logging

.Destination logging has issues but ...

- should we have provisions in the draft for logging destination information if it is required?
- IPFIX draft already provides the Information elements to log destination information
- In response to list comments, SYSLOG draft has removed them in -02 version and has text on reasons why destination logging is undesirable.

.WG verdict?

Issue 2 – Pre-NAT Address

.How to represent pre-NAT address?

- IPFIX draft represents v4 and v6 addresses and vlanID/ingressVRFID using separate encodings.
 - Missing general representation of GW-initiated DS-Lite tunnel identifier
- SYSLOG draft provides a single string field leaving it up to the implementation and operator to populate suitably.

.WG advice?

Issue 3 – Device Type

.SYSLOG draft provides a device type field to give context to the subscriber site identifier parameter.

- Example: distinguish between log from DS-Lite AFTR and NAT64 given subscriber site identifier is IPv6 address.
- Craftsperson does have clue from reporting device identifier in HostID or Device ID field.

.IPFIX lacks this parameter.

.WG verdict?

NATx4 BIB Entry Cr/Del Events

IPFIX

timeStamp
vlanID/ingressVRFID
sourceIPvXAddress
postNATSourceIPv4Address
protocolIdentifier
sourceTransportPort
postNAPTsourceTransportPort
natOriginatingAddressRealm
natEvent

SYSLOG

*Event identical to session
create/delete event when
destination logging omitted,
hence event dropped from
SYSLOG document.*

Address Exhausted Event

IPFIX

timeStamp
natEvent
natPoolName
-- no --
-- no --

SYSLOG

-- yes --
-- yes --
-- yes --
Device identifier
Device type

Ports Exhausted Event

IPFIX

timeStamp

natEvent

postNATSourceIPv4Address

protocolIdentifier

-- no --

-- no --

SYSLOG

-- yes --

-- yes --

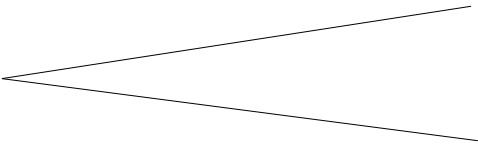
-- yes --

-- yes --

Device identifier

Device type

Quota Exceeded Event

IPFIX		SYSLOG
timeStamp		-- yes --
natEvent		-- yes --
natLimitEvent		Site scope
		Protocol scope
sourceIPvXaddress		Subscriber site identifier or VLANid or VRFFid
-- no --		Device identifier
-- no --		Device type

Issue 4 – Warning Levels

.List remark: should log events like high-water-mark values of address/port usage.

- Quota violations provide related information
- We believe anything else belongs in the MIB

.WG verdict?

Issue 5 – Complexity of Quota Event

.SYSLOG -01 expanded on IPFIX approach to make up for loss of distinction between sessions and BIB entries. List remark: hard to understand.

.In response, SYSLOG -02 broke quota type into two parameters, with presence of others conditional on them:

- Site scope: single, multiple defined by VLAN/VRF, NAT-global
- Protocol scope: specific protocol, sum over all protocols

.IPFIX has one scope parameter.

- scope is all sessions, all BIB entries, single user
- no breakout by protocol

.WG verdict?

Address Binding Event

IPFIX

timeStamp

natEvent

sourceIPvXaddress

postNATSourceIPv4Address

-- no --

-- no --

SYSLOG

-- yes --

-- yes --

Subscriber site identifier

-- yes --

Device identifier

Device type

Port Block Allocation

IPFIX

timeStamp

[natEvent]

sourceIPvXaddress

postNATSourceIPv4Address

portRangeStart

portRangeEnd

portRangeStepSize

portRangeNumPorts

-- no --

-- no --

-- no --

SYSLOG

-- yes --

-- yes --

Subscriber site identifier

-- yes --

-- no --

-- no --

-- no --

-- no --

List of port ranges

Device identifier

Device type

Issue 6 – Port Allocation

- .How many different port ranges need to be reported?
 - IPFIX draft supports description in form of starting point, ending point, interval between ranges, range size.
 - . Can describe potentially large number of equal-sized, equally spaced ranges.
 - SYSLOG draft format assumes a limited number of ranges, which are described explicitly.
- .WG verdict?

Invalid Port Detected Event

IPFIX

SYSLOG

Event not supported

timeStamp

natEvent

Device identifier

Subscriber site identifier

Port set identifier (PSID)

Issue 7 – Invalid Port Event

.Is this event required?

- Reported by MAP/4rd or LW4over6 BR.

.WG verdict?

Next steps

- .Any other events that ought to be reported?
- .Intention is to have IPFIX draft make informational reference to section 2 of SYSLOG draft.
- .WGLC for next versions?