OPSAWG
Internet-Draft
Intended status: Standards Track
Expires: May 24, 2015

T. Alexander
F. Detienne
S. Rao
T. Kandasamy
Cisco Systems, Inc.
November 20, 2014

IPFIX Information Elements for logging IPSec Events
draft-alexander-opsawg-ipfix-ipsec-logging-00

Abstract

Internet Protocol Security (IPSec) is an industry standard protocol suite that provides secure services for traffic between IP peers in the network. The purpose of IPSec is to provide key tenets of security that include authentication, integrity protection, access control and data confidentiality. The objectivities of IPSec are met using a collection of intertwined components namely, the security protocols, session and key management protocols and algorithms for authentication and encryption.

An end-to-end IPSec operation is typically multi-step involving various technologies. There are many events in IPSec process that are of interest, such as - identities and connection status of security peers, traffic or applications being protected, access control and encryption policies being enforced. While many of these are functionally discrete, they have an impact on end-to-end IPSec operations. While network elements involved in IPSec process do provide system logs, command line interfaces and management objects that reflect the various states of operations, these are however dissevered, inconsistent and not easily favorable for analyzing, monitoring, auditing of end-to-end behavior

This document proposes an approach for common representation and standardization of various IPSec operational data and events using industry standard IPFIX information model. The IPFIX approach helps to store and manage data in a consistent format, also provides opportunity for a collector to correlate various IPSec events which in turn can be exploited to obtain enriched end-to-end monitoring, reporting and troubleshooting capabilities and provide various security analytics on IPSec flows such as - host identification, application detection, track user policy violations, protocol failures and so on.

Status of This Memo

Copyright Notice

Table of Contents

1. Terminology

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].

IPSec terminology used in this document is as per [RFC4301].

The term "collector" here refers to any device that receives the binary data from a IPSec device and converts that into meaningful information. The usage of the term Information Element (IE) is

defined in [RFC7011]. Many of the IEs are reused from [IPFIX-IANA]. however IPSec related IEs are created with IPSec semantics.

2. Introduction

The intent of this document is to define and standardize information format of various functional events of an end-to-end IPSec operation. This provides an opportunity for collectors to receive and process information in a consistent way and instrument monitoring, troubleshooting, maintenance and analytics related to IPSec processes. The approach is to standardize the format of logging events using IPFIX [RFC7011] and SYSLOG [RFC5424]. While this document specifies IPFIX Information Elements that MUST be logged by devices participating in IPSec process, the SYSLOG format will be addressed in a separate document. The Information Elements are part of the following two main categories of events:

- IKE events

- IPSec events

There are cases when the IPFIX collector and the VPN gateway are out of sync. This can happen for various reasons such as network connectivity issues, software errors, device reloads etc. In such cases where the IPSec or IKE flow creation information is not recorded on the collector, subsequent updates for that flow may not be complete. Thus, some flow information has been made consciously redundant in subsequent IPFIX updates such that the collectors can rebuild a fair approximation of the flow timeline and creation details.

3. Scope

The existing IANA IPFIX Information Elements registry [IPFIX-IANA] already has assignments for many IPSec logging events. For being consistent, this document uses those same Information Elements.

The implementation details of the collector application is beyond the scope of this document.

The optimization of logging IPSec events are left to the

implementation and are beyond the scope of this document.

4. Applicability

IPFIX based IPSec logging is specifically applicable on network devices that are performing IPSec encryption and support IPFIX protocol. The binary encoding nature of IPFIX makes it efficient for use even on IPSec gateways or peers that can experience high session rates. As in an IPFIX model, there is a need for a collector applications that can receive and interpret binary encoded Information Elements and provide human visualization and other required analytics.

5. Event Logging

In the context of this specification, we make use of three types of events for IKE and IPsec. These events are:

- creation of an IKE or IPsec SA

- update (counters) of an IKE or IPsec SA

- deletion of an IKE or IPsec SA

While the creation and deletion events are triggered by protocol (parent or child SA creation/deletion) or configuration, the update

event is triggered exclusively by timers. The purpose of update events is to offer a chance to the IPFIX collector to capture information about a session even if the creation or deletion (or both) events are missed. For instance because of network connectivity issues between the gateway and the collector or because of the unavailability of the collector at the time the event was sent by the gateway. Update events frequency SHOULD be controllable by a user configurable element.

5.1. IKE Event Logging

5.1.1. IKE Information Elements

The following table lists all of the IKE Information Elements used in events send to a collector. The formats of the IE's and the IPFIX

IDs are listed below. Some of the IPFIX IE's are not assigned yet, and thus the detailed description of these fields are provided in the IANA considerations section. New IPFIX Information Elements must be allocated in IANA's IPFIX registry [IANA-IPFIX], as defined in the sub-sections of section 6. The templates may contain a subset of the Information Elements(IEs) shown in Table 1 depending upon the event being logged.

Table 1: IKE Informational Elements

IPFIX Field Name	Data Type	IANA IPFIX ID	Description
ikeEvent	unsigned8	TBD01	IKE event - start, udpate,stop
timeStamp	dateTimeMilliseconds	323	timestamp of event
sessionCreationTimeMilliSeconds	dateTimeMilliseconds	TBD02	Tracks when a session was created
ikeSessionId	unsigned32	TBD03	Session id used by IKE
interfaceName InterfaceId	str unsigned32	82 TBD04	Interface name
ikeTunLocalIdType	unsigned8	TBD05	Id type - fqdn, ip addr
ikeTunLocalId	str	TBD06	
ikeTunLocalIPAddr*	var	TBD07	ikeTunLocalIPv4Addr or ikeTunLocalIPv6Addr
ikeTunLocalName	str	TBD10	Tunnel local name
VRFname	str	236	virtual routing and Forwarding identifier
ikeTunRemoteIdtype	unsigned8	TBD1	ip addr, FQDN etc

		1	
ikeTunRemoteId	var	TBD1	remote id - fqdn,
		2	ip etc)
ikeTunRemoteIPAddr	var	TBD1	either ikeTunRemo
		3	teIPv4Addr or ike
			TunRemoteIPv6Addr
ikeTunRemoteName	str	TBD1	Remote peer
		6	logical name
ikeTunTransform	ike-encoding	TBD1	RFC5996 3.3.2 IKE
		7	encoding : DH,
			encryption algo,
			hash, PRF
ikeTunLocalAuthMethod	unsigned8	TBD1	values to
		8	indicate psk,eap,
			cert
ikeTunRemoteAuthMetho	unsigned8	TBD1	values to
d		9	indicate remote
			psk,eap, cert
ikeTunLifeTime	unsigned32	TBD2	sa lifetime
		0	
eventReason	unsigned8	TBD2	Reason - delete
		1	reason, rekey etc
ikeDPDSent	unsigned32	TBD2	DPD sent
		2	
ikeDPDRcvd	unsigned32	TBD2	DPD Received
		3	
ikePktsTX	unsigned32	TBD2	packets sent
		4	
ikePktsRX	unsigned32	TBD2	packets received
		5	
ikeRetransTX	unsigned32	TBD2	IKE retransmitted
		6	
ikeRetransRX	unsigned32	TBD2	SA lifetime
		7	
ikeDecryptFailed	unsigned32	TBD2	decrypt failed
		8	
ikeEncryptFailed	unsigned32	TBD2	encrypt failed
		9	
ikeInvalidPayload	unsigned32	TBD3	invalid payload
		0	

ikeFragFailed	unsigned32	TBD3	fragmentation

		1	failure	

Table 1: IKE Information Elements

5.1.2. Definition of IKE Events

Table 2 lists all the IKE event types related to a IKE session . The events are an IKE session create , update , and delete. The update session event type is used to provide updated statistics for the flow, or if the collector was unavilable at the time of the session create event and may have missed the create event. The Information element ikeEvent is used indicate the the IKE event type

Table 2: Definition of IKE Events

Event Name	Values
IKE Session Create	1
IKE Session Delete	2
IKE Session Update	3

Table 2: Definition of IKE Events

5.1.3. IKE Create, Update, Delete Events Template

Table 3 : IKE Create, Update, Delete Events Template

Field Name	Mandatory	Comments
ikeEvent	Yes	
timeStamp	Yes	
sessionCreationTimeMilliSeconds	Yes	
ikeSessionId	Yes	
InterfaceName	Yes	
InterfaceId	No	
ikeTunLocalIdType	Yes	
ikeTunLocalId	Yes	
ikeTunLocalIPAddr*	Yes	ikeTunLocalIPv4Addr or ikeTunLocalIPv6Addr
ikeTunLocalName	Yes	
VRFname	No	
ikeTunRemoteIdtype	Yes	
ikeTunRemoteIPAddr*	Yes	ikeTunLocalIPv4Addr or ikeTunLocalIPv6Addr
ikeTunRemoteName	Yes	
ikeTunTransform	Yes	
ikeTunLifeTime	Yes	
eventReason	No	

Table 3 : IKE Create, Update, Delete Events Template

5.1.4. IKE Statistics and Errors Template

Table 4 : IKE Statistics and Errors Template

Field Name	Mandatory	Comments
ikeEvent	Yes	
timeStamp	Yes	
SessCreationTimeMilliSeconds	Yes	
ikeSessionId	Yes	
ikeTunRemoteIP*	No	ikeTunLocalIPv4Addr or ikeTunLocalIPv6Addr
ikeTunRemoteName	No	
ikeDPDSent	No	
ikeDPDRcvd	No	
ikePktsTX	No	
ikePktsRX	No	
ikeRetransTX	No	
ikeRetransRX	No	
ikeDecryptFailed	No	
ikeEncryptFailed	No	
ikeInvalidPayload	No	
ikeFragFailed	No	

Table 4 : IKE Statistics and Errors Template

5.2. IPSec Event Logging

5.2.1. IPSec Information Elements

The following table lists all of the IPsec Information Elements used in events send to a collector. The formats of the IE's and the IPFIX IDs are listed below. Some of the IPFIX IE's are not assigned yet, and thus the detailed description of these fields are provided in the IANA considerations section. New IPFIX Information Elements must be allocated in IANA's IPFIX registry [IANA-IPFIX], as defined in the sub-sections of section 9. The templates may contain a subset of the Information Elements(IEs) shown in Table 5 depending upon the event being logged.

Table 5 : IPSec Information Elements

IPFIX Field Name	Data Type	IANA IPFIX ID	Description
ipsecEvent	unsigned8	TBD32	IPSec event - start, udpate,stop, error
timeStamp	unsigned64** *	323	timestamp of event
SessionCreationTimeMilliSeconds	unsigned64** *	TBD33	Tracks when a session was created
ipsecTunSessionId	unsigned32	TBD34	Session id used by IPSec
ikeSessionId	unsigned32	TBD03	Session id used by IKE
ipsecproxySrcType	unsigned8	TBD35	proxy type
ipSecSpi	unsigned32	295	SPI value
ipSecDirection	unsigned8	TBD37	inbound or outbound SA
ikeTunLocalIPAddr*	var	TBD08	ikeTunLocalIPv4Addr or ikeTunLocalIPv6Addr
ikeTunRemoteIPAddr*	var	TBD14	ikeTunRemoteIPv4Addr or ikeTunRemoteIPv6Addr
ikeTunRemoteName	str	TBD17	Remote peer name
ipSecFrontVrfName	str	TBD38	Front door vrf name
ipSecInsideVrfName	str	TBD39	Inside VRF name
ipSecTunLifeSize	unsigned32	TBD40	IPSec Tunnel data volume lifetime

ipSecTunLifeTime	unsigned32	TBD41	IPSec Tunnel lifetime
ipSecTunEncapMode	unsigned8	TBD42	Tunnel or Transport
ipSecTunSaTransform	unsigned32	TBD43	Sequence of Transform (RFC5996, section 3.3.2) includes dh,prot, encr, auth
ipSecTunSaCompAlgo	IKE	TBD44	check if it can combined with SaTransform

ipSecTrafficSelector	IKE	TBD45	RFC5996, section 3.13.1
eventReason	unsigned8	TBD46	Reason for event like create/delete
ipsecPktCount	unsigned64	TBD47	# of packet encrypted/decrypted
ipsecPktComp	unsigned64	TBD48	Packets compressed
ipsecPktDecomp	unsigned64	TBD49	Packets decompressed
ipsecByteCount	unsigned128	TBD50	Bytes encrypted or decrypted
ipsecReplayErrors	unsigned32	TBD51	Replay errors
ipsecReplayRollover	unsigned32	TBD52	Replay rollovers
ipsecMacErrors	unsigned32	TBD53	Hash compare failed
ipsecRecvdPktNotIpsec	unsigned32	TBD54	Packet received in clear and should have

				been encrypted
ipsecRecvdPktInvalidId	unsigned32	TBD55	Received packet did not match proxy id of SA
ipsecPktCompFailed	unsigned32	TBD56	Compression Failed
ipsecPktDecompFailed	unsigned32	TBD57	De Compression Failed

Table 5 : IPSec Information Elements

5.2.2. Definition of IPSec Events

Table 6 lists all the IPSEC event types related to a IPSEC session . The events are an IPSEC session create , update , and delete. The update session event type is used to either provide updated statistics for the flow, or notify the flow if collector was unavailable at the time of the session creation event and may have

missed the create event. The update event will also be used for IPSEC rekey event. The Information element ipsecEvent is used to indicate the the IPSEC event type

Table 6: Definition of IPSec Events

Event Name	Values
IPsec Session Create	1
IPsec Session Delete	2
IPsec Session Update	3

Table 6: Definition of IPSec Events

5.2.3. IPSec Create, Delete, Update Template

Table 7: IPSec Create, Delete, Update Template

IPFIX Field Name	Mandatory	Comments
ipsecEvent	Yes	
timeStamp	Yes	
SessionCreationMilliSeconds	Yes	
ipsecTunSessionId	Yes	
ikeSessionId	No	
ipsecproxySrcType	Yes	
ipSecSpi	Yes	
ipSecDirection	Yes	
ikeTunLocalIPAddr*	Yes	ikeTunLocalIPv4Addr or ikeTunLocalIPv6Addr
ikeTunRemoteIPAddr*	Yes	ikeTunLocalIPv4Addr or ikeTunLocalIPv6Addr
ipSecFrontVrfName	No	
ipSecInsideVrfName	No	
ipSecTunLifeSize	Yes	
ipSecTunLifeTime	Yes	
ipSecTunEncapMode	Yes	
ipSecTunSaTransform	Yes	
ipSecTunSacompAlgo	No	
ipSecTrafficSelector	Yes	
eventReason	No	

Table 7: IPSec Create, Delete, Update Template

5.2.4. IPSec Statistics and Errors Template

IPFIX Field Name	Mandatory	Comments
ipsecEvent	Yes	
timeStamp	Yes	
SessionCreationMilliSeconds	Yes	
ipsecTunSessionId	Yes	
ikeSessionId	No	
IPSecSPI	Yes	

ipSecDirection	Yes	
ipsecPktCount	No	
ipsecPktComp	No	
ipsecPktDecomp	No	
ipsecByteCount	No	
ipsecReplayErrors	No	
ipsecReplayRollover	No	
ipsecMacErrors	No	
ipsecRecvdPktNotIpsec	No	
ipsecRecvdPktInvalidId	No	
ipsecPktCompFailed	No	
ipsecPktDecompFailed	No	

IPSec Statistics and Error Template

6. Examples

TBD

7. Considerations

A collector may receive IPSec events from multiple devices and should be able to distinguish between the devices. Each device should have a unique source ID to identify themselves. The source ID is part of the IPFIX template and data exchange.

Prior to logging any events, an IPSec device MUST send the template of the record to the collector to advertise the format of the data record that it is using to send the events. The templates can be exchanged as frequently as required given the reliability of the connection. There SHOULD be a configurable timer for controlling the template refresh. IPSec device SHOULD combine as many events as possible in a single packet to effectively utilize the network bandwidth.

8. Acknowledgements

TBD

9. IANA Considerations

9.1. General Information Elements

9.1.1. timestamp

Description: Contains the timestamp of the flow record

Abstract Data Type: unsigned64

ElementId: 323

Semantics: identifier

9.1.2. sessCreatetimeStamp

Description: Used to track when the session was created especially if its a update flow

Abstract Data Type: unsigned64

ElementId: TBD02

Semantics: identifier

9.1.3. interfaceId

Description: Used to uniquely identify the interface identifier used on the system/device for IKE session

Abstract Data Type: unsigned32

ElementId: TBD04

Semantics: identifier

9.1.4. eventReason

Description: Reason for session delete or create / update. Example reason for sesion delete could be "Administrator reset" As its a

unsigned8 data type, we will use a eventreason id to name mapping. Example: 1 -> Delete by DPD Failure 2 -> Administrator Reset

Abstract Data Type: unsigned8

ElementId: TBD21

Semantics: identifier

9.2. IKE Information Elements

9.2.1. ikeEvent

Description: Contains the IKE Event Type 1=start, 2=update , 3=delete

Abstract Data Type: unsigned8

ElementId: TBD01

Semantics: identifier

9.2.2. ikeSessionId

Description: Its the session id used by IKE that will be used to uniquely identify a IKE session and can be correlate from an IPsec SA. A value of 0 is used for manual keying.

Abstract Data Type: unsigned32

ElementId: TBD03

Semantics: identifier

9.2.3. ikeTunLocalIdType

Description: Contains the IKE ID Type by the local device - FQDN, addr. Will use the same as per the IKE RFC

Abstract Data Type: unsigned8

ElementId: TBD05

Semantics: identifier

9.2.4. ikeTunLocalId

Description: Local identity to be used for the IKE session: ip addr, FQDN

Abstract Data Type: str

ElementId: TBD06

Semantics: identifier

9.2.5. ikeTunLocalIPAddr*

Description: ikeTunLocalIPv4Addr or ikeTunLocalIPv6Addr depending on whether its a IPv4 or IPv6. IP address used by the local IKE device. It will be either a IPv4 or a IPv6 address.

Abstract Data Type: var

ElementId: TBD07

Semantics: identifier

9.2.6. ikeTunLocalName

Description: A descriptive name given to identify the tunnel. Its locally signficant and not used for IKE negotiation purposes

Abstract Data Type: str

ElementId: TBD10

Semantics: identifier

9.2.7. ikeTunRemoteIdType

Description: Contains the IKE ID Type by the remote peer - FQDN, ip

addr etc. Will use the same as per the IKE RFC

Abstract Data Type: unsigned8

ElementId: TBD11

Semantics: identifier

9.2.8. ikeTunRemoteId

Description: Remote identity to be used for the IKE session: ip addr, FQDN

Abstract Data Type: var

ElementId: TBD12

Semantics: identifier

9.2.9. ikeTunRemoteIPAddr*

Description: exactlyOneOf (ikeTunRemoteIPv4Addr, ikeTunRemoteIPv6Addr). IP address used by the local IKE device. It will be either a IPv4 or a IPv6 address, thus a exactlyOneOf method is used to derive that.

Abstract Data Type: var

ElementId: TBD13

Semantics: identifier

9.2.10. ikeTunRemoteName

Description: A logical name used to identify the remote VPN peer. Is locally significant and not used in any IKE negotiation.

Abstract Data Type: str

ElementId: TBD16

Semantics: identifier

9.2.11. ikeTunTransform

Description: Transform used for IKE sa. Its based on RFC5996 3.3.2 IKE encoding : DH, encryption algo, hash, PRF. IKE encoding is used so that collectors can easily understand this.

Abstract Data Type: ike-encoding

ElementId: TBD17 - Possible use of Structured Data Type such as subTemplateList/SubTemplateMultiList

Semantics: identifier

9.2.12. ikeTunLocalAuthMethod

Description: Authentication method used by local device - pre-shared key, certificate, EAP

Values: 1=PSK, 2=certificate, 3=EAP

Abstract Data Type: unsigned8

ElementId: TBD18

Semantics: identifier

9.2.13. ikeTunRemoteAuthMethod

Description: Authentication method used by remote peer- pre-shared key, certificate, EAP

Values: 1=PSK, 2=certificate, 3=EAP

Abstract Data Type: unsigned8

ElementId: TBD19

Semantics: identifier

9.2.14. ikeTunLifeTime

Description: IKE SA lifetime in seconds

Abstract Data Type: unsigned32

ElementId: TBD20

Semantics: identifier

9.2.15. ikeDPDSent

Description: IKE Dead peer detection (DPD) packets sent

Abstract Data Type: unsigned32

ElementId: TBD22

Semantics: identifier

9.2.16. ikeDPDRcvd

Description: IKE Dead peer detection (DPD) packets received

Abstract Data Type: unsigned32

ElementId: TBD23

Semantics: identifier

9.2.17. ikePktsTX

Description: Number of IKE packets sent

Abstract Data Type: unsigned32

ElementId: TBD24

Semantics: identifier

9.2.18. ikePktsRX

Description: Number of IKE packets received

Abstract Data Type: unsigned32

ElementId: TBD25

Semantics: identifier

9.2.19. ikeRetransTX

Description: IKE Retransmitted

Abstract Data Type: unsigned32

ElementId: TBD26

Semantics: identifier

9.2.20. ikeRetransRX

Description: IKE Retransmitted

Abstract Data Type: unsigned32

ElementId: TBD27

Semantics: identifier

9.2.21. ikeDecryptFailed

Description: Number of IKE packets where the payload decryption failed

Abstract Data Type: unsigned32

ElementId: TBD28

Semantics: identifier

9.2.22. ikeEncryptFailed

Description: Number of IKE packets where the payload encryption failed

Abstract Data Type: unsigned32

ElementId: TBD29

Semantics: identifier

9.2.23. ikeInvalidPayload

Description: Number of packets received where the IKE payload was invalid

Abstract Data Type: unsigned32

ElementId: TBD30

Semantics: identifier

9.2.24. ikeFragFailed

Description: Number of packets where it failed due to fragmentation

Abstract Data Type: unsigned32

ElementId: TBD31

Semantics: identifier

9.3. IPSec Information Elements

9.3.1. ipsecEvent

Description: Contains the Ipsec Event Type 1=start, 2=update , 3=delete

Abstract Data Type: unsigned8

ElementId: TBD32

Semantics: identifier

9.3.2. ipsecTunSessionId

Description: Session used to uniquely identify a ipsec sa

Abstract Data Type: ipv6Address

ElementId: TBD34

Semantics: identifier

9.3.3. ipsecProxySrcType

Description: Proxy type used by IPSEC

Abstract Data Type: unsigned8

ElementId: TBD35

Semantics: identifier

9.3.4. ipSecDirection

Description: Direction of the IPSEC sa : 1=Inbound 2=Outbound

Abstract Data Type: unsigned8

ElementId: TBD37 -- Possible reuse of flowDirection (61)

Semantics: identifier

9.3.5. ipSecFrontVrfName

Description: VRF name used after IPSEC encapsulation

Abstract Data Type: var

ElementId: TBD38

Semantics: identifier

9.3.6. ipSecInsideVrfName

Description: VRF name where the clear text packet/data resides before IPsec encapsulation or after decryption

Abstract Data Type: str

ElementId: TBD39

Semantics: identifier

9.3.7. ipSecTunLifeSize

Description: The IPsec SA data volume based lifetime measured in bytes

Abstract Data Type: unsigned32

ElementId: TBD40

Semantics: identifier

9.3.8. ipSecTunLifeTime

Description: The IPsec sa lifetime measured in seconds

Abstract Data Type: unsigned32

ElementId: TBD41

Semantics: identifier

9.3.9. ipSecTunEncapMode

Description: Encapsulation mode used. 1=Tunnel 2=Transport

Abstract Data Type: unsigned8

ElementId: TBD42

Semantics: identifier

9.3.10. ipSecTunSaTransform

Description: IPsec Transform used for encryption, DH algorithm,authentication. IKE encoding is used as per RFC 5996 section 3.3.2

Abstract Data Type: IKE

ElementId: TBD43

Semantics: identifier

9.3.11. ipSecTunSaCompAlgo

Description: Compression algorithm used

Abstract Data Type: IKE

ElementId: TBD44

Semantics: identifier

9.3.12. ipSecTrafficSelector

Description: Defines the local and remote traffic selectors for encryption. Encoding is using IKE as per RFC 5996 3.13.1

Abstract Data Type: IKE

ElementId: TBD45

Semantics: identifier

9.3.13. ipsecPktCount

Description: The number of packets encrypted or decrypted through this IPsec SA

Abstract Data Type: unsigned64

ElementId: TBD47

Semantics: identifier

9.3.14. ipsecPktComp

Description: The number of packets compressed

Abstract Data Type: unsigned64

ElementId: TBD48

Semantics: identifier

9.3.15. ipsecPktDecomp

Description: The number of packets de-compressed

Abstract Data Type: unsigned64

ElementId: TBD49

Semantics: identifier

9.3.16. ipsecByteCount

Description: The number of bytes over an IPsec SA

Abstract Data Type: unsigned128

ElementId: TBD50

Semantics: identifier

9.3.17. ipsecReplayErrors

Description: The number of replay errors

Abstract Data Type: unsigned32

ElementId: TBD51

Semantics: identifier

9.3.18. ipsecReplayRollover

Description: The number of IPsec replay rollovers

Abstract Data Type: unsigned32

ElementId: TBD52

Semantics: identifier

9.3.19. ipsecMacErrors

Description: The number of mac authentication errors

Abstract Data Type: unsigned32

ElementId: TBD53

Semantics: identifier

9.3.20. ipsecRecvdPktNotIpsec

Description: The number of packets received which were not encrypted when they should have been as per security policy

Abstract Data Type: unsigned32

ElementId: TBD54

Semantics: identifier

9.3.21. ipsecRecvdPktInvalidId

Description: The number of packets received where after decryption did not match the traffic selector for that IPSEC sa

Abstract Data Type: unsigned32

ElementId: TBD55

Semantics: identifier

9.3.22. ipsecPktCompFailed

Description: The number of packets where compression failed

Abstract Data Type: unsigned32

ElementId: TBD56

Semantics: identifier

9.3.23. ipsecPktDecompFailed

Description: The number of packets where de-compression failed

Abstract Data Type: unsigned32

ElementId: TBD57

Semantics: identifier

10. Security Considerations

None.

11. Acknowledgements

We would like to thank Paul Aitken and Senthil Sivakumar for their detailed review and feedback on early versions of this document.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

12.2. Informative References

[IPFIX-IANA]
IANA, "IPFIX Information Elements registry", <http://www.iana.org/assignments/ipfix>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5101] Claise, B., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, January 2008.

[RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", RFC 5102, January 2008.

[RFC5470] Sadasivan, G., Brownlee, N., Claise, B., and J. Quittek, "Architecture for IP Flow Information Export", RFC 5470, March 2009.

[RFC7011] Claise, B., Trammell, B., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, September 2013.

Authors' Addresses

Tom Alexander
Cisco Systems, Inc.

Email: thalexan@cisco.com

Frederic Detienne
Cisco Systems, Inc.

Email: fd@cisco.com

Sandeep Rao
Cisco Systems, Inc.

Email: rsandeep@cisco.com

Thamilarasu Kandasamy
Cisco Systems, Inc.

Email: thamil@cisco.com