Internet Engineering Task Force
IPsec Working Group
INTERNET-DRAFT:
Expires in six months

C. Madson, Cisco Systems Inc.
L. Temoshenko, Cisco Systems.
C. Pellecuru, Cisco Systems.
B. Harrison, Tivoli Systems.
S. Ramakrishnan, Cisco Systems.
02 Mar 2003

**IPsec Flow Monitoring MIB**
**<draft-ietf-ipsec-flow-monitoring-mib-02.txt>**

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

This document is a submission to the IETF Internet Protocol Security Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@lists.tislabs.com) or to the editor(s).

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/1id-abstracts.html

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

To learn the current status of any Internet-Draft, please check the "id- abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2001-03). All Rights Reserved.

Abstract

This document describes a high-level MIB for monitoring, accounting trending and failure detection for IPsec-based networks. Optional features of the MIB include trending of IPsec-related metrics and archiving of VPN failures.

Table of Contents

# 1. Introduction

## 1.1. Overview

As VPN technology in the shape of IPsec is deployed, customers, particularly large enterprise and Service Providers, are requiring a standard way to monitor their VPNs. Service Providers in particular are often required to maintain service level agreements (SLAs) that guarantee quality and performance to their customers. In addition to this the provider must be able to accurately bill customers. Both enterprise customers and providers collect usage statistics for capacity planning and to ensure sufficient resources are available for redundancy and high availability.

This document defines a high level MIB for monitoring, trending and troubleshooting IPsec connections. The metrics defined by thi MIB may be used to identify trends and enforce service level agreements. The troubleshooting functionality is in the form of records of failure events and traps sent as a result of operational failures during the setting up, tearing down and normal lifetime of IPsec flows. It is meant as an indication of failure to the personnel of a Network Operation Center. This MIB does not present in-depth low level debugging and diagnostic support that may be used by implementers of IPsec, but rather, it may be seen as complementary to such a MIB. This MIB does not provide support for the configuration of IPsec-capable devices.

The definition presented is driven by customer requirements for a MIB encompassing statistics collection that may be used for accounting purposes, trending as well as status monitoring, error collection and real-time alerting via traps.

The MIB has been designed based on specific requirements from service providers that want to offer an outsourced VPN service to customers, with the main focuses being: provision of services in such a way that satisfies Service Level Agreements, support for a multi-vendor environment, and incorporation with existing network management software.

The MIB was designed in 1999 and has since evolved with the experience in its deployment in the field. While the MIB is likely to be deployed for managing IPsec VPNs, the MIB is not specifi to this application of IPsec. The MIB may be used equally well t manage any IPsec-based network.

Section 2 describes the architecture and abstractions defined by the MIB. This section is important for understanding the remaining

sections.

Section 3 describes various object groups defined in the MIB. These include the Levels group, the IPsec Phase-1 group, IPsec Phase-2 group, the history group, the VPN failure group and finally the notifications group. Important relationships between the groups have also been highlighted.

Section 4 lists the items that are planned to be included in the MI in the next revision.

Section 5 defines a collection of managed objects used to instrument IPsec structures and activities in the managed entity.

Sections 6, 7, 8, 9, 10 and 11 are administrative in nature.

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

## 1.2. The SNMPv2 Network Management Framework

The SNMP Management Framework presently consists of five major components:

1) An overall architecture, described in RFC 2271 [2271].

2) 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 RFC 1155 [1155], RFC 1212 [1212] and RFC 1215 [1215]. The second version, called SMIv2, is described in RFC 1902 [1902],RFC 1903 [1903] and RFC 1904 [1904].

3) Message protocols for transferring management information. The first version of the SNMP message protocol is called SNMPv1 and described in RFC 1157 [1157]. A second version of the SNMP message protocol, which is not an Internet standards track protocol, is called SNMPv2c and described in RFC 1901 [1901] and RFC 1906 [1906]. The third version of the message protocol is called SNMPv3 and described in RFC 1906 [1906], RFC 2272 [2272] and RFC 2274 [2274].

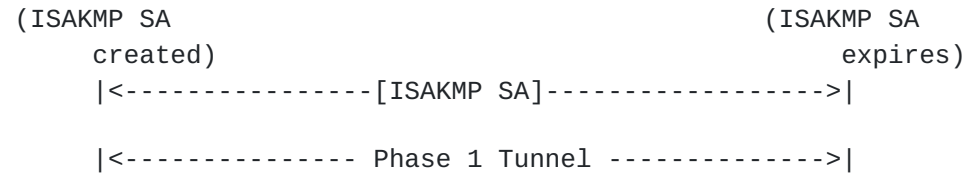
4) Protocol operations for accessing management information. The first set of protocol operations and associated PDU formats is described in RFC 1157 [1157]. A second set of protocol operations and associated PDU formats is described in RFC 1905 [1905].

5) A set of fundamental applications described in RFC 2273 [2273] and the view-based access control mechanism described in RFC 2275 [2275].

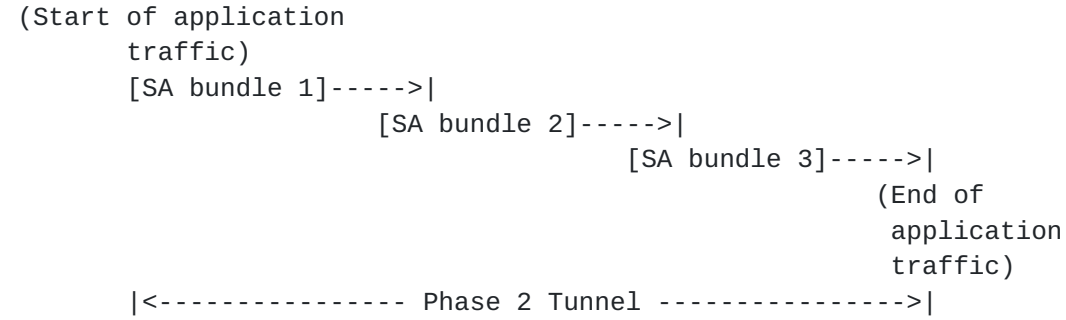
## 2. Architecture of the MIB

This section provides a view of the overall architecture, and describes the major MIB groups and table definitions. The MIB covers both Phase 1 Security Associations (SAs) and Phase 2 or IPsec SAs. An example of Phase 1 structures are the SAs created by the Interne Key Exchange (IKE) protocol.

The key component of this MIB is the abstraction of a traffic flow or a "tunnel". A tunnel signifies a sustained application traffic flow. A Phase 1 tunnel (IKE tunnel) is represented by a single ISAKMP SA which has been established after a successful completion of Phase 1. When the ISAKMP SA expires or is terminated, the tunnel is deeme to cease to exist as well.




In the context of Phase 2 SAs, an "IPsec tunnel" is defined as the virtual link formed by successsive Phase 2 SA bundles that share the same Phase 2 proxy identifiers. When the last SA budle expires and is not replaced by a new set of SA bundle, the tunnel is said to expire.




Another key component of this MIB is the monitoring of large numbers of dynamic tunnels. In the case of clients initiating connections to a gateway, it is not usually possible for the gateway to have

knowledge of all the attributes of the client, in particular the identity of the client, before the start of the session. The MIB must support these dynamic connections in addition to static tunnels that usually exist between gateway devices.

The information provided in the MIB includes statistics on individual SAs as well as global totals which allows the provider to report on individual customer SLAs as well as monitoring the overall health of the VPN service. Statistics are provided on packet counts and drops, notify messages, failures, deletes and exchanges between peers. This information is presented in the form of groups that cover specific aspects of the VPN to facilitate accurate evaluation of performance and the generation of meaningful reports.

### 2.1 Support for Different Control Protocols

This document uses the term Control Protocol to denote the protocol used to setup and maintain the IPsec (Phase 2) SAs. The architecture of the MIB supports the instrumentation of any control protocol. Th current version of the MIB defines an IKE group to support th deployment of IPsec with IKE. This is an optional group and henc need not be implemented to claim compliance with the MIB. As newe control protocols are standardized (IKEv2, KINK, etc), the module for these protocols can be plugged into this MIB as other optiona groups.

## 3. MIB Group Definitions

This section outlines the major MIB groups and table definitions. The MIB covers both Phase 1 or Internet key Exchange SAs and Phase 2 or IPsec SAs.

### 3.1. IPsec Levels Group

The Levels Group consists of global single instance objects accessed using an index of zero. Currently, the MIB Level object is the only object contained in this group. Initially the value of this object will be one (1) and incremented as changes are made to the MIB.

### 3.2. IPsec Phase-1 Group

Provides global statistics for all phase 1 tunnels, active and previous. The Internet Key Exchange Peer Table defines the peers involved in any Phase 1 tunnel associated with active Phase 2 tunnels. Statistics for each active phase 1 tunnel (including policy attributes) are contained in the IKE Tunnel table, and the IKE Peer

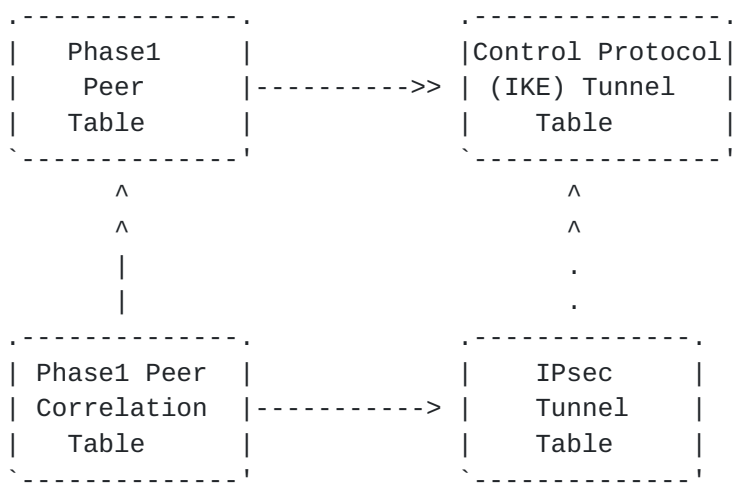
Association to Phase 2 Tunnel Correlation Table provides a link between each Phase 1 peer entry and any associated active Phase 2 tunnels.

ikeGlobalStats

All Phase 1 Tunnel Stats including statistics pertaining to IKE mode configuration.

```
ikeTunnelTable
            IkeTunnelEntry
            -----> ikePeerEntryTable
                        IkePeerEntry
                        -----> ikePeerCorrTable
                                    IkePeerCorrEntry
                                      -----> ipSecTunnelTable
                                               IpSecTunnelEntry
```

The relationships modeled in Phase-1 group are as follows:




Single arrow (>) represents a 1:1 relation. Double arrow represents a 1:n relationship. Dotted arrow (...) represents a relationship that is defined as a "softlink", i.e., a relationship that is implemented in the software but which is not enforced by SMI. The relationship between an IPsec tunnel and the Control tunnel that negotiated that IPsec tunnel is implemented using a softlink i order to facilitate "dangling" IPsec implementations (i.e. implementations where an ISAKMP SA may expire prior to the expiry o the Phase-2 SAs that were negotiated using the ISAKMP SA). Note tha control tunnel types other than IKE can be accomodated using thi architecture.

As the diagram above illustrates, there can be one or more IKE tunnels between a Phase 1 peer pair. There can be one or more IPsec tunnels between a given Phase 1 peer pair. When there are no Control (such as IKE) or IPsec tunnels to a peer, the peer entr corresponding to that peer is removed from the Phase 1 Peer table.

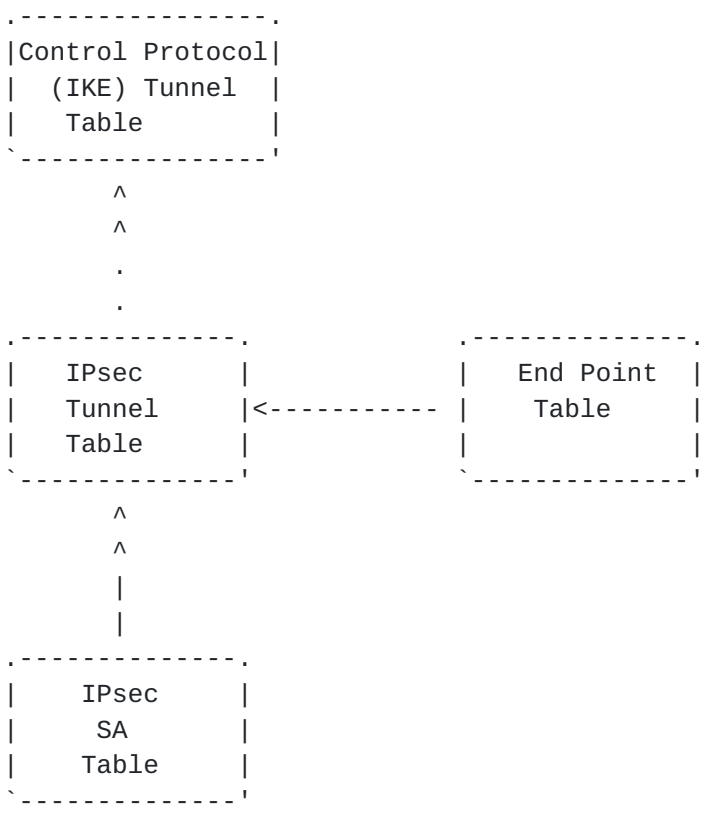
### 3.3. IPsec Phase-2 Group

This group defines six subgroups. The first is a Global Statistics table that accumulates statistics pertaining to various Phase-2 activities and tunnel statistics from all active and previous Phase 2 tunnels. The second group defines the active Phase 2 IPsec tunnel table. Each entry in this table corresponds to a single active Phase-2 IPsec flow on the managed entity and includes the algorithms used and counts of activities such as number of packets successfully encrypted or number of encryption failures. The tunnel endpoint table forms the third subgroup under Phase 2 group. This table identifies the clients using the active IPsec flows and the protocols riding on the flows. The clients are subnets, hosts or collection of IP addresses. The protocol for which the flow as setup is identified using the id of the protocol and the port number (eg: SMTP = TCP/25). Since endpoints are associated with active IPsec tunnels, each entry in te endpoint table refers to an entry in the active IPsec tunnel table.

The fourth subgroup under Phase-2 group is the IPsec security association table (ipSecSaTable). This table identifies the structure of each active IPsec tunnel by mapping the active IPsec tunnel into its component security associations. This table deprecates the previously defined ipSecSpiTable.

```
   ipSecGlobalStats

     All Phase 2 Tunnel Stats

     IpSecTunnelTable

       IpSecTunnelEntry

              -----> ipSecEndptTable
                           IpSecEntptEntry

                  -----> ipSecSaTable
                              IpSecSaEntry  (Inbound)
                              IpSecSaEntry  (Outbound)
```

The relationships modeled in Phase-1 group are as follows:



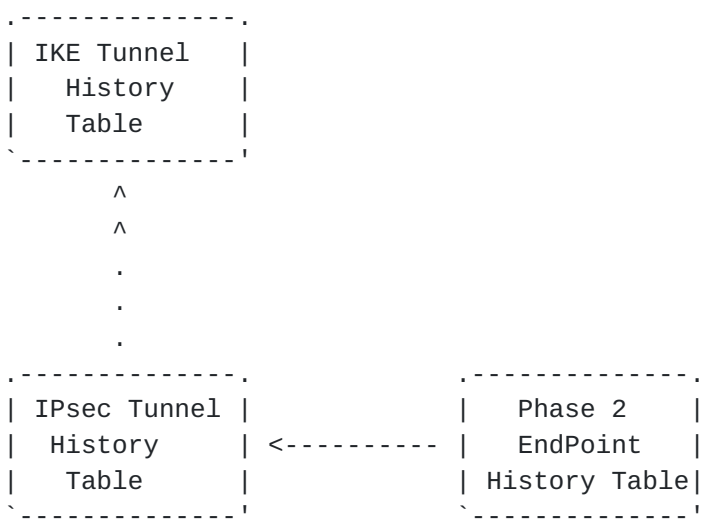

As the diagram above illustrates, for every entry in the End Point table, there is a unique entry in the active IPsec tunnel table. A number of entries in the IPsec SA table map to a specific entry in t he IPsec tunnel table. This is because an IPsec tunnel is composed of at least two Phase-2 security associations. Note also, that th relationshop between Phase-2 IPsec tunnels and Phase 2 IKE tunnels is n:1 and is implemented as a softlink, to accomodate dangling IPsec implementations.

## 3.4. IPsec History Group

This group includes tables for Phase-1 Tunnel History, Phase-2 Tunnel History, and Phase-2 Endpoint History. The number of entries in each table defined by the value of ipSecHistTablSize. The tables cover phase 1 and phase 2 statistics based on accumulating packet and octet counts and failures based on security policy parameters and tunnel lifetimes. Examples are a count of the total number of octets

encrypted using 3DES, or the number of authentication failures when the algorithm used was MD5.

The relationships modeled in Phase-1 group are as follows:




For every entry in the End Point History table, there is a unique entry in the IPsec Tunnel History table. This is because when an IPsec tunnel expires, the end point entry associated with the tunnel expires also. Also note that the IKE tunnel that negotiated an expired instance of IPsec tunnel may not be present in the IKE Tunnel History table; the IKE tunnel may instead be still in the active IKE tunnel table.

Implementation Hint: The failure group may be implemented using ring buffers of the prescribed maximum size. This will automatically cause the oldest entry to be phased out to accomodate a new entry, should the buffer be full.

### 3.4.1. Journaling Active Tunnels

The history group also allows for journaling active Phase 1 and Phase 2 sessions by taking a snapshot of the active tunnels into the respective history tables whenever required. By setting an appropriate value in the MIB object ipSecHistCheckPoint, the operator may initiate a snapshot operation.

## 3.5. IPsec Failure Group

This group includes tables for phase 1 and phase 2 failures. Failures include

1) tunnel setup failures (the failure of a tunnel to be setup)

2) tunnel operational failures (the tunnel was setip, but was terminated before the negotiated lifetime expired).

The size of each table is dependent on the value of the ipSecFailTableSize object. Each failure entry for either phase 1 or 2 includes the specific reason for the failure, for example a CRL failure, and the time of the failure.

There are two tables in the failure group - one corresponding to failure of Phase-1 operations (IKE failures) and the second correspondign to Phase-2 failures. There is no specific relationship between the two tables modeled in this group. Note, however, that for every tunnel failure recorded in the failure group, there is an entry in the corresponding (IKE or IPsec) Tunnel History table (unless such an entry has been phased out to accomodate a new entry).

Implementation Hint: The failure group may be implemented using ring buffers of the prescribed maximum size. This will automatically cause the oldest entry to be phased out to accomodate a new entry, should the buffer be full.

## 3.6. IPsec Trap Control Group

This group controls the sending of IPsec traps. Traps are considered to include both error conditions, and any events that cause a change in state on the device. Events that trigger traps include normal events such as tunnel starts and stops and failure events such as early tunnel terminations, receipt of an invalid SPI, system errors, failure to establish tunnels, certificate failures and protocol errors.

# 4. Elements Deferred to Future Versions

A number of information elements relevant to the management of IPsec-based VPNs have been postponed to the next revision of this document. These include the following.

1) Support for Stream Control Transmission Protocol Apart from the inclusion of a new IKE ID type, SCTP requires that an IKE/IPsec tunnel be able to support multiple endpoint entries (selectors).

Hence the mapping between IPsec tunnel table and the End Point table must be made 1:n.

2) Support for KINK As details pertaining to KINK are resolved, Phase 1 group in the MIB will be redefined to support multiple key management protocols.

3) Multicast/GDOI A future version if this MIB will include support for group key-negotiations and multicast over IPsec.

4) NAT with IPsec Many implementations use UDP encapsulation to support NAT with IPsec. The Phase-1 and Phase-2 tunnel tables will be expanded to include attributes pertaining to this configuration.

## 5. MIB Definitions

```
IPSEC-FLOW-MONITOR-MIB DEFINITIONS ::= BEGIN

   -- PREFACE:
   -- IPSEC-FLOW-MONITOR-MIB Module models
   -- the standard, dynamic aspects of IPsec.
   -- These include counters and objects that are of
   -- management interest in a standard IPSec
   -- implementation. The MIB does not define
   -- vendor-specific IPSec attributes.

   IMPORTS
      MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE,
      Counter32, Counter64, Gauge32, Integer32, experimental
        FROM SNMPv2-SMI
      TEXTUAL-CONVENTION, DisplayString, TimeStamp,
      TimeInterval, TruthValue
        FROM SNMPv2-TC
      MODULE-COMPLIANCE, OBJECT-GROUP, NOTIFICATION-GROUP
        FROM SNMPv2-CONF

      ControlProtocol,
      Phase1PeerIdentityType,
      IkeNegoMode,
      IkeHashAlgo,
      IkeAuthMethod,
      DiffHellmanGrp,
      EncapMode,
      EncryptAlgo,
      Spi,
```

```
        AuthAlgo,
        CompAlgo,
        EndPtType
          FROM IPSEC-FLOW-MIB-TC;


      ipSecFlowMonitorMIB MODULE-IDENTITY
         LAST-UPDATED "200302171158Z"
         ORGANIZATION "Tivoli Systems and Cisco Systems"
         CONTACT-INFO
            "Tivoli Systems
             Research Triangle Park, NC

             Cisco Systems
             170 W Tasman Drive
             San Jose, CA  95134
             USA

             Tel: +1 800 553-NETS
             E-mail: harrisob@us.ibm.com
                     cs-ipsecmib@external.cisco.com"

      DESCRIPTION
           "This is a MIB Module for monitoring the structure
        and status of IPSec-based networks. The MIB has bee
        designed to be adopted as an IETF standard. Henc
        vendor-specific features of IPSec protocol are exclude
        from this MIB.

        Acronyms
        The following acronyms are used in this document:

         IPSec:      Secure IP Protocol

         VPN:        Virtual Private Network

         ISAKMP:     Internet Security Association and Key Exchange
                     Protocol

         IKE:        Internet Key Exchange Protocol

         SA:         Security Association

         MM:         Main Mode - the process of setting up
                     a Phase 1 SA to secure the exchanges
                     required to setup Phase 2 SAs
```

QM: Quick Mode - the process of setting up Phase 2 Security Associations using a Phase 1 SA.

Phase 1 Tunnel:
An ISAKMP SA can be regarded as representing a flow of ISAKMP/IKE traffic. Hence an ISAKMP is referred to as a 'Phase 1 Tunnel' in this document

Control Tunnel:
Another term for a Phase 1 Tunnel.

Phase 2 Tunnel:
AN instance of a non-ISAKMP SA bundle in which all the SA share the same proxy identifiers (IDii,IDir) protect the same stream of application traffic. Such an SA bundle is termed a 'Phase 2 Tunnel'. Note that a Phase 2 tunnel may comprise different SA bundles and different number of SA bundles at different times (due to key refresh).

Overview of IPsec MIB

The MIB contains six major groups of objects which are used to manage the IPSec Protocol. These groups include a Levels Group, a Phase-1 Group, a Phase-2 Group, a History Group, a Failure Group and a TRAP Control Group. The following table illustrates the structure of the IPSec MIB.

The Phase 1 group models objects pertaining to IKE negotiations and Phase 1 tunnels.

The Phase 2 group models objects pertaining to IPSec data tunnels.

The History group is to aid applications that do trending analysis.

The Failure group is to enable an operator to do troubleshooting and debugging of the VPN Router. Further, counters are supported to aid detection of potential security violations.

In addition to the five major MIB Groups, there are

```
    a number of Notifications. The following table
    illustrates the name and description of the
    IPSec TRAPs.

    For a detailed discussion, please refer to the IETF
    draft draft-ietf-ipsec-flow-monitoring-mib-01.txt.
         "

    REVISION "9911041800Z"
    DESCRIPTION
      "Initial version of this MIB module proposed to IETF."

    REVISION    "2001031200Z"
    DESCRIPTION
      "Phase-1 group updated with mode config metrics in globals
      as well as IKE peer table.
      Phase-2 group updated with new group metrics. New grou
      failures added to Failure group.
      Notifications pertaining to new group added.
      SPI table deprecated and an updated IPsec SA table added.
      Compliance clauses updated."

    REVISION    "200303021158Z"
    DESCRIPTION
      "Third submission of the draft to IETF. Changes incorporated
      based on comments received on the second draft. Highlights:
        1) IKE Group made optional
        2) Provision to accomodate other Phase 1 protocols.
        3) Phase 1 Peer Association table decoupled from
           IKE group.
        4) Local and Remote value indices to Phase 1 Pee
           Association table constrained to 128-bit length by MD5
           hashing.
        5) Mapping of Phase 2 tunnels to Phase 1 tunnels
           made generic (non-IKE).
        6) Phase 1 traps redefined as `Control Channel' traps.
        7) High capacity counters defined for Phase-1 and Phase-2
           expired counters."

       -- Placeholder anchor
         --::= { xxx 171 }
         ::= { experimental 171 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++
   -- Local Textual Conventions
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++
      HashedString ::= TEXTUAL-CONVENTION
```

```
         STATUS     current
         DESCRIPTION
            "128-bit MD5 output string of an input string"
         SYNTAX  OCTET STRING(SIZE(16))

      IPSIpAddress ::= TEXTUAL-CONVENTION
         STATUS     current
         DESCRIPTION
            "An IP V4 or V6 Address."
         SYNTAX  OCTET STRING(SIZE(4 | 16))
                       -- IP V4 or V6 Address

      IkePeerType  ::= TEXTUAL-CONVENTION
         STATUS     deprecated
         DESCRIPTION
            "The type of IPsec Phase-1 IKE peer identity.
            The IKE peer may be identified by one of the
            ID types defined in IPSEC DOI.

            This textual convention has been deprecated in
            favour of the more generic `Phase1PeerType'.
            (defined in module IPSEC-FLOW-MIB-TC)."

         SYNTAX INTEGER {
                   reserved(0),
                   id_ipv4_addr(1),
                   id_fqdn(2),
                   id_dn(3),
                   id_ipv6_addr(4)
                }

      KeyType    ::= TEXTUAL-CONVENTION
         STATUS     deprecated
         DESCRIPTION
            "The type of key used by an IPsec Phase-2 Tunnel.

            This textual convention has been deprecated and has been
            repaced by the standard textual convention ControlProtocol
            (defined in module IPSEC-FLOW-MIB-TC)."

         SYNTAX INTEGER{
                  reserved(0),
                  key_ike(1),
                  key_manual(2),
                  key_kink(3),
                  key_ikev2(4)
                }
```

```
      TunnelStatus  ::= TEXTUAL-CONVENTION
         STATUS     current
         DESCRIPTION
            "The status of a Tunnel.  Objects of this type may
             be used to bring the tunnel down by setting
             value of this object to destroy(4).  Objects of this
             type cannot be used to create a Tunnel."
         SYNTAX INTEGER {
                   reserved(0),
                   awaitXauth(1),  -- in Phase 1.5
                   awaitCommit(2), -- waiting for commit bit
                   active(3),      -- ready for QM
                   destroy(4)
                }

      TrapStatus    ::= TEXTUAL-CONVENTION
         STATUS     current
         DESCRIPTION
            "The administrative status for sending a TRAP."
         SYNTAX INTEGER {
                   reserved(0),
                   enabled(1),
                   disabled(2)
                }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- IPsec MIB Object Groups
   --
   -- This MIB module contains the following groups:
   -- 1) IPsec Levels Group
   -- 2) IPsec Phase-1 Group
   -- 3) IPsec Phase-2 Group
   -- 4) IPsec History Group
   -- 5) IPsec Failure Group
   -- 6) IPsec TRAP Control Group
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++

      ipSecMIBObjects OBJECT IDENTIFIER  ::=
                  {ipSecFlowMonitorMIB 1}

      ipSecLevels OBJECT IDENTIFIER
                    ::= { ipSecMIBObjects 1 }
      ipSecPhaseOne OBJECT IDENTIFIER
                    ::= { ipSecMIBObjects 2 }
      ipSecPhaseTwo           OBJECT IDENTIFIER
                    ::= { ipSecMIBObjects 3 }
```

```
      ipSecHistory            OBJECT IDENTIFIER
                      ::= { ipSecMIBObjects 4 }
      ipSecFailures           OBJECT IDENTIFIER
                      ::= { ipSecMIBObjects 5 }
      ipSecTrapCntl           OBJECT IDENTIFIER
                      ::= { ipSecMIBObjects 6 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- IPsec Levels Group
   --
   -- This group consists of a:
   -- 1) IPsec MIB Level
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++

      ipSecMibLevel OBJECT-TYPE
         SYNTAX Integer32 (1..4096)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The version of the IPsec MIB."
         ::= { ipSecLevels 1 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-1 Internet Key Exchange (IKE) Group
   --
   -- This group consists of:
   -- 1) IPsec Phase-1 Global Statistics
   -- 2) IPsec Phase-1 Peer Table
   -- 3) IPsec Phase-1 Tunnel Table
   -- 4) IPsec Phase-1 Correlation Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-1 Global Statistics
   -- This entire group is optional and needs to be implemented
   -- only if the managed entity supports IKE.
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ikeGroup  OBJECT IDENTIFIER
                ::= { ipSecPhaseOne 1 }

      ikeGlobalStats  OBJECT IDENTIFIER
                ::= { ikeGroup 1 }

      ikeGlobalActiveTunnels OBJECT-TYPE
         SYNTAX Gauge32
         MAX-ACCESS read-only
         STATUS current
```

```
         DESCRIPTION
            "The number of currently active IPsec
            Phase-1 IKE Tunnels. This is equal to the
            number of ISAKMP SAs currently active."
         ::= { ikeGlobalStats 1 }

      ikeGlobalPreviousTunnels OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SAs"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of previously active
            IPsec Phase-1 IKE Tunnels. This is equal to
            the total number of ISAKMP SAs that were
            active since the bootup of the device
            but which have since expired."
         ::= { ikeGlobalStats 2 }

      ikeGlobalInOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets received by all currently
             and previously active IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 3 }

      ikeGlobalInPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets received by all
            currently and previously active IPsec
            Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 4 }

      ikeGlobalInDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets which were
```

```
            dropped during receive processing by all
            currently and previously
             active IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 5 }

      ikeGlobalInNotifys OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of notifys received by
            all currently and previously active IPsec
            Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 6 }

      ikeGlobalInP2Exchgs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            received by all currently and previously
            active IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 7 }

      ikeGlobalInP2ExchgInvalids OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            which were received and found to be contain
            references to unrecognized security parameters.
            This value is accumulated across all currently
            and previously active IPsec ISAKMP SAs."
         ::= { ikeGlobalStats 8 }

      ikeGlobalInP2ExchgRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
```

```
            which were received and validated but were
            rejected by the local policy. This value is
            accumulated across all currently and previously
            active IPsec ISAKMP SAs."
         ::= { ikeGlobalStats 9 }

      ikeGlobalInP2SaDelRequests OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 security
            association delete requests received by all
            currently and previously
             active and IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 10 }

      ikeGlobalOutOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets sent by all currently
             and previously active and IPsec Phase-1
             IKE Tunnels."
         ::= { ikeGlobalStats 11 }

      ikeGlobalOutPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets sent by all currently
             and previously active and IPsec Phase-1
             Tunnels."
         ::= { ikeGlobalStats 12 }

      ikeGlobalOutDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets which were dropped
```

```
            during send processing by all currently
            and previously
             active IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 13 }

      ikeGlobalOutNotifys OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of notifys sent by all currently
             and previously active IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 14 }

      ikeGlobalOutP2Exchgs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            which were sent by all currently and previously
            active IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 15 }

      ikeGlobalOutP2ExchgInvalids OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            which were sent and were flagged by the peer to
            contain references to unrecognized security
            parameters. This value is accumulated across all
            currently and previously active IPsec ISAKMP SAs."
         ::= { ikeGlobalStats 16 }

      ikeGlobalOutP2ExchgRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            which were sent, validated by the peer but were
```

```
            rejected by the peer's policy. This value is
            accumulated across all currently and previously
            active IPsec ISAKMP SAs."
         ::= { ikeGlobalStats 17 }

      ikeGlobalOutP2SaDelRequests OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 SA
             delete requests sent by all currently and
             previously active IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 18 }

      ikeGlobalInitTunnels OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SAs"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-1 IKE
            Tunnels which were locally initiated."
         ::= { ikeGlobalStats 19 }

      ikeGlobalInitTunnelFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SAs"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-1 IKE Tunnels
            which were locally initiated and failed to activate."
         ::= { ikeGlobalStats 20 }

      ikeGlobalRespTunnelFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SAs"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-1 IKE Tunnels
            which were remotely initiated and failed to activate."
         ::= { ikeGlobalStats 21 }

      ikeGlobalSysCapFails OBJECT-TYPE
```

```
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of system capcity failures
            which occurred during processing of all current
            and previously active IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 22 }

      ikeGlobalAuthFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of authentications which ended
             in failure by all current and previous IPsec Phase-1
             IKE Tunnels."
         ::= { ikeGlobalStats 23 }

      ikeGlobalDecryptFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of decryptions which ended
             in failure by all current and previous IPsec Phase-1
             IKE Tunnels."
         ::= { ikeGlobalStats 24 }

      ikeGlobalHashValidFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of hash validations which ended
             in failure by all current and previous IPsec Phase-1
             IKE Tunnels."
         ::= { ikeGlobalStats 25 }

      ikeGlobalNoSaFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The total number of non-existent Security Association
             in failures which occurred during processing of
             all current and previous IPsec Phase-1 IKE Tunnels."
         ::= { ikeGlobalStats 26 }

      ikeGlobalRespTunnels OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SAs"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-1 IKE
            Tunnels which were remotely initiated."
         ::= { ikeGlobalStats 27 }

      ikeGlobalInXauthFailures OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the extended authentication
            information supplied by an IKE peer was found
            to be invalid by the local entity."
         ::= { ikeGlobalStats 28 }

      ikeGlobalOutXauthFailures OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the extended authentication
            information supplied by the managed entity to an
            IKE peer was found to be invalid by the remote peer."
         ::= { ikeGlobalStats 29 }

      ikeGlobalInP1SaDelRequests OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of ISAKMP security association
            delete requests received by all currently and
```

```
            previously active and ISAKMP security associations."
         ::= { ikeGlobalStats 30 }

      ikeGlobalOutP1SaDelRequests OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of ISAKMP security association
            delete requests sent by all currently and
            previously active and ISAKMP security associations."
         ::= { ikeGlobalStats 31 }

      ikeGlobalInConfigs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            received (either CFG_REPLY or CFG_SET payloads)
            by this entity."
         ::= { ikeGlobalStats 32 }

      ikeGlobalOutConfigs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            dispatched (either CFG_REPLY or CFG_SET payloads)
            by this entity."
         ::= { ikeGlobalStats 33 }

      ikeGlobalInConfigsRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Acknowledgements"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            which were received (either CFG_REPLY or CFG_SET
            payloads) by this entity and which were rejected
            by the local entity."
         ::= { ikeGlobalStats 34 }
```

```
      ikeGlobalOutConfigsRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Acknowledgements"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            which were dispatched (either CFG_REPLY or CFG_SET
            payloads) by this entity and which were rejected
            by the client peer."
         ::= { ikeGlobalStats 35 }

      ikeGlobalHcPreviousTunnels OBJECT-TYPE
         SYNTAX Counter64
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of
            previously active IPsec Phase-1 IKE Tunnels. This i
            equal to the total number of ISAKMP SAs that were
            active since the bootup of the device but which
            have since expired."
         ::= { ikeGlobalStats 36 }

      ikeGlobalPreviousTunnelsWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
          "The number of times the quantit
          `ikeGlobalPreviousTunnels' (previously active IPse
          Phase-1 IKE tunnels) has wrapped."
         ::= { ikeGlobalStats 37 }


   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-1 Internet Key Exchange Tunnel Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ikeTunnelTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IkeTunnelEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-1 Internet Key Exchange Tunnel Table.
```

```
            There is one entry in this table for each active IPsec
            Phase-1 IKE Tunnel."
        ::= { ikeGroup 2 }

      ikeTunnelEntry OBJECT-TYPE
         SYNTAX IkeTunnelEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
               "Each entry contains the attributes associated with
                an active IPsec Phase-1 IKE Tunnel."
         INDEX { ikeTunIndex }
         ::= { ikeTunnelTable 1}

      IkeTunnelEntry ::= SEQUENCE {
         ikeTunIndex                Integer32,
         ikeTunLocalType            Phase1PeerIdentityType,
         ikeTunLocalValue           DisplayString,
         ikeTunLocalAddr            IPSIpAddress,
         ikeTunLocalName            DisplayString,
         ikeTunRemoteType           Phase1PeerIdentityType,
         ikeTunRemoteValue          DisplayString,
         ikeTunRemoteAddr           IPSIpAddress,
         ikeTunRemoteName           DisplayString,
         ikeTunNegoMode             IkeNegoMode,
         ikeTunDiffHellmanGrp       DiffHellmanGrp,
         ikeTunEncryptAlgo          EncryptAlgo,
         ikeTunHashAlgo             IkeHashAlgo,
         ikeTunAuthMethod           IkeAuthMethod,
         ikeTunLifeTime             Integer32,
         ikeTunActiveTime           TimeInterval,
         ikeTunSaRefreshThreshold   Integer32,
         ikeTunTotalRefreshes       Counter32,
         ikeTunInOctets             Counter32,
         ikeTunInPkts               Counter32,
         ikeTunInDropPkts           Counter32,
         ikeTunInNotifys            Counter32,
         ikeTunInP2Exchgs           Counter32,
         ikeTunInP2ExchgInvalids    Counter32,
         ikeTunInP2ExchgRejects     Counter32,
         ikeTunInP2SaDelRequests    Counter32,
         ikeTunOutOctets            Counter32,
         ikeTunOutPkts              Counter32,
         ikeTunOutDropPkts          Counter32,
         ikeTunOutNotifys           Counter32,
         ikeTunOutP2Exchgs          Counter32,
         ikeTunOutP2ExchgInvalids   Counter32,
```

```
      ikeTunOutP2ExchgRejects     Counter32,
      ikeTunOutP2SaDelRequests    Counter32,
      ikeTunStatus                TunnelStatus,
      ikeTunInNewGrpReqs          Counter32,
      ikeTunOutNewGrpReqs         Counter32,
      ikeTunInNewGrpReqsRejected  Counter32,
      ikeTunOutNewGrpReqsRejected Counter32,
      ikeTunInConfigs             Counter32,
      ikeTunOutConfigs            Counter32,
      ikeTunInConfigsRejects      Counter32,
      ikeTunOutConfigsRejects     Counter32,
      ikeTunEncryptKeySize        Integer32
   }

   ikeTunIndex OBJECT-TYPE
      SYNTAX Integer32 (1..2147483647)
      MAX-ACCESS not-accessible
      STATUS current
      DESCRIPTION
         "The index of the IPsec Phase-1 IKE Tunnel Table.
          The value of the index is a number which begins
          at one and is incremented with each tunnel that
          is created. The value of this object will
          wrap at 2,147,483,647."
      ::= { ikeTunnelEntry 1 }

   ikeTunLocalType OBJECT-TYPE
      SYNTAX Phase1PeerIdentityType
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
         "The type of local peer identity.  The local
         peer may be identified by:
          1. an IP address, or
          2. or a fully qualified domain name string.
          3. or a distinguished name string."
      ::= { ikeTunnelEntry 2 }

   ikeTunLocalValue OBJECT-TYPE
      SYNTAX DisplayString
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
         "The value of the local peer identity.

          If the local peer type is an IP Address, then this
          is the IP Address used to identify the local peer.
```

```
            If the local peer type is id_fqdn, then this is
            the FQDN of the remote peer.

            If the local peer type is a id_dn, then this is
            the distinguished name string of the local peer."
         ::= { ikeTunnelEntry 3 }

      ikeTunLocalAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the local endpoint for the IPsec
             Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 4 }

      ikeTunLocalName OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The DNS name of the local IP address for
            the IPsec Phase-1 IKE Tunnel. If the DNS
            name associated with the local tunnel endpoint
            is not known, then the value of this
             object will be a NULL string."
         ::= { ikeTunnelEntry 5 }

      ikeTunRemoteType OBJECT-TYPE
         SYNTAX Phase1PeerIdentityType
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The type of remote peer identity.
            The remote peer may be identified by:
             1. an IP address, or
             2. or a fully qualified domain name string.
             3. or a distinguished name string."
         ::= { ikeTunnelEntry 6 }

      ikeTunRemoteValue OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value of the remote peer identity.
```

```
            If the remote peer type is an IP Address, then this
            is the IP Address used to identify the remote peer.

            If the remote peer type is id_fqdn, then this is
            the FQDN of the remote peer.

            If the remote peer type is a id_dn, then this is
            the distinguished named string of the remote peer."
         ::= { ikeTunnelEntry 7 }

      ikeTunRemoteAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the remote endpoint for the IPsec
             Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 8 }

      ikeTunRemoteName OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The DNS name of the remote IP address of IPsec Phase-1
             IKE Tunnel. If the DNS name associated with the remote
             tunnel endpoint is not known, then the value of this
             object will be a NULL string."
         ::= { ikeTunnelEntry 9 }

      ikeTunNegoMode OBJECT-TYPE
         SYNTAX IkeNegoMode
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The negotiation mode of the IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 10 }

      ikeTunDiffHellmanGrp OBJECT-TYPE
         SYNTAX DiffHellmanGrp
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The Diffie Hellman Group used in IPsec Phase-1 IKE
             negotiations."
         ::= { ikeTunnelEntry 11 }
```

```
      ikeTunEncryptAlgo OBJECT-TYPE
         SYNTAX EncryptAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The encryption algorithm used in IPsec Phase-1 IKE
             negotiations."
         ::= { ikeTunnelEntry 12 }

      ikeTunHashAlgo OBJECT-TYPE
         SYNTAX IkeHashAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The hash algorithm used in IPsec Phase-1 IKE
             negotiations."
         ::= { ikeTunnelEntry 13 }

      ikeTunAuthMethod OBJECT-TYPE
         SYNTAX IkeAuthMethod
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication method used in IPsec Phase-1 IKE
             negotiations."
         ::= { ikeTunnelEntry 14 }

      ikeTunLifeTime OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         UNITS "seconds"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The negotiated LifeTime of the IPsec Phase-1 IKE Tunnel
             in seconds."
         ::= { ikeTunnelEntry 15 }

      ikeTunActiveTime OBJECT-TYPE
         SYNTAX TimeInterval
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The length of time the IPsec Phase-1 IKE tunnel has been
             active in hundredths of seconds."
         ::= { ikeTunnelEntry 16 }
```

```
      ikeTunSaRefreshThreshold OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         UNITS "seconds"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The security assoication refresh threshold in seconds."
         ::= { ikeTunnelEntry 17 }

      ikeTunTotalRefreshes OBJECT-TYPE
         SYNTAX Counter32
         UNITS "QM Exchanges"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of security associations
            refreshes performed."
         ::= { ikeTunnelEntry 18 }

      ikeTunInOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets received by
            this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 19 }

      ikeTunInPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets received by
            this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 20 }

      ikeTunInDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped
            by this IPsec Phase-1 IKE Tunnel during
```

```
            receive processing."
         ::= { ikeTunnelEntry 21 }

      ikeTunInNotifys OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of notifys received by
            this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 22 }

      ikeTunInP2Exchgs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2
            exchanges received by
             this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 23 }

      ikeTunInP2ExchgInvalids OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            received on this tunnel that were found to
            contain references to unrecognized security
            parameters."
         ::= { ikeTunnelEntry 24 }

      ikeTunInP2ExchgRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            received on this tunnel that were validated but were
            rejected by the local policy."
         ::= { ikeTunnelEntry 25 }
```

```
      ikeTunInP2SaDelRequests OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2
            security association delete requests received
            by this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 26 }

      ikeTunOutOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets sent by this IPsec Phase-1
             IKE Tunnel."
         ::= { ikeTunnelEntry 27 }

      ikeTunOutPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets sent by this IPsec Phase-1
             IKE Tunnel."
         ::= { ikeTunnelEntry 28 }

      ikeTunOutDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped by this
            IPsec Phase-1 IKE Tunnel during send processing."
         ::= { ikeTunnelEntry 29 }

      ikeTunOutNotifys OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
```

```
            "The total number of notifys sent by this
            IPsec Phase-1 Tunnel."
         ::= { ikeTunnelEntry 30 }

      ikeTunOutP2Exchgs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges sent by
             this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 31 }

      ikeTunOutP2ExchgInvalids OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            sent on this tunnel that were found by the peer
            to contain references to security parameters
            not recognized by the peer."
         ::= { ikeTunnelEntry 32 }

      ikeTunOutP2ExchgRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            sent on this tunnel that were validated by the peer
            but were rejected by the peer's policy."
         ::= { ikeTunnelEntry 33 }

      ikeTunOutP2SaDelRequests OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 security association
             delete requests sent by this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelEntry 34 }
```

```
      ikeTunStatus OBJECT-TYPE
         SYNTAX TunnelStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "The status of the MIB table row.

             This object can be used to bring the tunnel down
             by setting value of this object to destroy(2).

             This object cannot be used to create
             a MIB table row."
         ::= { ikeTunnelEntry 35 }

      ikeTunInNewGrpReqs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             remotely using this IKE tunnel."
         ::= { ikeTunnelEntry 36 }

      ikeTunOutNewGrpReqs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             locally using this IKE tunnel."
         ::= { ikeTunnelEntry 37 }

      ikeTunInNewGrpReqsRejected OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             remotely using this IKE tunnel that ended in a failure."
         ::= { ikeTunnelEntry 38 }

      ikeTunOutNewGrpReqsRejected OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
```

```
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             locally using this IKE tunnel that ended in a failure."
         ::= { ikeTunnelEntry 39 }

      ikeTunInConfigs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            received (either CFG_REPLY or CFG_SET payloads)
            by the local entity on the ISAKMP SA represented by this
            IKE tunnel."
         ::= { ikeTunnelEntry 40 }

      ikeTunOutConfigs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            dispatched (either CFG_REPLY or CFG_SET payloads)
            by the local entity on the ISAKMP SA represented by this
            IKE tunnel."
         ::= { ikeTunnelEntry 41 }

      ikeTunInConfigsRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            which were received (either CFG_REPLY or CFG_SET
            payloads) and rejected by this entity using the ISAKMP
            SA represented by this IKE tunnel."
         ::= { ikeTunnelEntry 42 }

      ikeTunOutConfigsRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            which were dispatched (either CFG_REPLY or CFG_SET
            payloads) by this entity and were rejected by the
            peer (client) using the ISAKMP SA represented by this
            IKE tunnel."
         ::= { ikeTunnelEntry 43 }

      ikeTunEncryptKeySize        OBJECT-TYPE
         SYNTAX Integer32
         UNITS "Bits"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The key size in bits of the negotiated key to be
            used with the algorithm denoted by the column
            'ikeTunEncryptAlgo'. For DES and 3DES the key size i
            respectively 56 and 168. For AES, this will denote th
            negotiated key size."
         ::= { ikeTunnelEntry 44 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-1 Internet Key Exchange Peer Table.
   -- This is a mandatory group. If all IPsec flows are manually
   -- administred, this table would be empty.
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      phase1PeerTable OBJECT-TYPE
         SYNTAX SEQUENCE OF Phase1PeerEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-1 Key Exchange Peer Table. Ther
            is one entry in this table for each IPsec Phase-1 pee
            with which the managed entity is currently associate
            by virtue of an active IPsec Phase-1 Control Tunnel.
            peer has an entry in this table, if and only if ther
            is at least one Phase-1 or Phase-2 tunnel terminatin
            on the managed entity from the peer. When all Phase-
            and Phase-2 tunnels to a peer have expired, the entr
            for the peer is deleted off this table."
        ::= { ipSecPhaseOne 2 }

      phase1PeerEntry OBJECT-TYPE
         SYNTAX Phase1PeerEntry
         MAX-ACCESS not-accessible
         STATUS current
```

```
         DESCRIPTION
               "Each entry contains the attributes associated
                with an IPsec Phase-1 IKE peer association."
         INDEX { phase1PeerLocalType,
                 phase1PeerHLocalValue,
                 phase1PeerRemoteType,
                 phase1PeerHRemoteValue,
                 phase1PeerIntIndex }
         ::= { phase1PeerTable 1}

      Phase1PeerEntry ::= SEQUENCE {
         phase1PeerLocalType               Phase1PeerIdentityType,
         phase1PeerLocalValue              DisplayString,
         phase1PeerHLocalValue             HashedString,
         phase1PeerRemoteType              Phase1PeerIdentityType,
         phase1PeerRemoteValue             DisplayString,
         phase1PeerHRemoteValue            HashedString,
         phase1PeerIntIndex                Integer32,
         phase1PeerLocalAddr               IPSIpAddress,
         phase1PeerRemoteAddr              IPSIpAddress,
         phase1PeerActiveTime              TimeInterval,
         phase1PeerActiveTunnelIndex       Integer32,
         phase1PeerConfigAppVersion        DisplayString,
         phase1PeerConfigAddress           IPSIpAddress,
         phase1PeerConfigNetmask           IPSIpAddress,
         phase1PeerConfigDns               IPSIpAddress,
         phase1PeerConfigNbns              IPSIpAddress,
         phase1PeerConfigDhcp              IPSIpAddress,
         phase1Protocol                    ControlProtocol
      }

      phase1PeerLocalType OBJECT-TYPE
         SYNTAX Phase1PeerIdentityType
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The type of local peer identity.  The local peer
             may be identified by:
             1. an IP address, or
             2. or a fully qualified domain name.
             3. or a distinguished name."
         ::= { phase1PeerEntry 1 }

      phase1PeerLocalValue OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
```

```
          DESCRIPTION
             "The value of the local peer identity.

              If the local peer type is an IP Address, then this
              is the IP Address used to identify the local peer.

              If the local peer type is a id_fqdn, then this is
              the FQDN of the local peer.

              If the local peer type is id_dn, then this is
              the DN string of the local peer. Value of this object
              could be arbitrarily large making this object unsuitable
              to be used for indexing this table (please refer to
              the definition of 'phase1PeerHLocalValue'."
          ::= { phase1PeerEntry 2 }

       phase1PeerHLocalValue OBJECT-TYPE
          SYNTAX HashedString
          MAX-ACCESS not-accessible
          STATUS current
          DESCRIPTION
             "The 128-bit MD5 hash output of the value represente
             by the element phase1PeerLocalValue. The hashing is
             required to restrict the length of the SNMP index
             to a legal size:

               phase1PeerHRemoteValue = MD5(phase1PeerLocalValue)."
          ::= { phase1PeerEntry 3 }

       phase1PeerRemoteType OBJECT-TYPE
          SYNTAX Phase1PeerIdentityType
          MAX-ACCESS not-accessible
          STATUS current
          DESCRIPTION
             "The type of remote peer identity.  The remote peer
              may be identified by:
              1. an IP address, or
              2. or a fully qualified domain name.
              3. or a distinguished name."
          ::= { phase1PeerEntry 4 }

       phase1PeerRemoteValue OBJECT-TYPE
          SYNTAX DisplayString
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
             "The value of the remote peer identity.
```

```
            If the remote peer type is an IP Address, then this
            is the IP Address used to identify the remote peer.

            If the remote peer type is id_fqdn, then this is
            the FQDN of the remote peer.

            If the remote peer type is a id_dn, then this is
            the DN string of the remote peer. Value of this object
            could be arbitrarily large making this object unsuitable
            to be used for indexing this table (please refer to
            the definition of 'phase1PeerHRemoteValue'."
         ::= { phase1PeerEntry 5 }

      phase1PeerHRemoteValue OBJECT-TYPE
         SYNTAX HashedString
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The 128-bit MD5 hash output of the value represente
            by the element phase1PeerRemoteValue. The hashing is
            required to restrict the length of the SNMP index
            to a legal size:

              phase1PeerHRemoteValue = MD5(phase1PeerRemoteValue)."
         ::= { phase1PeerEntry 6 }

      phase1PeerIntIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The internal index of the local-remote
            peer association.  This internal index is used
            to uniquely identify multiple associations between
            the local and remote peer."
         ::= { phase1PeerEntry 7 }

      phase1PeerLocalAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the local peer."
         ::= { phase1PeerEntry 8 }

      phase1PeerRemoteAddr OBJECT-TYPE
```

```
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the remote peer."
         ::= { phase1PeerEntry 9 }

      phase1PeerActiveTime OBJECT-TYPE
         SYNTAX TimeInterval
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The length of time that the peer association has
             existed in hundredths of a second."
         ::= { phase1PeerEntry 10 }

      phase1PeerActiveTunnelIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The index of the active IPsec Phase-1 IKE Tunnel
             (ikeTunIndex in the ikeTunnelTable) for this peer
             association.  If an IPsec Phase-1 IKE Tunnel is
             not currently active, then the value of this
             object will be zero."
         ::= { phase1PeerEntry 11 }

      phase1PeerConfigAppVersion OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The NULL terminated printable application version of the
            peer. If the peer did not issue the APPLICATION_VERSION
            attribute, this field is NULL."
         ::= { phase1PeerEntry 12 }

      phase1PeerConfigAddress OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address configured by the peer on this entity.
            If the local entity did not receive either
            INTERNAL_IP4_ADDRESS or INTERNAL_IP6_ADDRESS from
            the peer, this field should have the NULL IP address."
```

```
         ::= { phase1PeerEntry 13 }

      phase1PeerConfigNetmask OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The netmask configured by the peer on this entity.
            If the local entity did not receive either
            INTERNAL_V4_MASK or INTERNAL_IP6_MASK from
            the peer, this field should have the NULL IP address."
         ::= { phase1PeerEntry 14 }

      phase1PeerConfigDns OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The address of the DNS server configured by the peer
            on the local entity using CFG_SET or CFG_REPLY. If the
            local entity did not receive either INTERNAL_V4_DNS or
            INTERNAL_IP6_DNS from the peer, this field should have
            the NULL IP address."
         ::= { phase1PeerEntry 15 }

      phase1PeerConfigNbns OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The address of the NetBios Name Server configured by
            the peer on the local entity using CFG_SET or CFG_REPLY.
            If the local entity did not receive either INTERNAL_V4_NBNS
            INTERNAL_IP6_NBNS from the peer, this field should have
            the NULL IP address."
         ::= { phase1PeerEntry 16 }

      phase1PeerConfigDhcp OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The address of the DHCP Server configured by  the peer
            on the local entity using CFG_SET or CFG_REPLY.
            If the local entity did not receive either INTERNAL_V4_DHCP
            INTERNAL_IP6_DHCP from the peer, this field should have
            the NULL IP address."
```

```
         ::= { phase1PeerEntry 17 }

      phase1Protocol OBJECT-TYPE
         SYNTAX ControlProtocol
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The keying and control protocol used to setup
            and administer Phase-1 and Phase-2 tunnels to this
            peer."
         ::= { phase1PeerEntry 18 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The Phase-1 Peer Association to Phase-2 Tunnel Correlatio
   -- Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++
      phase1PeerCorrTable OBJECT-TYPE
         SYNTAX SEQUENCE OF Phase1PeerCorrEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-1 Peer Association to IPsec Phase-
         Tunnel Correlation Table. There is one entry in this tabl
         for each active IPsec Phase-2 Tunnel."
        ::= { ipSecPhaseOne 3 }

      phase1PeerCorrEntry OBJECT-TYPE
         SYNTAX Phase1PeerCorrEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
               "Each entry contains the attributes of an
         IPsec Phase-1 Peer Association to IPsec Phase-
         Tunnel Correlation."
         INDEX { phase1PeerCorrLocalType,
                 phase1PeerCorrLocalValue,
                 phase1PeerCorrRemoteType,
                 phase1PeerCorrRemoteValue,
                 phase1PeerCorrIntIndex,
                 phase1PeerCorrSeqNum }
         ::= { phase1PeerCorrTable 1}

      Phase1PeerCorrEntry ::= SEQUENCE {
         phase1PeerCorrLocalType               Phase1PeerIdentityType,
         phase1PeerCorrLocalValue              DisplayString,
         phase1PeerCorrRemoteType              Phase1PeerIdentityType,
         phase1PeerCorrRemoteValue             DisplayString,
```

```
         phase1PeerCorrIntIndex                Integer32,
         phase1PeerCorrSeqNum                  Integer32,
         phase1PeerCorrIpSecTunIndex           Integer32,
         phase1PeerCorrControlProtocol         ControlProtocol
      }

      phase1PeerCorrLocalType OBJECT-TYPE
         SYNTAX Phase1PeerIdentityType
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The type of local peer identity. The local peer
             may be identified by:
             1. an IP address, or
             2. or a fully qualified domain name.
             3. or a distinguished name."
         ::= { phase1PeerCorrEntry 1 }

      phase1PeerCorrLocalValue OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The value of the local peer identity.

             If the local peer type is an IP Address, then this
             is the IP Address used to identify the local peer.

             If the local peer type is id_fqdn, then this is
             the FQDN of the local entity.

             If the local peer type is a id_dn, then this is
             the distinguished named string of the local peer."
         ::= { phase1PeerCorrEntry 2 }

      phase1PeerCorrRemoteType OBJECT-TYPE
         SYNTAX Phase1PeerIdentityType
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The type of remote peer identity. The remote peer
             may be identified by:
             1. an IP address, or
             2. or a fully qualified domain name.
             3. or a distinguished name."
         ::= { phase1PeerCorrEntry 3 }
```

```
      phase1PeerCorrRemoteValue OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The value of the remote peer identity.

             If the remote peer type is an IP Address, then this
             is the IP Address used to identify the remote peer.

             If the remote peer type is id_fqdn, then this is
             the FQDN of the remote peer.

             If the remote peer type is a id_dn, then this is
             the distinguished named string of the remote peer."
         ::= { phase1PeerCorrEntry 4 }

      phase1PeerCorrIntIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The internal index of the local-remote
            peer association.  This internal index is
            used to uniquely identify multiple associations
            between the local and remote peer."
         ::= { phase1PeerCorrEntry 5 }

      phase1PeerCorrSeqNum   OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The sequence number of the local-remote
            peer association.  This sequence number is
            used to uniquely identify multiple instances
            of an unique association between
             the local and remote peer."
         ::= { phase1PeerCorrEntry 6 }

      phase1PeerCorrIpSecTunIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The index of the active IPsec Phase-2 Tunnel
             (ipSecTunIndex in the ipSecTunnelTable) for this
```

```
            IPsec Phase-1 IKE Peer Association."
         ::= { phase1PeerCorrEntry 7 }

      phase1PeerCorrControlProtocol OBJECT-TYPE
         SYNTAX ControlProtocol
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The keying and control protocol used to setup
            and administer the Phase-1 and Phase-2 tunnels thi
            table entry refers to."
         ::= { phase1PeerCorrEntry 8 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- IPsec Phase-2 Group
   --
   -- This group consists of:
   -- 1) IPsec Phase-2 Global Statistics
   -- 2) IPsec Phase-2 Tunnel Table
   -- 3) IPsec Phase-2 Endpoint Table
   -- 4) IPsec Phase-2 Security Protection Index Table
   -- 4) IPsec Phase-2 Security Protection Index Objects
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-2 Global Tunnel Statistics
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecGlobalStats          OBJECT IDENTIFIER
                       ::= { ipSecPhaseTwo 1 }

      ipSecGlobalActiveTunnels OBJECT-TYPE
         SYNTAX Gauge32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of currently active
            IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 1 }

      ipSecGlobalPreviousTunnels OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Phase-2 Tunnels"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of previously active
```

```
            IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 2 }

      ipSecGlobalInOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets received by all
            current and previous IPsec Phase-2 Tunnels.
            This value is
      accumulated BEFORE determining whether or not
      the packet should be decompressed. See also
      ipSecGlobalInOctWraps for the number of times
      this counter has wrapped."
         ::= { ipSecGlobalStats 3 }

      ipSecGlobalHcInOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of
      octets received by all current and previous
      IPsec Phase-2 Tunnels. This value is accumulated
      BEFORE determining whether or not the packet
      should be decompressed."
         ::= { ipSecGlobalStats 4 }

      ipSecGlobalInOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the global octets received
      counter (ipSecGlobalInOctets) has wrapped."
         ::= { ipSecGlobalStats 5 }

      ipSecGlobalInDecompOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of decompressed octets received
```

```
            by all current and previous IPsec Phase-2 Tunnels.
            This value is accumulated AFTER the packet is
            decompressed. If compression is not being used,
            this value will match the value of ipSecGlobalInOctets.
            See also ipSecGlobalInDecompOctWraps
             for the number of times this counter has wrapped."
         ::= { ipSecGlobalStats 6 }

      ipSecGlobalHcInDecompOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number
            of decompressed octets received by all current
            and previous IPsec Phase-2 Tunnels.  This value
            is accumulated AFTER the packet is decompressed.
             If compression is not being used, this value
             will match the value of ipSecGlobalHcInOctets."
         ::= { ipSecGlobalStats 7 }

      ipSecGlobalInDecompOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the global decompressed
            octets received counter
             (ipSecGlobalInDecompOctets) has wrapped."
         ::= { ipSecGlobalStats 8 }

      ipSecGlobalInPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets received
            by all current and previous
             IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 9 }

      ipSecGlobalInDrops OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The total number of packets dropped
            during receive processing by all current and previous
            IPsec Phase-2 Tunnels. This count does
            NOT include packets dropped due to
            Anti-Replay processing."
         ::= { ipSecGlobalStats 10 }

      ipSecGlobalInReplayDrops OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped during
            receive processing due to Anti-Replay
            processing by all current and previous IPsec
             Phase-2 Tunnels."
         ::= { ipSecGlobalStats 11 }

      ipSecGlobalInAuths OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Events"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound authentication's
            performed by all current and previous IPsec
            Phase-2 Tunnels."
         ::= { ipSecGlobalStats 12 }

      ipSecGlobalInAuthFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound authentication's
            which ended in failure by all current and previous
            IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 13 }

      ipSecGlobalInDecrypts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The total number of inbound decryption's
            performed by all current and previous IPsec
            Phase-2 Tunnels."
         ::= { ipSecGlobalStats 14 }

      ipSecGlobalInDecryptFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound decryption's
            which ended in failure by all current and
            previous IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 15 }

      ipSecGlobalOutOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets sent by all
            current and previous IPsec Phase-2 Tunnels.
            This value is accumulated AFTER determining
            whether or not the packet should be compressed.
            See also ipSecGlobalOutOctWraps for the
             number of times this counter has wrapped."
         ::= { ipSecGlobalStats 16 }

      ipSecGlobalHcOutOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number
            of octets sent by all current and previous
            IPsec Phase-2 Tunnels.  This value is accumulated
            AFTER determining whether or not the packet should
            be compressed."
         ::= { ipSecGlobalStats 17 }

      ipSecGlobalOutOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
```

```
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the global octets sent counter
             (ipSecGlobalOutOctets) has wrapped."
         ::= { ipSecGlobalStats 18 }

      ipSecGlobalOutUncompOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of uncompressed octets sent
          by all current and previous IPsec Phase-2 Tunnels.
          This value is accumulated BEFORE the packet is
          compressed. If compression is not being used, this
          value will match the value of ipSecGlobalOutOctets.
          See also ipSecGlobalOutDecompOctWraps for the number
          of times this counter has wrapped."
         ::= { ipSecGlobalStats 19 }

      ipSecGlobalHcOutUncompOctets OBJECT-TYPE
         SYNTAX Counter64
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
       "A high capacity count of the total number of
       uncompressed octets sent by all current and previous
       IPsec Phase-2 Tunnels.  This value is accumulated
       BEFORE the packet is compressed.  If compression is
       not being used, this value will match the
             value of ipSecGlobalHcOutOctets."
         ::= { ipSecGlobalStats 20 }

      ipSecGlobalOutUncompOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the global uncompressed
            octets sent counter (ipSecGlobalOutUncompOctets)
            has wrapped."
         ::= { ipSecGlobalStats 21 }
```

```
      ipSecGlobalOutPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets sent by all
            current and previous
             IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 22 }

      ipSecGlobalOutDrops OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped during send
            processing by all current and previous IPsec
            Phase-2 Tunnels."
         ::= { ipSecGlobalStats 23 }

      ipSecGlobalOutAuths OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Events"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound authentication's
            performed by all current and previous IPsec
            Phase-2 Tunnels."
         ::= { ipSecGlobalStats 24 }

      ipSecGlobalOutAuthFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound authentication's
            which ended in failure
             by all current and previous IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 25 }

      ipSecGlobalOutEncrypts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
```

```
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound encryption's performed
             by all current and previous IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 26 }

      ipSecGlobalOutEncryptFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound encryption's
            which ended in failure by all current and
            previous IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 27 }

      ipSecGlobalOutCompressedPkts    OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The cumulative number of outbound packets across all
            IPsec flows terminating at this device which were
            successfully compressed.
            This number is cumulative since the last system start."
         ::= { ipSecGlobalStats 28 }

      ipSecGlobalOutCompSkippedPkts   OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets across all IPsec
            flows terminating at this devices that were to be compressed
            but which were skipped due to the compression hysteresis.
            This number is cumulative since the last system start."
         ::= { ipSecGlobalStats 29 }

      ipSecGlobalOutCompFailPkts      OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
```

```
         DESCRIPTION
            "The total number of outbound packets across all IPsec
            flows terminating at this device that failed compression
            because they grew in size after compression.
            This number is cumulative since the last system start."
         ::= { ipSecGlobalStats 30 }

      ipSecGlobalOutCompTooSmallPkts  OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets across all IPsec
            flows terminating at this device that were to be compressed
            but were smaller than the compression threshold size.
            This number is cumulative since the last system start."
         ::= { ipSecGlobalStats 31 }

      ipSecGlobalProtocolUseFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of protocol use failures
            which occurred during processing of all current
            and previously active IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 32 }

      ipSecGlobalNoSaFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of non-existent Security Association
            in failures which occurred during processing of all
            current and previous IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 33 }

      ipSecGlobalSysCapFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
```

```
            "The total number of system capacity failures
            which occurred during processing of all current
            and previously active IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 34 }

      ipSecGlobalHcPreviousTunnels OBJECT-TYPE
         SYNTAX Counter64
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of
          previously active IPsec Phase-2 Tunnels."
         ::= { ipSecGlobalStats 35 }

      ipSecGlobalPreviousTunnelsWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
          "The number of times the quantit
          `ipSecGlobalPreviousTunnels' (previously active IPse
          Phase-2 tunnels) has wrapped."
         ::= { ipSecGlobalStats 36 }


   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-2 Tunnel Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecTunnelTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IpSecTunnelEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-2 Tunnel Table.
            There is one entry in this table for
            each active IPsec Phase-2 Tunnel."
         ::= { ipSecPhaseTwo 2 }

      ipSecTunnelEntry OBJECT-TYPE
         SYNTAX IpSecTunnelEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "Each entry contains the attributes
            associated with an active IPsec Phase-2 Tunnel."
```

```
      INDEX { ipSecTunIndex }
      ::= { ipSecTunnelTable 1 }

   IpSecTunnelEntry ::= SEQUENCE {
      ipSecTunIndex               Integer32,
      ipSecTunIkeTunnelIndex      Integer32,
      ipSecTunIkeTunnelAlive      TruthValue,
      ipSecTunLocalAddr           IPSIpAddress,
      ipSecTunRemoteAddr          IPSIpAddress,
      ipSecTunKeyType             KeyType,
      ipSecTunEncapMode           EncapMode,
      ipSecTunLifeSize            Integer32,
      ipSecTunLifeTime            Integer32,
      ipSecTunActiveTime          TimeInterval,
      ipSecTunSaLifeSizeThreshold Integer32,
      ipSecTunSaLifeTimeThreshold Integer32,
      ipSecTunTotalRefreshes      Counter32,
      ipSecTunExpiredSaInstances  Counter32,
      ipSecTunCurrentSaInstances  Gauge32,
      ipSecTunInSaDiffHellmanGrp  DiffHellmanGrp,
      ipSecTunInSaEncryptAlgo     EncryptAlgo,
      ipSecTunInSaAhAuthAlgo      AuthAlgo,
      ipSecTunInSaEspAuthAlgo     AuthAlgo,
      ipSecTunInSaDecompAlgo      CompAlgo,
      ipSecTunOutSaDiffHellmanGrp DiffHellmanGrp,
      ipSecTunOutSaEncryptAlgo    EncryptAlgo,
      ipSecTunOutSaAhAuthAlgo     AuthAlgo,
      ipSecTunOutSaEspAuthAlgo    AuthAlgo,
      ipSecTunOutSaCompAlgo       CompAlgo,
      ipSecTunPmtu                Integer32,
      ipSecTunInOctets            Counter32,
      ipSecTunHcInOctets          Counter64,
      ipSecTunInOctWraps          Counter32,
      ipSecTunInDecompOctets      Counter32,
      ipSecTunHcInDecompOctets    Counter64,
      ipSecTunInDecompOctWraps    Counter32,
      ipSecTunInPkts              Counter32,
      ipSecTunInDropPkts          Counter32,
      ipSecTunInReplayDropPkts    Counter32,
      ipSecTunInAuths             Counter32,
      ipSecTunInAuthFails         Counter32,
      ipSecTunInDecrypts          Counter32,
      ipSecTunInDecryptFails      Counter32,
      ipSecTunOutOctets           Counter32,
      ipSecTunHcOutOctets         Counter64,
      ipSecTunOutOctWraps         Counter32,
      ipSecTunOutUncompOctets     Counter32,
```

```
      ipSecTunHcOutUncompOctets    Counter64,
      ipSecTunOutUncompOctWraps    Counter32,
      ipSecTunOutPkts              Counter32,
      ipSecTunOutDropPkts          Counter32,
      ipSecTunOutAuths             Counter32,
      ipSecTunOutAuthFails         Counter32,
      ipSecTunOutEncrypts          Counter32,
      ipSecTunOutEncryptFails      Counter32,
      ipSecTunOutCompressedPkts    Counter32,
      ipSecTunOutCompSkippedPkts   Counter32,
      ipSecTunOutCompFailPkts      Counter32,
      ipSecTunOutCompTooSmallPkts  Counter32,
      ipSecTunStatus               TunnelStatus,
      ipSecTunControlProtocol      ControlProtocol,
      ipSecTunControlTunnelIndex   Integer32,
      ipSecTunControlTunnelAlive   TruthValue,
      ipSecTunInSaEncryptKeySize   Integer32,
      ipSecTunOutSaEncryptKeySize  Integer32
   }

   ipSecTunIndex OBJECT-TYPE
      SYNTAX Integer32 (1..2147483647)
      MAX-ACCESS not-accessible
      STATUS current
      DESCRIPTION
         "The index of the IPsec Phase-2 Tunnel Table.
          The value of the index is a number which begins
          at one and is incremented with each tunnel that
          is created. The value of this object will wrap
          at 2,147,483,647."
      ::= { ipSecTunnelEntry 1 }

   ipSecTunIkeTunnelIndex OBJECT-TYPE
      SYNTAX Integer32 (1..2147483647)
      MAX-ACCESS read-only
      STATUS deprecated
      DESCRIPTION
         "The index of the associated IPsec Phase-1
         IKE Tunnel.
          (ikeTunIndex in the ikeTunnelTable)"
      ::= { ipSecTunnelEntry 2 }

   ipSecTunIkeTunnelAlive OBJECT-TYPE
      SYNTAX TruthValue
      MAX-ACCESS read-only
      STATUS deprecated
      DESCRIPTION
```

```
            "An indicator which specifies whether or not the
             IPsec Phase-1 IKE Tunnel currently exists. This object
             has been deprecated in favour of more generic pointers
             to the control tunnel (ipSecTunControlTunnelIndex)."
         ::= { ipSecTunnelEntry 3 }

      ipSecTunLocalAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the local endpoint for the IPsec
             Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 4 }

      ipSecTunRemoteAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the remote endpoint for the IPsec
             Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 5 }

      ipSecTunKeyType OBJECT-TYPE
         SYNTAX KeyType
         MAX-ACCESS read-only
         STATUS deprecated
         DESCRIPTION
            "The type of key used by the IPsec Phase-2 Tunnel. This
            object has been deprecated in favour o
            ipSecTunControlProtocol."
         ::= { ipSecTunnelEntry 6 }

      ipSecTunEncapMode OBJECT-TYPE
         SYNTAX EncapMode
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The encapsulation mode used by the
            IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 7 }

      ipSecTunLifeSize OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         UNITS "KBytes"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The negotiated LifeSize of the
            IPsec Phase-2 Tunnel in kilobytes."
         ::= { ipSecTunnelEntry 8 }

      ipSecTunLifeTime OBJECT-TYPE
         SYNTAX Integer32 (0..2147483647)
         UNITS "Seconds"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The negotiated LifeTime of the IPsec Phase-
            Tunnel in seconds.

            If the tunnel was setup manually, the value of this
            MIB element should be 0."
         ::= { ipSecTunnelEntry 9 }

      ipSecTunActiveTime OBJECT-TYPE
         SYNTAX TimeInterval
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The length of time the IPsec Phase-2
            Tunnel has been
             active in hundredths of seconds."
         ::= { ipSecTunnelEntry 10 }

      ipSecTunSaLifeSizeThreshold OBJECT-TYPE
         SYNTAX Integer32 (0..2147483647)
         UNITS "KBytes"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The security association LifeSize refresh
            threshold in kilobytes.

            If the tunnel was setup manually, the value of this
            MIB element should be 0."
         ::= { ipSecTunnelEntry 11 }

      ipSecTunSaLifeTimeThreshold OBJECT-TYPE
         SYNTAX Integer32 (0..2147483647)
         UNITS "Seconds"
         MAX-ACCESS read-only
         STATUS current
```

```
         DESCRIPTION
            "The security association LifeTime refresh
            threshold in seconds.

            If the tunnel was setup manually, the value of this
            MIB element should be 0."
         ::= { ipSecTunnelEntry 12 }

      ipSecTunTotalRefreshes OBJECT-TYPE
         SYNTAX Counter32
         UNITS "QM Exchanges"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of security
            association refreshes performed."
         ::= { ipSecTunnelEntry 13 }

      ipSecTunExpiredSaInstances OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SAs"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of security associations
            which have expired.

            If the tunnel was setup manually, the value of this
            MIB element should be 0."
         ::= { ipSecTunnelEntry 14 }

      ipSecTunCurrentSaInstances OBJECT-TYPE
         SYNTAX Gauge32
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of security associations
            which are currently active or expiring."
         ::= { ipSecTunnelEntry 15 }

      ipSecTunInSaDiffHellmanGrp OBJECT-TYPE
        SYNTAX DiffHellmanGrp
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The Diffie Hellman Group used
            by the inbound security association of the
```

```
            IPsec Phase-2 Tunnel.

            If the tunnel was setup manually, the value of this
            MIB element would be `none'."
         ::= { ipSecTunnelEntry 16 }

      ipSecTunInSaEncryptAlgo OBJECT-TYPE
         SYNTAX EncryptAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The encryption algorithm used by the inbound security
             association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 17 }

      ipSecTunInSaAhAuthAlgo OBJECT-TYPE
         SYNTAX AuthAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication algorithm used by the inbound
             authentication header (AH) security association of
             the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 18 }

      ipSecTunInSaEspAuthAlgo OBJECT-TYPE
         SYNTAX AuthAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication algorithm used by the inbound
             ecapsulation security protocol (ESP) security
             association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 19 }

      ipSecTunInSaDecompAlgo OBJECT-TYPE
         SYNTAX CompAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The decompression algorithm used by the inbound
             security association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 20 }

      ipSecTunOutSaDiffHellmanGrp OBJECT-TYPE
         SYNTAX DiffHellmanGrp
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The Diffie Hellman Group used by the outbound security
             association of the IPsec Phase-2 Tunnel.

             If the tunnel was setup manually, the value of this
             MIB element would be 'none'."
         ::= { ipSecTunnelEntry 21 }

      ipSecTunOutSaEncryptAlgo OBJECT-TYPE
         SYNTAX EncryptAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The encryption algorithm used by the outbound security
             association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 22 }

      ipSecTunOutSaAhAuthAlgo OBJECT-TYPE
         SYNTAX AuthAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication algorithm used by the outbound
             authentication header (AH) security association of
             the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 23 }

      ipSecTunOutSaEspAuthAlgo OBJECT-TYPE
         SYNTAX AuthAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication algorithm used by the inbound
             encapsulation security protocol (ESP)
             security association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 24 }

      ipSecTunOutSaCompAlgo OBJECT-TYPE
         SYNTAX CompAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The compression algorithm used by the inbound
             security association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 25 }
```

```
      ipSecTunPmtu OBJECT-TYPE
         SYNTAX Integer32 (68..1500)
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The Path MTU for this IPsec Phase-2 tunnel, which ha
            been either learnt from the network or which has been
            specified by the administrator. The lower end of the
            range is 68 which is the minimum MTU for IPv4."
         ::= { ipSecTunnelEntry 26 }

      ipSecTunInOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets received by this IPsec
             Phase-2 Tunnel.  This value is accumulated
             BEFORE determining whether or not the packet should be
             decompressed.  See also ipSecTunInOctWraps for the
             number of times this counter has wrapped."
         ::= { ipSecTunnelEntry 27 }

      ipSecTunHcInOctets OBJECT-TYPE
         SYNTAX Counter64
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of octets
             received by this IPsec Phase-2 Tunnel.  This value is
             accumulated BEFORE determining whether or not the packet
             should be decompressed."
         ::= { ipSecTunnelEntry 28 }

      ipSecTunInOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the octets received counter
             (ipSecTunInOctets) has wrapped."
         ::= { ipSecTunnelEntry 29 }
```

```
      ipSecTunInDecompOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of decompressed octets received
            by this IPsec Phase-2 Tunnel. This value is
            accumulated AFTER the packet is decompressed.
            If compression is not being
             used, this value will match the value of
             ipSecTunInOctets.  See also ipSecTunInDecompOctWraps
             for the number of times
             this counter has wrapped."
         ::= { ipSecTunnelEntry 30 }

      ipSecTunHcInDecompOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of decompressed
             octets received by this IPsec Phase-2 Tunnel.  This value
             is accumulated AFTER the packet is decompressed. If
             compression is not being used, this value will match the
             value of ipSecTunHcInOctets."
         ::= { ipSecTunnelEntry 31 }

      ipSecTunInDecompOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the decompressed
            octets received counter
             (ipSecTunInDecompOctets) has wrapped."
         ::= { ipSecTunnelEntry 32 }

      ipSecTunInPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets received
            by this IPsec Phase-2 Tunnel."
```

```
         ::= { ipSecTunnelEntry 33 }

      ipSecTunInDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped
            during receive processing by this IPsec Phase-2
            Tunnel. This count does NOT include
             packets dropped due to Anti-Replay processing."
         ::= { ipSecTunnelEntry 34 }

      ipSecTunInReplayDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped during
            receive processing due to Anti-Replay processing
            by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 35 }

      ipSecTunInAuths OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Events"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound
            authentication's performed by this
            IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 36 }

      ipSecTunInAuthFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound authentication's
            which ended in
             failure by this IPsec Phase-2 Tunnel ."
         ::= { ipSecTunnelEntry 37 }
```

```
      ipSecTunInDecrypts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound decryption's performed
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 38 }

      ipSecTunInDecryptFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound decryption's
            which ended in failure
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 39 }

      ipSecTunOutOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets sent by this IPsec
             Phase-2 Tunnel.  This value is accumulated
             AFTER determining whether or not the packet should
             be compressed.  See also ipSecTunOutOctWraps for
             the number of times this counter has wrapped."
         ::= { ipSecTunnelEntry 40 }

      ipSecTunHcOutOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of octets
             sent by this IPsec Phase-2 Tunnel.  This value is
             accumulated AFTER determining whether or not the
             packet
             should be compressed."
         ::= { ipSecTunnelEntry 41 }

      ipSecTunOutOctWraps OBJECT-TYPE
```

```
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the out octets counter
             (ipSecTunOutOctets) has wrapped."
         ::= { ipSecTunnelEntry 42 }

      ipSecTunOutUncompOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of uncompressed octets sent
            by this IPsec Phase-2 Tunnel.  This value
            is accumulated BEFORE the packet is compressed.
            If compression is not being used, this value
            will match the value of ipSecTunOutOctets.
             See also ipSecTunOutDecompOctWraps for the
             number of times this counter has wrapped."
         ::= { ipSecTunnelEntry 43 }

      ipSecTunHcOutUncompOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number
            of uncompressed octets sent by this IPsec
            Phase-2 Tunnel.  This value is accumulated BEFORE
            the packet is compressed. If compression
             is not being used, this value will match the value
             of ipSecTunHcOutOctets."
         ::= { ipSecTunnelEntry 44 }

      ipSecTunOutUncompOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the uncompressed octets sent
             counter (ipSecTunOutUncompOctets) has wrapped."
         ::= { ipSecTunnelEntry 45 }
```

```
      ipSecTunOutPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets sent by this
            IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 46 }

      ipSecTunOutDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped during
            send processing by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 47 }

      ipSecTunOutAuths OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Events"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound authentication's performed
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 48 }

      ipSecTunOutAuthFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound
            authentication's which ended in failure
            by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 49 }

      ipSecTunOutEncrypts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
```

```
            "The total number of outbound encryption's performed
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 50 }

      ipSecTunOutEncryptFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound encryption's
            which ended in failure by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelEntry 51 }

      ipSecTunOutCompressedPkts    OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets
            which were successfully compressed."
         ::= { ipSecTunnelEntry 52 }

      ipSecTunOutCompSkippedPkts   OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets that were to be
            compressed but which were skipped due to the compression
            hysteresis."
         ::= { ipSecTunnelEntry 53 }

      ipSecTunOutCompFailPkts      OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets that failed
            compression because they grew in size after compression."
         ::= { ipSecTunnelEntry 54 }

      ipSecTunOutCompTooSmallPkts  OBJECT-TYPE
         SYNTAX Counter32
```

```
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets that were to be
            compressed but were smaller than the compression threshold
            size."
         ::= { ipSecTunnelEntry 55 }

      ipSecTunStatus OBJECT-TYPE
         SYNTAX TunnelStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "The status of the MIB table row.

             This object can be used to bring the tunnel down
             by setting value of this object to destroy(2).
             When the value is set to destroy(2), the SA
             bundle is destroyed and this row is deleted
             from this table.

             When this MIB value is queried, the value of
             active(1) is always returned, if the instance
             exists.

             This object cannot be used to create a MIB
             table row."
         ::= { ipSecTunnelEntry 56 }

      ipSecTunControlProtocol OBJECT-TYPE
         SYNTAX ControlProtocol
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "Identifies the protocol used to setup and administer this
            Phase-2 Ipsec tunnel. If IKE was used to setup this tunnel,
            then this value of this column would be `cp_ike'. A value of
            cp_none is indicative of a manually installed and administered
            Phase-2 tunnel."
         ::= { ipSecTunnelEntry 57 }

      ipSecTunControlTunnelIndex OBJECT-TYPE
         SYNTAX Integer32 (0..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
```

```
            "The index of the associated IPsec Phase-1
            Tunnel (in case of IKE, this value would refer t
            ikeTunIndex in the ikeTunnelTable).

            A value of 0 identifies that this Phase-2 tunne
            was setup manually."
         ::= { ipSecTunnelEntry 58 }

      ipSecTunControlTunnelAlive OBJECT-TYPE
         SYNTAX TruthValue
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "An indicator which specifies whether or not the
             IPsec Phase-1 Tunnel that spawned this Phase-2
             tunnel currently exists."
         ::= { ipSecTunnelEntry 59 }

      ipSecTunInSaEncryptKeySize   OBJECT-TYPE
         SYNTAX Integer32
         UNITS "Bits"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The key size in bits of the negotiated key to be
            used with the algorithm denoted by ipSecTunInSaEncryptAlgo.
            For DES and 3DES the key size is respectively 56 and
            168. For AES, this will denote the negotiated key size."
         ::= { ipSecTunnelEntry 60 }

      ipSecTunOutSaEncryptKeySize  OBJECT-TYPE
         SYNTAX Integer32
         UNITS "Bits"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The key size in bits of the negotiated key to be
            used with the algorithm denoted by ipSecTunOutSaEncryptAlgo.
            For DES and 3DES the key size is respectively 56 and
            168. For AES, this will denote the negotiated key size."
         ::= { ipSecTunnelEntry 61 }


   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-2 Tunnel Endpoint Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecEndPtTable OBJECT-TYPE
```

```
         SYNTAX SEQUENCE OF IpSecEndPtEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-2 Tunnel Endpoint Table.
            This table contains an entry for each
            active endpoint associated with an IPsec
             Phase-2 Tunnel."
         ::= { ipSecPhaseTwo 3 }

      ipSecEndPtEntry OBJECT-TYPE
         SYNTAX IpSecEndPtEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "An IPsec Phase-2 Tunnel Endpoint entry."
         INDEX { ipSecTunIndex,  -- from ipSecTunnelTable
                 ipSecEndPtIndex  }
         ::= { ipSecEndPtTable 1 }

      IpSecEndPtEntry ::= SEQUENCE {
         ipSecEndPtIndex               Integer32,
         ipSecEndPtLocalName           DisplayString,
         ipSecEndPtLocalType           EndPtType,
         ipSecEndPtLocalAddr1          IPSIpAddress,
         ipSecEndPtLocalAddr2          IPSIpAddress,
         ipSecEndPtLocalProtocol       Integer32,
         ipSecEndPtLocalPort           Integer32,
         ipSecEndPtRemoteName          DisplayString,
         ipSecEndPtRemoteType          EndPtType,
         ipSecEndPtRemoteAddr1         IPSIpAddress,
         ipSecEndPtRemoteAddr2         IPSIpAddress,
         ipSecEndPtRemoteProtocol      Integer32,
         ipSecEndPtRemotePort          Integer32
      }

      ipSecEndPtIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The number of the Endpoint associated with the
             IPsec Phase-2 Tunnel Table.  The value of this
             index is a number which begins at one and
             is incremented with each Endpoint associated
             with an IPsec Phase-2 Tunnel.
             The value of this object will wrap at 2,147,483,647."
```

```
         ::= { ipSecEndPtEntry 1 }

      ipSecEndPtLocalName OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The DNS name of the local Endpoint."
         ::= { ipSecEndPtEntry 2 }

      ipSecEndPtLocalType OBJECT-TYPE
         SYNTAX EndPtType
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The type of identity for the local Endpoint.
             Possible values are:
             1) a single IP address, or
             2) an IP address range, or
             3) an IP subnet."
         ::= { ipSecEndPtEntry 3 }

      ipSecEndPtLocalAddr1 OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
           "The local Endpoint's first IP address specification.

            If the local Endpoint type is single IP address,
            then this is the value of the IP address.

            If the local Endpoint type is IP subnet, then this
            is the value of the subnet.

            If the local Endpoint type is IP address range,
            then this is the value of beginning IP address
            of the range."
         ::= { ipSecEndPtEntry 4 }

      ipSecEndPtLocalAddr2 OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
           "The local Endpoint's second IP address specification.
```

```
            If the local Endpoint type is single IP address,
            then this is the value of the IP address.

            If the local Endpoint type is IP subnet, then this
            is the value of the subnet mask.

            If the local Endpoint type is IP address range,
            then this is the value of ending IP address
            of the range."
         ::= { ipSecEndPtEntry 5 }

      ipSecEndPtLocalProtocol OBJECT-TYPE
         SYNTAX Integer32 (0..255)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The protocol number of the local Endpoint's traffic."
         ::= { ipSecEndPtEntry 6 }

      ipSecEndPtLocalPort OBJECT-TYPE
         SYNTAX Integer32 (0..65535)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The port number of the local Endpoint's traffic."
         ::= { ipSecEndPtEntry 7 }

      ipSecEndPtRemoteName OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The DNS name of the remote Endpoint."
         ::= { ipSecEndPtEntry 8 }

      ipSecEndPtRemoteType OBJECT-TYPE
         SYNTAX EndPtType
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The type of identity for the remote Endpoint.
             Possible values are:
             1) a single IP address, or
             2) an IP address range, or
             3) an IP subnet."
         ::= { ipSecEndPtEntry 9 }
```

```
      ipSecEndPtRemoteAddr1 OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
           "The remote Endpoint's first IP address specification.

            If the remote Endpoint type is single IP address,
            then this is the value of the IP address.

            If the remote Endpoint type is IP subnet, then this
            is the value of the subnet.

            If the remote Endpoint type is IP address range,
            then this is the value of beginning IP address
            of the range."
         ::= { ipSecEndPtEntry 10 }

      ipSecEndPtRemoteAddr2 OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
           "The remote Endpoint's second IP address specification.

            If the remote Endpoint type is single IP address,
            then this is the value of the IP address.

            If the remote Endpoint type is IP subnet, then this
            is the value of the subnet mask.

            If the remote Endpoint type is IP address range,
            then this is the value of ending IP address of
            the range."
         ::= { ipSecEndPtEntry 11 }

      ipSecEndPtRemoteProtocol OBJECT-TYPE
         SYNTAX Integer32 (0..255)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The protocol number of the remote Endpoint's traffic."
         ::= { ipSecEndPtEntry 12 }

      ipSecEndPtRemotePort OBJECT-TYPE
         SYNTAX Integer32 (0..65535)
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The port number of the remote Endpoint's traffic."
         ::= { ipSecEndPtEntry 13 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-2 Security Protection Index Table (deprecated)
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++

   -- The tunnel SA decomposition table: This table has been deprecaterd
   -- and has been replaced ipSecSaTable. New IPsec devices will not
   -- support this table.  Older products will continue to support
   -- this table for some time in order to be backwards compatible with
   -- existing network management applications.

      ipSecSpiTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IpSecSpiEntry
         MAX-ACCESS not-accessible
         STATUS deprecated
         DESCRIPTION
            "The IPsec Phase-2 Security Protection Index Table.
            This table contains an entry for each active
            and expiring security
             association."
         ::= { ipSecPhaseTwo 4 }

      ipSecSpiEntry OBJECT-TYPE
         SYNTAX IpSecSpiEntry
         MAX-ACCESS not-accessible
         STATUS deprecated
         DESCRIPTION
            "Each entry contains the attributes associated with
             active and expiring IPsec Phase-2
             security associations."
         INDEX { ipSecTunIndex,  -- from ipSecTunnelTable
                 ipSecSpiIndex  }
         ::= { ipSecSpiTable 1 }

      IpSecSpiEntry ::= SEQUENCE {
         ipSecSpiIndex               Integer32,
         ipSecSpiDirection           INTEGER,
         ipSecSpiValue               Spi,
         ipSecSpiProtocol            INTEGER,
         ipSecSpiStatus              INTEGER
      }

      ipSecSpiIndex OBJECT-TYPE
```

```
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS deprecated
         DESCRIPTION
            "The number of the SPI associated with the
            Phase-2 Tunnel Table.  The value of this
            index is a number which begins at one and is
            incremented with each SPI associated with an
            IPsec Phase-2 Tunnel.  The value of this
            object will wrap at 2,147,483,647."
         ::= { ipSecSpiEntry 1 }

      ipSecSpiDirection OBJECT-TYPE
         SYNTAX INTEGER{
                   in(1),
                   out(2)
                 }
         MAX-ACCESS read-only
         STATUS deprecated
         DESCRIPTION
            "The direction of the SPI."
         ::= { ipSecSpiEntry 2 }

      ipSecSpiValue OBJECT-TYPE
         SYNTAX Spi
         MAX-ACCESS read-only
         STATUS deprecated
         DESCRIPTION
            "The value of the SPI."
         ::= { ipSecSpiEntry 3 }

      ipSecSpiProtocol OBJECT-TYPE
         SYNTAX INTEGER{
                   ah(1),
                   esp(2),
                   ipcomp(3)
                 }
         MAX-ACCESS read-only
         STATUS deprecated
         DESCRIPTION
            "The protocol of the SPI."
         ::= { ipSecSpiEntry 4 }

      ipSecSpiStatus OBJECT-TYPE
         SYNTAX INTEGER{
                   active(1),
                   expiring(2)
```

```
               }
        MAX-ACCESS read-only
        STATUS deprecated
        DESCRIPTION
           "The status of the SPI."
        ::= { ipSecSpiEntry 5 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec New Group metrics
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecGlobalNewGrpStats OBJECT IDENTIFIER
         ::= { ipSecPhaseTwo 5 }

      ipSecGlobalInNewGrpReqs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             remotely."
         ::= { ipSecGlobalNewGrpStats 1 }

      ipSecGlobalOutNewGrpReqs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             locally."
         ::= { ipSecGlobalNewGrpStats 2 }

      ipSecGlobalInNewGrpReqsRejected OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             remotely that ended in a failure."
         ::= { ipSecGlobalNewGrpStats 3 }

      ipSecGlobalOutNewGrpReqsRejected OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             locally that ended in a failure."
         ::= { ipSecGlobalNewGrpStats 4 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-2 Security Association Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++

   -- The tunnel SA decomposition table: This table replaces the
   -- now deprecated ipSecSpiTable.

      ipSecSaTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IpSecSaEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-2 Security Association Table.
            This table identifies the structure (in terms of
            component SAs) of each active Phase-2 IPsec tunnel.
            This table contains an entry for each active and
            expiring security association and maps each entry
            in the active Phase-2 tunnel table (ipSecTunTable)
            into a number of entries in this table. The index of this
            table reflects the

                <destination-address, protocol, spi>

            rule for identifying Security Associations."
         ::= { ipSecPhaseTwo 6 }

      ipSecSaEntry OBJECT-TYPE
         SYNTAX IpSecSaEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "Each entry contains the attributes associated with
             active and expiring IPsec Phase-2
             security associations."
         INDEX { ipSecTunIndex,  -- from ipSecTunnelTable
                 ipSecSaProtocol,
                 ipSecSaIndex  }
         ::= { ipSecSaTable 1 }

      IpSecSaEntry ::= SEQUENCE {
         ipSecSaIndex               Integer32,
```

```
         ipSecSaDirection            INTEGER,
         ipSecSaValue                Spi,
         ipSecSaProtocol             INTEGER,
         ipSecSaStatus               INTEGER
      }

      ipSecSaIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
          "The index, in the context of the IPsec tunnel ipSecTunIndex,
          of the security association represented by this table entry.
          The value of this index is a number which begins at one and
          is incremented with each SPI associated with an IPsec Phase-2
          Tunnel.  The value of this object will wrap at 2,147,483,647."
         ::= { ipSecSaEntry 1 }

      ipSecSaDirection OBJECT-TYPE
         SYNTAX INTEGER{
                   in(1),
                   out(2)
                 }
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "Phase-2 IPsec security associations are simplex. Hence
             a particular security association is used either
             for securing outgoing traffic or decoding incoming traffic.
             This column identifies the direction of the security
             association represented by this entry."
         ::= { ipSecSaEntry 2 }

      ipSecSaValue OBJECT-TYPE
         SYNTAX Spi
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
          "This is the value of the Security Protection Index (SPI)
          assigned by the system to the security association represented
          by this entry."
         ::= { ipSecSaEntry 3 }

      ipSecSaProtocol OBJECT-TYPE
         SYNTAX INTEGER{
                   reserved(0),
                   ah(1),
```

```
                  esp(2),
                  ipcomp(3)
               }
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "This column represents the security protocol (AH, ESP or
             IPComp) for which this security association was setup."
         ::= { ipSecSaEntry 4 }

      ipSecSaStatus OBJECT-TYPE
         SYNTAX INTEGER{
                  unknown(0),
                  active(1),
                  expiring(2)
               }
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
          "This column represents the status of the security association
          represented by this tabel entry. If the status of the SA is
          'active', the SA is ready for active use. The status
          'expiring' represents any of the various states that the
          security association transitions through before being purged."
         ::= { ipSecSaEntry 5 }


   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec History Group
   --
   -- This group consists of a:
   -- 1) IPsec History Global Objects
   -- 2) IPsec Phase-1 History Objects
   -- 3) IPsec Phase-2 History Objects
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecHistGlobal           OBJECT IDENTIFIER
                        ::= { ipSecHistory 1 }
      ipSecHistPhaseOne         OBJECT IDENTIFIER
                        ::= { ipSecHistory 2 }
      ipSecHistPhaseTwo         OBJECT IDENTIFIER
                        ::= { ipSecHistory 3 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- IPsec History Global Control Objects
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecHistGlobalCntl OBJECT IDENTIFIER
                        ::= { ipSecHistGlobal 1 }
```

```
      ipSecHistTableSize  OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "The window size of the IPsec Phase-1 and Phase-2
             History Tables.

             The IPsec Phase-1 and Phase-2 History Tables are
             implemented as a sliding window in which only the
             last n entries are maintained.  This object is used
             specify the number of entries which will be
             maintained in the IPsec Phase-1 and
             Phase-2 History Tables.

             An implementation may choose suitable minimum and
             maximum values for this element based on the local
             policy and available resources. If an SNMP SET request
             specifies a value outside this window for this element,
             a BAD VALUE may be returned."

         ::= { ipSecHistGlobalCntl 1 }

      ipSecHistCheckPoint OBJECT-TYPE
         SYNTAX INTEGER {
                   ready(1),
                   checkPoint(2)
                 }

         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
             "The current state of check point processing.

              This object will return ready when the agent is
              ready to create on-demand history entries for
              active IPsec Tunnels or checkPoint when the
              agent is currently creating on-demand history
              entries for active IPsec Tunnels.

              By setting this value to checkPoint, the agent
              will create:
              a) an entry in the IPsec Phase-1 Tunnel History
                 for each active IPsec Phase-1 Tunnel and
              b) an entry in the IPsec Phase-2 Tunnel History
                 Table and an entry in the IPsec Phase-2
```

```
                Tunnel EndPoint History Table
                for each active IPsec Phase-2 Tunnel."
        ::= { ipSecHistGlobalCntl 2 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-1 Tunnel History Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ikeTunnelHistTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IkeTunnelHistEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-1 Internet Key Exchange Tunnel
            History Table.  This table is implemented as a
            sliding window in which only the last n entries
            are maintained.  The maximum number of entries
             is specified by the ipSecHistTableSize object."
        ::= { ipSecHistPhaseOne 1 }

      ikeTunnelHistEntry OBJECT-TYPE
         SYNTAX IkeTunnelHistEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
               "Each entry contains the attributes
               associated with a previously active IPsec
               Phase-1 IKE Tunnel."
         INDEX { ikeTunHistIndex }
         ::= { ikeTunnelHistTable 1}

      IkeTunnelHistEntry ::= SEQUENCE {
         ikeTunHistIndex                Integer32,
         ikeTunHistTermReason           INTEGER,
         ikeTunHistActiveIndex          Integer32,
         ikeTunHistPeerLocalType        Phase1PeerIdentityType,
         ikeTunHistPeerLocalValue       DisplayString,
         ikeTunHistPeerIntIndex         Integer32,
         ikeTunHistPeerRemoteType       Phase1PeerIdentityType,
         ikeTunHistPeerRemoteValue      DisplayString,
         ikeTunHistLocalAddr            IPSIpAddress,
         ikeTunHistLocalName            DisplayString,
         ikeTunHistRemoteAddr           IPSIpAddress,
         ikeTunHistRemoteName           DisplayString,
         ikeTunHistNegoMode             IkeNegoMode,
         ikeTunHistDiffHellmanGrp       DiffHellmanGrp,
         ikeTunHistEncryptAlgo          EncryptAlgo,
         ikeTunHistHashAlgo             IkeHashAlgo,
```

```
      ikeTunHistAuthMethod            IkeAuthMethod,
      ikeTunHistLifeTime              Integer32,
      ikeTunHistStartTime             TimeStamp,
      ikeTunHistActiveTime            TimeInterval,
      ikeTunHistTotalRefreshes        Counter32,
      ikeTunHistTotalSas              Counter32,
      ikeTunHistInOctets              Counter32,
      ikeTunHistInPkts                Counter32,
      ikeTunHistInDropPkts            Counter32,
      ikeTunHistInNotifys             Counter32,
      ikeTunHistInP2Exchgs            Counter32,
      ikeTunHistInP2ExchgInvalids     Counter32,
      ikeTunHistInP2ExchgRejects      Counter32,
      ikeTunHistInP2SaDelRequests     Counter32,
      ikeTunHistOutOctets             Counter32,
      ikeTunHistOutPkts               Counter32,
      ikeTunHistOutDropPkts           Counter32,
      ikeTunHistOutNotifys            Counter32,
      ikeTunHistOutP2Exchgs           Counter32,
      ikeTunHistOutP2ExchgInvalids    Counter32,
      ikeTunHistOutP2ExchgRejects     Counter32,
      ikeTunHistOutP2SaDelRequests    Counter32,
      ikeTunHistInNewGrpReqs          Counter32,
      ikeTunHistOutNewGrpReqs         Counter32,
      ikeTunHistInNewGrpReqsRejected  Counter32,
      ikeTunHistOutNewGrpReqsRejected Counter32,
      ikeTunHistInConfigs             Counter32,
      ikeTunHistOutConfigs            Counter32,
      ikeTunHistInConfigsRejects      Counter32,
      ikeTunHistOutConfigsRejects     Counter32,
      ikeTunHistEncryptKeySize        Integer32
   }

   ikeTunHistIndex OBJECT-TYPE
      SYNTAX Integer32 (1..2147483647)
      MAX-ACCESS not-accessible
      STATUS current
      DESCRIPTION
         "The index of the IPsec Phase-1 IKE Tunnel History
         Table.  The value of the index is a number which
         begins at one and is incremented with each
         tunnel that ends. The value of this object
         will wrap at 2,147,483,647."
      ::= { ikeTunnelHistEntry 1 }

   ikeTunHistTermReason  OBJECT-TYPE
      SYNTAX INTEGER {
```

```
                    other(1),
                    normal(2),
                    operRequest(3),
                    peerDelRequest(4),
                    peerLost(5),
                    applicationInitiated(6),
                    xauthFailure(7),
                    localFailure(8),
                    checkPointReg(9)
                  }
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
           "The reason the IPsec Phase-1 IKE Tunnel was terminated.
           Possible reasons include:
           1 = other
           2 = normal termination
           3 = operator request
           4 = peer delete request was received
           5 = contact with peer was lost
           6 = applicationInitiated (eg: L2TP requesting the termination)
           7 = failure of extended authentication
           8 = local failure occurred.
           9 = operator initiated check point request"
          ::= { ikeTunnelHistEntry 2 }

      ikeTunHistActiveIndex OBJECT-TYPE
          SYNTAX Integer32 (1..2147483647)
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
             "The index of the previously active IPsec
             Phase-1 IKE Tunnel."
          ::= { ikeTunnelHistEntry 3 }

      ikeTunHistPeerLocalType OBJECT-TYPE
          SYNTAX Phase1PeerIdentityType
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
             "The type of local peer identity.  The local peer
             may be indentified by:
              1. an IP address, or
              2. or a fully qualified domain name.
              3. or a distinguished name."
          ::= { ikeTunnelHistEntry 4 }
```

```
      ikeTunHistPeerLocalValue OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value of the local peer identity.

             If the local peer type is an IP Address, then this
             is the IP Address used to identify the local peer.

             If the local peer type is id_fqdn, then this is
             the FQDN of the local entity.

             If the local peer type is a id_dn, then this is
             the distinguished named string of the local entity."
         ::= { ikeTunnelHistEntry 5 }

      ikeTunHistPeerIntIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The internal index of the local-remote peer
            association.  This internal index is used to
            uniquely identify multiple associations between
            the local and remote peer."
         ::= { ikeTunnelHistEntry 6 }

      ikeTunHistPeerRemoteType OBJECT-TYPE
         SYNTAX Phase1PeerIdentityType
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The type of remote peer identity.  The remote
            peer may be indentified by:
             1. an IP address, or
             2. or a fully qualified domain name.
             3. or a distinguished name."
         ::= { ikeTunnelHistEntry 7 }

      ikeTunHistPeerRemoteValue OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value of the remote peer identity.
```

```
            If the remote peer type is an IP Address, then this
            is the IP Address used to identify the remote peer.

            If the remote peer type is id_fqdn, then this is
            the FQDN of the remote peer.

            If the remote peer type is a id_dn, then this is
            the distinguished named string of the remote peer."
         ::= { ikeTunnelHistEntry 8 }

      ikeTunHistLocalAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the local endpoint for the IPsec
             Phase-1 IKE Tunnel."
         ::= { ikeTunnelHistEntry 9 }

      ikeTunHistLocalName OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The DNS name of the local IP address for
            the IPsec Phase-1 IKE Tunnel. If the DNS
            name associated with the local tunnel endpoint
            is not known, then the value of this
             object will be a NULL string."
         ::= { ikeTunnelHistEntry 10 }

      ikeTunHistRemoteAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the remote endpoint for the IPsec
             Phase-1 IKE Tunnel."
         ::= { ikeTunnelHistEntry 11 }

      ikeTunHistRemoteName OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The DNS name of the remote IP address of IPsec Phase-1
             IKE Tunnel. If the DNS name associated with the remote
```

```
            tunnel endpoint is not known, then the value of this
            object will be a NULL string."
         ::= { ikeTunnelHistEntry 12 }

      ikeTunHistNegoMode OBJECT-TYPE
         SYNTAX IkeNegoMode
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The negotiation mode of the IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelHistEntry 13 }

      ikeTunHistDiffHellmanGrp OBJECT-TYPE
         SYNTAX DiffHellmanGrp
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The Diffie Hellman Group used in IPsec Phase-1 IKE
             negotiations."
         ::= { ikeTunnelHistEntry 14 }

      ikeTunHistEncryptAlgo OBJECT-TYPE
         SYNTAX EncryptAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The encryption algorithm used in IPsec Phase-1 IKE
             negotiations."
         ::= { ikeTunnelHistEntry 15 }

      ikeTunHistHashAlgo OBJECT-TYPE
         SYNTAX IkeHashAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The hash algorithm used in IPsec Phase-1 IKE
             negotiations."
         ::= { ikeTunnelHistEntry 16 }

      ikeTunHistAuthMethod OBJECT-TYPE
         SYNTAX IkeAuthMethod
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication method used in IPsec Phase-1 IKE
             negotiations."
         ::= { ikeTunnelHistEntry 17 }
```

```
      ikeTunHistLifeTime OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The negotiated LifeTime of the IPsec Phase-1 IKE Tunnel
             in seconds."
         ::= { ikeTunnelHistEntry 18 }

      ikeTunHistStartTime OBJECT-TYPE
         SYNTAX TimeStamp
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value of sysUpTime in hundredths of seconds
            when the IPsec Phase-1 IKE tunnel was started."
         ::= { ikeTunnelHistEntry 19 }

      ikeTunHistActiveTime OBJECT-TYPE
         SYNTAX TimeInterval
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The length of time the IPsec Phase-1 IKE tunnel was been
             active in hundredths of seconds."
         ::= { ikeTunnelHistEntry 20 }

      ikeTunHistTotalRefreshes OBJECT-TYPE
         SYNTAX Counter32
         UNITS "QM Exchanges"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of security associations
            refreshes performed."
         ::= { ikeTunnelHistEntry 21 }

      ikeTunHistTotalSas       OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SAs"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of security associations
            used during the
             life of the IPsec Phase-1 IKE Tunnel."
```

```
         ::= { ikeTunnelHistEntry 22 }

      ikeTunHistInOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets received by this
             IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelHistEntry 23 }

      ikeTunHistInPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets received
            by this IPsec Phase-1
             IKE Tunnel."
         ::= { ikeTunnelHistEntry 24 }

      ikeTunHistInDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped
            by this IPsec Phase-1
             IKE Tunnel during receive processing."
         ::= { ikeTunnelHistEntry 25 }

      ikeTunHistInNotifys OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of notifys received
            by this IPsec Phase-1
             IKE Tunnel."
         ::= { ikeTunnelHistEntry 26 }

      ikeTunHistInP2Exchgs OBJECT-TYPE
         SYNTAX Counter32
```

```
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2
            exchanges received by
             this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelHistEntry 27 }

      ikeTunHistInP2ExchgInvalids OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            received on this tunnel that were found to
            contain references to unrecognized security
            parameters."
         ::= { ikeTunnelHistEntry 28 }

      ikeTunHistInP2ExchgRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            received on this tunnel that were validated but were
            rejected by the local policy."
         ::= { ikeTunnelHistEntry 29 }

      ikeTunHistInP2SaDelRequests OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 security association
             delete requests received by this IPsec
             Phase-1 IKE Tunnel."
         ::= { ikeTunnelHistEntry 30 }

      ikeTunHistOutOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The total number of octets sent by this IPsec Phase-1
             IKE Tunnel."
         ::= { ikeTunnelHistEntry 31 }

      ikeTunHistOutPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets sent by this IPsec Phase-1
             IKE Tunnel."
         ::= { ikeTunnelHistEntry 32 }

      ikeTunHistOutDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped
            by this IPsec Phase-1
             IKE Tunnel during send processing."
         ::= { ikeTunnelHistEntry 33 }

      ikeTunHistOutNotifys OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of notifys sent by this IPsec Phase-1
             IKE Tunnel."
         ::= { ikeTunnelHistEntry 34 }

      ikeTunHistOutP2Exchgs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges sent by
             this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelHistEntry 35 }
```

```
      ikeTunHistOutP2ExchgInvalids OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            sent on this tunnel that were found by the peer
            to contain references to security parameters
            not recognized by the peer."
         ::= { ikeTunnelHistEntry 36 }

      ikeTunHistOutP2ExchgRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SA Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 exchanges
            sent on this tunnel that were validated by the peer
            but were rejected by the peer's policy."
         ::= { ikeTunnelHistEntry 37 }

      ikeTunHistOutP2SaDelRequests OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Notification Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of IPsec Phase-2 security association
             delete requests sent by this IPsec Phase-1 IKE Tunnel."
         ::= { ikeTunnelHistEntry 38 }

      ikeTunHistInNewGrpReqs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             remotely using this IKE tunnel during its lifetime."
         ::= { ikeTunnelHistEntry 39 }

      ikeTunHistOutNewGrpReqs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             locally using this IKE tunnel during its lifetime."
         ::= { ikeTunnelHistEntry 40 }

      ikeTunHistInNewGrpReqsRejected OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             remotely using this IKE tunnel during its lifetime
             that ended in a failure."
         ::= { ikeTunnelHistEntry 41 }

      ikeTunHistOutNewGrpReqsRejected OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Negotiations"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of New Group exchanges initiated
             locally using this IKE tunnel during its lifetime
             that ended in a failure."
         ::= { ikeTunnelHistEntry 42 }

      ikeTunHistInConfigs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            received (either CFG_REPLY or CFG_SET payloads)
            by the local entity on the ISAKMP SA represented by this
            IKE tunnel."
         ::= { ikeTunnelHistEntry 43 }

      ikeTunHistOutConfigs OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
```

```
            dispatched (either CFG_REPLY or CFG_SET payloads)
            by the local entity on the ISAKMP SA represented by this
            IKE tunnel."
         ::= { ikeTunnelHistEntry 44 }

      ikeTunHistInConfigsRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            which were received (either CFG_REPLY or CFG_SET
            payloads) and rejected by this entity using the ISAKMP
            SA represented by this IKE tunnel."
         ::= { ikeTunnelHistEntry 45 }

      ikeTunHistOutConfigsRejects OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Mode Configuration Setting Payloads"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of Mode Configuration settings
            which were dispatched (either CFG_REPLY or CFG_SET
            payloads) by this entity and were rejected by the
            peer (client) using the ISAKMP SA represented by this
            IKE tunnel."
         ::= { ikeTunnelHistEntry 46 }

      ikeTunHistEncryptKeySize        OBJECT-TYPE
         SYNTAX Integer32
         UNITS "Bits"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The size in bits of the key which was negotiated
            for the IKE tunnel to be used with the algorithm denote
            by the column 'ikeTunEncryptAlgo'. For DES and 3DES the ke
            size is respectively 56 and 168. For AES, this will denot
            the negotiated key size."
         ::= { ikeTunnelHistEntry 47 }


   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-2 Tunnel History Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

```
      ipSecTunnelHistTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IpSecTunnelHistEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-2 Tunnel History Table.
             This table is implemented as a sliding
             window in which only the
             last n entries are maintained.  The maximum number
             of entries
             is specified by the ipSecHistTableSize object."
         ::= { ipSecHistPhaseTwo 1 }

      ipSecTunnelHistEntry OBJECT-TYPE
         SYNTAX IpSecTunnelHistEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "Each entry contains the attributes associated with
             a previously active IPsec Phase-2 Tunnel."
         INDEX { ipSecTunHistIndex }
         ::= { ipSecTunnelHistTable 1 }

      IpSecTunnelHistEntry ::= SEQUENCE {
         ipSecTunHistIndex               Integer32,
         ipSecTunHistTermReason          INTEGER,
         ipSecTunHistActiveIndex         Integer32,
         ipSecTunHistIkeTunnelIndex      Integer32,
         ipSecTunHistLocalAddr           IPSIpAddress,
         ipSecTunHistRemoteAddr          IPSIpAddress,
         ipSecTunHistKeyType             KeyType,
         ipSecTunHistEncapMode           EncapMode,
         ipSecTunHistLifeSize            Integer32,
         ipSecTunHistLifeTime            Integer32,
         ipSecTunHistStartTime           TimeStamp,
         ipSecTunHistActiveTime          TimeInterval,
         ipSecTunHistTotalRefreshes      Counter32,
         ipSecTunHistTotalSas            Counter32,
         ipSecTunHistInSaDiffHellmanGrp  DiffHellmanGrp,
         ipSecTunHistInSaEncryptAlgo     EncryptAlgo,
         ipSecTunHistInSaAhAuthAlgo      AuthAlgo,
         ipSecTunHistInSaEspAuthAlgo     AuthAlgo,
         ipSecTunHistInSaDecompAlgo      CompAlgo,
         ipSecTunHistOutSaDiffHellmanGrp DiffHellmanGrp,
         ipSecTunHistOutSaEncryptAlgo    EncryptAlgo,
         ipSecTunHistOutSaAhAuthAlgo     AuthAlgo,
         ipSecTunHistOutSaEspAuthAlgo    AuthAlgo,
```

```
        ipSecTunHistOutSaCompAlgo       CompAlgo,
        ipSecTunHistPmtu                Integer32,
        ipSecTunHistInOctets            Counter32,
        ipSecTunHistHcInOctets          Counter64,
        ipSecTunHistInOctWraps          Counter32,
        ipSecTunHistInDecompOctets      Counter32,
        ipSecTunHistHcInDecompOctets    Counter64,
        ipSecTunHistInDecompOctWraps    Counter32,
        ipSecTunHistInPkts              Counter32,
        ipSecTunHistInReplayDropPkts    Counter32,
        ipSecTunHistInDropPkts          Counter32,
        ipSecTunHistInAuths             Counter32,
        ipSecTunHistInAuthFails         Counter32,
        ipSecTunHistInDecrypts          Counter32,
        ipSecTunHistInDecryptFails      Counter32,
        ipSecTunHistOutOctets           Counter32,
        ipSecTunHistHcOutOctets         Counter64,
        ipSecTunHistOutOctWraps         Counter32,
        ipSecTunHistOutUncompOctets     Counter32,
        ipSecTunHistHcOutUncompOctets   Counter64,
        ipSecTunHistOutUncompOctWraps   Counter32,
        ipSecTunHistOutPkts             Counter32,
        ipSecTunHistOutDropPkts         Counter32,
        ipSecTunHistOutAuths            Counter32,
        ipSecTunHistOutAuthFails        Counter32,
        ipSecTunHistOutEncrypts         Counter32,
        ipSecTunHistOutEncryptFails     Counter32,
        ipSecTunHistOutCompressedPkts   Counter32,
        ipSecTunHistOutCompSkippedPkts  Counter32,
        ipSecTunHistOutCompFailPkts     Counter32,
        ipSecTunHistOutCompTooSmallPkts Counter32,
        ipSecTunHistControlProtocol     ControlProtocol,
        ipSecTunHistControlTunnelIndex  Integer32,
        ipSecTunHistInSaEncryptKeySize  Integer32,
        ipSecTunHistOutSaEncryptKeySize Integer32
    }

    ipSecTunHistIndex OBJECT-TYPE
        SYNTAX Integer32 (1..2147483647)
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
            "The index of the IPsec Phase-2 Tunnel History Table.
             The value of the index is a number which
             begins at one and is incremented with each tunnel
             that ends. The value
             of this object will wrap at 2,147,483,647."
```

```
         ::= { ipSecTunnelHistEntry 1 }

      ipSecTunHistTermReason  OBJECT-TYPE
         SYNTAX INTEGER {
                   other(1),
                   normal(2),
                   operRequest(3),
                   peerDelRequest(4),
                   peerLost(5),
                   applicationInitiated(6),
                   xauthFailure(7),
                   seqNumRollOver(8),
                   checkPointReq(9)
                 }
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
          "The reason the IPsec Phase-2 Tunnel was terminated.
          Possible reasons include:
          1 = other
          2 = normal termination
          3 = operator request
          4 = peer delete request was received
          5 = contact with peer was lost
          6 = applicationInitiated (eg: L2TP requesting the termination)
          7 = failure of extended authentication
          8 = local failure occurred
          9 = operator initiated check point request"
         ::= { ipSecTunnelHistEntry 2 }

      ipSecTunHistActiveIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The index of the previously active
            IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 3 }

      ipSecTunHistIkeTunnelIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS deprecated
         DESCRIPTION
            "The index of the associated IPsec Phase-1 Tunnel
             (ikeTunIndex in the ikeTunnelTable)."
         ::= { ipSecTunnelHistEntry 4 }
```

```
      ipSecTunHistLocalAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the local endpoint for the IPsec
             Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 5 }

      ipSecTunHistRemoteAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the remote endpoint for the IPsec
             Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 6 }

      ipSecTunHistKeyType OBJECT-TYPE
         SYNTAX KeyType
         MAX-ACCESS read-only
         STATUS deprecated
         DESCRIPTION
            "The type of key used by the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 7 }

      ipSecTunHistEncapMode OBJECT-TYPE
         SYNTAX EncapMode
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The encapsulation mode used by the
            IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 8 }

      ipSecTunHistLifeSize OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         UNITS "KBytes"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The negotiated LifeSize of the IPsec Phase-2 Tunnel in
             kilobytes."
         ::= { ipSecTunnelHistEntry 9 }

      ipSecTunHistLifeTime OBJECT-TYPE
```

```
         SYNTAX Integer32 (1..2147483647)
         UNITS "Seconds"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The negotiated LifeTime of the IPsec Phase-2 Tunnel in
             seconds."
         ::= { ipSecTunnelHistEntry 10 }

      ipSecTunHistStartTime OBJECT-TYPE
         SYNTAX TimeStamp
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value of sysUpTime in hundredths of seconds
            when the IPsec Phase-2 Tunnel was started."
         ::= { ipSecTunnelHistEntry 11 }

      ipSecTunHistActiveTime OBJECT-TYPE
         SYNTAX TimeInterval
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The length of time the IPsec Phase-2 Tunnel has been
             active in hundredths of seconds."
         ::= { ipSecTunnelHistEntry 12 }

      ipSecTunHistTotalRefreshes OBJECT-TYPE
         SYNTAX Counter32
         UNITS "QM Exchanges"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of security association refreshes
            performed."
         ::= { ipSecTunnelHistEntry 13 }

      ipSecTunHistTotalSas OBJECT-TYPE
         SYNTAX Counter32
         UNITS "SAs"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of security associations used
            during the
             life of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 14 }
```

```
      ipSecTunHistInSaDiffHellmanGrp OBJECT-TYPE
         SYNTAX DiffHellmanGrp
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The Diffie Hellman Group used by the inbound security
             association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 15 }

      ipSecTunHistInSaEncryptAlgo OBJECT-TYPE
         SYNTAX EncryptAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The encryption algorithm used by the inbound security
             association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 16 }

      ipSecTunHistInSaAhAuthAlgo OBJECT-TYPE
         SYNTAX AuthAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication algorithm used by the inbound
             authentication header (AH) security association of
             the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 17 }

      ipSecTunHistInSaEspAuthAlgo OBJECT-TYPE
         SYNTAX AuthAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication algorithm used by the inbound
             encapsulation security protocol (ESP)
             security association of
             the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 18 }

      ipSecTunHistInSaDecompAlgo OBJECT-TYPE
         SYNTAX CompAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The decompression algorithm used by the inbound
             security association of the IPsec Phase-2 Tunnel."
```

```
         ::= { ipSecTunnelHistEntry 19 }

      ipSecTunHistOutSaDiffHellmanGrp OBJECT-TYPE
         SYNTAX DiffHellmanGrp
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The Diffie Hellman Group used by the outbound security
             association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 20 }

      ipSecTunHistOutSaEncryptAlgo OBJECT-TYPE
         SYNTAX EncryptAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The encryption algorithm used by the outbound security
             association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 21 }

      ipSecTunHistOutSaAhAuthAlgo OBJECT-TYPE
         SYNTAX AuthAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication algorithm used by the outbound
             authentication header (AH) security association of
             the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 22 }

      ipSecTunHistOutSaEspAuthAlgo OBJECT-TYPE
         SYNTAX AuthAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The authentication algorithm used by the inbound
             ecapsulation security protocol (ESP)
             security association of the IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 23 }

      ipSecTunHistOutSaCompAlgo OBJECT-TYPE
         SYNTAX CompAlgo
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The compression algorithm used by the inbound
             security association of the IPsec Phase-2 Tunnel."
```

```
         ::= { ipSecTunnelHistEntry 24 }

      ipSecTunHistPmtu OBJECT-TYPE
         SYNTAX Integer32 (21..576)
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The Path MTU that was determined for this IPsec
            Phase-2 tunnel."
         ::= { ipSecTunnelHistEntry 25 }

      ipSecTunHistInOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets received by this IPsec
             Phase-2 Tunnel.  This value is accumulated
             BEFORE determining whether or not the packet should
             be decompressed.  See also ipSecTunInOctWraps for
             the number of times this counter has wrapped."
         ::= { ipSecTunnelHistEntry 26 }

      ipSecTunHistHcInOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of octets
             received by this IPsec Phase-2 Tunnel.  This value is
             accumulated BEFORE determining whether or not
             the packet should be decompressed."
         ::= { ipSecTunnelHistEntry 27 }

      ipSecTunHistInOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the octets received counter
             (ipSecTunInOctets) has wrapped."
         ::= { ipSecTunnelHistEntry 28 }

      ipSecTunHistInDecompOctets OBJECT-TYPE
```

```
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of decompressed octets received by this
             IPsec Phase-2 Tunnel.  This value is accumulated AFTER
             the packet is decompressed. If compression is not being
             used, this value will match the value of ipSecTunInOctets.
             See also ipSecTunInDecompOctWraps for the number of times
             this counter has wrapped."
         ::= { ipSecTunnelHistEntry 29 }

      ipSecTunHistHcInDecompOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of decompressed
             octets received by this IPsec Phase-2 Tunnel.  This value
             is accumulated AFTER the packet is decompressed. If
             compression is not being used, this value will match the
             value of ipSecTunHcInOctets."
         ::= { ipSecTunnelHistEntry 30 }

      ipSecTunHistInDecompOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the decompressed octets
            received counter (ipSecTunInDecompOctets) has wrapped."
         ::= { ipSecTunnelHistEntry 31 }

      ipSecTunHistInPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets received by this
            IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 32 }

      ipSecTunHistInDropPkts OBJECT-TYPE
         SYNTAX Counter32
```

```
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped during
            receive processing by this IPsec Phase-2 Tunnel.
            This count does NOT include packets
             dropped due to Anti-Replay processing."
         ::= { ipSecTunnelHistEntry 33 }

      ipSecTunHistInReplayDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped during
            receive processing due to Anti-Replay processing
            by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 34 }

      ipSecTunHistInAuths OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Events"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound authentication's
            performed
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 35 }

      ipSecTunHistInAuthFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound authentication's
            which ended in
             failure by this IPsec Phase-2 Tunnel ."
         ::= { ipSecTunnelHistEntry 36 }

      ipSecTunHistInDecrypts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The total number of inbound decryption's performed
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 37 }

      ipSecTunHistInDecryptFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of inbound decryption's
            which ended in failure
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 38 }

      ipSecTunHistOutOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of octets sent by this IPsec
             Phase-2 Tunnel.  This value is accumulated
             AFTER determining whether or not the
             packet should be
             compressed.  See also ipSecTunOutOctWraps for the
             number of times this counter has wrapped."
         ::= { ipSecTunnelHistEntry 39 }

      ipSecTunHistHcOutOctets OBJECT-TYPE
         SYNTAX Counter64
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total number of octets
             sent by this IPsec Phase-2 Tunnel.  This value
             is accumulated AFTER determining whether or not
             the packet should be
             compressed."
         ::= { ipSecTunnelHistEntry 40 }

      ipSecTunHistOutOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
```

```
         STATUS current
         DESCRIPTION
            "The number of times the octets sent counter
             (ipSecTunOutOctets) has wrapped."
         ::= { ipSecTunnelHistEntry 41 }

      ipSecTunHistOutUncompOctets OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of uncompressed octets sent by this
             IPsec Phase-2 Tunnel.  This value is accumulated BEFORE
             the packet is compressed. If compression is not being
             used, this value will match the value of
             ipSecTunOutOctets.  See also
             ipSecTunOutDecompOctWraps for the number of times
             this counter has wrapped."
         ::= { ipSecTunnelHistEntry 42 }

      ipSecTunHistHcOutUncompOctets OBJECT-TYPE
         SYNTAX Counter64
         UNITS "Octets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "A high capacity count of the total
            number of uncompressed octets sent by this
            IPsec Phase-2 Tunnel.  This value is accumulated
            BEFORE the packet is compressed. If compression
             is not being used, this value will match the value of
             ipSecTunHcOutOctets."
         ::= { ipSecTunnelHistEntry 43 }

      ipSecTunHistOutUncompOctWraps OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Integral units"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The number of times the uncompressed octets sent counter
             (ipSecTunOutUncompOctets) has wrapped."
         ::= { ipSecTunnelHistEntry 44 }

      ipSecTunHistOutPkts OBJECT-TYPE
         SYNTAX Counter32
```

```
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets sent by this
            IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 45 }

      ipSecTunHistOutDropPkts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of packets dropped
            during send processing
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 46 }

      ipSecTunHistOutAuths OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Events"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound authentication's performed
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 47 }

      ipSecTunHistOutAuthFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound authentication's
            which ended in
             failure by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 48 }

      ipSecTunHistOutEncrypts OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound encryption's performed
```

```
            by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 49 }

      ipSecTunHistOutEncryptFails OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Failures"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound encryption's
            which ended in failure
             by this IPsec Phase-2 Tunnel."
         ::= { ipSecTunnelHistEntry 50 }

      ipSecTunHistOutCompressedPkts    OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets
            which were successfully compressed."
         ::= { ipSecTunnelHistEntry 51 }

      ipSecTunHistOutCompSkippedPkts   OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets that were to be
            compressed but which were skipped due to the compression
            hysteresis."
         ::= { ipSecTunnelHistEntry 52 }

      ipSecTunHistOutCompFailPkts      OBJECT-TYPE
         SYNTAX Counter32
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets that failed
            compression because they grew in size after compression."
         ::= { ipSecTunnelHistEntry 53 }

      ipSecTunHistOutCompTooSmallPkts  OBJECT-TYPE
         SYNTAX Counter32
```

```
         UNITS "Packets"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The total number of outbound packets that were to be
            compressed but were smaller than the compression threshold
            size."
         ::= { ipSecTunnelHistEntry 54 }

      ipSecTunHistControlProtocol OBJECT-TYPE
         SYNTAX ControlProtocol
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
          "Identifies the protocol that was used to setup and administer
          Phase-2 IPsec tunnel. If IKE was used to setup this tunnel,
          then this value of this column would be `cp_ike'."
         ::= { ipSecTunnelHistEntry 55 }

      ipSecTunHistControlTunnelIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The index of the IPsec Phase-1 Tunnel that spawned this
            Phase-2 tunnel (in case of IKE, this value would refer t
            ikeTunIndex in the ikeTunnelTable)"
         ::= { ipSecTunnelHistEntry 56 }

      ipSecTunHistInSaEncryptKeySize   OBJECT-TYPE
         SYNTAX Integer32
         UNITS "Bits"
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The size in bits of the key which was negotiated to be use
            with the encryption transform used with this tunnel denote
            by ipSecTunHistInSaEncryptAlgo.
            For DES and 3DES the key size is respectively 56 and
            168. For AES, this will denote the negotiated key size."
         ::= { ipSecTunnelHistEntry 57 }

      ipSecTunHistOutSaEncryptKeySize  OBJECT-TYPE
         SYNTAX Integer32
         UNITS "Bits"
         MAX-ACCESS read-only
         STATUS current
```

```
         DESCRIPTION
            "The size in bits of the key which was negotiated to be use
            with the encryption transform used with this tunnel denote
            by ipSecTunHistOutSaEncryptAlgo.
            For DES and 3DES the key size is respectively 56 and
            168. For AES, this will denote the negotiated key size."
         ::= { ipSecTunnelHistEntry 58 }


   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-2 Tunnel Endpoint History Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecEndPtHistTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IpSecEndPtHistEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-2 Tunnel Endpoint History Table.
             This table is implemented as a
             sliding window in which only the
             last n entries are maintained.
             The maximum number of entries
             is specified by the ipSecHistTableSize object."
         ::= { ipSecHistPhaseTwo 2 }

      ipSecEndPtHistEntry OBJECT-TYPE
         SYNTAX IpSecEndPtHistEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "Each entry contains the attributes associated with
             a previously active IPsec Phase-2 Tunnel Endpoint."
         INDEX { ipSecEndPtHistIndex }
         ::= { ipSecEndPtHistTable 1 }

      IpSecEndPtHistEntry ::= SEQUENCE {
         ipSecEndPtHistIndex               Integer32,
         ipSecEndPtHistTunIndex            Integer32,
         ipSecEndPtHistActiveIndex         Integer32,
         ipSecEndPtHistLocalName           DisplayString,
         ipSecEndPtHistLocalType           EndPtType,
         ipSecEndPtHistLocalAddr1          IPSIpAddress,
         ipSecEndPtHistLocalAddr2          IPSIpAddress,
         ipSecEndPtHistLocalProtocol       Integer32,
         ipSecEndPtHistLocalPort           Integer32,
         ipSecEndPtHistRemoteName          DisplayString,
         ipSecEndPtHistRemoteType          EndPtType,
```

```
         ipSecEndPtHistRemoteAddr1          IPSIpAddress,
         ipSecEndPtHistRemoteAddr2          IPSIpAddress,
         ipSecEndPtHistRemoteProtocol       Integer32,
         ipSecEndPtHistRemotePort           Integer32
      }

      ipSecEndPtHistIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The number of the previously active
            Endpoint associated
             with a IPsec Phase-2 Tunnel Table.  The value
             of this index is a number which begins at
             one and is incremented with each Endpoint
             associated with an IPsec Phase-2 Tunnel.
             The value of this object will wrap at 2,147,483,647."
         ::= { ipSecEndPtHistEntry 1 }

      ipSecEndPtHistTunIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The index  of the previously active IPsec
            Phase-2 Tunnel Table."
         ::= { ipSecEndPtHistEntry 2 }

      ipSecEndPtHistActiveIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The index  of the previously active Endpoint."
         ::= { ipSecEndPtHistEntry 3 }

      ipSecEndPtHistLocalName OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The DNS name of the local Endpoint."
         ::= { ipSecEndPtHistEntry 4 }

      ipSecEndPtHistLocalType OBJECT-TYPE
         SYNTAX EndPtType
```

```
                --INTEGER {
                   --singleIpAddr(1),
                   --ipAddrRange(2),
                   --ipSubnet(3)
                --}
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
             "The type of identity for the local Endpoint.
              Possible values are:
              1) a single IP address, or
              2) an IP address range, or
              3) an IP subnet."
          ::= { ipSecEndPtHistEntry 5 }

       ipSecEndPtHistLocalAddr1 OBJECT-TYPE
          SYNTAX IPSIpAddress
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            "The local Endpoint's first IP address specification.

             If the local Endpoint type is single IP address,
             then this is the value of the IP address.

             If the local Endpoint type is IP subnet, then this
             is the value of the subnet.

             If the local Endpoint type is IP address range,
             then this is the value of beginning IP address of
             the range."
          ::= { ipSecEndPtHistEntry 6 }

       ipSecEndPtHistLocalAddr2 OBJECT-TYPE
          SYNTAX IPSIpAddress
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            "The local Endpoint's second IP address specification.

             If the local Endpoint type is single IP address,
             then this is the value of the IP address.

             If the local Endpoint type is IP subnet, then this
             is the value of the subnet mask.

             If the local Endpoint type is IP address range,
```

```
            then this is the value of ending IP address of
            the range."
         ::= { ipSecEndPtHistEntry 7 }

      ipSecEndPtHistLocalProtocol OBJECT-TYPE
         SYNTAX Integer32 (0..255)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The protocol number of the local Endpoint's traffic."
         ::= { ipSecEndPtHistEntry 8 }

      ipSecEndPtHistLocalPort OBJECT-TYPE
         SYNTAX Integer32 (0..65535)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The port number of the local Endpoint's traffic."
         ::= { ipSecEndPtHistEntry 9 }

      ipSecEndPtHistRemoteName OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The DNS name of the remote Endpoint."
         ::= { ipSecEndPtHistEntry 10 }

      ipSecEndPtHistRemoteType OBJECT-TYPE
         SYNTAX EndPtType
                --INTEGER {
                   --singleIpAddr(1),
                   --ipAddrRange(2),
                   --ipSubnet(3)
                --}
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The type of identity for the remote Endpoint.
             Possible values are:
             1) a single IP address, or
             2) an IP address range, or
             3) an IP subnet."
         ::= { ipSecEndPtHistEntry 11 }

      ipSecEndPtHistRemoteAddr1 OBJECT-TYPE
         SYNTAX IPSIpAddress
```

```
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            "The remote Endpoint's first IP address specification.

             If the remote Endpoint type is single IP address,
             then this is the value of the IP address.

             If the remote Endpoint type is IP subnet, then this
             is the value of the subnet.

             If the remote Endpoint type is IP address range,
             then this is the value of beginning IP address of
             the range."
          ::= { ipSecEndPtHistEntry 12 }

       ipSecEndPtHistRemoteAddr2 OBJECT-TYPE
          SYNTAX IPSIpAddress
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            "The remote Endpoint's second IP address specification.

             If the remote Endpoint type is single IP address,
             then this
             is the value of the IP address.

             If the remote Endpoint type is IP subnet, then this
             is the value of the subnet mask.

             If the remote Endpoint type is IP address range,
             then this
             is the value of ending IP address of the range."
          ::= { ipSecEndPtHistEntry 13 }

       ipSecEndPtHistRemoteProtocol OBJECT-TYPE
          SYNTAX Integer32 (0..255)
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
             "The protocol number of the remote Endpoint's traffic."
          ::= { ipSecEndPtHistEntry 14 }

       ipSecEndPtHistRemotePort OBJECT-TYPE
          SYNTAX Integer32 (0..65535)
          MAX-ACCESS read-only
          STATUS current
```

```
         DESCRIPTION
            "The port number of the remote Endpoint's traffic."
         ::= { ipSecEndPtHistEntry 15 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Failure Group
   --
   -- This group consists of a:
   -- 1) IPsec Failure Global Objects
   -- 2) IPsec Phase-1 Tunnel Failure Table
   -- 3) IPsec Phase-2 Tunnel Failure Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecFailGlobal         OBJECT IDENTIFIER
                      ::= { ipSecFailures 1 }
      ipSecFailPhaseOne       OBJECT IDENTIFIER
                      ::= { ipSecFailures 2 }
      ipSecFailPhaseTwo       OBJECT IDENTIFIER
                      ::= { ipSecFailures 3 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Failure Global Control Objects
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecFailGlobalCntl  OBJECT IDENTIFIER
                      ::= { ipSecFailGlobal 1 }

      ipSecFailTableSize  OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "The window size of the IPsec Phase-1 and Phase-2
             Failure Tables.

             The IPsec Phase-1 and Phase-2 Failure Tables are
             implemented as a sliding window in which only the
             last N entries are maintained.  This object is used
             specify the number of entries which will be
             maintained in the IPsec Phase-1 and Phase-2 Failure
             Tables.

             An implementation may choose suitable minimum and
             maximum values for this element based on the local
             policy and available resources. If an SNMP SET request
             specifies a value outside this window for this element,
             a BAD VALUE may be returned."

         ::= { ipSecFailGlobalCntl 1 }
```

```
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-1 Failure Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ikeFailTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IkeFailEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-1 Failure Table.
             This table is implemented as a sliding
             window in which only the last n entries are
             maintained.  The maximum number of entries
             is specified by the ipSecFailTableSize object."
         ::= { ipSecFailPhaseOne 1 }

      ikeFailEntry OBJECT-TYPE
         SYNTAX IkeFailEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
               "Each entry contains the attributes associated
               with an IPsec Phase-1 failure."
         INDEX { ikeFailIndex }
         ::= { ikeFailTable 1 }

      IkeFailEntry ::= SEQUENCE {
         ikeFailIndex                Integer32,
         ikeFailReason               INTEGER,
         ikeFailTime                 TimeStamp,
         ikeFailLocalType            Phase1PeerIdentityType,
         ikeFailLocalValue           DisplayString,
         ikeFailRemoteType           Phase1PeerIdentityType,
         ikeFailRemoteValue          DisplayString,
         ikeFailLocalAddr            IPSIpAddress,
         ikeFailRemoteAddr           IPSIpAddress
      }

      ikeFailIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-1 Failure Table index.
             The value of the index is a number which
             begins at one and is incremented with each
             IPsec Phase-1 failure. The value
```

```
            of this object will wrap at 2,147,483,647."
         ::= { ikeFailEntry 1 }

      ikeFailReason OBJECT-TYPE
         SYNTAX INTEGER{
                  other(1),
                  peerDelRequest(2),
                  peerLost(3),
                  localFailure(4),
                  authFailure(5),
                  hashValidation(6),
                  encryptFailure(7),
                  internalError(8),
                  sysCapExceeded(9),
                  proposalFailure(10),
                  peerCertUnavailable(11),
                  peerCertNotValid(12),
                  localCertExpired(13),
                  crlFailure(14),
                  peerEncodingError(15),
                  nonExistentSa(16),
                  xauthFailure(17),
                  operRequest(18)
                }
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The reason for the failure.  Possible reasons include:
              1 = other
              2 = peer delete request was received
              3 = contact with peer was lost
              4 = local failure occurred
              5 = authentication failure
              6 = hash validation failure
              7 = encryption failure
              8 = internal error occurred
              9 = system capacity failure
             10 = proposal failure
             11 = peer's certificate is unavailable
             12 = peer's certificate was found invalid
             13 = local certificate expired
             14 = certificate revoke list (crl) failure
             15 = peer encoding error
             16 = ISAKMP PDU has pointer to non-existent cookie
             17 = operator requested termination."
         ::= { ikeFailEntry 2 }
```

```
      ikeFailTime OBJECT-TYPE
         SYNTAX TimeStamp
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value of sysUpTime in hundredths of seconds
            at the time of the failure."
         ::= { ikeFailEntry 3 }

      ikeFailLocalType OBJECT-TYPE
         SYNTAX Phase1PeerIdentityType
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The type of local peer identity.  The local peer
            may be indentified by:
             1. an IP address, or
             2. or a fully qualified domain name.
             3. or a distinguished name."
         ::= { ikeFailEntry 4 }

      ikeFailLocalValue OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value of the local peer identity.

             If the local peer type is an IP Address, then this
             is the IP Address used to identify the local peer.

             If the local peer type is id_fqdn, then this is
             the FQDN of the local entity.

             If the local peer type is a id_dn, then this is
             the distinguished named string of the local entity."
         ::= { ikeFailEntry 5 }

      ikeFailRemoteType OBJECT-TYPE
         SYNTAX Phase1PeerIdentityType
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The type of remote peer identity.  The remote
            peer may be identified by:
             1. an IP address, or
             2. or a fully qualified domain name.
```

```
            3. or a distinguished name."
         ::= { ikeFailEntry 6 }

      ikeFailRemoteValue OBJECT-TYPE
         SYNTAX DisplayString
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The value of the remote peer identity.

             If the remote peer type is an IP Address, then this
             is the IP Address used to identify the remote peer.

             If the remote peer type is id_fqdn, then this is
             the FQDN of the remote peer.

             If the remote peer type is a id_dn, then this is
             the distinguished named string of the remote peer."
         ::= { ikeFailEntry 7 }

      ikeFailLocalAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the local peer."
         ::= { ikeFailEntry 8 }

      ikeFailRemoteAddr OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The IP address of the remote peer."
         ::= { ikeFailEntry 9 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec Phase-2 Failure Table
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecFailTable OBJECT-TYPE
         SYNTAX SEQUENCE OF IpSecFailEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-2 Failure Table.
             This table is implemented as a sliding window
             in which only the last n entries are maintained.
```

```
            The maximum number of entries
            is specified by the ipSecFailTableSize object."
         ::= { ipSecFailPhaseTwo 1 }

      ipSecFailEntry OBJECT-TYPE
         SYNTAX IpSecFailEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "Each entry contains the attributes associated with
             an IPsec Phase-1 failure."
         INDEX { ipSecFailIndex }
         ::= { ipSecFailTable 1 }

      IpSecFailEntry ::= SEQUENCE {
         ipSecFailIndex                Integer32,
         ipSecFailReason               INTEGER,
         ipSecFailTime                 TimeStamp,
         ipSecFailTunnelIndex          Integer32,
         ipSecFailSaSpi                Integer32,
         ipSecFailPktSrcAddr           IPSIpAddress,
         ipSecFailPktDstAddr           IPSIpAddress
      }

      ipSecFailIndex OBJECT-TYPE
         SYNTAX Integer32 (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
            "The IPsec Phase-2 Failure Table index.
             The value of the index is a number which
             begins at one and is incremented with each
             IPsec Phase-1 failure. The value
             of this object will wrap at 2,147,483,647."
         ::= { ipSecFailEntry 1 }

      ipSecFailReason OBJECT-TYPE
         SYNTAX INTEGER{
                  other(1),
                  internalError(2),
                  peerEncodingError(3),
                  proposalFailure(4),
                  protocolUseFail(5),
                  nonExistentSa(6),
                  decryptFailure(7),
                  encryptFailure(8),
                  inAuthFailure(9),
```

```
                  outAuthFailure(10),
                  compression(11),
                  sysCapExceeded(12),
                  peerDelRequest(13),
                  peerLost(14),
                  seqNumRollOver(15),
                  operRequest(16)
                }
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
         "The reason for the failure.  Possible reasons
         include:
           1 = other
           2 = internal error occurred
           3 = peer encoding error
           4 = proposal failure
           5 = protocol use failure
           6 = non-existent security association
           7 = decryption failure
           8 = encryption failure
           9 = inbound authentication failure
          10 = outbound authentication failure
          11 = compression failure
          12 = system capacity failure
          13 = peer delete request was received
          14 = contact with peer was lost
          15 = sequence number rolled over
          16 = operator requested termination."
      ::= { ipSecFailEntry 2 }

   ipSecFailTime OBJECT-TYPE
      SYNTAX TimeStamp
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
         "The value of sysUpTime in hundredths of seconds
         at the time of the failure."
      ::= { ipSecFailEntry 3 }

   ipSecFailTunnelIndex OBJECT-TYPE
      SYNTAX Integer32 (1..2147483647)
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
         "The Phase-2 Tunnel index (ipSecTunIndex)."
      ::= { ipSecFailEntry 4 }
```

```
      ipSecFailSaSpi  OBJECT-TYPE
         SYNTAX Integer32 (0..2147483647)
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The security association SPI value."
         ::= { ipSecFailEntry 5 }

      ipSecFailPktSrcAddr  OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The packet's source IP address."
         ::= { ipSecFailEntry 6 }

      ipSecFailPktDstAddr  OBJECT-TYPE
         SYNTAX IPSIpAddress
         MAX-ACCESS read-only
         STATUS current
         DESCRIPTION
            "The packet's destination IP address."
         ::= { ipSecFailEntry 7 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- The IPsec TRAP Control Group
   --
   -- This group of objects controls the sending of IPsec TRAPs.
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecTrapCntlIkeTunnelStart OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state of
            sending the IPsec IKE Phase-1 Tunnel Start TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 1 }

      ipSecTrapCntlIkeTunnelStop OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the
```

```
            IPsec IKE Phase-1 Tunnel Stop TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 2 }

      ipSecTrapCntlIkeSysFailure OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the
             IPsec IKE Phase-1 System Failure TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 3 }

      ipSecTrapCntlIkeCertCrlFailure OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative
            state of sending the
             IPsec IKE Phase-1 Certificate/CRL Failure TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 4 }

      ipSecTrapCntlIkeProtocolFail OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative
            state of sending the
             IPsec IKE Phase-1 Protocol Failure TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 5 }

      ipSecTrapCntlIkeNoSa OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative
            state of sending the IPsec IKE Phase-1
            No Security Association TRAP."
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 6 }
```

```
      ipSecTrapCntlIpSecTunnelStart OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the IPsec
             Phase-2 Tunnel Start TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 7 }

      ipSecTrapCntlIpSecTunnelStop OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative
            state of sending the IPsec
            Phase-2 Tunnel Stop TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 8 }

      ipSecTrapCntlIpSecSysFailure OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the IPsec
             Phase-2 System Failure TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 9 }

      ipSecTrapCntlIpSecSetUpFailure OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the IPsec
             Phase-2 Set Up Failure TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 10 }

      ipSecTrapCntlIpSecEarlyTunTerm OBJECT-TYPE
         SYNTAX TrapStatus
```

```
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the IPsec
             Phase-2 Early Tunnel Termination TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 11 }

      ipSecTrapCntlIpSecProtocolFail OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the IPsec
             Phase-2 Protocol Failure TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 12 }

      ipSecTrapCntlIpSecNoSa OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the IPsec Phase-2  No Security
            Association TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 13 }

      ipSecTrapCntlInNewGrpRejected OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
            "This object defines the administrative state
            of sending the IPsec Phase-2  No Security
            Association TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 14 }

      ipSecTrapCntlOutNewGrpRejected OBJECT-TYPE
         SYNTAX TrapStatus
         MAX-ACCESS read-write
         STATUS current
         DESCRIPTION
```

```
            "This object defines the administrative state
            of sending the IPsec Phase-2  No Security
            Association TRAP "
         DEFVAL { disabled }
         ::= { ipSecTrapCntl 15 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- IPsec Notifications - TRAPs
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++

      ipSecMIBNotificationPrefix   OBJECT IDENTIFIER
                ::= {ipSecFlowMonitorMIB 2}

      ipSecMIBNotifications   OBJECT IDENTIFIER
                ::= { ipSecMIBNotificationPrefix   0}

      ikeTunnelStart NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr,
                   ikeTunLifeTime
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when an IPsec Phase-1
             IKE Tunnel becomes active."
         ::= { ipSecMIBNotifications 1 }

      ikeTunnelStop NOTIFICATION-TYPE
         OBJECTS {
                   ikeTunHistTermReason,
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr,
                   ikeTunActiveTime
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when an IPsec Phase-1
             IKE Tunnel becomes inactive."
         ::= { ipSecMIBNotifications 2 }

      ikeSysFailure NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr
                 }
         STATUS  current
```

```
         DESCRIPTION
            "This notification is generated when the processing for
             an IPsec Phase-1 IKE Tunnel experiences an internal
             or system capacity error."
         ::= { ipSecMIBNotifications 3 }

      ikeCertCrlFailure NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when the processing for
             an IPsec Phase-1 IKE Tunnel experiences a Certificate
             or a Certificate Revoke List (CRL) related error."
         ::= { ipSecMIBNotifications 4 }

      ikeProtocolFailure NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when the processing for
             an IPsec Phase-1 IKE Tunnel experiences a protocol
             related error."
         ::= { ipSecMIBNotifications 5 }

      ikeNoSa NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when the IKE entity
           recieves an ISAKMP PDU  with a reference to a non-existent
           cookie."
         ::= { ipSecMIBNotifications 6 }

      ipSecTunnelStart NOTIFICATION-TYPE
         OBJECTS {
                   ipSecTunLifeTime,
                   ipSecTunLifeSize
                 }
```

```
         STATUS  current
         DESCRIPTION
            "This notification is generated when an IPsec Phase-2
             Tunnel becomes active."
          ::= { ipSecMIBNotifications 7 }

      ipSecTunnelStop NOTIFICATION-TYPE
         OBJECTS {
                   ipSecTunHistTermReason,
                   ipSecTunActiveTime
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when an IPsec Phase-2
             Tunnel becomes inactive."
         ::= { ipSecMIBNotifications 8 }

      ipSecSysFailure NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr,
                   ipSecTunActiveTime,
                   ipSecSpiProtocol
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when the processing for
             an IPsec Phase-2 Tunnel experiences an internal
             or system capacity error."
         ::= { ipSecMIBNotifications 9 }

      ipSecSetUpFailure NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when the setup for
             an IPsec Phase-2 Tunnel fails."
         ::= { ipSecMIBNotifications 10 }

      ipSecEarlyTunTerm NOTIFICATION-TYPE
         OBJECTS {
                   ipSecTunActiveTime,
                   ipSecSpiProtocol
                 }
```

```
         STATUS  current
         DESCRIPTION
            "This notification is generated when an an IPsec Phase-2
             Tunnel is terminated earily or before expected."
         ::= { ipSecMIBNotifications 11 }

      ipSecProtocolFailure NOTIFICATION-TYPE
         OBJECTS {
                   ipSecTunActiveTime,
                   ipSecSpiProtocol
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when the processing for
             an IPsec Phase-2 Tunnel experiences a protocol
             related error."
         ::= { ipSecMIBNotifications 12 }

      ipSecNoSa NOTIFICATION-TYPE
         STATUS  current
         DESCRIPTION
            "This notification is generated when the managed entity
             receives an IPsec packet with a non-existent SPI."
         ::= { ipSecMIBNotifications 13 }

      ipSecInNewGrpRejected NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr
                 }
         STATUS  current
         DESCRIPTION
            "This notification is generated when the managed entity
             receives and rejects an incoming new group proposal
             from an IKE peer (ikePeerRemoteAddr). The ISAKMP
             context of the exchange can be obtained from the IKE
             tunnel index which is contained in the index of the
             varbind objects of this trap."
         ::= { ipSecMIBNotifications 14 }

      ipSecOutNewGrpRejected NOTIFICATION-TYPE
         OBJECTS {
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr
                 }
         STATUS  current
         DESCRIPTION
```

```
            "This notification is generated when the managed entity
             issues a new group proposal to the peer (ikePeerRemoteAddr)
             and the peer rejects the proposal. The ISAKMP context of
             the exchange can be obtained from the IKE tunnel index
             which is contained in the index of the varbind objects
             of this trap."
         ::= { ipSecMIBNotifications 15 }


   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- Conformance Information
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecMIBConformance   OBJECT IDENTIFIER
                     ::= { ipSecFlowMonitorMIB 3 }

      ipSecMIBGroups        OBJECT IDENTIFIER
                     ::= { ipSecMIBConformance 1 }

      ipSecMIBCompliances   OBJECT IDENTIFIER
                     ::= { ipSecMIBConformance 2 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- Compliance Statements
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecMIBCompliance       MODULE-COMPLIANCE
         STATUS      current
         DESCRIPTION
           "The compliance statement for SNMP entities
            the IP Security Protocol."

         MODULE -- this module
           MANDATORY-GROUPS  { ipSecLevelsGroup,
                               ipSecPeerAssociationGroup,
                               ipSecPhaseTwoGroup
                             }

           --GROUP ipSecLevelsGroup
           --DESCRIPTION   "The ipSecLevelsGroup is a mandatory group
                       --containing objects  providing meta-information
                       --about the MIB itself and its version."

           --GROUP ipSecPhaseOneGroup
           --DESCRIPTION   "The ipSecPhaseOneGroup is a mandatory group
                       --containing objects providing information
                       --about IKE and ISAKMP activity and structures
                       --resulting from such activity in the managed
                       --entity."
```

```
        GROUP ipSecIkeGroup
        DESCRIPTION   "The ipSecIkeGroup is a conditional group
                       containing objects providing information
                       about IKE and ISAKMP activity and structures
                       resulting from such activity in the managed
                       entity."

        --GROUP ipSecPeerAssociationGroup
        --DESCRIPTION   "The ipSecPeerAssociationGroup is a mandator
                     --group containing objects providing information
                     --about association of the managed entity
                     --with peers in Phase 1."

        --GROUP ipSecIkeGroup
        --DESCRIPTION   "The ipSecIkeGroup encloses all thge IKE
                     --related MIB elements. This is an optional
                     --group and needs to be implemented only if
                     --the managed entity implements IKE protocol."

        --GROUP ipSecPhaseTwoGroup
        --DESCRIPTION   "The ipSecPhaseTwoGroup is a mandatory group
                     --containing objects providing information
                     --about Phase-2 IPsec (Quick Mode & New Grp
                     --Grp Mode) activity and structures resulting
                     --from such --activity in the managed entity."

        GROUP ipSecHistoryGroup
        DESCRIPTION   "The ipSecHistoryGroup is an optional group
                       containing objects providing information
                       about expired structures pertaining to
                       Phase-1 (IKE & ISAKMP) and Phase-2 IPsec
                       (Quick Mode & New Grp Mode) activity.

                       This group consists of:
                        1) IPsec History Global Objects
                        2) IPsec Phase-1 History Objects
                        3) IPsec Phase-2 History Objects"

        GROUP ipSecFailuresGroup
        DESCRIPTION   "The ipSecFailuresGroup is an optional group
                       containing objects providing information
                       about failures of operations pertaining to
                       Phase-1 (IKE & ISAKMP) and Phase-2 IPsec
                       (Quick Mode & New Grp Mode) activity.

                      This group consists of:
```

```
                    1) IPsec Failure Global Objects
                    2) IPsec Phase-1 Tunnel Failure Table
                    3) IPsec Phase-2 Tunnel Failure Table"

          GROUP ipSecTrapCntlGroup
          DESCRIPTION   "The ipSecTrapCntlGroup is an optional group
                         containing objects providing control of
                         notifications pertaining to Phase-1 (IKE &
                         ISAKMP) and Phase-2 IPsec (Quick Mode &
                         New Grp Mode) activity."

          GROUP ipSecModeConfigGroup
          DESCRIPTION   "The ipSecModeConfigGroup is an optional group
                         containing objects providing information
                         about the IKE Mode Configuration activity
                         on the managed entity.

                         This group consists of:
                          1) Global metrics about IKE Mod
                             Configuration activity
                          2) Phase-1 IKE Tunnel-wise Mode Configuration
                             metrics
                          3) Historical IKE Mode Configuration metrics
                             on a per expired tunnel basis."

          GROUP ipSecNewGrpGroup
          DESCRIPTIO
           "The ipSecNewGrpGroup is an optional group
            containing objects providing information
            about the Phase-2 New Group activity on the
            managed entity.

            This group consists of:
              1) Global metrics about new group negotiations
              2) Phase-1 IKE Tunnel-wise new group metrics
              3) Historical new group metrics on a per tunnel basis.
              4) Notifications pertaining to new grp failures."

          OBJECT   ikeTunStatus
          MIN-ACCESS read-only
          DESCRIPTION
            "Write access is not required."

          OBJECT   ipSecTunStatus
          MIN-ACCESS read-only
          DESCRIPTION
            "Write access is not required."
```

```
          ::= { ipSecMIBCompliances 1 }

   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
   -- Units of Conformance
   -- ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
      ipSecLevelsGroup OBJECT-GROUP
         OBJECTS {
                   ipSecMibLevel
                 }
         STATUS current
         DESCRIPTION
            "This group consists of a:
             1) IPsec MIB Level"
         ::= { ipSecMIBGroups 1 }

      ipSecIkeGroup OBJECT-GROUP
         OBJECTS {
                   -- The IPsec Phase-1 Global Statistics
                   ikeGlobalActiveTunnels,
                   ikeGlobalPreviousTunnels,
                   ikeGlobalHcPreviousTunnels,
                   ikeGlobalPreviousTunnelsWraps,
                   ikeGlobalInOctets,
                   ikeGlobalInPkts,
                   ikeGlobalInDropPkts,
                   ikeGlobalInNotifys,
                   ikeGlobalInP2Exchgs,
                   ikeGlobalInP2ExchgInvalids,
                   ikeGlobalInP2ExchgRejects,
                   ikeGlobalInP2SaDelRequests,
                   ikeGlobalOutOctets,
                   ikeGlobalOutPkts,
                   ikeGlobalOutDropPkts,
                   ikeGlobalOutNotifys,
                   ikeGlobalOutP2Exchgs,
                   ikeGlobalOutP2ExchgInvalids,
                   ikeGlobalOutP2ExchgRejects,
                   ikeGlobalOutP2SaDelRequests,
                   ikeGlobalInitTunnels,
                   ikeGlobalInitTunnelFails,
                   ikeGlobalRespTunnelFails,
                   ikeGlobalSysCapFails,
                   ikeGlobalAuthFails,
                   ikeGlobalDecryptFails,
                   ikeGlobalHashValidFails,
                   ikeGlobalNoSaFails,
```

```
                    ikeGlobalRespTunnels,
                    ikeGlobalInP1SaDelRequests,
                    ikeGlobalOutP1SaDelRequests,

                    -- The IPsec Phase-1 Internet Key Exchange
                    -- Tunnel Table
                    ikeTunLocalType,
                    ikeTunLocalValue,
                    ikeTunLocalAddr,
                    ikeTunLocalName,
                    ikeTunRemoteType,
                    ikeTunRemoteValue,
                    ikeTunRemoteAddr,
                    ikeTunRemoteName,
                    ikeTunNegoMode,
                    ikeTunDiffHellmanGrp,
                    ikeTunEncryptAlgo,
                    ikeTunHashAlgo,
                    ikeTunAuthMethod,
                    ikeTunLifeTime,
                    ikeTunActiveTime,
                    ikeTunSaRefreshThreshold,
                    ikeTunTotalRefreshes,
                    ikeTunInOctets,
                    ikeTunInPkts,
                    ikeTunInDropPkts,
                    ikeTunInNotifys,
                    ikeTunInP2Exchgs,
                    ikeTunInP2ExchgInvalids,
                    ikeTunInP2ExchgRejects,
                    ikeTunInP2SaDelRequests,
                    ikeTunOutOctets,
                    ikeTunOutPkts,
                    ikeTunOutDropPkts,
                    ikeTunOutNotifys,
                    ikeTunOutP2Exchgs,
                    ikeTunOutP2ExchgInvalids,
                    ikeTunOutP2ExchgRejects,
                    ikeTunOutP2SaDelRequests,
                    ikeTunStatus,
                    ikeTunEncryptKeySize
                  }
        STATUS current
        DESCRIPTION
           "This group consists of:
            1) IKE Global Objects
            2) IKE Tunnel table."
```

```
         ::= { ipSecMIBGroups 2 }

      ipSecPeerAssociationGroup OBJECT-GROUP
         OBJECTS {
                   -- The Phase-1 Peer Association group
                   phase1PeerLocalValue,
                   phase1PeerRemoteValue,
                   phase1PeerLocalAddr,
                   phase1PeerRemoteAddr,
                   phase1PeerActiveTime,
                   phase1PeerActiveTunnelIndex,
                   phase1PeerConfigAppVersion,
                   phase1PeerConfigAddress,
                   phase1PeerConfigNetmask,
                   phase1PeerConfigDns,
                   phase1PeerConfigNbns,
                   phase1PeerConfigDhcp,
                   phase1Protocol,
                   --
                   --phase1PeerCorrLocalType,
                   --phase1PeerCorrLocalValue,
                   --phase1PeerCorrRemoteType,
                   --phase1PeerCorrRemoteValue,
                   --phase1PeerCorrIntIndex,
                   --phase1PeerCorrSeqNum,
                   phase1PeerCorrIpSecTunIndex,
                   phase1PeerCorrControlProtocol
                 }
         STATUS current
         DESCRIPTION
            "This group consists of:
             1) IPsec Phase-1 Peer Association table.
             2) IPsec Phase-1 Correlation Table"
         ::= { ipSecMIBGroups 3 }

      ipSecXauthGroup OBJECT-GROUP
         OBJECTS {
                   -- The IPsec extended authentication (Phase-1.5)
                   -- Global Statistics
                   ikeGlobalInXauthFailures,
                   ikeGlobalOutXauthFailures
                 }
         STATUS current
         DESCRIPTION
            "This group consists of metrics pertaining to
             IKE extended authentication. Devices that do
             not support Xauth need not implement this group."
```

```
        ::= { ipSecMIBGroups 4 }

    ipSecPhaseTwoGroup OBJECT-GROUP
        OBJECTS {
                -- The IPsec Phase-2 Global Tunnel Statistics
                ipSecGlobalActiveTunnels,
                ipSecGlobalPreviousTunnels,
                ipSecGlobalHcPreviousTunnels,
                ipSecGlobalPreviousTunnelsWraps,
                ipSecGlobalInOctets,
                ipSecGlobalHcInOctets,
                ipSecGlobalInOctWraps,
                ipSecGlobalInDecompOctets,
                ipSecGlobalHcInDecompOctets,
                ipSecGlobalInDecompOctWraps,
                ipSecGlobalInPkts,
                ipSecGlobalInDrops,
                ipSecGlobalInReplayDrops,
                ipSecGlobalInAuths,
                ipSecGlobalInAuthFails,
                ipSecGlobalInDecrypts,
                ipSecGlobalInDecryptFails,
                ipSecGlobalOutOctets,
                ipSecGlobalHcOutOctets,
                ipSecGlobalOutOctWraps,
                ipSecGlobalOutUncompOctets,
                ipSecGlobalHcOutUncompOctets,
                ipSecGlobalOutUncompOctWraps,
                ipSecGlobalOutPkts,
                ipSecGlobalOutDrops,
                ipSecGlobalOutAuths,
                ipSecGlobalOutAuthFails,
                ipSecGlobalOutEncrypts,
                ipSecGlobalOutEncryptFails,
                ipSecGlobalProtocolUseFails,
                ipSecGlobalNoSaFails,
                ipSecGlobalSysCapFails,
                ipSecGlobalOutCompressedPkts,
                ipSecGlobalOutCompSkippedPkts,
                ipSecGlobalOutCompFailPkts,
                ipSecGlobalOutCompTooSmallPkts,

                -- The IPsec Phase-2 Tunnel Table
                -- ipSecTunIndex,
                -- ipSecTunIkeTunnelIndex,
                -- ipSecTunIkeTunnelAlive,
                ipSecTunLocalAddr,
```

```
                    ipSecTunRemoteAddr,
                    -- ipSecTunKeyType,
                    ipSecTunEncapMode,
                    ipSecTunLifeSize,
                    ipSecTunLifeTime,
                    ipSecTunActiveTime,
                    ipSecTunSaLifeSizeThreshold,
                    ipSecTunSaLifeTimeThreshold,
                    ipSecTunTotalRefreshes,
                    ipSecTunExpiredSaInstances,
                    ipSecTunCurrentSaInstances,
                    ipSecTunInSaDiffHellmanGrp,
                    ipSecTunInSaEncryptAlgo,
                    ipSecTunInSaAhAuthAlgo,
                    ipSecTunInSaEspAuthAlgo,
                    ipSecTunInSaDecompAlgo,
                    ipSecTunOutSaDiffHellmanGrp,
                    ipSecTunOutSaEncryptAlgo,
                    ipSecTunOutSaAhAuthAlgo,
                    ipSecTunOutSaEspAuthAlgo,
                    ipSecTunOutSaCompAlgo,
                    ipSecTunPmtu,
                    ipSecTunInOctets,
                    ipSecTunHcInOctets,
                    ipSecTunInOctWraps,
                    ipSecTunInDecompOctets,
                    ipSecTunHcInDecompOctets,
                    ipSecTunInDecompOctWraps,
                    ipSecTunInPkts,
                    ipSecTunInDropPkts,
                    ipSecTunInReplayDropPkts,
                    ipSecTunInAuths,
                    ipSecTunInAuthFails,
                    ipSecTunInDecrypts,
                    ipSecTunInDecryptFails,
                    ipSecTunOutOctets,
                    ipSecTunHcOutOctets,
                    ipSecTunOutOctWraps,
                    ipSecTunOutUncompOctets,
                    ipSecTunHcOutUncompOctets,
                    ipSecTunOutUncompOctWraps,
                    ipSecTunOutPkts,
                    ipSecTunOutDropPkts,
                    ipSecTunOutAuths,
                    ipSecTunOutAuthFails,
                    ipSecTunOutEncrypts,
                    ipSecTunOutEncryptFails,
```

```
                ipSecTunOutCompressedPkts,
                ipSecTunOutCompSkippedPkts,
                ipSecTunOutCompFailPkts,
                ipSecTunOutCompTooSmallPkts,
                ipSecTunStatus,
                ipSecTunControlTunnelIndex,
                ipSecTunControlProtocol,
                ipSecTunControlTunnelAlive,
                ipSecTunInSaEncryptKeySize,
                ipSecTunOutSaEncryptKeySize,

                -- The IPsec Phase-2 Tunnel Endpoint Table
                -- ipSecEndPtIndex,
                ipSecEndPtLocalName,
                ipSecEndPtLocalType,
                ipSecEndPtLocalAddr1,
                ipSecEndPtLocalAddr2,
                ipSecEndPtLocalProtocol,
                ipSecEndPtLocalPort,
                ipSecEndPtRemoteName,
                ipSecEndPtRemoteType,
                ipSecEndPtRemoteAddr1,
                ipSecEndPtRemoteAddr2,
                ipSecEndPtRemoteProtocol,
                ipSecEndPtRemotePort,

                -- The IPsec Phase-2 Security Assocaition Table
                -- ipSecTunIndex
                ipSecSaDirection,
                ipSecSaValue,
                ipSecSaProtocol,
                ipSecSaStatus
              }
      STATUS current
      DESCRIPTION
         "This group consists of:
          1) IPsec Phase-2 Global Statistics
          2) IPsec Phase-2 Tunnel Table
          3) IPsec Phase-2 Endpoint Table
          4) IPsec Phase-2 Security Protection Index Table"
      ::= { ipSecMIBGroups 5 }

   ipSecHistoryGroup OBJECT-GROUP
      OBJECTS {
                -- IPsec History Global Control Objects
                ipSecHistTableSize,
                ipSecHistCheckPoint,
```

```
                    -- The IPsec Phase-1 Tunnel History Table
                    ikeTunHistTermReason,
                    ikeTunHistActiveIndex,
                    ikeTunHistPeerLocalType,
                    ikeTunHistPeerLocalValue,
                    ikeTunHistPeerIntIndex,
                    ikeTunHistPeerRemoteType,
                    ikeTunHistPeerRemoteValue,
                    ikeTunHistLocalAddr,
                    ikeTunHistLocalName,
                    ikeTunHistRemoteAddr,
                    ikeTunHistRemoteName,
                    ikeTunHistNegoMode,
                    ikeTunHistDiffHellmanGrp,
                    ikeTunHistEncryptAlgo,
                    ikeTunHistEncryptKeySize,
                    ikeTunHistHashAlgo,
                    ikeTunHistAuthMethod,
                    ikeTunHistLifeTime,
                    ikeTunHistStartTime,
                    ikeTunHistActiveTime,
                    ikeTunHistTotalRefreshes,
                    ikeTunHistTotalSas,
                    ikeTunHistInOctets,
                    ikeTunHistInPkts,
                    ikeTunHistInDropPkts,
                    ikeTunHistInNotifys,
                    ikeTunHistInP2Exchgs,
                    ikeTunHistInP2ExchgInvalids,
                    ikeTunHistInP2ExchgRejects,
                    ikeTunHistInP2SaDelRequests,
                    ikeTunHistOutOctets,
                    ikeTunHistOutPkts,
                    ikeTunHistOutDropPkts,
                    ikeTunHistOutNotifys,
                    ikeTunHistOutP2Exchgs,
                    ikeTunHistOutP2ExchgInvalids,
                    ikeTunHistOutP2ExchgRejects,
                    ikeTunHistOutP2SaDelRequests,

                    -- The IPsec Phase-2 Tunnel History Table
                    -- ipSecTunHistIndex,
                    ipSecTunHistTermReason,
                    ipSecTunHistActiveIndex,
                    --ipSecTunHistIkeTunnelIndex,
                    ipSecTunHistLocalAddr,
```

```
                    ipSecTunHistRemoteAddr,
                    -- ipSecTunHistKeyType,
                    ipSecTunHistEncapMode,
                    ipSecTunHistLifeSize,
                    ipSecTunHistLifeTime,
                    ipSecTunHistStartTime,
                    ipSecTunHistActiveTime,
                    ipSecTunHistTotalRefreshes,
                    ipSecTunHistTotalSas,
                    ipSecTunHistInSaDiffHellmanGrp,
                    ipSecTunHistInSaEncryptAlgo,
                    ipSecTunHistInSaAhAuthAlgo,
                    ipSecTunHistInSaEspAuthAlgo,
                    ipSecTunHistInSaDecompAlgo,
                    ipSecTunHistOutSaDiffHellmanGrp,
                    ipSecTunHistOutSaEncryptAlgo,
                    ipSecTunHistOutSaAhAuthAlgo,
                    ipSecTunHistOutSaEspAuthAlgo,
                    ipSecTunHistOutSaCompAlgo,
                    ipSecTunHistPmtu,
                    ipSecTunHistInOctets,
                    ipSecTunHistHcInOctets,
                    ipSecTunHistInOctWraps,
                    ipSecTunHistInDecompOctets,
                    ipSecTunHistHcInDecompOctets,
                    ipSecTunHistInDecompOctWraps,
                    ipSecTunHistInPkts,
                    ipSecTunHistInDropPkts,
                    ipSecTunHistInReplayDropPkts,
                    ipSecTunHistInAuths,
                    ipSecTunHistInAuthFails,
                    ipSecTunHistInDecrypts,
                    ipSecTunHistInDecryptFails,
                    ipSecTunHistOutOctets,
                    ipSecTunHistHcOutOctets,
                    ipSecTunHistOutOctWraps,
                    ipSecTunHistOutUncompOctets,
                    ipSecTunHistHcOutUncompOctets,
                    ipSecTunHistOutUncompOctWraps,
                    ipSecTunHistOutPkts,
                    ipSecTunHistOutDropPkts,
                    ipSecTunHistOutAuths,
                    ipSecTunHistOutAuthFails,
                    ipSecTunHistOutEncrypts,
                    ipSecTunHistOutEncryptFails,
                    ipSecTunHistOutCompressedPkts,
                    ipSecTunHistOutCompSkippedPkts,
```

```
                    ipSecTunHistOutCompFailPkts,
                    ipSecTunHistOutCompTooSmallPkts,
                    ipSecTunHistControlProtocol,
                    ipSecTunHistControlTunnelIndex,
                    ipSecTunHistInSaEncryptKeySize,
                    ipSecTunHistOutSaEncryptKeySize,

                    -- The IPsec Phase-2 End Point History Table
                    -- ipSecEndPtHistIndex,
                    ipSecEndPtHistTunIndex,
                    ipSecEndPtHistActiveIndex,
                    ipSecEndPtHistLocalName,
                    ipSecEndPtHistLocalType,
                    ipSecEndPtHistLocalAddr1,
                    ipSecEndPtHistLocalAddr2,
                    ipSecEndPtHistLocalProtocol,
                    ipSecEndPtHistLocalPort,
                    ipSecEndPtHistRemoteName,
                    ipSecEndPtHistRemoteType,
                    ipSecEndPtHistRemoteAddr1,
                    ipSecEndPtHistRemoteAddr2,
                    ipSecEndPtHistRemoteProtocol,
                    ipSecEndPtHistRemotePort
                  }
      STATUS current
      DESCRIPTION
         "This group consists of:
          1) IPsec History Global Objects
          2) IPsec Phase-1 History Objects
          3) IPsec Phase-2 History Objects"
      ::= { ipSecMIBGroups 6 }

   ipSecFailuresGroup OBJECT-GROUP
      OBJECTS {
                    -- The IPsec Failure Global Control Objects
                    ipSecFailTableSize,

                    -- The IPsec Phase-1 Failure Table
                    ikeFailReason,
                    ikeFailTime,
                    ikeFailLocalType,
                    ikeFailLocalValue,
                    ikeFailRemoteType,
                    ikeFailRemoteValue,
                    ikeFailLocalAddr,
                    ikeFailRemoteAddr,
```

```
                -- The IPsec Phase-2 Failure Table
                -- ipSecFailIndex,
                ipSecFailReason,
                ipSecFailTime,
                ipSecFailTunnelIndex,
                ipSecFailSaSpi,
                ipSecFailPktSrcAddr,
                ipSecFailPktDstAddr
              }
      STATUS current
      DESCRIPTION
         "This group consists of:
          1) IPsec Failure Global Objects
          2) IPsec Phase-1 Tunnel Failure Table
          3) IPsec Phase-2 Tunnel Failure Table"
      ::= { ipSecMIBGroups 7 }

   ipSecTrapCntlGroup OBJECT-GROUP
      OBJECTS {
                ipSecTrapCntlIkeTunnelStart,
                ipSecTrapCntlIkeTunnelStop,
                ipSecTrapCntlIkeSysFailure,
                ipSecTrapCntlIkeCertCrlFailure,
                ipSecTrapCntlIkeProtocolFail,
                ipSecTrapCntlIkeNoSa,
                ipSecTrapCntlIpSecTunnelStart,
                ipSecTrapCntlIpSecTunnelStop,
                ipSecTrapCntlIpSecSysFailure,
                ipSecTrapCntlIpSecSetUpFailure,
                ipSecTrapCntlIpSecEarlyTunTerm,
                ipSecTrapCntlIpSecProtocolFail,
                ipSecTrapCntlIpSecNoSa,
                ipSecTrapCntlInNewGrpRejected,
                ipSecTrapCntlOutNewGrpRejected
              }
      STATUS current
      DESCRIPTION
         "This group of objects controls the sending of IPsec TRAPs."
      ::= { ipSecMIBGroups 8 }

    ipSecNotificationGroup    NOTIFICATION-GROUP
       NOTIFICATIONS {
                       ikeTunnelStart,
                       ikeTunnelStop,
                       ikeSysFailure,
                       ikeCertCrlFailure,
                       ikeProtocolFailure,
```

```
                        ikeNoSa,
                        ipSecTunnelStart,
                        ipSecTunnelStop,
                        ipSecSysFailure,
                        ipSecSetUpFailure,
                        ipSecEarlyTunTerm,
                        ipSecProtocolFailure,
                        ipSecNoSa,
                        ipSecInNewGrpRejected,
                        ipSecOutNewGrpRejected
                      }
          STATUS current
          DESCRIPTION
             "This group contains the notifications for the IPsec MIB."
          ::= { ipSecMIBGroups 9 }

      ipSecModeConfigGroup OBJECT-GROUP
         OBJECTS {
                   -- The IPsec Mode Configuration group
                    ikeGlobalInConfigs,
                    ikeGlobalOutConfigs,
                    ikeGlobalInConfigsRejects,
                    ikeGlobalOutConfigsRejects,
                    --ikePeerConfigAppVersion,
                    --ikePeerConfigAddress,
                    --ikePeerConfigNetmask,
                    --ikePeerConfigDns,
                    --ikePeerConfigNbns,
                    --ikePeerConfigDhcp,
                    ikeTunInConfigs,
                    ikeTunOutConfigs,
                    ikeTunInConfigsRejects,
                    ikeTunOutConfigsRejects,
                    ikeTunHistInConfigs,
                    ikeTunHistOutConfigs,
                    ikeTunHistInConfigsRejects,
                    ikeTunHistOutConfigsRejects
                  }
         STATUS current
         DESCRIPTION
            "This group consists of:
             1) Global metrics about IKE Mode Configuration activity
             2) Phase-1 IKE Tunnel-wise Mode Configuration metrics
             3) Historical IKE Mode Configuration metrics on a per
                expired tunnel basis."
         ::= { ipSecMIBGroups 10 }
```

```
      ipSecNewGrpGroup OBJECT-GROUP
         OBJECTS {
                   -- The IPsec New Group negotiation group
                   ikeTunInNewGrpReqs,
                   ikeTunOutNewGrpReqs,
                   ikeTunInNewGrpReqsRejected,
                   ikeTunOutNewGrpReqsRejected,
                   ikeTunHistInNewGrpReqs,
                   ikeTunHistOutNewGrpReqs,
                   ikeTunHistInNewGrpReqsRejected,
                   ikeTunHistOutNewGrpReqsRejected,
                   ipSecGlobalInNewGrpReqs,
                   ipSecGlobalOutNewGrpReqs,
                   ipSecGlobalInNewGrpReqsRejected,
                   ipSecGlobalOutNewGrpReqsRejected
                 }
         STATUS current
         DESCRIPTION
            "This group consists of:
             1) Global metrics about new group negotiations
             2) Phase-1 IKE Tunnel-wise new group metrics
             3) Historical new group metrics on a per tunnel basis.
             4) Notifications pertaining to new grp failures."
         ::= { ipSecMIBGroups 11 }

      deprecatedObjectGroup OBJECT-GROUP
           OBJECTS {
               -- The deprecated table 'ipSecSpiTable'
               ipSecSpiDirection,
               ipSecSpiValue,
               ipSecSpiProtocol,
               ipSecSpiStatus,
               ipSecTunIkeTunnelIndex,
               ipSecTunIkeTunnelAlive,
               ipSecTunKeyType,
               ipSecTunHistIkeTunnelIndex,
               ipSecTunHistKeyType
           }
           STATUS        deprecated
           DESCRIPTION   "A collection of objects that have bee
                         deprecated."
         ::= { ipSecMIBGroups 12 }

   END
```

## 6. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

## 7. Acknowledgements

The editors would like to thank: Ajay Dankar, Jamal Mohamed, Mayank Jain, Roy Pereira, David McGrew and Lauren Heintz.

## 8. Security Considerations

This document describes how a management station can monitor structure and acivity of IPsec based VPNs. Applications have access to data which is not secured. Applications SHOULD take reasonable steps to protect the data from disclosure.

This document also contains a MIB definition module. The information contained in this MIB describes a VPN service whose variables may be read and in some cases set.

It is important that access to the MIB is limited to the appropriate users, and that information exchanges between users, management stations, agents and any other devices is provided via a secure mechanism such as an encrypted session.

## 9. References

[RFC2407] Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[RFC2401] Kent, S., Atkinson, R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2409] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE), RFC 2409, November 1998.

[RFC2408] Maughan, D., Schertler, M., Schneider, M., and Turner, J., "Internet Security Association and Key Management Protocol (ISAKMP)_,RFC 2408, November 1998.

[IGMIB] McCloghrie, K., Kastenholz, F., "The Interfaces Group MIB using SMIv2", RFC2233

[RFC1902] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1902, January 1996.

[RFC2271] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", RFC 2271, January 1998

[RFC1155] Rose, M. and K. McCloghrie, "Structure and Identification of Management Information for TCP/IP-based internets", STD 16, RFC 1155, 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

[RFC1903] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1903,January 1996.

[RFC1904] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1904,January 1996.

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol", RFC 1157, May

1990.

[RFC1901] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Introduction to Community-based SNMPv2", RFC 1901, January 1996.

[RFC1906] SNMPv2 Working Group, 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.

[RFC2272] Case, J., Harrington D., Presuhn R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", RFC 2272, January 1998.

[RFC2274] Blumenthal, U., and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", RFC 2274, January 1998.

[RFC1905] SNMPv2 Working Group, 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.

## 10. Editor's Addresses

Cheryl Madson
Cisco Systems
170 W Tasman Drive
San Jose, Ca 95134
Phone: +1 (408) 527 2817
EMail: cmadson@cisco.com

Leo Temoshenko
Cisco Systems
170 W Tasman Drive
San Jose, Ca 95134
USA
Phone: +1 (919) 392 8381
EMail: leot@cisco.com

Chinna Narasimha Reddy Pellacuru
Cisco Systems
170 W Tasman Drive
San Jose, Ca 95134

USA
Phone: +1 (408) 527 3109
EMail: pcn@cisco.com

Bret Harrison
Tivoli Systems Inc.
3901 S. Miami Blvd
Durham, NC. 27703
Phone: +1 (919) 224-1000
EMail: bret_harrison@tivoli.com

S Ramakrishnan
Cisco Systems
170 W Tasman Drive
San Jose, Ca 95134
USA
Phone: +1 (408) 527 7309
EMail: rks@cisco.com

## 11. Expiration

This draft expires Aug 16, 2003.

## 12. Full Copyright Statement

Copyright (C) The Internet Society (2001). All Rights Reserved. This document and translations of it may be copied and furnished t others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, publishe and distributed, in whole or in part, without restriction of an kind, provided that the above copyright notice and this paragraph ar included on all such copies and derivative works. However, thi document itself may not be modified in any way, such as by removin the copyright notice or references to the Internet Society or othe Internet organizations, except as needed for the purpose o developing Internet standards in which case the procedures fo copyrights defined in the Internet Standards process must b followed, or as required to translate it into languages other tha English.

The limited permissions granted above are perpetual and will not b revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERIN

TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATIO HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.