

Internet Draft
[draft-ietf-ipsec-monitor-mib-06.txt](#)
April 15, 2003
Expires in six months

Editor: Paul Hoffman
VPN Consortium

IPsec Monitoring MIB

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

Table of Contents

[[Needs to be generated in the RFC publication step]]

1. Introduction

This document defines low level monitoring and status MIBs for IPsec security associations (SAs). It does not define MIBs that may be used for configuring IPsec implementations or for providing low-level diagnostic or debugging information. It assumes no specific use of IPsec. Further, it does not provide policy information.

The purpose of the MIBs is to allow system administrators to determine operating conditions and perform system operational level monitoring of the IPsec portion of their network. Statistics are provided as well. Additionally, it may be used as the basis for application specific MIBs for specific uses of IPsec SAs.

2. The SNMP Management Framework

The SNMP Management Framework presently consists of five major components:

- o An overall architecture, described in [RFC 2571](#) [[RFC2571](#)].
- o Mechanisms for describing and naming objects and events for the purpose of management. The first version of this Structure of Management Information (SMI) is called SMIV1 and described in STD 16, [RFC 1155](#) [[RFC1155](#)], STD 16, [RFC 1212](#) [[RFC1212](#)] and [RFC 1215](#) [[RFC1215](#)]. The second version, called SMIV2, is described in STD 58, [RFC 2578](#) [[RFC2578](#)], [RFC 2579](#) [[RFC2579](#)] and [RFC 2580](#) [[RFC2580](#)].
- o Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in STD 15, [RFC 1157](#) [[RFC1157](#)]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in [RFC 1901](#) [[RFC1901](#)] and [RFC 1906](#) [[RFC1906](#)]. The third version of the message protocol is called SNMPv3 and described in [RFC 1906](#) [[RFC1906](#)], [RFC 2572](#) [[RFC2572](#)] and [RFC 2574](#) [[RFC2574](#)].
- o Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in STD 15, [RFC 1157](#) [[RFC1157](#)]. A second set of protocol operations and associated PDU formats is described in [RFC 1905](#) [[RFC1905](#)].
- o A set of fundamental applications described in [RFC 2573](#) [[RFC2573](#)] and the view-based access control mechanism described in [RFC 2575](#) [[RFC2575](#)].

A more detailed introduction to the current SNMP Management Framework can be found in [RFC 2570](#) [[RFC2570](#)].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the mechanisms defined in the SMI.

This memo specifies a MIB module that is compliant to the SMIV2. A MIB conforming to the SMIV1 can be produced through the appropriate translations. The resulting translated MIB must be semantically equivalent, except where objects or events are omitted because no translation is possible (use of Counter64). Some machine-readable information in SMIV2 will be converted into textual descriptions in SMIV1 during the translation process. However, this loss of machine-readable information is not considered to change the semantics of the MIB.

2.1 Object Definitions

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the subset of Abstract Syntax Notation One (ASN.1)

defined in the SMI. In particular, each object type is named by an OBJECT IDENTIFIER, an administratively assigned name. The object type together with an object instance serves to uniquely identify a specific instantiation of the object. For human convenience, we often use a textual string, termed the descriptor, to refer to the object type.

3. Definitions

3.1 Security Association

These MIBs use the [RFC 2401](#) [ISAKMP] [Section 4.1](#) identification of a security association (SA).

"A security association is uniquely identified by a triple consisting of a Security Parameter Index (SPI), an IP Destination Address, and a security protocol (AH or ESP) identifier."

As such, an SA in these MIBs is a unidirectional entity. IKE negotiates these in pairs, outbound and inbound.

For IPcomp [IPCOMP] SAs, a CPI (Compression Parameter Index) replaces the SPI.

3.2 Inbound

In the inbound direction, a packet crosses an interface of a logical or physical entity and enters the entity. No assumption is made about what happens to the packet after it enters the entity.

An inbound SA then is an SA that processes inbound packets at an interface.

3.3 Outbound

In the outbound direction, a packet crosses an interface of a logical or physical entity and leaves the entity. No assumption is made about the origins of the packet before it exits the entity.

An outbound SA then is an SA that processes outbound packets at an interface.

4. IPsec MIB Objects Architecture

The IPsec MIB consists of tables for the display of raw IPsec security associations (SAs), some entity statistics and traps. Configuration about the SAs is provided as are statistics related to

the SAs themselves. However, no ability is provided to configure the SAs themselves.

The intent is that these MIBs may be used by any entity that somehow creates IPsec SAs. That creation mechanism can be IKE, static configuration or some other key exchange protocol.

System administrators may use the traps to help detect mis-configurations or possible attacks.

4.1 IPsec Security Association Tables

Due to the definition of the identification of an SA (see [Section 3.1](#)), individual SAs in these MIBs are indexed by the equivalent three objects, where the security protocol is implicit by the SA's appearance in a particular table. Further, for the purposes of these MIBs, IPcomp is considered a security protocol.

Individual IPsec phase 2 SAs are separated by both direction and security protocol, resulting in the creation of six separate tables.

All tables contain common information, such as the selectors and expiration limits, in addition to protocol specific information. The selectors are important objects with respect to phase 2 SAs and can be shared across multiple SAs, so there is a table of SA selectors.

The SAs in the tables may have been statically created, created by IKE or by some other mechanism.

When SAs expire, they are removed from the table. There is no SA history kept with the exception of some global counters.

4.1.1 Phase 2 Selector Table

This table provides a list of SA selectors. This table is arbitrarily indexed. It contains the local phase 2 ID, then the remote phase 2 ID, a layer 4 protocol number, and finally the local and remote layer 4 port numbers.

The SA table uses entries in this table.

4.1.2 IPcomp Security Associations

For IPcomp SAs, the following assumptions are made:

- o IPcomp SAs don't care about policy errors.
- o IPcomp SAs don't care about expiration.
- o The selector can be empty (0) if IPcomp is shared across multiple

security association suites. This may happen if an implementation chooses to use a CPI in the range of 1 to 63, representing the specific compression protocol chosen.

- o There are no transmission errors; an outbound SA will send packets uncompressed if it is unable to compress them for any reason.
- o The outbound SA also makes decisions about which packets are compressed or not compressed.
- o Packets which were not compressed by an outbound IPcomp SA are still passed to an inbound IPcomp SA for processing when the IPcomp SA is part of a security association suite. This is for accounting purposes only, and is not intended to force any particular implementation.

A compression performance metric can be calculated for IPcomp SAs by dividing the SAs' output traffic counter value by the SAs' input traffic counter.

Also provided for IPcomp SAs are the total number of packets and traffic that was compressed. The total for packets that were not compressed can be calculated using the available objects.

4.2 IPsec MIB Traps

Traps are provided to let system administrators know about the existence of error conditions occurring in the entity. These errors are associated with operational errors and may also indicate the presence of attacks on the system.

Traps are not provided when SAs come up or go down.

Traps may also be enabled or disabled as required, using configurable configuration objects. Note that support for these objects is optional, so that system administrators that have concerns about SNMP security can choose to implement objects that are write-only.

4.3 IPsec Entity Level Objects

This part of the MIB carries statistics global to the IPsec device. Statistics included are aggregate numbers of SAs and aggregate errors for SAs.

5. MIB Definitions

```
IPSEC-SA-MON-MIB DEFINITIONS ::= BEGIN
```

```
IMPORTS
```

```

MODULE-IDENTITY, OBJECT-TYPE, Counter32, Gauge32,
Integer32, Unsigned32, NOTIFICATION-TYPE,
OBJECT-IDENTITY, Counter64
-- remove this and next line before release
, experimental

                                FROM SNMPv2-SMI
TEXTUAL-CONVENTION, TruthValue
                                FROM SNMPv2-TC
OBJECT-GROUP, NOTIFICATION-GROUP, MODULE-COMPLIANCE
                                FROM SNMPv2-CONF
ifIndex                        FROM IF-MIB
-- uncomment next line before release (and remove this one)
-- mib-2                        FROM RFC1213-MIB
InetAddressType, InetAddress
                                FROM INET-ADDRESS-MIB

IpsecDoiIdentType,
IpsecDoiEncapsulationMode,
IpsecDoiEspTransform,
IpsecDoiAhTransform,
IpsecDoiAuthAlgorithm,
IpsecDoiIpcompTransform,
IpsecDoiSecProtocolId
                                FROM IPSEC-ISAKMP-IKE-DOI-TC;

ipsecSaMonModule MODULE-IDENTITY
LAST-UPDATED "0110031200Z"
ORGANIZATION "IETF IPsec Working Group"
CONTACT-INFO
    "    Tim Jenkins
        Catena Networks
        307 Legget Drive
        Kanata, ON
        Canada
        K2K 3C8

        +1 (613) 599-6430
        tjenkins@catena.com

        John Shriver
        Intel Corporation
        28 Crosby Drive Bedford, MA
        01730

        +1 (781) 687-1329
        John.Shriver@intel.com
    "

DESCRIPTION
    "The MIB module to describe generic IPsec objects, and
    entity level objects and events for those types."

```

```

REVISION      "9906031200Z"
DESCRIPTION
    "Initial revision."
REVISION      "9906251200Z"
DESCRIPTION
    "Add module compliance requirements.
    Added common textual conventions.
    Other minor edits and clarifications."
REVISION      "9910211200Z"
DESCRIPTION
    "Group and compliance statements added.
    OID value under experimental tree added.
    Authentication algorithm key length values added."
REVISION      "0007101200Z"
DESCRIPTION
    "Added optional replay counter tables.
    Added more statistics to IPcomp SAs.
    Make packet and traffic counts definitions more explicit.
    Use Internet address formats from INET-ADDRESS-MIB.
    Added and used selector table."
REVISION      "0102071200Z"
DESCRIPTION
    "Change MAX-ACCESS clause of all index object to
    not-accessible. This lead to other changes due to
    restrictions on the use of objects with MAX-ACCESS clauses
    of not-accessible."
REVISION      "0110031200Z"
DESCRIPTION
    "A number of typo errors corrected. Also:
    -- selectorGroup made mandatory
    -- add (SIZE (4|16|20)) to ipsecLocalAddress and
       ipsecPeerAddress
    -- change kilobytes to Kilobytes and make it 1024 bytes
    -- used plurals in names in replay tables"

-- replace xxx in next line before release and uncomment it
-- ::= { mib-2 xxx }
-- delete this and next line before release
::= { experimental 98 }

IpssecSaCreatorIdent ::= TEXTUAL-CONVENTION
    DISPLAY-HINT      "d"
    STATUS              current
    DESCRIPTION
        "A value indicating how an SA was created."
    SYNTAX              INTEGER {
                            unknown(0),
                            static(1),      -- statically created
                            ike(2),          -- IKE
                            other(3)

```

```
}
```

```
IpsecRawId ::= TEXTUAL-CONVENTION
```

```
    DISPLAY-HINT    "x"
```

```
    STATUS          current
```

```
    DESCRIPTION
```

```
        "This data type is used to model the ID values used by  
        entities that have negotiated and created SAs.
```

```
        The values are taken directly from any payloads exchanged,  
        independent of the type of ID transmitted.
```

```
        In some cases, the payload may be truncated. Note also that  
        some IDs have human readable forms that are not used by this  
        textual convention."
```

```
    SYNTAX          OCTET STRING (SIZE (0..255))
```

```
-- the main MIB branch
```

```
ipsecSaMonitorMIB OBJECT-IDENTITY
```

```
    STATUS          current
```

```
    DESCRIPTION
```

```
        "This is the base object identifier for all IPsec branches."
```

```
    ::= { ipsecSaMonModule 1 }
```

```
-- significant branches
```

```
saTables OBJECT-IDENTITY
```

```
    STATUS          current
```

```
    DESCRIPTION
```

```
        "This is the base object identifier for all SA tables."
```

```
    ::= { ipsecSaMonitorMIB 1 }
```

```
saStatistics OBJECT-IDENTITY
```

```
    STATUS          current
```

```
    DESCRIPTION
```

```
        "This is the base object identifier for all objects which  
        are global counters for IPsec security associations."
```

```
    ::= { ipsecSaMonitorMIB 2 }
```

```
saErrors OBJECT-IDENTITY
```

```
    STATUS          current
```

```
    DESCRIPTION
```

```
        "This is the base object identifier for all objects which  
        are global error counters for IPsec security associations."
```

```
    ::= { ipsecSaMonitorMIB 3 }
```

```
saTraps OBJECT-IDENTITY
```

```
    STATUS          current
```

```
    DESCRIPTION
```

```
        "This is the base object identifier for all objects which
```

```

        are traps for IPsec security associations."
 ::= { ipsecSaMonitorMIB 4 }

saTrapObjects OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION
        "This is the base object identifier for objects which are
        used as part of traps."
 ::= { ipsecSaMonitorMIB 5 }

saTrapControl OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION
        "This is the base object identifier for all objects which
        are trap controls for IPsec security associations."
 ::= { ipsecSaMonitorMIB 6 }

saGroups      OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION
        "This is the base object identifier for all objects which
        describe the groups in this MIB."
 ::= { ipsecSaMonitorMIB 7 }

saConformance OBJECT-IDENTITY
    STATUS      current

    DESCRIPTION
        "This is the base object identifier for all objects which
        describe the conformance for this MIB."
 ::= { ipsecSaMonitorMIB 8 }

--
-- the Selector MIB-Group
--
-- a collection of objects providing information about
-- the phase 2 selectors in the entity
--

selectorTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SelectorEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The (conceptual) table containing the phase 2 selectors.

        The number of rows in this table is the same as the number
        of selectors in the entity. The entity may create rows for
        any purpose; no corresponding phase 2 SA or SA suite is

```

required.

The maximum number of rows is implementation dependent."
::= { saTables 1 }

selectorEntry OBJECT-TYPE

SYNTAX SelectorEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

"An entry (conceptual row) containing the information on a particular phase 2 selector.

A row in this table cannot be created or deleted by SNMP operations on columns of the table."

INDEX { selectorIndex }
::= { selectorTable 1 }

SelectorEntry ::= SEQUENCE {

-- index
selectorIndex Unsigned32,

-- the values
selectorLocalId IpsecRawId,
selectorLocalIdType IpsecDoiIdentType,
selectorRemoteId IpsecRawId,
selectorRemoteIdType IpsecDoiIdentType,
selectorProtocol Integer32,
selectorLocalPort Integer32,
selectorRemotePort Integer32

}

selectorIndex OBJECT-TYPE

SYNTAX Unsigned32 (1..16777215)
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

"A unique value, greater than zero, for each selector. It is recommended that values are assigned contiguously starting from 1."

::= { selectorEntry 1 }

selectorLocalId OBJECT-TYPE

SYNTAX IpsecRawId
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The local identifier of the selector.

This corresponds to the source identifier of outbound SAs that use this selector, and to the destination identifier of

inbound SAs that use this selector.

This value is taken directly from the optional ID payloads that are exchanged during phase 2 negotiations.

If those negotiations are for transport mode SAs, then this value should be the IP address of the local entity."

REFERENCE ["RFC 2401 section 4.4.2"](#)

::= { selectorEntry 2 }

selectorLocalIdType OBJECT-TYPE

SYNTAX IpsecDoiIdentType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The type of ID used for 'selectorLocalId'.

This value is taken directly from the optional ID payloads that are exchanged during phase 2 negotiations.

If those negotiations are for transport mode SAs, then this value should indicate that an IP address is used by the local entity."

REFERENCE ["RFC 2401 section 4.4.2"](#)

::= { selectorEntry 3 }

selectorRemoteId OBJECT-TYPE

SYNTAX IpsecRawId

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The remote identifier of the selector.

This corresponds to the destination identifier of outbound SAs that use this selector, and to the source identifier of inbound SAs that use this selector.

This value is taken directly from the optional ID payloads that are exchanged during phase 2 negotiations of SAs.

If those negotiations are for transport mode SAs, then this value should be the IP address of the remote peer."

REFERENCE ["RFC 2401 section 4.4.2"](#)

::= { selectorEntry 4 }

selectorRemoteIdType OBJECT-TYPE

SYNTAX IpsecDoiIdentType

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The type of ID used for 'selectorRemoteId'.

This value is taken directly from the optional ID payloads that are exchanged during phase 2 negotiations of SAs.

If those negotiations are for transport mode SAs, then this value should indicate that an IP address is used by the remote peer."

REFERENCE ["RFC 2401 section 4.4.2"](#)

::= { selectorEntry 5 }

selectorProtocol OBJECT-TYPE

SYNTAX Integer32 (0..255)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The transport-layer protocol number that to which this selector allows, or 0 if it selects any protocol.

This value is taken directly from the optional ID payloads that are exchanged during phase 2 negotiations of SAs."

REFERENCE ["RFC 2401 section 4.4.2"](#)

::= { selectorEntry 6 }

selectorLocalPort OBJECT-TYPE

SYNTAX Integer32 (0..65535)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The local port number of the protocol that this selector uses, or 0 if it carries any port number.

This corresponds to the source port number of outbound SAs that use this selector, and to the destination port number of inbound SAs that use this selector.

This value is taken directly from the optional ID payloads that are exchanged during phase 2 negotiations of SAs."

REFERENCE ["RFC 2401 section 4.4.2"](#)

::= { selectorEntry 7 }

selectorRemotePort OBJECT-TYPE

SYNTAX Integer32 (0..65535)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The remote port number of the protocol that this selector uses, or 0 if it allows any port number.

This corresponds to the destination port number of outbound SAs that use this selector, and to the source port number of

inbound SAs that use this selector.

This value is taken directly from the optional ID payloads that are exchanged during phase 2 negotiations of SA suites."

REFERENCE ["RFC 2401 section 4.4.2"](#)

::= { selectorEntry 8 }

-- the IPsec Inbound ESP MIB-Group

--

-- a collection of objects providing information about

-- IPsec Inbound ESP SAs

ipsecSaEspInTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpsecSaEspInEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The (conceptual) table containing information on IPsec inbound ESP SAs.

There should be one row for every inbound ESP security association that exists in the entity. The maximum number of rows is implementation dependent."

::= { saTables 2 }

ipsecSaEspInEntry OBJECT-TYPE

SYNTAX IpsecSaEspInEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An entry (conceptual row) containing the information on a particular IPsec inbound ESP SA.

A row in this table cannot be created or deleted by SNMP operations on columns of the table."

INDEX {
 ipsecSaEspInAddressType,
 ipsecSaEspInAddress,
 ipsecSaEspInSpi
 }

::= { ipsecSaEspInTable 1 }

IpsecSaEspInEntry ::= SEQUENCE {

-- identification

ipsecSaEspInAddressType InetAddressType,

ipsecSaEspInAddress InetAddress,

ipsecSaEspInSpi Unsigned32,

```

-- selector
ipsecSaEspInSelector          Unsigned32,

-- how created
ipsecSaEspInCreator           IpcsecSaCreatorIdent,

-- security services description
ipsecSaEspInEncapsulation     IpcsecDoiEncapsulationMode,
ipsecSaEspInEncAlg            IpcsecDoiEspTransform,
ipsecSaEspInEncKeyLength      Unsigned32,
ipsecSaEspInAuthAlg           IpcsecDoiAuthAlgorithm,
ipsecSaEspInAuthKeyLength     Unsigned32,
ipsecSaEspInRepWinSize        Unsigned32,

-- expiration limits
ipsecSaEspInLimitSeconds      Unsigned32, -- sec., 0 if none
ipsecSaEspInLimitKbytes       Unsigned32, -- 0 if none

-- current operating statistics
ipsecSaEspInAccSeconds        Counter32,
ipsecSaEspInAccKbytes         Counter32,
ipsecSaEspInUserOctets        Counter64,
ipsecSaEspInPackets           Counter64,

-- error statistics
ipsecSaEspInDecryptErrors     Counter32,
ipsecSaEspInAuthErrors        Counter32,
ipsecSaEspInReplayErrors      Counter32,
ipsecSaEspInPolicyErrors      Counter32,
ipsecSaEspInPadErrors         Counter32,
ipsecSaEspInOtherReceiveErrors Counter32

}

ipsecSaEspInAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "The type of address used for the destination address of the
        SA."
    ::= { ipsecSaEspInEntry 1 }

ipsecSaEspInAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE(4|16|20))
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION
        "The destination address of the SA."
    ::= { ipsecSaEspInEntry 2 }

```

```

ipsecSaEspInSpi OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The security parameters index of the SA."
    REFERENCE   "RFC 2406 Section 2.1"
    ::= { ipsecSaEspInEntry 3 }

ipsecSaEspInSelector OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The index of the selector table row for this SA. In other
        words, the value of 'selectorIndex' for the appropriate row
        ('SelectorEntry') from the 'selectorTable'"
    ::= { ipsecSaEspInEntry 4 }

ipsecSaEspInCreator OBJECT-TYPE
    SYNTAX      IpsecSaCreatorIdent
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The creator of this SA.

        This MIB makes no assumptions about how the SAs are created.
        They may be created statically, or by a key exchange
        protocol such as IKE, or by some other method."
    ::= { ipsecSaEspInEntry 5 }

ipsecSaEspInEncapsulation OBJECT-TYPE
    SYNTAX      IpsecDoiEncapsulationMode
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The type of encapsulation used by this SA."
    ::= { ipsecSaEspInEntry 6 }

ipsecSaEspInEncAlg OBJECT-TYPE
    SYNTAX      IpsecDoiEspTransform
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "A unique value representing the encryption algorithm
        applied to traffic."
    ::= { ipsecSaEspInEntry 7 }

ipsecSaEspInEncKeyLength OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65531)

```

UNITS "bits"
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The length of the encryption key in bits used for the algorithm specified in the ipsecSaEspInEncAlg object. It may be 0 if the key length is implicit in the specified algorithm or there is no encryption specified."

::= { ipsecSaEspInEntry 8 }

ipsecSaEspInAuthAlg OBJECT-TYPE

SYNTAX IpsecDoiAuthAlgorithm
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"A unique value representing the hash algorithm applied to traffic."

::= { ipsecSaEspInEntry 9 }

ipsecSaEspInAuthKeyLength OBJECT-TYPE

SYNTAX Unsigned32 (0..65531)
UNITS "bits"
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The length of the authentication key in bits used for the algorithm specified in the ipsecSaEspInAuthAlg. It may be 0 if the key length is implicit in the specified algorithm or there is no authentication specified."

::= { ipsecSaEspInEntry 10 }

ipsecSaEspInRepWinSize OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The size of the anti-replay window used by this SA, or 0 if anti-replay checking is not being done."

REFERENCE "[Section 3.4.3 of RFC 2406](#)"

::= { ipsecSaEspInEntry 11 }

ipsecSaEspInLimitSeconds OBJECT-TYPE

SYNTAX Unsigned32
UNITS "seconds"
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The maximum lifetime in seconds of the SA, or 0 if there is no time constraint on its expiration, or 4294967295 if the

maximum lifetime is 4294967295 seconds or more but not infinite."

::= { ipsecSaEspInEntry 12 }

ipsecSaEspInLimitKbytes OBJECT-TYPE

SYNTAX Unsigned32

UNITS "Kilobytes"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The maximum lifetime in Kilobytes (1024 bytes) of the SA, or 0 if there is no traffic constraint on its expiration, or 4294967295 if the maximum lifetime is 4294967295 Kilobytes or more but not infinite."

::= { ipsecSaEspInEntry 13 }

ipsecSaEspInAccSeconds OBJECT-TYPE

SYNTAX Counter32

UNITS "seconds"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of seconds accumulated against the SA's expiration by time.

This is also the number of seconds that the SA has existed."

::= { ipsecSaEspInEntry 14 }

ipsecSaEspInAccKbytes OBJECT-TYPE

SYNTAX Counter32

UNITS "Kilobytes"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The amount of traffic handled by the SA that could accumulate against a traffic expiration limit, measured in Kilobytes (1024 bytes).

If the SA expires based on traffic, this value counts against the SA's expiration by traffic limitation. If the SA does not expire based on traffic, this value may be 0 to indicate that the counter is not being used."

::= { ipsecSaEspInEntry 15 }

ipsecSaEspInUserOctets OBJECT-TYPE

SYNTAX Counter64

UNITS "bytes"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The amount of user level traffic measured in bytes successfully handled by the SA. This is the number of bytes of the decrypted IP packet, including the original IP header of that decrypted packet.

This is not necessarily the same as the amount of traffic applied against the traffic expiration limit due to padding or other protocol specific overhead."

::= { ipsecSaEspInEntry 16 }

ipsecSaEspInPackets OBJECT-TYPE

SYNTAX Counter64

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets received and successfully processed by the SA. This does not include received packets that were discarded during processing by the SA."

::= { ipsecSaEspInEntry 17 }

ipsecSaEspInDecryptErrors OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets discarded by the SA due to detectable decryption errors. Not all decryption errors are detectable within SA processing, so this count should not be considered definitive."

::= { ipsecSaEspInEntry 18 }

ipsecSaEspInAuthErrors OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets discarded by the SA due to authentication errors."

::= { ipsecSaEspInEntry 19 }

ipsecSaEspInReplayErrors OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets discarded by the SA due to replay errors."

```

 ::= { ipsecSaEspInEntry 20 }

ipsecSaEspInPolicyErrors OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "packets"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The number of packets discarded by the SA due to policy
        errors. This includes packets where the next protocol is
        invalid."
    ::= { ipsecSaEspInEntry 21 }

ipsecSaEspInPadErrors OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "packets"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The number of packets discarded by the SA due to pad value
        errors.

        Implementations that do not check this must not support this
        object."
    REFERENCE    "RFC 2406 section 2.4"
    ::= { ipsecSaEspInEntry 22 }

ipsecSaEspInOtherReceiveErrors OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "packets"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The number of packets discarded by the SA due to errors
        other than decryption, authentication, replay errors or,
        when supported, invalid padding errors. This may include

        packets dropped due to a lack of receive buffers, and may
        include packets dropped due to congestion at the decryption
        element."
    ::= { ipsecSaEspInEntry 23 }

-- the IPsec Inbound AH MIB-Group
--
-- a collection of objects providing information about
-- IPsec Inbound AH SAs

ipsecSaAhInTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IpcsecSaAhInEntry

```

```

MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION
    "The (conceptual) table containing information on IPsec
    inbound AH SAs.

    There should be one row for every inbound AH security
    association that exists in the entity. The maximum number of
    rows is implementation dependent."
::= { saTables 3 }

```

```

ipsecSaAhInEntry OBJECT-TYPE
    SYNTAX      IpsecSaAhInEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry (conceptual row) containing the information on a
        particular IPsec inbound AH SA.

        A row in this table cannot be created or deleted by SNMP
        operations on columns of the table."
    INDEX       {
        ipsecSaAhInAddressType,
        ipsecSaAhInAddress,
        ipsecSaAhInSpi
    }
    ::= { ipsecSaAhInTable 1 }

```

```

IpsecSaAhInEntry ::= SEQUENCE {

    -- identification
    ipsecSaAhInAddressType    InetAddressType,
    ipsecSaAhInAddress        InetAddress,
    ipsecSaAhInSpi            Unsigned32,

    -- SA selector
    ipsecSaAhInSelector       Unsigned32,

    -- how created
    ipsecSaAhInCreator        IpsecSaCreatorIdent,

    -- security services description
    ipsecSaAhInEncapsulation  IpsecDoiEncapsulationMode,
    ipsecSaAhInAuthAlg        IpsecDoiAhTransform,
    ipsecSaAhInAuthKeyLength  Unsigned32,
    ipsecSaAhInRepWinSize     Unsigned32,

    -- expiration limits
    ipsecSaAhInLimitSeconds   Unsigned32, -- sec., 0 if none
    ipsecSaAhInLimitKbytes    Unsigned32, -- 0 if none

    -- current operating statistics

```

```

ipsecSaAhInAccSeconds      Counter32,
ipsecSaAhInAccKbytes       Counter32,
ipsecSaAhInUserOctets      Counter64,
ipsecSaAhInPackets         Counter64,

-- error statistics
ipsecSaAhInAuthErrors      Counter32,
ipsecSaAhInReplayErrors    Counter32,
ipsecSaAhInPolicyErrors    Counter32,
ipsecSaAhInOtherReceiveErrors Counter32
}

```

ipsecSaAhInAddressType OBJECT-TYPE

```

SYNTAX      InetAddressType
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "The type of address that is the destination address of the
    SA."
 ::= { ipsecSaAhInEntry 1 }

```

ipsecSaAhInAddress OBJECT-TYPE

```

SYNTAX      InetAddress (SIZE(4|16|20))
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "The destination address of the SA."
 ::= { ipsecSaAhInEntry 2 }

```

ipsecSaAhInSpi OBJECT-TYPE

```

SYNTAX      Unsigned32
MAX-ACCESS  not-accessible
STATUS      current
DESCRIPTION
    "The security parameters index of the SA."
REFERENCE   "RFC 2402 Section 2.4"
 ::= { ipsecSaAhInEntry 3 }

```

ipsecSaAhInSelector OBJECT-TYPE

```

SYNTAX      Unsigned32
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The index of the selector table row for this SA. In other
    words, the value of 'selectorIndex' for the appropriate row
    ('SelectorEntry') from the 'selectorTable'"
 ::= { ipsecSaAhInEntry 4 }

```

ipsecSaAhInCreator OBJECT-TYPE

```

SYNTAX      IpsecSaCreatorIdent
MAX-ACCESS  read-only

```

```

STATUS      current
DESCRIPTION
    "The creator of this SA.

    This MIB makes no assumptions about how the SAs are created.
    They may be created statically, or by a key exchange
    protocol such as IKE, or by some other method."
 ::= { ipsecSaAhInEntry 5 }

ipsecSaAhInEncapsulation OBJECT-TYPE
    SYNTAX      IsecDoiEncapsulationMode
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The type of encapsulation used by this SA."
    ::= { ipsecSaAhInEntry 6 }

ipsecSaAhInAuthAlg OBJECT-TYPE
    SYNTAX      IsecDoiAhTransform
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "A unique value representing the hash algorithm applied to
        traffic carried by this SA."
    ::= { ipsecSaAhInEntry 7 }

ipsecSaAhInAuthKeyLength OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65531)
    UNITS        "bits"
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The length of the authentication key in bits used for the
        algorithm specified in the ipsecSaAhInAuthAlg object. It may
        be 0 if the key length is implicit in the specified
        algorithm."
    ::= { ipsecSaAhInEntry 8 }

ipsecSaAhInRepWinSize OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "The size of the anti-replay window used by this SA, or 0 if
        anti-replay checking is not being done."
    REFERENCE    "Section 3.4.3 of RFC 2402"
    ::= { ipsecSaAhInEntry 9 }

ipsecSaAhInLimitSeconds OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS        "seconds"

```

MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The maximum lifetime in seconds of the SA, or 0 if there is
 no time constraint on its expiration, or 4294967295 if the
 maximum lifetime is 4294967295 seconds or more but not
 infinite."
 ::= { ipsecSaAhInEntry 10 }

ipsecSaAhInLimitKbytes OBJECT-TYPE

SYNTAX Unsigned32
UNITS "Kilobytes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The maximum lifetime in Kilobytes (1024 bytes) of the SA,
 or 0 if there is no traffic constraint on its expiration, or
 4294967295 if the maximum lifetime is 4294967295 Kilobytes
 or more but not infinite."
 ::= { ipsecSaAhInEntry 11 }

ipsecSaAhInAccSeconds OBJECT-TYPE

SYNTAX Counter32
UNITS "seconds"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The number of seconds accumulated against the SA's
 expiration by time.

 This is also the number of seconds that the SA has existed."
 ::= { ipsecSaAhInEntry 12 }

ipsecSaAhInAccKbytes OBJECT-TYPE

SYNTAX Counter32
UNITS "Kilobytes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The amount of traffic handled by the SA that could
 accumulate against a traffic expiration limit, measured in
 Kilobytes (1024 bytes).

 If the SA expires based on traffic, this value counts
 against the SA's expiration by traffic limitation. If the SA
 does not expire based on traffic, this value may be 0 to
 indicate that the counter is not being used."
 ::= { ipsecSaAhInEntry 13 }

ipsecSaAhInUserOctets OBJECT-TYPE

SYNTAX Counter64

```

UNITS          "bytes"
MAX-ACCESS     read-only
STATUS         current
DESCRIPTION
    "The amount of user level traffic measured in bytes handled
    successfully by the SA. This is the number of bytes of the
    de-processed IP packet, including the original IP header of
    that de-processed packet.

    This is not necessarily the same as the amount of traffic
    applied against the traffic expiration limit due to padding
    or other protocol specific overhead."
::= { ipsecSaAhInEntry 14 }

```

ipsecSaAhInPackets OBJECT-TYPE

```

SYNTAX         Counter64
UNITS          "packets"
MAX-ACCESS     read-only
STATUS         current

```

DESCRIPTION

```

    "The number of packets received and successfully processed
    by the SA. This does not include packets that were discarded
    during processing by the SA."
::= { ipsecSaAhInEntry 15 }

```

ipsecSaAhInAuthErrors OBJECT-TYPE

```

SYNTAX         Counter32
UNITS          "packets"
MAX-ACCESS     read-only
STATUS         current

```

DESCRIPTION

```

    "The number of packets discarded by the SA due to
    authentication errors."
::= { ipsecSaAhInEntry 16 }

```

ipsecSaAhInReplayErrors OBJECT-TYPE

```

SYNTAX         Counter32
UNITS          "packets"
MAX-ACCESS     read-only
STATUS         current

```

DESCRIPTION

```

    "The number of packets discarded by the SA due to replay
    errors."
::= { ipsecSaAhInEntry 17 }

```

ipsecSaAhInPolicyErrors OBJECT-TYPE

```

SYNTAX         Counter32
UNITS          "packets"

```

```

MAX-ACCESS    read-only
STATUS        current
DESCRIPTION
    "The number of packets discarded by the SA due to policy
    errors. This includes packets where the next protocol is
    invalid."
::= { ipsecSaAhInEntry 18 }

ipsecSaAhInOtherReceiveErrors OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "packets"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The number of packets discarded by the SA due to errors
        other than decryption, authentication or replay errors. This
        may include packets dropped due to a lack of receive

        buffers, and may include packets dropped due to congestion
        at the authentication element."
    ::= { ipsecSaAhInEntry 19 }

-- the IPsec Inbound IPcomp MIB-Group
--
-- a collection of objects providing information about
-- IPsec Inbound IPcomp SAs

ipsecSaIpcompInTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF IpsecSaIpcompInEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "The (conceptual) table containing information on IPsec
        inbound IPcomp SAs.

        There should be one row for every inbound IPcomp (security)
        association that exists in the entity. The maximum number of
        rows is implementation dependent."
    ::= { saTables 4 }

ipsecSaIpcompInEntry OBJECT-TYPE
    SYNTAX      IpsecSaIpcompInEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "An entry (conceptual row) containing the information on a
        particular IPsec inbound IPcomp SA.

        A row in this table cannot be created or deleted by SNMP

```

```

        operations on columns of the table."
INDEX    {
    ipsecSaIpcompInAddressType,
    ipsecSaIpcompInAddress,
    ipsecSaIpcompInCpi
}
:= { ipsecSaIpcompInTable 1 }

IpssecSaIpcompInEntry ::= SEQUENCE {

-- identification
ipsecSaIpcompInAddressType      InetAddressType,
ipsecSaIpcompInAddress          InetAddress,
ipsecSaIpcompInCpi              IpsecDoiIpcompTransform,

-- SA selector (if needed)
ipsecSaIpcompInSelector         Unsigned32,

-- how created
ipsecSaIpcompInCreator          IpsecSaCreatorIdent,

-- security services description
ipsecSaIpcompInEncapsulation    IpsecDoiEncapsulationMode,
ipsecSaIpcompInDecompAlg        IpsecDoiIpcompTransform,

-- current operating statistics
ipsecSaIpcompInSeconds          Counter32,
ipsecSaIpcompInUserOctets       Counter64,
ipsecSaIpcompInUserPackets      Counter64,
ipsecSaIpcompInCompressedOctets Counter64,
ipsecSaIpcompInCompressedPackets Counter64,
ipsecSaIpcompInInputOctets      Counter64,

-- error statistics
ipsecSaIpcompInDecompErrors      Counter32,
ipsecSaIpcompInOtherReceiveErrors Counter32
}

ipsecSaIpcompInAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The type of address used for the destination address of the
        SA.

        If the IPcomp SA is shared across multiple SAs in security
        association suites, this value may be 0."
    ::= { ipsecSaIpcompInEntry 1 }

ipsecSaIpcompInAddress OBJECT-TYPE

```

SYNTAX InetAddress (SIZE(0|4|16|20))
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

"The destination address of the SA.

If the IPcomp SA is shared across multiple SAs in security association suites, this value may be zero-length."

::= { ipsecSaIpcompInEntry 2 }

ipsecSaIpcompInCpi OBJECT-TYPE

SYNTAX IpsecDoiIpcompTransform
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION

"The CPI of the SA. Since the lower values of CPIs are reserved to be the same as the algorithm, the syntax for this object is the same as the transform."

REFERENCE "[RFC 2393 Section 3.3](#)"

::= { ipsecSaIpcompInEntry 3 }

ipsecSaIpcompInSelector OBJECT-TYPE

SYNTAX Unsigned32
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The index of the selector table row for this SA. In other words, the value of 'selectorIndex' for the appropriate row ('SelectorEntry') from the 'selectorTable'

This value may be 0 if this SA is used with multiple SAs in security association suites."

::= { ipsecSaIpcompInEntry 4 }

ipsecSaIpcompInCreator OBJECT-TYPE

SYNTAX IpsecSaCreatorIdent
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The creator of this SA.

This MIB makes no assumptions about how the SAs are created. They may be created statically, or by a key exchange protocol such as IKE, or by some other method."

::= { ipsecSaIpcompInEntry 5 }

ipsecSaIpcompInEncapsulation OBJECT-TYPE

SYNTAX IpsecDoiEncapsulationMode
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The type of encapsulation used by this SA."
::= { ipsecSaIpcompInEntry 6 }

ipsecSaIpcompInDecompAlg OBJECT-TYPE
SYNTAX IpsecDoiIpcompTransform
MAX-ACCESS read-only
STATUS current

DESCRIPTION
"A unique value representing the decompression algorithm
applied to traffic."
::= { ipsecSaIpcompInEntry 7 }

ipsecSaIpcompInSeconds OBJECT-TYPE
SYNTAX Counter32
UNITS "seconds"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of seconds that the SA has existed."
::= { ipsecSaIpcompInEntry 8 }

ipsecSaIpcompInUserOctets OBJECT-TYPE
SYNTAX Counter64
UNITS "bytes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The amount of user level traffic measured in bytes handled
by the SA. This includes traffic on packets that were both
compressed and uncompressed. Packets that were not
compressed that count in this total may include packets that
were received in a security association suite that included
IPcomp."
::= { ipsecSaIpcompInEntry 9 }

ipsecSaIpcompInUserPackets OBJECT-TYPE
SYNTAX Counter64
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"The number of packets sent from the SA after inbound
processing, whether they were compressed or not."

When used in a security association suite, this value is the
total number of packets sent by the suite. If this SA is
shared across multiple SA suites, this value is the sum of
the number of packets sent from those suites."
::= { ipsecSaIpcompInEntry 10 }

ipsecSaIpcompInCompressedOctets OBJECT-TYPE

SYNTAX Counter64

UNITS "bytes"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The amount of traffic measured in bytes that is received by the SA that was compressed. This includes the IPcomp and IP headers that are not compressed.

The amount of traffic that is not compressed (for any reason) is the value of ipsecSaIpcompInInputOctets minus ipsecSaIpcompInCompressedOctets."

::= { ipsecSaIpcompInEntry 11 }

ipsecSaIpcompInCompressedPackets OBJECT-TYPE

SYNTAX Counter64

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets received by the SA that were compressed.

The number of packets that were not compressed (for any reason) is the value of ipsecSaIpcompInUserPackets minus ipsecSaIpcompInCompressedPackets.

When used in a security association suite, this value is the total number of compressed packets received by the suite. If this SA is shared across multiple SA suites, this value is the sum of the number of compressed packets received by those suites."

::= { ipsecSaIpcompInEntry 12 }

ipsecSaIpcompInInputOctets OBJECT-TYPE

SYNTAX Counter64

UNITS "bytes"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The total amount of traffic measured in bytes that is received by the SA, compressed or not. This includes the IPcomp header if present and the IP header of each packet.

When the IPcomp SA is shared across multiple security association suites, this value is the sum of the output of all SAs before this SA in those SA suites.

When used in a security association suite, this value is the

same as the traffic sent from the previous SA in the suite.
If this SA is shared across multiple SA suites, this value

is the sum of all traffic sent from the previous SAs in
those suites "

::= { ipsecSaIpcompInEntry 13 }

ipsecSaIpcompInDecompErrors OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets discarded by the SA due to
decompression errors."

::= { ipsecSaIpcompInEntry 14 }

ipsecSaIpcompInOtherReceiveErrors OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets discarded by the SA due to errors
other than decompression errors. This may include packets
dropped due to a lack of receive buffers, and packets
dropped due to congestion at the decompression element."

::= { ipsecSaIpcompInEntry 15 }

-- the IPsec Outbound ESP MIB-Group

--

-- a collection of objects providing information about

-- IPsec Outbound ESP SAs

ipsecSaEspOutTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpsecSaEspOutEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The (conceptual) table containing information on IPsec
Outbound ESP SAs.

There should be one row for every outbound ESP security
association that exists in the entity. The maximum number of
rows is implementation dependent."

::= { saTables 5 }

ipsecSaEspOutEntry OBJECT-TYPE

SYNTAX IpsecSaEspOutEntry

MAX-ACCESS not-accessible

```

STATUS      current
DESCRIPTION
    "An entry (conceptual row) containing the information on a
    particular IPsec Outbound ESP SA.

    A row in this table cannot be created or deleted by SNMP
    operations on columns of the table."
INDEX    {
        ipsecSaEspOutAddressType,
        ipsecSaEspOutAddress,
        ipsecSaEspOutSpi
    }
::= { ipsecSaEspOutTable 1 }

IpsecSaEspOutEntry ::= SEQUENCE {

    -- identification
    ipsecSaEspOutAddressType      InetAddressType,
    ipsecSaEspOutAddress          InetAddress,
    ipsecSaEspOutSpi              Unsigned32,

    -- SA selector
    ipsecSaEspOutSelector         Unsigned32,

    -- how created
    ipsecSaEspOutCreator          IpsecSaCreatorIdent,

    -- security services description
    ipsecSaEspOutEncapsulation    IpsecDoiEncapsulationMode,
    ipsecSaEspOutEncAlg           IpsecDoiEspTransform,
    ipsecSaEspOutEncKeyLength     Unsigned32,
    ipsecSaEspOutAuthAlg          IpsecDoiAuthAlgorithm,
    ipsecSaEspOutAuthKeyLength    Unsigned32,

    -- expiration limits
    ipsecSaEspOutLimitSeconds     Unsigned32, -- sec., 0 if none
    ipsecSaEspOutLimitKbytes      Unsigned32, -- 0 if none

    -- current operating statistics
    ipsecSaEspOutAccSeconds       Counter32,
    ipsecSaEspOutAccKbytes        Counter32,
    ipsecSaEspOutUserOctets       Counter64,
    ipsecSaEspOutPackets          Counter64,

    -- error statistics
    ipsecSaEspOutSendErrors       Counter32

}

ipsecSaEspOutAddressType OBJECT-TYPE
    SYNTAX      InetAddressType

```

```

MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
    "The type of address used by the destination address of the
    SA."
 ::= { ipsecSaEspOutEntry 1 }

ipsecSaEspOutAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE(4|16|20))
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
        "The destination address of the SA."
    ::= { ipsecSaEspOutEntry 2 }

ipsecSaEspOutSpi OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS not-accessible
    STATUS      current
    DESCRIPTION
        "The security parameters index of the SA."
    REFERENCE RFC 2406 Section 2.1
    ::= { ipsecSaEspOutEntry 3 }

ipsecSaEspOutSelector OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS read-only
    STATUS      current
    DESCRIPTION
        "The index of the selector table row for this suite. In
        other words, the value of 'selectorIndex' for the
        appropriate row ('SelectorEntry') from the 'selectorTable'"
    ::= { ipsecSaEspOutEntry 4 }

ipsecSaEspOutCreator OBJECT-TYPE
    SYNTAX      IpsecSaCreatorIdent
    MAX-ACCESS read-only
    STATUS      current
    DESCRIPTION
        "The creator of this SA."

    This MIB makes no assumptions about how the SAs are created.
    They may be created statically, or by a key exchange
    protocol such as IKE, or by some other method."
    ::= { ipsecSaEspOutEntry 5 }

ipsecSaEspOutEncapsulation OBJECT-TYPE
    SYNTAX      IpsecDoiEncapsulationMode

```

MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The type of encapsulation used by this SA."
::= { ipsecSaEspOutEntry 6 }

ipsecSaEspOutEncAlg OBJECT-TYPE
SYNTAX IsecDoiEspTransform
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "A unique value representing the encryption algorithm
 applied to traffic."
::= { ipsecSaEspOutEntry 7 }

ipsecSaEspOutEncKeyLength OBJECT-TYPE
SYNTAX Unsigned32 (0..65531)
UNITS "bits"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The length of the encryption key in bits used for the
 algorithm specified in the ipsecSaEspOutEncAlg object. It
 may be 0 if the key length is implicit in the specified
 algorithm or there is no encryption specified."
::= { ipsecSaEspOutEntry 8 }

ipsecSaEspOutAuthAlg OBJECT-TYPE
SYNTAX IsecDoiAuthAlgorithm
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "A unique value representing the hash algorithm applied to
 traffic."
::= { ipsecSaEspOutEntry 9 }

ipsecSaEspOutAuthKeyLength OBJECT-TYPE
SYNTAX Unsigned32 (0..65531)
UNITS "bits"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The length of the authentication key in bits used for the
 algorithm specified in the ipsecSaEspOutAuthAlg object. It
 may be 0 if the key length is implicit in the specified
 algorithm or there is no authentication specified."
::= { ipsecSaEspOutEntry 10 }

ipsecSaEspOutLimitSeconds OBJECT-TYPE
SYNTAX Unsigned32
UNITS "seconds"

MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The maximum lifetime in seconds of the SA, or 0 if there is no time constraint on its expiration.

 The display value is limited to 4294967295 seconds (more than 136 years); values greater than that value will be truncated."
::= { ipsecSaEspOutEntry 11 }

ipsecSaEspOutLimitKbytes OBJECT-TYPE

SYNTAX Unsigned32
UNITS "Kilobytes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The maximum traffic in Kilobytes (1024 bytes) that the SA is allowed to process, or 0 if there is no traffic constraint on its expiration.

 The display value is limited to 4294967295 Kilobytes; values greater than that value will be truncated."
::= { ipsecSaEspOutEntry 12 }

ipsecSaEspOutAccSeconds OBJECT-TYPE

SYNTAX Counter32
UNITS "seconds"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The number of seconds accumulated against the SA's expiration by time.

 This is also the number of seconds that the SA has existed."
::= { ipsecSaEspOutEntry 13 }

ipsecSaEspOutAccKbytes OBJECT-TYPE

SYNTAX Counter32
UNITS "Kilobytes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The amount of traffic handled by the SA that could accumulate against a traffic expiration limit, measured in Kilobytes (1024 bytes).

 If the SA expires based on traffic, this value counts against the SA's expiration by traffic limitation. If the SA does not expire based on traffic, this value may be 0 to

```
        indicate that the counter is not being used."
 ::= { ipsecSaEspOutEntry 14 }
```

ipsecSaEspOutUserOctets OBJECT-TYPE

```
SYNTAX      Counter64
UNITS       "bytes"
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The amount of user level traffic measured in bytes handled
    by the SA. This is the number of bytes of the unencrypted IP
    packet, including the original IP header of that unencrypted
    packet.

    Traffic from packets dropped due to errors is not included
    in this total.

    This is not necessarily the same as the amount of traffic
    applied against the traffic expiration limit due to padding
    or other protocol specific overhead."
 ::= { ipsecSaEspOutEntry 15 }
```

ipsecSaEspOutPackets OBJECT-TYPE

```
SYNTAX      Counter64
UNITS       "packets"
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The number of packets successfully handled by the SA.
    Packets dropped due to errors are not included in this
    count."
 ::= { ipsecSaEspOutEntry 16 }
```

ipsecSaEspOutSendErrors OBJECT-TYPE

```
SYNTAX      Counter32
UNITS       "packets"
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "The number of packets discarded by the SA due to any error.
    This may include errors due to a lack of transmit buffers."
 ::= { ipsecSaEspOutEntry 17 }
```

```
-- the IPsec Outbound AH MIB-Group
--
-- a collection of objects providing information about
-- IPsec Outbound AH SAs
```

ipsecSaAhOutTable OBJECT-TYPE

```
SYNTAX      SEQUENCE OF IpsecSaAhOutEntry
```

```

MAX-ACCESS    not-accessible
STATUS        current
DESCRIPTION
    "The (conceptual) table containing information on IPsec
    Outbound AH SAs.

    There should be one row for every outbound AH security
    association that exists in the entity. The maximum number of
    rows is implementation dependent."
::= { saTables 6 }

```

```

ipsecSaAhOutEntry OBJECT-TYPE
    SYNTAX      IpsecSaAhOutEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "An entry (conceptual row) containing the information on a
        particular IPsec Outbound AH SA.

        A row in this table cannot be created or deleted by SNMP
        operations on columns of the table."
    INDEX       {
        ipsecSaAhOutAddressType,
        ipsecSaAhOutAddress,
        ipsecSaAhOutSpi
    }
    ::= { ipsecSaAhOutTable 1 }

```

```

IpsecSaAhOutEntry ::= SEQUENCE {

    -- identification
    ipsecSaAhOutAddressType      InetAddressType,
    ipsecSaAhOutAddress          InetAddress,
    ipsecSaAhOutSpi              Unsigned32,

    -- SA selector
    ipsecSaAhOutSelector         Unsigned32,

    -- how created
    ipsecSaAhOutCreator          IpsecSaCreatorIdent,

    -- security services description
    ipsecSaAhOutEncapsulation    IpsecDoiEncapsulationMode,
    ipsecSaAhOutAuthAlg          IpsecDoiAhTransform,
    ipsecSaAhOutAuthKeyLength    Unsigned32,

    -- expiration limits
    ipsecSaAhOutLimitSeconds     Unsigned32, -- sec., 0 if none
    ipsecSaAhOutLimitKbytes      Unsigned32, -- 0 if none

    -- current operating statistics
    ipsecSaAhOutAccSeconds       Counter32,

```

```
ipsecSaAhOutAccKbytes      Counter32,  
ipsecSaAhOutUserOctets    Counter64,  
ipsecSaAhOutPackets       Counter64,
```

```
-- error statistics  
ipsecSaAhOutSendErrors    Counter32
```

```
}
```

```
ipsecSaAhOutAddressType OBJECT-TYPE
```

```
    SYNTAX      InetAddressType
```

```
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The type of address used by the destination address of the  
        SA."
```

```
    ::= { ipsecSaAhOutEntry 1 }
```

```
ipsecSaAhOutAddress OBJECT-TYPE
```

```
    SYNTAX      InetAddress (SIZE(4|16|20))
```

```
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The destination address of the SA."
```

```
    ::= { ipsecSaAhOutEntry 2 }
```

```
ipsecSaAhOutSpi OBJECT-TYPE
```

```
    SYNTAX      Unsigned32
```

```
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The security parameters index of the SA."
```

```
    REFERENCE "RFC 2402 Section 2.4"
```

```
    ::= { ipsecSaAhOutEntry 3 }
```

```
ipsecSaAhOutSelector OBJECT-TYPE
```

```
    SYNTAX      Unsigned32
```

```
    MAX-ACCESS  read-only
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The index of the selector table row for this suite. In  
        other words, the value of 'selectorIndex' for the  
        appropriate row ('SelectorEntry') from the 'selectorTable'"
```

```
    ::= { ipsecSaAhOutEntry 4 }
```

```
ipsecSaAhOutCreator OBJECT-TYPE
```

```
    SYNTAX      IpsecSaCreatorIdent
```

```
    MAX-ACCESS  read-only
```

```
    STATUS      current
```

DESCRIPTION

"The creator of this SA.

This MIB makes no assumptions about how the SAs are created. They may be created statically, or by a key exchange protocol such as IKE, or by some other method."

::= { ipsecSaAhOutEntry 5 }

ipsecSaAhOutEncapsulation OBJECT-TYPE

SYNTAX IpsecDoiEncapsulationMode

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The type of encapsulation used by this SA."

::= { ipsecSaAhOutEntry 6 }

ipsecSaAhOutAuthAlg OBJECT-TYPE

SYNTAX IpsecDoiAhTransform

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"A unique value representing the hash algorithm applied to traffic carried by this SA."

::= { ipsecSaAhOutEntry 7 }

ipsecSaAhOutAuthKeyLength OBJECT-TYPE

SYNTAX Unsigned32 (0..65531)

UNITS "bits"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The length of the authentication key in bits used for the algorithm specified in the ipsecSaAhOutAuthAlg object. It may be 0 if the key length is implicit in the specified algorithm."

::= { ipsecSaAhOutEntry 8 }

ipsecSaAhOutLimitSeconds OBJECT-TYPE

SYNTAX Unsigned32

UNITS "seconds"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The maximum lifetime in seconds of the SA, or 0 if there is no time constraint on its expiration.

The display value is limited to 4294967295 seconds (more than 136 years); values greater than that value will be truncated."

::= { ipsecSaAhOutEntry 9 }

ipsecSaAhOutLimitKbytes OBJECT-TYPE

SYNTAX Unsigned32
UNITS "Kilobytes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The maximum traffic in Kilobytes (1024 bytes) that the SA is allowed to process, or 0 if there is no traffic constraint on its expiration.

The display value is limited to 4294967295 Kilobytes; values greater than that value will be truncated."

::= { ipsecSaAhOutEntry 10 }

ipsecSaAhOutAccSeconds OBJECT-TYPE

SYNTAX Counter32
UNITS "seconds"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The number of seconds accumulated against the SA's expiration by time.

This is also the number of seconds that the SA has existed."

::= { ipsecSaAhOutEntry 11 }

ipsecSaAhOutAccKbytes OBJECT-TYPE

SYNTAX Counter32
UNITS "Kilobytes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The amount of traffic handled by the SA that could accumulate against a traffic expiration limit, measured in Kilobytes (1024 bytes).

If the SA expires based on traffic, this value counts against the SA's expiration by traffic limitation. If the SA does not expire based on traffic, this value may be 0 to indicate that the counter is not being used."

::= { ipsecSaAhOutEntry 12 }

ipsecSaAhOutUserOctets OBJECT-TYPE

SYNTAX Counter64
UNITS "bytes"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The amount of user level traffic measured in bytes handled by the SA. This is the number of bytes of the unprocessed IP packet, including the original IP header of that unprocessed

packet.

Traffic from packets dropped due to errors is not included in this total.

This is not necessarily the same as the amount of traffic applied against the traffic expiration limit due to padding or other protocol specific overhead."

::= { ipsecSaAhOutEntry 13 }

ipsecSaAhOutPackets OBJECT-TYPE

SYNTAX Counter64
UNITS "packets"
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The number of packets successfully handled by the SA. Packets dropped due to errors are not included in this count."

::= { ipsecSaAhOutEntry 14 }

ipsecSaAhOutSendErrors OBJECT-TYPE

SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current

DESCRIPTION

"The number of packets discarded by the SA due to any error. This may include errors due to a lack of transmit buffers."

::= { ipsecSaAhOutEntry 15 }

-- the IPsec Outbound IPcomp MIB-Group

--

-- a collection of objects providing information about

-- IPsec Outbound IPcomp SAs

ipsecSaIpcompOutTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpsecSaIpcompOutEntry
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION

"The (conceptual) table containing information on IPsec Outbound IPcomp SAs.

There should be one row for every outbound IPcomp (security) association that exists in the entity. The maximum number of rows is implementation dependent."

```
::= { saTables 7 }
```

```
ipsecSaIpcompOutEntry OBJECT-TYPE
```

```
SYNTAX      IpsecSaIpcompOutEntry
```

```
MAX-ACCESS  not-accessible
```

```
STATUS      current
```

```
DESCRIPTION
```

```
    "An entry (conceptual row) containing the information on a  
    particular IPsec Outbound IPcomp SA.
```

```
    A row in this table cannot be created or deleted by SNMP  
    operations on columns of the table."
```

```
INDEX      {  
            ipsecSaIpcompOutAddressType,  
            ipsecSaIpcompOutAddress,  
            ipsecSaIpcompOutCpi  
            }
```

```
::= { ipsecSaIpcompOutTable 1 }
```

```
IpsecSaIpcompOutEntry ::= SEQUENCE {
```

```
-- identification
```

```
ipsecSaIpcompOutAddressType      InetAddressType,
```

```
ipsecSaIpcompOutAddress          InetAddress,
```

```
ipsecSaIpcompOutCpi              IpsecDoiIpcompTransform,
```

```
-- SA selector
```

```
ipsecSaIpcompOutSelector          Unsigned32,
```

```
-- how created
```

```
ipsecSaIpcompOutCreator            IpsecSaCreatorIdent,
```

```
-- security services description
```

```
ipsecSaIpcompOutEncapsulation      IpsecDoiEncapsulationMode,
```

```
ipsecSaIpcompOutCompAlg            IpsecDoiIpcompTransform,
```

```
-- current operating statistics
```

```
ipsecSaIpcompOutSeconds            Counter32,
```

```
ipsecSaIpcompOutUserOctets         Counter64,
```

```
ipsecSaIpcompOutUserPackets        Counter64,
```

```
ipsecSaIpcompOutOutputOctets       Counter64,
```

```
ipsecSaIpcompOutCompressedPackets  Counter64,
```

```
ipsecSaIpcompOutCompressedOctets   Counter64
```

```
}
```

```
ipsecSaIpcompOutAddressType OBJECT-TYPE
```

```
SYNTAX      InetAddressType
```

```
MAX-ACCESS  not-accessible
```

```
STATUS      current
```

```
DESCRIPTION
```

"The type of address used by the destination address of the SA.

If the IPcomp SA is shared across multiple SAs in security association suites, this value may be 0 to indicate that the addresses to which this SA apply cannot be expressed with a single InetAddressType/InetAddress pair."

::= { ipsecSaIpcompOutEntry 1 }

ipsecSaIpcompOutAddress OBJECT-TYPE

SYNTAX InetAddress (SIZE(0|4|16|20))

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The destination address of the SA.

If the IPcomp SA is shared across multiple SAs in security association suites, this value may be zero-length to indicate that the addresses to which this SA apply cannot be expressed with a single InetAddressType/InetAddress pair."

::= { ipsecSaIpcompOutEntry 2 }

ipsecSaIpcompOutCpi OBJECT-TYPE

SYNTAX IsecDoiIpcompTransform

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"The CPI of the SA. Since the lower values of CPIs are reserved to be the same as the algorithm, the syntax for this object is the same as the transform."

REFERENCE ["RFC 2393 Section 3.3"](#)

::= { ipsecSaIpcompOutEntry 3 }

ipsecSaIpcompOutSelector OBJECT-TYPE

SYNTAX Unsigned32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The index of the selector table row for this suite. In other words, the value of 'selectorIndex' for the appropriate row ('SelectorEntry') from the 'selectorTable'

This value may be 0 if this SA is used with multiple SAs in security association suites to indicate that this SA is applied to multiple rows from the 'selectorTable'."

::= { ipsecSaIpcompOutEntry 4 }

ipsecSaIpcompOutCreator OBJECT-TYPE

SYNTAX IsecSaCreatorIdent

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The creator of this SA.

This MIB makes no assumptions about how the SAs are created.
They may be created statically, or by a key exchange
protocol such as IKE, or by some other method."

::= { ipsecSaIpcompOutEntry 11 }

ipsecSaIpcompOutEncapsulation OBJECT-TYPE

SYNTAX IpsecDoiEncapsulationMode

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The type of encapsulation used by this SA."

::= { ipsecSaIpcompOutEntry 12 }

ipsecSaIpcompOutCompAlg OBJECT-TYPE

SYNTAX IpsecDoiIpcompTransform

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"A unique value representing the compression algorithm
applied to traffic."

::= { ipsecSaIpcompOutEntry 13 }

ipsecSaIpcompOutSeconds OBJECT-TYPE

SYNTAX Counter32

UNITS "seconds"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of seconds that the SA has existed."

::= { ipsecSaIpcompOutEntry 14 }

ipsecSaIpcompOutUserOctets OBJECT-TYPE

SYNTAX Counter64

UNITS "bytes"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The amount of user level traffic measured in bytes received
by the SA. This is the number of bytes of the uncompressed
IP packet, including the original IP header of that
uncompressed packet."

::= { ipsecSaIpcompOutEntry 15 }

ipsecSaIpcompOutUserPackets OBJECT-TYPE

SYNTAX Counter64

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets received for handling by the SA. This includes packets that were both compressed and not compressed."

::= { ipsecSaIpcompOutEntry 16 }

ipsecSaIpcompOutOutputOctets OBJECT-TYPE

SYNTAX Counter64

UNITS "bytes"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The amount of traffic measured in bytes output by the SA. This includes byte counts from packets compressed by the SA and also packets not modified by the SA."

This object can be divided into the ipsecSaIpcompOutUserOctets object to get a compression performance metric for the SA."

::= { ipsecSaIpcompOutEntry 17 }

ipsecSaIpcompOutCompressedPackets OBJECT-TYPE

SYNTAX Counter64

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets sent from the SA that were compressed."

The number of packets sent from the SA that were not compressed can be calculated by subtracting the value of this object from the value of ipsecSaIpcompOutUserPackets."

::= { ipsecSaIpcompOutEntry 18 }

ipsecSaIpcompOutCompressedOctets OBJECT-TYPE

SYNTAX Counter64

UNITS "bytes"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The amount of traffic measured in bytes output by the SA that is in packets that were compressed."

The amount of uncompressed traffic can be calculated by subtracting the value of this object from the value of ipsecSaIpcompOutOutputOctets."

::= { ipsecSaIpcompOutEntry 19 }

```
-- optional tables for monitoring network performance via statistics
-- on the anti-replay counter mechanisms in incoming ESP and AH SAs.
--
```

```
--
-- ESP table
--
```

```
ipsecSaEspReplayTable OBJECT-TYPE
```

```
    SYNTAX      SEQUENCE OF IpsecSaEspReplayEntry
```

```
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "The (conceptual) table containing information on the replay
        counter events on IPsec inbound ESP SAs.
```

```
        There should be one row in this table for every inbound ESP
        security association where ipsecSaEspInRepWinSize is non-
        zero in ipsecSaEspInTable. The maximum number of rows is
        implementation dependent.
```

```
        If any variable in this table is non-zero, it indicates that
        the underlying IP network is reordering, losing, or
        duplicating packets. While these are perfectly legal things
        for it to do, they can and will affect the performance of
        this security association."
```

```
 ::= { saTables 8 }
```

```
ipsecSaEspReplayEntry OBJECT-TYPE
```

```
    SYNTAX      IpsecSaEspReplayEntry
```

```
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
```

```
    DESCRIPTION
```

```
        "An entry (conceptual row) containing the information on the
        replay counter events in a particular IPsec inbound ESP SA.
```

```
        A row in this table cannot be created or deleted by SNMP
        operations on columns of the table."
```

```
    INDEX      {
                ipsecSaEspInAddressType,
                ipsecSaEspInAddress,
                ipsecSaEspInSpi
            }
```

```
 ::= { ipsecSaEspReplayTable 1 }
```

```
IpsecSaEspReplayEntry ::= SEQUENCE {
```

```
-- event counters
```

```
ipsecSaEspReplaysBeyondWindow    Counter32,
```

```
ipsecSaEspReplaysOutOfOrder      Counter32,
```

```
-- error counters
ipsecSaEspReplaysBeforeWindow Counter32,
ipsecSaEspReplaysDuplicate Counter32,
ipsecSaEspReplaysZero Counter32
}
```

ipsecSaEspReplaysBeyondWindow OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of packets received on this SA where the anti-
    replay value in the packet was greater than the previous
    highest received anti-replay value by the replay window size
    or greater.

    This may be caused by either significant packet losses by
    the IP network, or by major reordering of packets."
REFERENCE "RFC 2401 Appendix C: /* This packet has a 'way
larger' */ "
 ::= { ipsecSaEspReplayEntry 1 }
```

ipsecSaEspReplaysOutOfOrder OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of packets received on this SA where the anti-
    replay value in the packet was less than the highest
    received value, but was within the replay window.

    This may be caused by packet reordering by the IP network."
REFERENCE "RFC 2401 Appendix C: /* out of order but good */ "
 ::= { ipsecSaEspReplayEntry 2 }
```

ipsecSaEspReplaysBeforeWindow OBJECT-TYPE

```
SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The number of packets received on this SA where the anti-
    replay value in the packet was less than the previous
    highest received anti-replay value by at least the replay
    window size.

    This may be caused by significant packet reordering by the
    IP network, very delayed packet duplication, or by a replay
    attack."
```

The object ipsecSaEspInReplayErrors (of same INDEX) will be incremented by one each time this object is incremented."
REFERENCE ["RFC 2401 Appendix C: /* too old or wrapped */ "](#)
::= { ipsecSaEspReplayEntry 3 }

ipsecSaEspReplaysDuplicate OBJECT-TYPE

SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The number of packets received on this SA where the anti-replay value in the packet was within the replay window size, and the same anti-replay value had already been seen.

 This may be caused by packet duplication by the IP network, or by a replay attack.

 The object ipsecSaEspInReplayErrors (of same INDEX) will be incremented by one each time this object is incremented."
REFERENCE ["RFC 2401 Appendix C: /* already seen */ "](#)
::= { ipsecSaEspReplayEntry 4 }

ipsecSaEspReplaysZero OBJECT-TYPE

SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION
 "The number of packets received on this SA where the anti-replay value in the packet is zero.

 This may be caused by a programming error at the remote node causing it to send an initial anti-replay value of 0, or continuing to transmit after the anti-replay counter wraps.

 The object ipsecSaEspInReplayErrors (of same INDEX) will be incremented by one each time this object is incremented."
REFERENCE ["RFC 2401 Appendix C: /* first == 0 or wrapped */ "](#)
::= { ipsecSaEspReplayEntry 5 }

--
-- AH table
--

ipsecSaAhReplayTable OBJECT-TYPE

SYNTAX SEQUENCE OF IpsecSaAhReplayEntry
MAX-ACCESS not-accessible
STATUS current

DESCRIPTION

"The (conceptual) table containing information on the replay counter events on IPsec inbound AH SAs.

There should be one row in this table for every inbound AH security association where ipsecSaAhInRepWinSize is non-zero in ipsecSaAhInTable. The maximum number of rows is implementation dependent.

If any variable in this table is non-zero, it indicates that the underlying IP network is reordering, losing, or duplicating packets. While these are perfectly legal things for it to do, they can and will affect the performance of this security association."

::= { saTables 9 }

ipsecSaAhReplayEntry OBJECT-TYPE

SYNTAX IpsecSaAhReplayEntry

MAX-ACCESS not-accessible

STATUS current

DESCRIPTION

"An entry (conceptual row) containing the information on the replay counter events in a particular IPsec inbound AH SA.

A row in this table cannot be created or deleted by SNMP operations on columns of the table."

INDEX {
 ipsecSaAhInAddressType,
 ipsecSaAhInAddress,
 ipsecSaAhInSpi
}

::= { ipsecSaAhReplayTable 1 }

IpsecSaAhReplayEntry ::= SEQUENCE {

-- event counters

ipsecSaAhReplaysBeyondWindow Counter32,

ipsecSaAhReplaysOutOfOrder Counter32,

-- error counters

ipsecSaAhReplaysBeforeWindow Counter32,

ipsecSaAhReplaysDuplicate Counter32,

ipsecSaAhReplaysZero Counter32

}

ipsecSaAhReplaysBeyondWindow OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets received on this SA where the anti-replay value in the packet was greater than the previous highest received anti-replay value by the replay window size or greater.

This may be caused by either significant packet losses by the IP network, or by major reordering of packets."

REFERENCE "[RFC 2401 Appendix C](#): /* This packet has a way larger */ "

::= { ipsecSaAhReplayEntry 1 }

ipsecSaAhReplaysOutOfOrder OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets received on this SA where the anti-replay value in the packet was less than the highest received value, but was within the replay window.

This may be caused by packet reordering by the IP network."

REFERENCE "[RFC 2401 Appendix C](#): /* out of order but good */ "

::= { ipsecSaAhReplayEntry 2 }

ipsecSaAhReplaysBeforeWindow OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets received on this SA where the anti-replay value in the packet was less than the previous highest received anti-replay value by at least the replay window size.

This may be caused by significant packet reordering by the IP network, very delayed packet duplication, or by a replay attack.

The object ipsecSaAhInReplayErrors (of same INDEX) will be incremented by one each time this object is incremented."

REFERENCE "[RFC 2401 Appendix C](#): /* too old or wrapped */ "

::= { ipsecSaAhReplayEntry 3 }

ipsecSaAhReplaysDuplicate OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets received on this SA where the anti-replay value in the packet was within the replay window size, and the same anti-replay value had already been seen.

This may be caused by packet duplication by the IP network, or by a replay attack.

The object ipsecSaAhInReplayErrors (of same INDEX) will be incremented by one each time this object is incremented."

REFERENCE ["RFC 2401 Appendix C: /* already seen */ "](#)
::= { ipsecSaAhReplayEntry 4 }

ipsecSaAhReplaysZero OBJECT-TYPE

SYNTAX Counter32

UNITS "packets"

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The number of packets received on this SA where the anti-replay value in the packet is zero.

This may be caused by a programming error at the remote node causing it to send an initial anti-replay value of 0, or continuing to transmit after the anti-replay counter wraps.

The object ipsecSaAhInReplayErrors (of same INDEX) will be incremented by one each time this object is incremented."

REFERENCE ["RFC 2401 Appendix C: /* first == 0 or wrapped */ "](#)
::= { ipsecSaAhReplayEntry 5 }

--

-- entity IPsec statistics

--

ipsecEspCurrentInboundSAs OBJECT-TYPE

SYNTAX Gauge32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The current number of inbound ESP SAs in the entity."

::= { saStatistics 1 }

ipsecEspTotalInboundSAs OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The total number of inbound ESP SAs created in the entity since boot time."

```
::= { saStatistics 2 }
```

ipsecEspCurrentOutboundSAs OBJECT-TYPE

SYNTAX Gauge32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The current number of outbound ESP SAs in the entity."

```
::= { saStatistics 3 }
```

ipsecEspTotalOutboundSAs OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The total number of outbound ESP SAs created in the entity
since boot time."

```
::= { saStatistics 4 }
```

ipsecAhCurrentInboundSAs OBJECT-TYPE

SYNTAX Gauge32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The current number of inbound AH SAs in the entity."

```
::= { saStatistics 5 }
```

ipsecAhTotalInboundSAs OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The total number of inbound AH SAs created in the entity
since boot time."

```
::= { saStatistics 6 }
```

ipsecAhCurrentOutboundSAs OBJECT-TYPE

SYNTAX Gauge32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The current number of outbound AH SAs in the entity."

```
::= { saStatistics 7 }
```

ipsecAhTotalOutboundSAs OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The total number of outbound AH SAs created in the entity

```

        since boot time."
    ::= { saStatistics 8 }

ipsecIpcompCurrentInboundSAs OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The current number of inbound IPcomp SAs in the entity."
    ::= { saStatistics 9 }

ipsecIpcompTotalInboundSAs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The total number of inbound IPcomp SAs created in the
        entity since boot time."
    ::= { saStatistics 10 }

ipsecIpcompCurrentOutboundSAs OBJECT-TYPE
    SYNTAX      Gauge32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The current number of outbound IPcomp SAs in the entity."
    ::= { saStatistics 11 }

ipsecIpcompTotalOutboundSAs OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The total number of outbound IPcomp SAs created in the
        entity since boot time."
    ::= { saStatistics 12 }

--
-- IPsec error counts
--

ipsecDecryptionErrors OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "packets"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "The total number of packets received by the entity in SAs
        since boot time with detectable decryption errors. Not all

```

decryption errors are detectable within SA processing, so
this count should not be considered definitive."
::= { saErrors 1 }

ipsecAuthenticationErrors OBJECT-TYPE

SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The total number of packets received by the entity in SAs
since boot time with authentication errors.

This includes all packets in which the hash value is
determined to be invalid, for both ESP and AH SAs."

::= { saErrors 2 }

ipsecReplayErrors OBJECT-TYPE

SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The total number of packets received by the entity in SAs
since boot time with replay errors."

::= { saErrors 3 }

ipsecPolicyErrors OBJECT-TYPE

SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The total number of packets received by the entity in SAs
since boot time and discarded due to policy errors. This
includes packets that had selectors that were invalid for
the SA that carried them, and also includes packets that
arrived at the entity in the clear and that should have been
protected by IPsec or should have been dropped."

::= { saErrors 4 }

ipsecOtherReceiveErrors OBJECT-TYPE

SYNTAX Counter32
UNITS "packets"
MAX-ACCESS read-only
STATUS current
DESCRIPTION

"The total number of packets received by the entity in SAs
since boot time and discarded due to errors not due to
decryption, authentication, replay or policy."

```

        ::= { saErrors 5 }

ipsecSendErrors OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets to be sent by the entity in SAs
        since boot time and discarded due to errors."
    ::= { saErrors 6 }

ipsecUnknownSpiErrors OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The total number of packets received by the entity since
        boot time with SPIs or CPIs that were not valid."
    ::= { saErrors 7 }

--
-- traps
--

--
-- some objects used in trap reporting
--

ipsecSecurityProtocol OBJECT-TYPE
    SYNTAX      IppsecDoiSecProtocolId
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "A security protocol associated with the trap."
    ::= { saTrapObjects 1 }

ipsecSPI OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "An SPI associated with a trap. Where the security protocol
        associated with the trap is IPcomp, this value has a maximum
        of 65535."
    ::= { saTrapObjects 2 }

ipsecLocalAddressType OBJECT-TYPE
    SYNTAX      InetAddressType

```

```

MAX-ACCESS    accessible-for-notify
STATUS        current
DESCRIPTION
    "The type of a local IP address associated with a trap."
::= { saTrapObjects 3 }

ipsecLocalAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE (4|16|20))
    MAX-ACCESS  accessible-for-notify
    STATUS      current

    DESCRIPTION
        "A local IP address associated with a trap."
        ::= { saTrapObjects 4 }

ipsecPeerAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "The type of a peer IP address associated with a trap."
        ::= { saTrapObjects 5 }

ipsecPeerAddress OBJECT-TYPE
    SYNTAX      InetAddress (SIZE (4|16|20))
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "A peer IP address associated with a trap."
        ::= { saTrapObjects 6 }

--
-- trap control
--

espAuthFailureTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Indicates whether espAuthFailureTrap traps should be
        generated."
    DEFVAL { false }
    ::= { saTrapControl 1 }

ahAuthFailureTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION

```

```

        "Indicates whether ahAuthFailureTrap traps should be
        generated."
    DEFVAL { false }
    ::= { saTrapControl 2 }

espReplayFailureTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Indicates whether espReplayFailureTrap traps should be
        generated."
    DEFVAL { false }
    ::= { saTrapControl 3 }

ahReplayFailureTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Indicates whether ahReplayFailureTrap traps should be
        generated."
    DEFVAL { false }
    ::= { saTrapControl 4 }

espPolicyFailureTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Indicates whether espPolicyFailureTrap traps should be
        generated."
    DEFVAL { false }
    ::= { saTrapControl 5 }

ahPolicyFailureTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Indicates whether ahPolicyFailureTrap traps should be
        generated."
    DEFVAL { false }
    ::= { saTrapControl 6 }

invalidSpiTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Indicates whether invalidSpiTrap traps should be

```

```

        generated."
    DEFVAL { false }
    ::= { saTrapControl 7 }

otherPolicyFailureTrapEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Indicates whether otherPolicyFailureTrap traps should be
        generated."
    DEFVAL { false }
    ::= { saTrapControl 8 }

--
-- the traps themselves
--

espAuthFailureTrap NOTIFICATION-TYPE
    OBJECTS {
        ipsecSaEspInAuthErrors
    }
    STATUS      current
    DESCRIPTION
        "IPsec packets with invalid hashes were found in an inbound
        ESP SA. The total number of authentication errors
        accumulated is sent for the specific row of the
        ipsecSaEspInTable table for the SA; this provides the
        identity of the SA in which the error occurred.

        Implementations SHOULD send one trap per SA (within a
        reasonable time period), rather than sending one trap per
        packet."
    ::= { saTraps 0 1 }

ahAuthFailureTrap NOTIFICATION-TYPE
    OBJECTS {
        ipsecSaAhInAuthErrors
    }
    STATUS      current
    DESCRIPTION
        "IPsec packets with invalid hashes were found in an inbound
        AH SA. The total number of authentication errors accumulated
        is sent for the specific row of the ipsecSaAhInTable table
        for the SA; this provides the identity of the SA in which
        the error occurred.

        Implementations SHOULD send one trap per SA (within a
        reasonable time period), rather than sending one trap per
        packet."
    ::= { saTraps 0 2 }

```

espReplayFailureTrap NOTIFICATION-TYPE

```
OBJECTS {
    ipsecSaEspInReplayErrors
}
STATUS      current
DESCRIPTION
    "IPsec packets with invalid sequence numbers were found in
    an inbound ESP SA. The total number of replay errors
    accumulated is sent for the specific row of the
    ipsecSaEspInTable table for the SA; this provides the
    identity of the SA in which the error occurred.

    Implementations SHOULD send one trap per SA (within a
    reasonable time period), rather than sending one trap per
    packet."
::= { saTraps 0 3 }
```

ahReplayFailureTrap NOTIFICATION-TYPE

```
OBJECTS {
    ipsecSaAhInReplayErrors
}
STATUS      current
DESCRIPTION
    "IPsec packets with invalid sequence numbers were found in
    the specified AH SA. The total number of replay errors
    accumulated is sent for the specific row of the
    ipsecSaAhInTable table for the SA; this provides the
    identity of the SA in which the error occurred.

    Implementations SHOULD send one trap per SA (within a
    reasonable time period), rather than sending one trap per
    packet."
::= { saTraps 0 4 }
```

espPolicyFailureTrap NOTIFICATION-TYPE

```
OBJECTS {
    ipsecSaEspInPolicyErrors
}
STATUS      current
DESCRIPTION
    "IPsec packets carrying packets with invalid selectors for
    the specified ESP SA were found. The total number of policy
    errors accumulated is sent for the specific row of the
    ipsecSaEspInTable table for the SA; this provides the
    identity of the SA in which the error occurred.

    Implementations SHOULD send one trap per SA (within a
    reasonable time period), rather than sending one trap per
    packet."
::= { saTraps 0 5 }
```

ahPolicyFailureTrap NOTIFICATION-TYPE

```
OBJECTS {
    ipsecSaAhInPolicyErrors
}
STATUS      current
DESCRIPTION
    "IPsec packets carrying packets with invalid selectors for
    the specified AH SA were found. The total number of policy
    errors accumulated is sent for the specific row of the
    ipsecSaAhInTable table for the SA; this provides the
    identity of the SA in which the error occurred.

    Implementations SHOULD send one trap per SA (within a
    reasonable time period), rather than sending one trap per
    packet."
::= { saTraps 0 6 }
```

espInvalidSpiTrap NOTIFICATION-TYPE

```
OBJECTS {
    ipsecLocalAddress,
    ipsecSecurityProtocol,
    ipsecPeerAddress,
    ipsecSPI,
    ifIndex
}
STATUS      current
DESCRIPTION
    "A packet with an unknown SPI was detected from the
    specified peer with the specified SPI using the specified
    protocol. The destination address of the received packet is
    specified by ipsecLocalAddress.

    The value ifIndex may be 0 if this optional linkage is
    unsupported.

    If the object ipsecSecurityProtocol has the value for
    IPcomp, then the ipsecSPI object is the CPI of the packet.

    Implementations SHOULD send one trap per peer (within a
    reasonable time period), rather than sending one trap per
    packet."
::= { saTraps 0 7 }
```

otherPolicyFailureTrap NOTIFICATION-TYPE

```
OBJECTS {
    ipsecPolicyErrors,
    ipsecPeerAddress,
    ipsecLocalAddress
}
STATUS      current
```

DESCRIPTION

"Clear packets were found that should not have been sent to the entity in the clear. The total number of policy errors accumulated by the entity is sent, along with the source and destination addresses of the packet that triggered the trap.

Implementations SHOULD send one trap per source address pair (within a reasonable time period), rather than sending one trap per packet."

::= { saTraps 0 8 }

--

-- Units of Conformance (Object Groups)

--

--

-- Authors' note: Index objects are commented out, since the current SMI does not allow objects with a MAX-ACCESS clause of 'not-accessible' to be put in groups.

--

selectorGroup OBJECT-GROUP

OBJECTS

```
{
    -- selectorIndex,
    selectorLocalId, selectorLocalIdType, selectorRemoteId,
    selectorRemoteIdType, selectorProtocol, selectorLocalPort,
    selectorRemotePort
}
```

STATUS current

DESCRIPTION

"A collection of objects that describe IKE phase 2 selectors."

::= { saGroups 1 }

ipsecSaEspGroup OBJECT-GROUP

OBJECTS

```
{
    -- ipsecSaEspInAddressType, ipsecSaEspInAddress,
    -- ipsecSaEspInSpi,
    ipsecSaEspInSelector, ipsecSaEspInCreator,
    ipsecSaEspInEncapsulation, ipsecSaEspInEncAlg,
    ipsecSaEspInEncKeyLength, ipsecSaEspInAuthAlg,
    ipsecSaEspInAuthKeyLength, ipsecSaEspInRepWinSize,
    ipsecSaEspInLimitSeconds, ipsecSaEspInLimitKbytes,
    ipsecSaEspInAccSeconds, ipsecSaEspInAccKbytes,
    ipsecSaEspInUserOctets, ipsecSaEspInPackets,
    ipsecSaEspInDecryptErrors, ipsecSaEspInAuthErrors,
    ipsecSaEspInReplayErrors, ipsecSaEspInPolicyErrors,
    ipsecSaEspInPadErrors, ipsecSaEspInOtherReceiveErrors,
    -- ipsecSaEspOutAddressType, ipsecSaEspOutAddress,
    -- ipsecSaEspOutSpi,
```

```

    ipsecSaEspOutSelector, ipsecSaEspOutCreator,
    ipsecSaEspOutEncapsulation, ipsecSaEspOutEncAlg,
    ipsecSaEspOutAuthKeyLength, ipsecSaEspOutEncKeyLength,
    ipsecSaEspOutAuthAlg, ipsecSaEspOutLimitSeconds,
    ipsecSaEspOutLimitKbytes, ipsecSaEspOutAccSeconds,
    ipsecSaEspOutAccKbytes, ipsecSaEspOutUserOctets,
    ipsecSaEspOutPackets, ipsecSaEspOutSendErrors,
    ipsecEspCurrentInboundSAs, ipsecEspTotalInboundSAs,
    ipsecEspCurrentOutboundSAs, ipsecEspTotalOutboundSAs
}
STATUS          current
DESCRIPTION
    "A collection of objects that describe the state of the
    security associations of the ESP protocol."
:= { saGroups 2 }

ipsecSaAhGroup OBJECT-GROUP
OBJECTS      {
    -- ipsecSaAhInAddressType, ipsecSaAhInAddress,
    -- ipsecSaAhInSpi,
    ipsecSaAhInSelector, ipsecSaAhInCreator,
    ipsecSaAhInEncapsulation, ipsecSaAhInAuthAlg,
    ipsecSaAhInAuthKeyLength, ipsecSaAhInRepWinSize,
    ipsecSaAhInLimitSeconds, ipsecSaAhInLimitKbytes,
    ipsecSaAhInAccSeconds, ipsecSaAhInAccKbytes,
    ipsecSaAhInUserOctets, ipsecSaAhInPackets,
    ipsecSaAhInAuthErrors, ipsecSaAhInReplayErrors,
    ipsecSaAhInPolicyErrors, ipsecSaAhInOtherReceiveErrors,
    -- ipsecSaAhOutAddressType, ipsecSaAhOutAddress,
    -- ipsecSaAhOutSpi,
    ipsecSaAhOutSelector, ipsecSaAhOutCreator,
    ipsecSaAhOutEncapsulation, ipsecSaAhOutAuthAlg,
    ipsecSaAhOutAuthKeyLength, ipsecSaAhOutLimitSeconds,
    ipsecSaAhOutLimitKbytes, ipsecSaAhOutAccSeconds,
    ipsecSaAhOutAccKbytes, ipsecSaAhOutUserOctets,
    ipsecSaAhOutPackets, ipsecSaAhOutSendErrors,
    ipsecAhCurrentInboundSAs, ipsecAhTotalInboundSAs,
    ipsecAhCurrentOutboundSAs, ipsecAhTotalOutboundSAs
}
STATUS          current

DESCRIPTION
    "A collection of objects that describe the state of the
    security associations of the AH protocol."
:= { saGroups 3 }

ipsecSaIpcompGroup OBJECT-GROUP
OBJECTS      {
    -- ipsecSaIpcompInAddressType, ipsecSaIpcompInAddress,
    -- ipsecSaIpcompInCpi,

```

```

    ipsecSaIpcmpInSelector, ipsecSaIpcmpInCreator,
    ipsecSaIpcmpInEncapsulation, ipsecSaIpcmpInDecompAlg,
    ipsecSaIpcmpInSeconds, ipsecSaIpcmpInInputOctets,
    ipsecSaIpcmpInUserOctets, ipsecSaIpcmpInUserPackets,
    ipsecSaIpcmpInCompressedPackets,
    ipsecSaIpcmpInCompressedOctets,
    ipsecSaIpcmpInDecompErrors,
    ipsecSaIpcmpInOtherReceiveErrors,
    -- ipsecSaIpcmpOutAddressType, ipsecSaIpcmpOutAddress,
    -- ipsecSaIpcmpOutCpi,
    ipsecSaIpcmpOutSelector, ipsecSaIpcmpOutCreator,
    ipsecSaIpcmpOutEncapsulation, ipsecSaIpcmpOutCompAlg,
    ipsecSaIpcmpOutSeconds, ipsecSaIpcmpOutUserOctets,
    ipsecSaIpcmpOutOutputOctets, ipsecSaIpcmpOutUserPackets,
    ipsecSaIpcmpOutCompressedPackets,
    ipsecSaIpcmpOutCompressedOctets,
    ipsecIpcmpCurrentInboundSAs, ipsecIpcmpTotalInboundSAs,
    ipsecIpcmpCurrentOutboundSAs, ipsecIpcmpTotalOutboundSAs
}
STATUS      current
DESCRIPTION
    "A collection of objects that describe the state of the
    security associations of the IPcomp protocol."
::= { saGroups 4 }

ipsecSaErrorsGroup OBJECT-GROUP
OBJECTS      {
    ipsecDecryptionErrors, ipsecAuthenticationErrors,
    ipsecReplayErrors, ipsecPolicyErrors,
    ipsecOtherReceiveErrors, ipsecUnknownSpiErrors,
    ipsecSendErrors
}
STATUS      current
DESCRIPTION
    "A collection of objects providing global IPsec error
    counters."
::= { saGroups 5 }

ipsecSaFailureTrapEnableGroup OBJECT-GROUP
OBJECTS      {
    espAuthFailureTrapEnable, ahAuthFailureTrapEnable,
    espReplayFailureTrapEnable, ahReplayFailureTrapEnable,
    espPolicyFailureTrapEnable, ahPolicyFailureTrapEnable,
    invalidSpiTrapEnable, otherPolicyFailureTrapEnable
}
STATUS      current
DESCRIPTION
    "A collection of objects providing control over trap
    generation."
::= { saGroups 6 }

```

```

ipsecSaTrapArgumentGroup OBJECT-GROUP
    OBJECTS      {
        ipsecSecurityProtocol, ipsecSPI, ipsecLocalAddressType,
        ipsecLocalAddress, ipsecPeerAddressType, ipsecPeerAddress
    }
    STATUS        current
    DESCRIPTION
        "A collection of objects used only as arguments in traps."
    ::= { saGroups 7 }

ipsecSaEspReplayGroup OBJECT-GROUP
    OBJECTS      {
        ipsecSaEspReplaysBeyondWindow, ipsecSaEspReplaysOutOfOrder,
        ipsecSaEspReplaysBeforeWindow, ipsecSaEspReplaysDuplicate,
        ipsecSaEspReplaysZero
    }
    STATUS        current
    DESCRIPTION
        "A collection of objects used to monitor anti-replay events
        on inbound ESP SAs."
    ::= { saGroups 8 }

ipsecSaAhReplayGroup OBJECT-GROUP
    OBJECTS      {
        ipsecSaAhReplaysBeyondWindow, ipsecSaAhReplaysOutOfOrder,
        ipsecSaAhReplaysBeforeWindow, ipsecSaAhReplaysDuplicate,
        ipsecSaAhReplaysZero
    }
    STATUS        current
    DESCRIPTION
        "A collection of objects used to monitor anti-replay events
        on inbound AH SAs."
    ::= { saGroups 9 }

ipsecSaFailureTrapGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
        espAuthFailureTrap, ahAuthFailureTrap, espReplayFailureTrap,
        ahReplayFailureTrap, espPolicyFailureTrap,
        ahPolicyFailureTrap, espInvalidSpiTrap,
        otherPolicyFailureTrap
    }
    STATUS        current
    DESCRIPTION
        "A collection of traps."
    ::= { saGroups 10 }

--
-- Compliance statements

```

--

ipsecSaMonitorCompliance MODULE-COMPLIANCE

STATUS current

DESCRIPTION

"The compliance statement for SNMPv2 entities which implement the IPsec Monitoring MIB."

MODULE -- this module

MANDATORY-GROUPS {

selectorGroup, ipsecSaEspGroup, ipsecSaAhGroup,
ipsecSaErrorsGroup, ipsecSaFailureTrapEnableGroup,
ipsecSaTrapArgumentGroup, ipsecSaFailureTrapGroup

}

-- Anti-replay monitoring tables are optional

GROUP ipsecSaEspReplayGroup

DESCRIPTION

"This group is optional, to be implemented on those systems which want to provide detailed counters for specific unusual and error events in the anti-replay monitoring function for ESP SAs."

GROUP ipsecSaAhReplayGroup

DESCRIPTION

"This group is optional, to be implemented on those systems which want to provide detailed counters for specific unusual and error events in the anti-replay monitoring function for AH SAs."

GROUP ipsecSaIpcompGroup

DESCRIPTION

"This group is mandatory only for those systems that implement the IPcomp protocol as a part of the IPsec suite."

-- DNS names support is not required

-- Authors' note: The following statements are commented out,
-- since the current SMI does not allow objects with a
-- MAX-ACCESS clause of not-accessible to be put in groups,
-- and objects that are not in groups cannot be in
-- compliance statements.

-- OBJECT ipsecSaEspInAddressType

-- SYNTAX INTEGER { ipv4(1), ipv6(2) }

-- DESCRIPTION

-- "An implementation is only required to support IPv4
-- and IPv6 addresses."

```

-- OBJECT ipsecSaAhInAddressType
--     SYNTAX INTEGER { ipv4(1), ipv6(2) }
--     DESCRIPTION
--         "An implementation is only required to support IPv4
--         and IPv6 addresses."

-- OBJECT ipsecSaIpcompInAddressType
--     SYNTAX INTEGER { unknown(0), ipv4(1), ipv6(2) }
--     DESCRIPTION
--         "An implementation is only required to support IPv4
--         and IPv6 addresses. Also, if it supports IPcomp SAs,
--         it must be able to support an unknown address type
--         for IPcomp SAs that may be shared across security
--         association suites."

-- OBJECT ipsecSaEspOutAddressType
--     SYNTAX INTEGER { ipv4(1), ipv6(2) }
--     DESCRIPTION
--         "An implementation is only required to support IPv4
--         and IPv6 addresses."

-- OBJECT ipsecSaAhOutAddressType
--     SYNTAX INTEGER { ipv4(1), ipv6(2) }
--     DESCRIPTION
--         "An implementation is only required to support IPv4
--         and IPv6 addresses."

-- OBJECT ipsecSaIpcompOutAddressType
--     SYNTAX INTEGER { unknown(0), ipv4(1), ipv6(2) }
--     DESCRIPTION
--         "An implementation is only required to support IPv4
--         and IPv6 addresses. Also, if it supports IPcomp SAs,
--         it must be able to support an unknown address type
--         for IPcomp SAs that may be shared across security
--         association suites."

-- OBJECT ipsecLocalAddressType
--     SYNTAX INTEGER { ipv4(1), ipv6(2) }
--     DESCRIPTION
--         "An implementation is only required to support IPv4
--         and IPv6 addresses."

-- OBJECT ipsecPeerAddressType
--     SYNTAX INTEGER { ipv4(1), ipv6(2) }
--     DESCRIPTION
--         "An implementation is only required to support IPv4
--         and IPv6 addresses."

```

```

-- Allow all the trap controls to be read-only

```

OBJECT espAuthFailureTrapEnable
MIN-ACCESS read-only
DESCRIPTION
"If an implementation cannot properly secure this variable against unauthorized write access, it SHOULD implement it as read-only, to prevent the security risk of enabling the traps. Of course, there must be other means of controlling the generation of the associated trap."

OBJECT ahAuthFailureTrapEnable
MIN-ACCESS read-only
DESCRIPTION
"If an implementation cannot properly secure this variable against unauthorized write access, it SHOULD implement it as read-only, to prevent the security risk of enabling the traps. Of course, there must be other means of controlling the generation of the associated trap."

OBJECT espReplayFailureTrapEnable
MIN-ACCESS read-only
DESCRIPTION
"If an implementation cannot properly secure this variable against unauthorized write access, it SHOULD implement it as read-only, to prevent the security risk of enabling the traps. Of course, there must be other means of controlling the generation of the associated trap."

OBJECT ahReplayFailureTrapEnable
MIN-ACCESS read-only
DESCRIPTION
"If an implementation cannot properly secure this variable against unauthorized write access, it SHOULD implement it as read-only, to prevent the security risk of enabling the traps. Of course, there must be other means of controlling the generation of the associated trap."

OBJECT espPolicyFailureTrapEnable
MIN-ACCESS read-only
DESCRIPTION
"If an implementation cannot properly secure this variable against unauthorized write access, it SHOULD implement it as read-only, to prevent the security risk of enabling the traps. Of course, there must be other means of controlling the generation of the associated trap."

OBJECT ahPolicyFailureTrapEnable

MIN-ACCESS read-only

DESCRIPTION

"If an implementation cannot properly secure this variable against unauthorized write access, it SHOULD implement it as read-only, to prevent the security risk of enabling the traps. Of course, there must be other means of controlling the generation of the associated trap."

OBJECT invalidSpiTrapEnable

MIN-ACCESS read-only

DESCRIPTION

"If an implementation cannot properly secure this variable against unauthorized write access, it SHOULD implement it as read-only, to prevent the security risk of enabling the traps. Of course, there must be other means of controlling the generation of the associated trap."

OBJECT otherPolicyFailureTrapEnable

MIN-ACCESS read-only

DESCRIPTION

"If an implementation cannot properly secure this variable against unauthorized write access, it SHOULD implement it as read-only, to prevent the security risk of enabling the traps. Of course, there must be other means of controlling the generation of the associated trap."

::= { saConformance 1 }

END

6. Security Considerations

This MIB contains readable objects whose values provide information related to IPsec SAs. While some of the information is readily available by monitoring the traffic into an entity, other information may provide attackers with more information than an administrator may desire.

Some of the specific concerns are related to the display of the algorithms and key lengths associated with encryption, and the feedback of error counters and traps that enable an attacker to quickly determine the effect of his or her attacks.

Specific examples of this include, but are not limited to:

- o Replay counts that tell attackers that replay values are being checked, and what the current window is.

- o Specific algorithms and key lengths are displayed, giving attackers a better idea of how to attack.
- o Specific traffic counts, giving attackers more information for traffic analysis.

Of particular concern is the ability to disable the transmission of traps. The traps defined in this MIB may appear due to badly configured systems and transient error conditions, but they may also appear due to attacks. If an attacker can disable these traps, they reduce some of the warnings that may be provided to system administrators.

It is thus important to control even GET access to these objects and possibly to even encrypt the values of these object when sending them over the network via SNMP. Not all versions of SNMP provide features for such a secure environment.

SNMPv1 by itself is not a secure environment. Even if the network itself is secure (for example by using IPsec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB.

It is recommended that the implementers consider the security features as provided by the SNMPv3 framework. Specifically, the use of the User-based Security Model [RFC 2574](#) [[RFC2574](#)] and the View-based Access Control Model [RFC 2575](#) [[RFC2575](#)] is recommended.

It is then a customer/user responsibility to ensure that the SNMP entity giving access to an instance of this MIB, is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

[7. Acknowledgments](#)

This document was begun and mostly developed by Tim Jenkins and John Shriver. The editor listed for this document (Paul Hoffman) only sheperded the last steps before final publication.

This document is based in part on an earlier proposal titled "[draft-ietf-ipsec-mib-xx.txt](#)". That series was abandoned, since it included application specific constructs in addition to the IPsec only objects.

Portions of the original document's origins were based on the working paper "IP Security Management Information Base" by R. Thayer and U. Blumenthal.

Contribution to the IPsec MIB series of documents comes from D.

McDonald, M. Baugher, C. Brooks, C. Powell, M. Daniele, T. Kivinen, J. Walker, S. Kelly, J. Leonard, M. Richardson, R. Charlet, S. Waters, M. Zallocco, R. Murphy and others participating in the IPsec WG.

8. References

8.1 Normative references

- [ADDRMIB] Daniele, M., Haberman, B., Routhier, S., Schoenwaelder, J., "Textual Conventions for Internet Network Addresses", [RFC 2851](#), June, 2000
- [IGMIB] McCloghrie, K., Kastenholz, F., "The Interfaces Group MIB using SMIV2", [RFC2233](#)
- [IPSECTC] Shriver, J., "IPsec DOI Textual Conventions MIB, [draft-ietf-ipsec-doi-tc-mib-05](#), work in progress
- [RFC1155] Rose, M., and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based Internets", STD 16, [RFC 1155](#), May 1990
- [RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", STD 15, [RFC 1157](#), May 1990.
- [RFC1212] Rose, M., and K. McCloghrie, "Concise MIB Definitions", STD 16, [RFC 1212](#), March 1991
- [RFC1215] M. Rose, "A Convention for Defining Traps for use with the SNMP", [RFC 1215](#), March 1991
- [RFC1901] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Introduction to Community-based SNMPv2", [RFC 1901](#), January 1996.
- [RFC1905] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1905](#), January 1996.
- [RFC1906] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)", [RFC 1906](#), January 1996.
- [RFC2570] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", [RFC 2570](#), April 1999
- [RFC2571] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", [RFC 2571](#), April 1999

- [RFC2572] Case, J., Harrington D., Presuhn R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", [RFC 2572](#), April 1999
- [RFC2573] Levi, D., Meyer, P., and B. Stewart, "SNMPv3 Applications", [RFC 2573](#), April 1999
- [RFC2574] Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", [RFC 2574](#), April 1999
- [RFC2575] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", [RFC 2575](#), April 1999
- [RFC2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, [RFC 2578](#), April 1999
- [RFC2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, [RFC 2579](#), April 1999
- [RFC2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, [RFC 2580](#), April 1999

8.2 Non-normative references

- [AH] Kent, S., Atkinson, R., "IP Authentication Header", [RFC 2402](#), November 1998
- [ESP] Kent, S., Atkinson, R., "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998
- [IKE] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", [RFC 2409](#), November 1998
- [IPCOMP] Shacham, A., Monsour, R., Pereira, R., Thomas, M., "IP Payload Compression Protocol (IPcomp)", [RFC 3173](#), September 2001
- [IPDOI] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", [RFC 2407](#), November 1998
- [ISAKMP] Maughan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)", [RFC 2408](#), November 1998
- [SECARCH] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998

[A.](#) Changes from -05 to -06

`[[ To be removed when published as an RFC ]]`

- Changed the authors' names to the editor's name.
- Added acknowledgement for the original authors.
- Minor formatting changes.
- Split the references into normative and non-normative.

NOTE: There are still lines that talk about things that need to be changed before release of the RFC (search for "release").