ipsp working group
Internet Draft
Expires October 2004

Man Li
Nokia
David Arneson
N/A
Avri Doria
ETRI
Jamie Jason
Intel
Cliff Wang
SmartPipe
Markus Stenberg
SSH

April 2004

IPsec Policy Information Base
draft-ietf-ipsp-ipsecpib-10.txt

Status of this Memo

Abstract

This document describes a portion of the Policy Information Base (PIB) for a device implementing the IP Security (IPsec) Architecture. The provisioning classes defined here provide control of IPsec policy. These provisioning classes can be used with other non-IPsec provisioning classes (defined in other PIB modules) to

provide for a comprehensive policy controlled mapping of service requirement to device capability and usage.

Table of Contents

Conventions used in this document

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 RFC-2119 [2].

1. Introduction

The policy rule classes (PRC) defined in this document contain parameters for Internet Key Exchange (IKE) phase one and phase two negotiations. Details of these parameters can be found in [3], [7], [8], [10], [11], [12] and [14]. The PIB defined in this document is based on the IPsec configuration policy model [12]. The concept of "Roles" described in [9], which scales to large networks, is adopted for distributing IPsec policy over the COPS-

PR protocol [6].

2. Operation Overview

As defined in [13], the management entity that downloads policy to IPsec-enabled devices will be called a Policy Decision Point (PDP) and the target IPsec-enabled devices will be called Policy Enforcement Points (PEP).

After connecting to a PDP using COPS-PR [6] that is an extension of COPS [5], a PEP reports to the PDP the PIB Provisioning Classes (PRCs) it supports as well as any limitations related to the implementations of theses classes and parameters. The PEP provides the above information using the frwkPrcSupportTable and the frwkCompLimitsTable defined in the framework PIB [9]. In addition, the PEP also reports the interface type capabilities and role combinations it supports using the frwkCapabilitySetTable and the

frwkRoleComboTable. Each row of the frwkCapabilitySetTable contains a capability set name and a reference to an instance of a PRC that describes the capabilities of the interface type. The capability instances may reside in the ipSecIfCapsTable or in a class defined in another PIB. Each row of the frwkRoleComboTable contains an interface capability set name and a role combination.

Based on the interface capabilities and role combinations, the PDP provides the PEP with IPsec policy information. Later on, if any of the interface capabilities or role combinations of the PEP change, the PEP notifies the PDP. The PDP will then send a new set of IPsec policy information to the PEP. In addition, if the policy associated with a given interface capability and role combination changes, the PDP will deliver the new IPsec policy to all the PEPs that have registered with that interface capability and role combination.

3. Structure of IPsec PIB

An IPsec policy consists of an ordered list of IPsec rules. Each rule is composed of a set of conditions and a set of actions. If a packet matches any of the conditions, the actions will be applied accordingly.

The IPsec PIB module consists of nine groups. The selector group describes conditions to be associated with IPsec rules. The IPsec association group, Authentication Header (AH) transform group, Encapsulating Security Payload (ESP) transform group, IP Payload

Compression Protocol (COMP) transform group, IKE association group and the credential group together describe actions to be associated with IPsec rules. The policy time period group specifies time periods during which a rule is valid. The interface capability group is used by a PEP to report the capabilities associated with its interface types.

The IPsec PIB defined in this document is based on the IPsec configuration policy information model [12]. The structure and modularity of this PIB are similar to that of the IPsec configuration policy model. It is easy to observe the mapping of the IPsec association group, AH transform group, ESP transform group, COMP transform group, IKE association group, the credential group and the policy time period group into the configuration model. Note that the policy time period condition is included in the IPsec configuration policy information model [12] but it is specified in the policy core information model[23]. The IPsec selector group corresponds to the filters specified in the IPsec configuration policy model but it is in a slightly different structure in order to provide a scalable way of specifying a large number of filters.

The modular design of the IPsec PIB provides many flexibilities. For example, the key exchange protocol and selectors used in a policy rule are specified by pointing to the corresponding policy

rule classes. Hence, to use key exchange protocols or selectors other than those specified in this PIB, simply direct the pointers to the corresponding policy rule classes specified in other PIB modules.

The nine IPsec PIB groups are discussed in the following sections.

3.1 IPsec association group

This group specifies IPsec Security Associations.

3.1.1 IPsec rules

The ipSecRuleTable is the starting point for specifying an IPsec policy. It contains an ordered list of IPsec rules. Each rule is associated with IfCapSetName, Roles and Direction attributes to indicate the interface type and role combinations as well as the direction of the interface to which this rule is to be applied. Each rule points to a set of selectors and, optionally, a set of IP Security Options (IPSO) filters to indicate the conditions associated with this rule. In addition, each rule has a pointer to a set of actions to indicate the actions associated with this rule. Hence if a packet matches a selector in the selector set and, if the reference to the IPSO filter set is not zero, it matches a filter in the IPSO filter set, the action(s) associated with this rule will be applied to the packet.

When a rule involves multiple actions, the ExecutionStrategy attribute indicates how these actions are executed. A value of "DoAll" means that all the actions MUST be applied to the packet according to a predefined order. A value of "DoUntilSuccess" means that the actions MUST be tried in sequence until a successful execution of a single action.

For example, in a nested Security Associations (SA) case the actions of an initiator's rule might be structured as:

```
ExecutionStrategy='Do All'
|
+---1--- IPsecTunnelAction    // set up SA from host to gateway
|
+---2--- IPsecTransportAction // set up SA from host through
                              // tunnel to remote host
```

Another example, showing a rule with fallback actions might be structured as:

```
ExecutionStrategy='Do Until Success'
|
+---1--- IPsecTunnelAction // set up SA from host to gateway [A]
|
+---2--- IPsecTunnelAction // set up SA from host to gateway [B]
```

As an optional feature, IPsec associations may be established without being prompted by IP packets. The AutoStart attribute indicates if the IPsec association(s) of this rule should be set up automatically. Support of this attribute is optional.

3.1.2 IPsec actions

IPsec actions may be of two types: Static Action and Negotiation Action.

Static Actions do not require any negotiations. They include by-pass, discard, IKE rejection, pre-configured transport and pre-configured tunnel actions. The ipSecStaticActionTable specifies

IPsec Static Actions. For a pre-configured transport or pre-configured tunnel action, it further points to a valid instance in another class that describes a transform to be used, for example, the ipSecEspTransformTable. In addition, the SPI used for the transform is also defined in the table.

Negotiation Actions require negotiations in order to establish Security Associations. They include transport and tunnel actions. The ipSecNegotiationActionTable specifies IPsec Negotiation Actions. It points to a valid instance in the ipSecAssociationTable that further defines the IPsec association to be established. For key exchange policy, the KeyExchangeId points to a valid instance in another class that describes key exchange procedures. If a single IKE phase one negotiation is used for the key exchange, this attribute MUST point to an instance in the ipSecIkeAssociationTable. If multiple IKE phase one negotiations (e.g., with different modes) are to be tried until success, this attribute SHOULD point to ipSecIkeRuleTable. For other key exchange methods, this attribute MAY point to an instance of a PRC defined in some other PIB module.

The ipSecActionSetTable specifies sets of actions. Actions within a set form an ordered list. If an action within a set is a Static Action, the ActionId MUST point to a valid instance in the ipSecStaticActionTable. If the action is a Negotiation Action, the ActionId MUST point to a valid instance in the ipSecNegotiationActionTable. For other actions, the ActionId MAY point to an instance of a PRC defined in some other PIB module.

3.1.3 IPsec associations

The ipSecAssociationTable specifies attributes associated with IPsec associations. For each association, it points to a set of proposals in the ipSecProposalSetTable that is associated with this association.

The MinLifetimeSeconds and MinLifetimeKilobytes in the ipSecAssociationTable indicate the lifetime to propose for the IPsec association to be negotiated. They are different from the

time periods indicated by the IpSecRuleTimePeriodGroupId in the IpsecRuleTable. Those time periods specify when the given IPsec rule is valid.

3.1.4 IPsec proposals

The ipSecProposalSetTable specifies sets of proposals. Proposals within a set are ordered with a preference value.

The ipSecProposalTable specifies proposals. It points to sets of ESP transforms, AH transforms and IP COMP transforms. Within a proposal, sets of transforms of different types are logically ANDed. Transforms of the same type within a transform set are to be logically ORed. For example, if the proposal were

```
ESP = { (HMAC-MD5, 3DES), (HMAC-MD5, DES) }
AH  = { MD5, SHA-1 }
```

then the one sending the proposal would want the other side to pick one from the ESP transform (preferably (HMAC-MD5, 3DES)) list AND one from the AH transform list (preferably MD5).

3.2 AH transform group

The AH transform group describes sets of AH transforms.

3.3 ESP transform group

The ESP transform group describes sets of ESP transforms.

3.4 COMP transform group

The COMP transform group describes sets of COMP transforms.

3.5 IKE association group

This group specifies rules associated with IKE phase one negotiation. The rules are IKEv1 rules as specified in [10].

The ipSecIkeRuleTable and the ipSecIkeActionSetTable are optional tables. Support of these tables is required only when a policy contains:

- Multiple IKE phase one actions (e.g., with different exchange modes) that are associated with one IPsec association. These actions are to be tried in sequence till one success.

- IKE phase one actions that start automatically.

For the latter case, IKE rules may be distributed independently and the IfCapSetName and Roles attributes in the ipSecIkeRuleTable indicate the interface type and role combinations to which this rule is to be applied.

The ipSecIkeActionSetTable specifies sets of actions. Actions within a set form an ordered list.

The ipSecIkeAssociationTable contains parameters associated with IKE associations including the IKE identities to be used during IKE phase one negotiation. It points to a set of credentials specified in the ipSecCredentialTable. Any of the credentials in this set may be used during IKE phase one negotiation. In addition, each IKE association points to a set of IKE proposals to be associated with this association. If the Authentication Method for one or more of the IKE proposals is specified as PresharedKey in the ipSecIkeProposalTable, the ipSecIkeAssociationPresharedKey attribute contains the actual pre-shared key to be used for the proposal(s). This attribute is optional. If this attribute is not supported or contains a zero length octet, the pre-shared key MUST be obtained through other methods.

The ipSecIkeProposalSetTable specifies sets of proposals. Proposals within a set are ordered with a preference value.The ipSecIkeProposalTable contains parameters associated with IKE proposals.

The ipSecIkePeerEndpointTable specifies IKE peer endpoint information that includes acceptable peer identity and credentials for IKE phase one negotiation. It points to a set of credentials specified in the ipSecCredentialSetTable. Any of the credentials in the set is acceptable as a peer credential.

3.6 Credential group

This group specifies credentials to be used for IKE phase one negotiations.

The ipSecCredentialSetTable specifies sets of credentials. The ipSecCredentialTable and ipSecCredentialFieldsTable together specify credentials. Each credential may contain multiple sub-fields. For example, a certificate may contain a unique serial number sub-field and an issuer name sub-field, etc. The ipSecCredentialFieldsTable defines the sub-fields and their values that MUST be matched against. The ipSecCredentialTable points to a set of criteria defined in the ipSecCredentialFieldsTable. The criteria MUST all be satisfied in order for a credential to be considered as acceptable. Certificates may also be revoked. The CrlDistributionPoint attribute in the ipSecCredentialTable indicates the Certificate Revocation List (CRL) distribution point where CRLs may be fetched.

3.7 Selector group

This group specifies the selectors for IPsec rules.

The ipSecSelectorSetTable specifies sets of selectors. Selectors within a set form an ordered list. The SelectorId attribute points to a valid instance in another class that describes a selector. To achieve scalability in policy distribution for large networks, it SHOULD point to the ipSecSelectorTable.

The ipSecAddressTable specifies individual or ranges of IP addresses and the ipSecL4PortTable specifies individual or ranges of layer 4 ports. The ipSecSelectorTable has references to these two tables. Each row in the selector class can represent multiple selectors. These selectors are constructed as follows:

1. Substitute the ipSecSelectorSrcAddressGroupId with all the IP addresses from the ipSecAddressTable whose ipSecAddressGroupId matches the ipSecSelectorSrcAddressGroupId.

2. Substitute the ipSecSelectorDstAddressGroupId with all the IP addresses from the ipSecAddressTable whose ipSecAddressGroupId matches the ipSecSelectorDstAddressGroupId.

3. Substitute the ipSecSelectorSrcPortGroupId with all the ports or ranges of port whose ipSecL4PortGroupId matches the ipSecSelectorSrcPortGroupId.

4. Substitute the ipSecSelectorDstPortGroupId with all the ports or ranges of port whose ipSecL4PortGroupId matches the ipSecSelectorDstPortGroupId.

5. Construct all the possible combinations of the above four fields. Then add to the combinations the ipSecSelectorProtocol, ipSecSelectorDscp and ipSecSelectorFlowLabel attributes to form the list of selectors.

Selectors constructed from a single row have the same order within a selector set. The order is indicated by the Order attribute of the ipSecSelectorSetTable. The relative order among selectors constructed from a single row is unspecified. This is not an issue as long as these selectors are not over-lapping.

The use of references in the ipSecSelectorTable instead of real IP addresses and port numbers reduces the number of bytes being pushed down to the PEP. Grouping of IP addresses and layer 4 ports serves the same purpose.

The ipSecIpsoFilterSetTable specifies sets of IPSO filters.

Filters within a set form an ordered list. The ipSecIpsoFilterTable contains IPSO filters.

3.8 Policy time period group

This group specifies time periods during which a policy rule is valid. The ipSecRuleTimePeriodTable specifies a single time period

of a day (or days). The ipSecRuleTimePeriodSetTable allows the specification of multiple time periods.

Implementation of this group is optional.

3.9 Interface capability group

PEPs may have different capabilities. For example, some PEPs support nested Security Associations whereas others do not. This group allows a PEP to specify the capabilities associated with its different interface types.

For ease of reference, a concise summary of the groups and tables is included in the next section.

4. Summary of the IPsec PIB

4.1 ipSecAssociation group

This group specifies IPsec Security Associations.

4.1.1 ipSecRuleTable

This class is the starting point for specifying an IPsec policy.
It contains an ordered list of IPsec rules.

4.1.2 ipSecActionSetTable

Specifies IPsec action sets.

4.1.3 ipSecStaticActionTable

Specifies IPsec static actions.

4.1.4 ipSecNegotiationActionTable

Specifies IPsec negotiation actions.

4.1.5 ipSecAssociationTable

Specifies IPsec associations.

4.1.6 ipSecProposalSetTable

Specifies IPsec proposal sets.

4.1.7 ipSecProposalTable
Specifies IPsec proposals.

4.2 ipSecAhTransform group
This group specifies AH Transforms.

4.2.1 ipSecAhTransformSetTable
Specifies AH transform sets.

4.2.2 ipSecAhTransformTable
Specifies AH transforms.

4.3 ipSecEspTransform group
This group specifies ESP Transforms.

4.3.1 ipSecEspTransformSetTable
Specifies ESP transform sets.

4.3.2 ipSecEspTransformTable
Specifies ESP transforms.

4.4 ipSecCompTransform group
This group specifies Compression Transforms.

4.4.1 ipSecCompTransformSetTable
Specifies IP compression transform sets.

4.4.2 ipSecCompTransformTable
Specifies IP compression algorithms.

4.5 ipSecIkeAssociation group
This group specifies IKEv1 Security Associations.

4.5.1 ipSecIkeRuleTable
Specifies IKEv1 rules.

4.5.2 ipSecIkeActionSetTable
Specifies IKEv1 action sets.

4.5.3 ipSecIkeAssociationTable
Specifies IKEv1 associations.

4.5.4 ipSecIkeProposalSetTable
Specifies IKEv1 proposal sets.

4.5.5 ipSecIkeProposalTable

Specifies IKEv1 proposals.

4.5.6 ipSecIkePeerEndpointTable

Specifies IKEv1 peer endpoints.

4.6 ipSecCredential group

This group specifies credentials for IKEv1 phase one negotiations.

4.6.1 ipSecCredentialSetTable

Specifies credential sets.

4.6.2 ipSecCredentialTable

Specifies credentials.

4.6.3 ipSecCredentialFieldsTable

Specifies sets of credential sub-fields and their values to be matched against.

4.7 ipSecSelector group

This group specifies selectors for IPsec associations.

4.7.1 ipSecSelectorSetTable

Specifies IPsec selector sets.

4.7.2 ipSecSelectorTable

Specifies IPsec selectors.

4.7.3 ipSecAddressTable

Specifies IP addresses.

4.7.4 ipSecL4PortTable

Specifies layer four port numbers.

4.7.5 ipSecIpsoFilterSetTable

Specifies IPSO filter sets.

4.7.6 ipSecIpsoFilterTable

Specifies IPSO filters.

4.8 ipSecPolicyTimePeriod group

This group specifies the time periods during which a policy rule is valid.

4.8.1 ipSecRuleTimePeriodTable

Specifies the time periods during which a policy rule is valid.

4.8.2 ipSecRuleTimePeriodSetTable

Specifies time period sets.

4.9 ipSecIfCapability group

This group specifies capabilities associated with interface types.

4.9.1 ipSecIfCapsTable

Specifies capabilities that may be associated with an interface of a specific type.

4.10 ipSecPolicyPibConformance group

This group specifies requirements for conformance to the IPsec Policy PIB.

5. The IPsec PIB Module

```
IPSEC-POLICY-PIB PIB-DEFINITIONS ::= BEGIN

IMPORTS
Unsigned32, Unsigned64, MODULE-IDENTITY,
OBJECT-TYPE, TEXTUAL-CONVENTION, MODULE-COMPLIANCE,
OBJECT-GROUP, pib
FROM COPS-PR-SPPI           --[RFC3159]
TruthValue
FROM SNMPv2-TC              --[RFC2579]
InstanceId, ReferenceId, TagId, TagReferenceId, Prid
FROM COPS-PR-SPPI-TC        --[RFC3159]
```

```
   SnmpAdminString
     FROM SNMP-FRAMEWORK-MIB     --[RFC3411]
InetAddress, InetAddressType,
InetAddressPrefixLength, InetPortNumber
     FROM INET-ADDRESS-MIB       --[RFC3291]
DscpOrAny
     FROM DIFFSERV-DSCP-TC       --[RFC3289]
IPv6FlowLabelOrAny
            FROM IPV6-FLOW-LABEL-MIB  --[RFC3595]
RoleCombination
FROM FRAMEWORK-TC-PIB      --[RFC3318]
 IpsecDoiIpcompTransform,IpsecDoiEspTransform,
 IpsecDoiIdentType,IpsecDoiAuthAlgorithm
     FROM IPSEC-IPSECACTION-MIB
        --[draft-ietf-ipsp-ipsecaction-mib-00.txt]
 IkeEncryptionAlgorithm,IkeAuthMethod,IkeHashAlgorithm,
 IkeGroupDescription
     FROM IPSEC-IKEACTION-MIB;
```

```
        --[ draft-ietf-ipsp-ikeaction-mib-00.txt]

--
-- module identity
--

ipSecPolicyPib MODULE-IDENTITY
SUBJECT-CATEGORIES { xxxx (nn)  } -- IPsec Client Type
-- to be assigned by IANA. Suggest to use ipSec for xxxx
LAST-UPDATED "200404041800Z"
ORGANIZATION "IETF ipsp WG"
CONTACT-INFO "
Man Li
Nokia
5 Wayside Road,
Burlington, MA 01803
Phone: +1 781 993 3923
Email: man.m.li@nokia.com

Avri Doria
ETRI
161 Gajeong-dong, Yuseong-gu
Deajeon 305-350 Korea
Email: avri@acm.org

Jamie Jason
Intel Corporation
MS JF3-206
2111 NE 25th Ave.
Hillsboro, OR 97124
Phone: +1 503 264 9531
Fax: +1 503 264 9428
Email: jamie.jason@intel.com

Cliff Wang
```

```
SmartPipes Inc.
Suite 300, 565 Metro Place South
Dublin, OH 43017
Phone: +1 614 923 6241
Email: CWang@smartpipes.com

 Markus Stenberg
 SSH Communications Security Corp.
 Fredrikinkatu 42
 FIN-00100 Helsinki, Finland
 Phone: +358 20 500 7466
 Email: fingon@iki.fi"


DESCRIPTION
"This PIB module contains a set of policy rule classes that
describe IPsec policies.

Copyright (C) The Internet Society (2004). This version of this
PIB module is part of RFC xxxx; see the RFC itself for full legal
notices"

REVISION "200404041800Z"
DESCRIPTION
"Initial version, published as RFC xxxx."
-- xxxx to be assigned by IANA --
::= { pib yyy } -- yyy to be assigned by IANA --

--
-- Textual Conventions
--


Unsigned16TC ::= TEXTUAL-CONVENTION
  DISPLAY-HINT "d"
  STATUS       current
  DESCRIPTION
  "An unsigned 16 bit integer."
  SYNTAX    Unsigned32 (0..65535)

LocalOrUtcTimeTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  " Indicates whether to use local times or universal time (UTC)
times. "
  SYNTAX    INTEGER {localTime(1),utcTime(2)}

TimePeriodTC ::= TEXTUAL-CONVENTION
  DISPLAY-HINT "255t"
  STATUS       current
  DESCRIPTION
  " An octet string that identifies an overall range of calendar
dates and times.  It reuses the format for an explicit time period
```

```
defined in [RFC 2445] : a string representing a starting date and
time, in which the character 'T'  indicates the beginning of the
time portion, followed by the solidus character '/', followed by a
similar string representing an end date and time.  The first date
```

```
indicates the beginning of the range, while the second date
indicates the end.  Thus, the second date and time must be later
than the first.  Date/times are expressed as substrings of the
form yyyymmddThhmmss.

There are also two special cases:

-  If the first date/time is replaced with the string
THISANDPRIOR, then the property indicates that a policy rule is
valid [from now] until the date/time that appears after the '/'.

- If the second date/time is replaced with the string
THISANDFUTURE, then the property indicates that a policy rule
becomes valid on the date/time that appears before the '/', and
remains valid from that point on.

This information is represented using the ISO/IEC IS 10646-1
character set, encoded as an octet string using the UTF-8
transformation format described in [RFC2279]."
  SYNTAX    OCTET STRING

TimeOfDayTC ::= TEXTUAL-CONVENTION
  DISPLAY-HINT "255t"
  STATUS       current
  DESCRIPTION
  " An octet string that specifies a range of times in a day. It
is formatted as follows:

A  time  string beginning with the character 'T', followed by the
solidus character '/', followed by a second time string.  The
first time indicates the beginning of the range, while the second
time indicates the end.  Times are expressed as substrings of the
form Thhmmss.

The second substring always identifies a later time than the first
substring.  To allow for ranges that span midnight, however, the
value of the second string may be smaller than the value of the
first substring.  Thus, T080000/T210000 identifies the range from
0800 until 2100, while T210000/T080000 identifies the range from
2100 until 0800 of the following day.

This information is represented using the ISO/IEC IS 10646-1
character set, encoded as an octet string using the UTF-8
transformation format described in [RFC2279]."
  SYNTAX    OCTET STRING

MonthOfYearTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  "Defines months of a year"
  SYNTAX BITS {january(0),february(1),march(2),april(3),
               may(4),june(5),july(6),august(7),september(8),
               october(9),november(10),december(11)}

DayOfWeekTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  "Defines days of a week"
  SYNTAX BITS {sunday(0),monday(1),tuesday(2),wednesday(3),
              thursday(4),friday(5),saturday(6)}

DayOfMonthTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  "Defines days of a month"
  SYNTAX BITS
{first(0),second(1),third(2),fourth(3),fifth(4),sixth(5),
 seventh(6),eighth(7),ninth(8),tenth(9),eleventh(10),
twelfth(11),thirteenth(12),fourteenth(13),fifteenth(14),
sixteenth(15),seventeenth(16),eighteenth(17),nineteenth(18),
twentieth(19),twenty-first(20),twenty-second(21),
twenty-third(22),twenty-fourth(23), twenty-fifth(24),
twenty-sixth(25), twenty-seventh(26),twenty-eighth(27),
twenty-ninth(28), thirty(29), thirty-first(30)}

IpSecOrderTC ::= TEXTUAL-CONVENTION
  DISPLAY-HINT "d"
  STATUS       current
  DESCRIPTION
  "An unsigned 16 bit integer that defines the order of a set of
rules. A smaller value indicates a higher precedence order"
  SYNTAX    Unsigned32 (0..65535)

IpSecDirectionTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  "Specifies the direction of traffic to which an IPsec rule shall
be applied"
  SYNTAX    INTEGER {in(1),out(2),bi-directional(3)}

IpSecDFBitTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  " For tunnel security associations, this attribute specifies how
the DF bit is managed.  Copy (1) indicates to copy the DF bit from
the internal IP header to the external IP header. Set (2)
indicates to set the DF bit of the external IP header to 1. Clear
```

```
(3) indicates to clear the DF bit of the external IP header to 0.
"
  SYNTAX    INTEGER {copy(1),set(2),clear(3)}

IpSecExchangeModeTC ::= TEXTUAL-CONVENTION
```

```
  STATUS       current
  DESCRIPTION
  " Specifies the negotiation mode that the Internet Key Exchange
(IKE) server will use for phase one."
  SYNTAX    INTEGER {baseMode(0),mainMode(1),aggressiveMode(2)}

IpSecActionTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  " Specifies the IPsec action to be applied to the traffic.
transport(1) means that the packet should be protected with a
security association in transport mode. tunnel(2) means that the
packet should be protected with a security association in tunnel
mode."
  SYNTAX    INTEGER {transport(1),tunnel(2)}

IpSecCredTypeTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  " Specifies the type of credentials used for IKE phase one."
  SYNTAX    INTEGER {certificateX509(1),kerberosTicket(2)}

IpSecGranularityTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  "Specifies how the proposed selector for the security
association will be created. Subnet (0) indicates that the source
and destination subnet masks of the filter entry are used. Address
(1) indicates that only the source and destination IP addresses of
the triggering packet are used. Protocol(2) indicates that the
source and destination IP addresses and the IP protocol of the
triggering packet are used. Port (3) indicates that the source and
destination IP addresses and the IP protocol and the source and
destination layer 4 ports of the triggering packet are used. "
  SYNTAX BITS {subnet(0),address(1),protocol(2),port(3)}

IpSecIpsoClassificationTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  " Specifies IP security options (IPSO) classification level."
  REFERENCE "RFC 1108"
  SYNTAX    INTEGER {topSecret(61),secret(90),
                     confidential(150),unclassified(171)}

IpSecIpsoProtectionTC ::= TEXTUAL-CONVENTION
  STATUS       current
  DESCRIPTION
  " Specifies IPSO protection level."
  REFERENCE "RFC 1108"
  SYNTAX    INTEGER {genser(0),siop-esi(1),sci(2),
                     nsa(3),doe(4)}
```

```
--
-- Object identifiers
--



ipSecAssociation
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 1 }
ipSecAhTransform
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 2 }
ipSecEspTransform
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 3 }
ipSecCompTransform
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 4 }
ipSecIkeAssociation
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 5 }
ipSecCredential
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 6 }
ipSecSelector
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 7 }
ipSecPolicyTimePeriod
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 8 }
ipSecIfCapability
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 9 }
ipSecPolicyPibConformance
            OBJECT IDENTIFIER ::= {ipSecPolicyPib 10 }


--
--
-- The ipSecRuleTable
--
```

```
ipSecRuleTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecRuleEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"This class is the starting point for specifying an IPsec policy.
It contains an ordered list of IPsec rules.

For each entry:

1. ipSecRuleIfCapSetName must reference an existing capability set
name in frwkCapabilitySetTable [FRC3318] .

2. ipSecRuleRoles must reference an existing Role Combination in
frwkRoleComboTable [RFC3318].

If any or both of these requirements is not satisfied, the entry
shall not be installed."
  ::= { ipSecAssociation  1 }
```

```
ipSecRuleEntry OBJECT-TYPE
  SYNTAX IpSecRuleEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecRulePrid }
  UNIQUENESS {
    ipSecRuleIfCapSetName,
    ipSecRuleRoles,
    ipSecRuleOrder
    }
  ::= { ipSecRuleTable 1 }

  IpSecRuleEntry ::= SEQUENCE {
     ipSecRulePrid InstanceId,
     ipSecRuleIfCapSetName SnmpAdminString,
     ipSecRuleRoles RoleCombination,
     ipSecRuleDirection IpSecDirectionTC,
     ipSecRuleIpSecSelectorSetId TagReferenceId,
     ipSecRuleIpSecIpsoFilterSetId TagReferenceId,
     ipSecRuleIpSecActionSetId TagReferenceId,
     ipSecRuleActionExecutionStrategy INTEGER,
     ipSecRuleOrder IpSecOrderTC,
     ipSecRuleLimitNegotiation INTEGER,
     ipSecRuleAutoStart TruthValue,
     ipSecRuleIpSecRuleTimePeriodGroupId TagReferenceId
}

ipSecRulePrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecRuleEntry  1 }

ipSecRuleIfCapSetName OBJECT-TYPE
  SYNTAX SnmpAdminString
  STATUS current
  DESCRIPTION
"The interface capability set to which this IPsec rule applies.
The interface capability name specified by this attribute MUST
exist in an entry of the frwkCapabilitySetTable [RFC3318] prior to
association with an instance of this class. The
frwkCapabilitySetCapability attribute of that entry shall in turn
point to an entry in the ipSecIfCaps table."
  ::= { ipSecRuleEntry  2 }

ipSecRuleRoles OBJECT-TYPE
  SYNTAX RoleCombination
  STATUS current
  DESCRIPTION
```

```
"Specifies the role combination of the interface to which this
IPsec rule should apply. There must exist an instance in the
frwkRoleComboTable [RFC3318] specifying this role combination,
together with the interface capability set specified by
ipSecRuleIfCapSetName, prior to association with an instance of
this class."
  ::= { ipSecRuleEntry  3 }

ipSecRuleDirection OBJECT-TYPE
  SYNTAX IpSecDirectionTC
  STATUS current
  DESCRIPTION
"Specifies the direction of traffic to which this rule should
apply."
  ::= { ipSecRuleEntry  4 }

ipSecRuleIpSecSelectorSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecSelectorSetSelectorSetId }
  STATUS current
  DESCRIPTION
"Identifies a set of selectors to be associated with this IPsec
rule. "
  ::= { ipSecRuleEntry  5 }

ipSecRuleIpSecIpsoFilterSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecIpsoFilterSetFilterSetId }
  STATUS current
  DESCRIPTION
"Identifies a set of IPSO filters to be associated with this IPsec
rule. A value of zero indicates that there are no IPSO filters
associated with this rule.

When the value of this attribute is not zero, the set of IPSO
filters is ANDed with the set of Selectors specified by
ipSecRuleIpSecSelectorSetId. In other words, a packet MUST match a
selector in the selector sets and a filter in the IPSO filter sets
before the actions associated with this rule can be applied."
  ::= { ipSecRuleEntry  6 }

ipSecRuleIpSecActionSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecActionSetActionSetId }
  STATUS current
  DESCRIPTION
"Identifies a set of IPsec actions to be associated with this
rule."
  ::= { ipSecRuleEntry  7 }

ipSecRuleActionExecutionStrategy OBJECT-TYPE
  SYNTAX INTEGER {
    doAll(1),
```

```
    doUntilSuccess(2)
    }
  STATUS current
  DESCRIPTION
"Specifies the strategy to be used in executing the sequenced
actions in the action set identified by ipSecRuleIpSecActionSetId.

DoAll (1) causes the execution of all the actions in the action
set according to their defined precedence order. The precedence
order is specified by the ipSecActionSetOrder in the
```

```
ipSecActionSetTable.

DoUntilSuccess (2) causes the execution of actions according to
their defined precedence order until a successful execution of a
single action. The precedence order is specified by the
ipSecActionSetOrder in the ipSecActionSetTable."
  ::= { ipSecRuleEntry  8 }

ipSecRuleOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"Specifies the precedence order of the rule within all the rules
associated with {IfCapSetName, Roles}."
  ::= { ipSecRuleEntry  9 }

ipSecRuleLimitNegotiation OBJECT-TYPE
  SYNTAX INTEGER {
    initiator(1),
    responder(2),
    both(3)
    }
  STATUS current
  DESCRIPTION
"Limits the negotiation method. Before proceeding with a phase 2
negotiation, the LimitNegotiation property of the IPsecRule is
first checked to determine if the negotiation part indicated for
the rule matches that of the current negotiation (Initiator,
Responder, or Either).

This attribute is ignored when an attempt is made to refresh an
expiring security association (SA) since either side can initiate
a refresh operation.  The system can determine that the
negotiation is a refresh operation by checking to see if the
selector information matches that of an existing SA. If
LimitNegotiation does not match and the selector corresponds to a
new SA, the negotiation is stopped. "
  ::= { ipSecRuleEntry  10 }

ipSecRuleAutoStart OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
```

```
"Indicates if this rule shall be activated when it is
instantiated, i.e., start negotiate or statically set security
```

```
associations. If the value is changed to false later, there is no
impact on the security associations that have already started.
"
  ::= { ipSecRuleEntry  11 }

ipSecRuleIpSecRuleTimePeriodGroupId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecRuleTimePeriodSetRuleTimePeriodSetId }
  STATUS current
  DESCRIPTION
"Identifies an IPsec rule time period set, specified in
ipSecRuleTimePeriodSetTable, that is associated with this rule.

A value of zero indicates that this IPsec rule is always valid."
  ::= { ipSecRuleEntry  12 }


--
--
-- The ipSecActionSetTable
--

ipSecActionSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecActionSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies a set of IPsec actions."
  ::= { ipSecAssociation  2 }

ipSecActionSetEntry OBJECT-TYPE
  SYNTAX IpSecActionSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecActionSetPrid }
  UNIQUENESS {
    ipSecActionSetActionSetId,
    ipSecActionSetOrder
    }
  ::= { ipSecActionSetTable 1 }

  IpSecActionSetEntry ::= SEQUENCE {
     ipSecActionSetPrid InstanceId,
     ipSecActionSetActionSetId TagId,
     ipSecActionSetActionId Prid,
     ipSecActionSetDoActionLogging TruthValue,
     ipSecActionSetDoPacketLogging TruthValue,
     ipSecActionSetOrder IpSecOrderTC
}
```

```
ipSecActionSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecActionSetEntry  1 }

ipSecActionSetActionSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An IPsec action set is composed of one or more IPsec actions.
Actions belonging to the same set have the same ActionSetId."
  ::= { ipSecActionSetEntry  2 }

ipSecActionSetActionId OBJECT-TYPE
  SYNTAX Prid
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in another table that describes an
action to be taken.

For IPsec static actions, it MUST point to an instance in the
ipSecStaticActionTable. For IPsec negotiation actions, it MUST
point to an instance in the ipSecNegotiationActionTable. For other
actions, it may point to an instance of a class specified by other
PIB modules."
  ::= { ipSecActionSetEntry  3 }

ipSecActionSetDoActionLogging OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"Specifies whether a log message is to be generated when the
action is performed.  This applies for ipSecNegotiationActions
with the meaning of logging a message when the negotiation is
attempted (with the success or failure result). This also applies
for ipSecStaticAction only for PreconfiguredTransport action
(ipSecStaticActionAction = 4)  or PreconfiguredTunnel action
(ipSecStaticActionAction = 5) with the meaning of logging a
message when the preconfigured security association is actually
installed in the security association database (SADB)."
  ::= { ipSecActionSetEntry  4 }
```

```
ipSecActionSetDoPacketLogging OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"Specifies whether to log when the resulting security association
is used to process a packet. For ipSecStaticActions, a log message
is to be generated when the IPsecBypass (ipSecStaticActionAction =
```

```
1), IpsecDiscard (ipSecStaticActionAction = 2) or IKEReject
(ipSecStaticActionAction = 3) actions are executed. "
  ::= { ipSecActionSetEntry  5 }

ipSecActionSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"Specifies the precedence order of the action within the action
set."
  ::= { ipSecActionSetEntry  6 }


--
--
-- The ipSecStaticActionTable
--

ipSecStaticActionTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecStaticActionEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IPsec static actions."
  ::= { ipSecAssociation  3 }

ipSecStaticActionEntry OBJECT-TYPE
  SYNTAX IpSecStaticActionEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecStaticActionPrid }
  UNIQUENESS {
    ipSecStaticActionAction,
    ipSecStaticActionTunnelEndpointId,
    ipSecStaticActionDfHandling,
    ipSecStaticActionSpi,
    ipSecStaticActionLifetimeSeconds,
    ipSecStaticActionLifetimeKilobytes,
    ipSecStaticActionSaTransformId
    }
  ::= { ipSecStaticActionTable 1 }

  IpSecStaticActionEntry ::= SEQUENCE {
     ipSecStaticActionPrid InstanceId,
     ipSecStaticActionAction INTEGER,
     ipSecStaticActionTunnelEndpointId ReferenceId,
     ipSecStaticActionDfHandling IpSecDFBitTC,
     ipSecStaticActionSpi Unsigned32,
     ipSecStaticActionLifetimeSeconds Unsigned32,
     ipSecStaticActionLifetimeKilobytes Unsigned64,
     ipSecStaticActionSaTransformId Prid
}
```

```
ipSecStaticActionPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecStaticActionEntry  1 }

ipSecStaticActionAction OBJECT-TYPE
  SYNTAX INTEGER {
    byPass(1),
    discard(2),
    ikeRejection(3),
    preConfiguredTransport(4),
    preConfiguredTunnel(5)
    }
  STATUS current
  DESCRIPTION
"Specifies the IPsec action to be applied to the traffic. byPass
(1) means that packets are to be allowed to pass in the clear.
discard (2) means that packets are to be discarded. ikeRejection
(3) means that that an IKE negotiation should not even be
attempted or continued. preConfiguredTransport (4) means that an
IPsec transport SA is pre-configured. preConfiguredTunnel (5)
means that an IPsec tunnel SA is pre-configured. "
  ::= { ipSecStaticActionEntry  2 }

ipSecStaticActionTunnelEndpointId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecAddressEntry }
  STATUS current
  DESCRIPTION
"When ipSecStaticActionAction is preConfiguredTunnel (5), this
attribute indicates the peer gateway IP address. This address MUST
be a single endpoint address.

When ipSecStaticActionAction is not preConfiguredTunnel, this
attribute MUST be zero."
  ::= { ipSecStaticActionEntry  3 }

ipSecStaticActionDfHandling OBJECT-TYPE
  SYNTAX IpSecDFBitTC
  STATUS current
  DESCRIPTION
"When ipSecStaticActionAction is preConfiguredTunnel, this
attribute specifies how the DF bit is managed. When
ipSecStaticActionAction is not preConfiguredTunnel, this attribute
MUST be ignored. "
  ::= { ipSecStaticActionEntry  4 }

ipSecStaticActionSpi OBJECT-TYPE
  SYNTAX Unsigned32
```

```
  STATUS current
  DESCRIPTION
"Specifies the Security Parameter Index (SPI) to be used with the
SA Transform identified by ipSecStaticActionSaTransformId.

When ipSecStaticActionAction is neither
preConfiguredTransportAction nor preConfiguredTunnelAction, this
attribute MUST be ignored."
  ::= { ipSecStaticActionEntry  5 }

ipSecStaticActionLifetimeSeconds OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
"Specifies the amount of time (in seconds) that a security
association derived from this action should be used. When
ipSecStaticActionAction is neither preConfiguredTransportAction
nor preConfiguredTunnelAction, this attribute MUST be ignored.

A value of zero indicates that there is not a lifetime in seconds
associated with this action (i.e., infinite lifetime in seconds).
This is consistent with [RFC3585].
```

```
The actual lifetime of the preconfigured SA will be the smallest
of the value of this LifetimeSeconds property and of the value of
the MaxLifetimeSeconds property of the associated SA Transform.
Except if the value of this LifetimeSeconds property is zero, then
there will be no lifetime associated to this SA.

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecStaticActionEntry  6 }

ipSecStaticActionLifetimeKilobytes OBJECT-TYPE
  SYNTAX Unsigned64
  UNITS  "kilobytes"
  STATUS current
  DESCRIPTION
"Specifies the SA lifetime in kilobytes. When
ipSecStaticActionAction is neither preConfiguredTransportAction
nor preConfiguredTunnelAction, this attribute MUST be ignored.

A value of zero indicates that there is not a lifetime in byte
count associated with this action (i.e., infinite lifetime in byte
count). This is consistent with [RFC3585].

The actual lifetime of the preconfigured SA will be the smallest
of the value of this LifetimeKilobytes property and of the value
of the MaxLifetimeKilobytes property of the associated SA
transform. Except if the value of this LifetimeKilobytes property
is zero, then there will be no lifetime associated with this
action.
```

```
When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence.
"
  ::= { ipSecStaticActionEntry  7 }

ipSecStaticActionSaTransformId OBJECT-TYPE
  SYNTAX Prid
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in another table that describes an
SA transform, e.g, ipSecEspTransformTable, ipSecAhTransformTable."
  ::= { ipSecStaticActionEntry  8 }


--
```

```
--
-- The ipSecNegotiationActionTable
--

ipSecNegotiationActionTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecNegotiationActionEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IPsec negotiation actions."
  ::= { ipSecAssociation  4 }

ipSecNegotiationActionEntry OBJECT-TYPE
  SYNTAX IpSecNegotiationActionEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecNegotiationActionPrid }
  UNIQUENESS {
    ipSecNegotiationActionAction,
    ipSecNegotiationActionTunnelEndpointId,
    ipSecNegotiationActionDfHandling,
    ipSecNegotiationActionIpSecAssociationId,
    ipSecNegotiationActionKeyExchangeId
    }
  ::= { ipSecNegotiationActionTable 1 }

  IpSecNegotiationActionEntry ::= SEQUENCE {
     ipSecNegotiationActionPrid InstanceId,
     ipSecNegotiationActionAction IpSecActionTC,
     ipSecNegotiationActionTunnelEndpointId ReferenceId,
     ipSecNegotiationActionDfHandling IpSecDFBitTC,
     ipSecNegotiationActionIpSecAssociationId ReferenceId,
     ipSecNegotiationActionKeyExchangeId Prid
}

ipSecNegotiationActionPrid OBJECT-TYPE
```

```
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecNegotiationActionEntry  1 }

ipSecNegotiationActionAction OBJECT-TYPE
```

```
  SYNTAX IpSecActionTC
  STATUS current
  DESCRIPTION
"Specifies the IPsec action to be applied to the traffic.  If
tunnel (2) is specified, ipSecActionTunnelEndpointId MUST also be
specified."
  ::= { ipSecNegotiationActionEntry  2 }

ipSecNegotiationActionTunnelEndpointId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecAddressEntry }
  STATUS current
  DESCRIPTION
"When ipSecActionAction is tunnel (2), this attribute indicates
the peer gateway IP address. This address MUST be a single
endpoint address.

When ipSecActionAction is not tunnel, this attribute MUST be
zero."
  ::= { ipSecNegotiationActionEntry  3 }

ipSecNegotiationActionDfHandling OBJECT-TYPE
  SYNTAX IpSecDFBitTC
  STATUS current
  DESCRIPTION
"When ipSecActionAction is tunnel, this attribute specifies how
the DF bit is managed. When ipSecActionAction is not tunnel, this
attribute MUST be ignored. "
  ::= { ipSecNegotiationActionEntry  4 }

ipSecNegotiationActionIpSecAssociationId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecAssociationEntry }
  STATUS current
  DESCRIPTION
"Pointer to a valid instance in the ipSecAssociationTable."
  ::= { ipSecNegotiationActionEntry  5 }

ipSecNegotiationActionKeyExchangeId OBJECT-TYPE
  SYNTAX Prid
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in another table that describes key
exchange associations. If a single IKEv1 phase one negotiation is
used for the key exchange, this attribute MUST point to an
```

```
instance in the ipSecIkeAssociationTable. If multiple IKEv1 phase
one negotiations (e.g., with different modes) are to be tried
until success, this attribute SHOULD point to ipSecIkeRuleTable.

For other key exchange methods, this attribute may point to an
instance of a PRC defined in some other PIB.

A value of zeroDotZero means that there is no key exchange
procedure associated."
  ::= { ipSecNegotiationActionEntry  6 }


--
--
-- The ipSecAssociationTable
--

ipSecAssociationTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecAssociationEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IPsec associations."
  ::= { ipSecAssociation  5 }

ipSecAssociationEntry OBJECT-TYPE
  SYNTAX IpSecAssociationEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecAssociationPrid }
  UNIQUENESS {
    ipSecAssociationMinLifetimeSeconds,
    ipSecAssociationMinLifetimeKilobytes,
    ipSecAssociationIdleDurationSeconds,
    ipSecAssociationUsePfs,
    ipSecAssociationUseKeyExchangeGroup,
    ipSecAssociationDhGroup,
    ipSecAssociationGranularity,
    ipSecAssociationProposalSetId
    }
  ::= { ipSecAssociationTable 1 }

  IpSecAssociationEntry ::= SEQUENCE {
     ipSecAssociationPrid InstanceId,
     ipSecAssociationMinLifetimeSeconds Unsigned32,
     ipSecAssociationMinLifetimeKilobytes Unsigned64,
     ipSecAssociationIdleDurationSeconds Unsigned32,
     ipSecAssociationUsePfs TruthValue,
     ipSecAssociationUseKeyExchangeGroup TruthValue,
     ipSecAssociationDhGroup IkeGroupDescription,
     ipSecAssociationGranularity IpSecGranularityTC,
     ipSecAssociationProposalSetId TagReferenceId
```

```
}

ipSecAssociationPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecAssociationEntry  1 }

ipSecAssociationMinLifetimeSeconds OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
"Specifies the minimum SA seconds lifetime that will be accepted
from a peer while negotiating an SA based upon this action.
A value of zero indicates that there is no minimum lifetime in
seconds enforced. This is consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecAssociationEntry  2 }

ipSecAssociationMinLifetimeKilobytes OBJECT-TYPE
  SYNTAX Unsigned64
  UNITS  "kilobytes"
  STATUS current
  DESCRIPTION
"Specifies the minimum kilobyte lifetime that will be accepted
from a negotiating peer while negotiating an SA based upon this
action.  A value of zero indicates that there is no minimum
lifetime in byte count enforced. This is consistent with
[RFC3585].


When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecAssociationEntry  3 }

ipSecAssociationIdleDurationSeconds OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
"Specifies how long, in seconds, a security association may remain
unused before it is deleted.

A value of zero indicates that idle detection should not be used
for the security association (only the seconds and kilobyte
lifetimes will be used). This is consistent with [RFC3585]. "
  ::= { ipSecAssociationEntry  4 }
```

```
ipSecAssociationUsePfs OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"Specifies whether or not to use PFS when refreshing keys."
  ::= { ipSecAssociationEntry  5 }

ipSecAssociationUseKeyExchangeGroup OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"Specifies whether or not to use the same GroupId for phase 2 as
was used in phase 1.  If UsePFS is false, then this attribute is
ignored.

A value of true indicates that the phase 2 GroupId should be the
same as phase 1.  A value of false indicates that the group number
specified by the ipSecAssociationDhGroup attribute SHALL be used
for phase 2. "
  ::= { ipSecAssociationEntry  6 }

ipSecAssociationDhGroup OBJECT-TYPE
  SYNTAX IkeGroupDescription
  STATUS current
  DESCRIPTION
"Specifies the key exchange group to use for phase 2 when the
property ipSecAssociationUsePfs is true and the property
ipSecAssociationUseKeyExchangeGroup is false.

"
  ::= { ipSecAssociationEntry  7 }

ipSecAssociationGranularity OBJECT-TYPE
  SYNTAX IpSecGranularityTC
  STATUS current
  DESCRIPTION
"Specifies how the proposed selector for the security association
```

```
will be created."
  ::= { ipSecAssociationEntry  8 }

ipSecAssociationProposalSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecProposalSetProposalSetId }
  STATUS current
  DESCRIPTION
"Identifies a set of IPsec proposals that is associated with this
IPsec association."
  ::= { ipSecAssociationEntry  9 }


--
--
-- The ipSecProposalSetTable
```

```
--

ipSecProposalSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecProposalSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IPsec proposal sets. Proposals within a set are ORed
with preference order. "
  ::= { ipSecAssociation  6 }

ipSecProposalSetEntry OBJECT-TYPE
  SYNTAX IpSecProposalSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecProposalSetPrid }
  UNIQUENESS {
    ipSecProposalSetProposalSetId,
    ipSecProposalSetOrder
    }
  ::= { ipSecProposalSetTable 1 }

  IpSecProposalSetEntry ::= SEQUENCE {
     ipSecProposalSetPrid InstanceId,
     ipSecProposalSetProposalSetId TagId,
     ipSecProposalSetProposalId ReferenceId,
     ipSecProposalSetOrder IpSecOrderTC
}
```

```
ipSecProposalSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecProposalSetEntry  1 }

ipSecProposalSetProposalSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An IPsec proposal set is composed of one or more IPsec proposals.
Proposals belonging to the same set have the same ProposalSetId."
  ::= { ipSecProposalSetEntry  2 }

ipSecProposalSetProposalId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecProposalEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in the ipSecProposalTable."
  ::= { ipSecProposalSetEntry  3 }
```

```
ipSecProposalSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"An integer that specifies the precedence order of the proposal
identified by ipSecProposalSetProposalId in a proposal set. The
proposal set is identified by ipSecProposalSetProposalSetId.
Proposals within a set are ORed with preference order. "
  ::= { ipSecProposalSetEntry  4 }


--
--
-- The ipSecProposalTable
--

ipSecProposalTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecProposalEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IPsec proposals. It has references to Encapsulating
```

```
Security Payload (ESP), Authentication Header (AH) and IP Payload
Compression Protocol (COMP) Transform sets. Within a proposal,
different types of transforms are ANDed. Multiple transforms of
the same type are ORed with preference order."
  ::= { ipSecAssociation  7 }

ipSecProposalEntry OBJECT-TYPE
  SYNTAX IpSecProposalEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecProposalPrid }
  UNIQUENESS {
    ipSecProposalEspTransformSetId,
    ipSecProposalAhTransformSetId,
    ipSecProposalCompTransformSetId
    }
  ::= { ipSecProposalTable 1 }

  IpSecProposalEntry ::= SEQUENCE {
     ipSecProposalPrid InstanceId,
     ipSecProposalEspTransformSetId TagReferenceId,
     ipSecProposalAhTransformSetId TagReferenceId,
     ipSecProposalCompTransformSetId TagReferenceId
}

ipSecProposalPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
```

```
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecProposalEntry  1 }

ipSecProposalEspTransformSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecEspTransformSetTransformSetId }
  STATUS current
  DESCRIPTION
"An integer that identifies a set of ESP transforms, specified in
ipSecEspTransformSetTable, that is associated with this proposal."
  ::= { ipSecProposalEntry  2 }

ipSecProposalAhTransformSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecAhTransformSetTransformSetId }
  STATUS current
  DESCRIPTION
"An integer that identifies an AH transform set, specified in
ipSecAhTransformSetTable, that is associated with this proposal."
  ::= { ipSecProposalEntry  3 }

ipSecProposalCompTransformSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecCompTransformSetTransformSetId }
  STATUS current
  DESCRIPTION
"An integer that identifies a set of IPComp transforms, specified
in ipSecCompTransformSetTable, that is associated with this
proposal."
  ::= { ipSecProposalEntry  4 }


--
--
-- The ipSecAhTransformSetTable
--

ipSecAhTransformSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecAhTransformSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies AH transform sets. Within a transform set, the
transforms are ORed with preference order. "
  ::= { ipSecAhTransform  1 }

ipSecAhTransformSetEntry OBJECT-TYPE
  SYNTAX IpSecAhTransformSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecAhTransformSetPrid }
```

```
  UNIQUENESS {
    ipSecAhTransformSetTransformSetId,
    ipSecAhTransformSetOrder
    }
  ::= { ipSecAhTransformSetTable 1 }

  IpSecAhTransformSetEntry ::= SEQUENCE {
     ipSecAhTransformSetPrid InstanceId,
     ipSecAhTransformSetTransformSetId TagId,
     ipSecAhTransformSetTransformId ReferenceId,
     ipSecAhTransformSetOrder IpSecOrderTC
}

ipSecAhTransformSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class. "
  ::= { ipSecAhTransformSetEntry  1 }

ipSecAhTransformSetTransformSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An AH transform set is composed of one or more AH transforms.
Transforms belonging to the same set have the same
TransformSetId."
  ::= { ipSecAhTransformSetEntry  2 }

ipSecAhTransformSetTransformId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecAhTransformEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in the ipSecAhTransformTable."
  ::= { ipSecAhTransformSetEntry  3 }

ipSecAhTransformSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"An integer that specifies the precedence order of the transform
identified by ipSecAhTransformSetTransformId within a transform
set. The transform set is identified by
ipSecAhTransformSetTransformSetId. Transforms within a set are
ORed with preference order."
  ::= { ipSecAhTransformSetEntry  4 }


--
--
-- The ipSecAhTransformTable
```

```
--
```

```
ipSecAhTransformTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecAhTransformEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies AH transforms."
  ::= { ipSecAhTransform  2 }

ipSecAhTransformEntry OBJECT-TYPE
  SYNTAX IpSecAhTransformEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecAhTransformPrid }
  UNIQUENESS {
    ipSecAhTransformTransformId,
    ipSecAhTransformIntegrityKey,
    ipSecAhTransformUseReplayPrevention,
    ipSecAhTransformReplayPreventionWindowSize,
    ipSecAhTransformMaxLifetimeSeconds,
    ipSecAhTransformMaxLifetimeKilobytes
    }
  ::= { ipSecAhTransformTable 1 }

  IpSecAhTransformEntry ::= SEQUENCE {
     ipSecAhTransformPrid InstanceId,
     ipSecAhTransformTransformId IpsecDoiAuthAlgorithm,
     ipSecAhTransformIntegrityKey OCTET STRING,
     ipSecAhTransformUseReplayPrevention TruthValue,
     ipSecAhTransformReplayPreventionWindowSize Unsigned32,
     ipSecAhTransformMaxLifetimeSeconds Unsigned32,
     ipSecAhTransformMaxLifetimeKilobytes Unsigned64
}

ipSecAhTransformPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class. "
  ::= { ipSecAhTransformEntry  1 }

ipSecAhTransformTransformId OBJECT-TYPE
  SYNTAX IpsecDoiAuthAlgorithm
  STATUS current
  DESCRIPTION
"Specifies the transform ID of the AH algorithm to propose."
  ::= { ipSecAhTransformEntry  2 }

ipSecAhTransformIntegrityKey OBJECT-TYPE
```

```
  SYNTAX OCTET STRING
```

```
  STATUS current
  DESCRIPTION
"When this AH transform instance is used for a Static Action, this
attribute specifies the integrity key to be used. This attribute
MUST be ignored when this AH transform instance is used for a
Negotiation Action."
  ::= { ipSecAhTransformEntry  3 }

ipSecAhTransformUseReplayPrevention OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"Specifies whether to enable replay prevention detection."
  ::= { ipSecAhTransformEntry  4 }

ipSecAhTransformReplayPreventionWindowSize OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "bits"
  STATUS current
  DESCRIPTION
"Specifies, in bits, the length of the sliding window used by the
replay prevention detection mechanism. The value of this property
is ignored if UseReplayPrevention is false. It is assumed that the
window size will take a value that is a power of 2."
  ::= { ipSecAhTransformEntry  5 }

ipSecAhTransformMaxLifetimeSeconds OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
"Specifies the maximum amount of time to propose for a security
association to remain valid.

A value of zero indicates that the default of 8 hours be used.  A
non-zero value indicates the maximum seconds lifetime. This is
consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecAhTransformEntry  6 }

ipSecAhTransformMaxLifetimeKilobytes OBJECT-TYPE
  SYNTAX Unsigned64
  UNITS  "kilobytes"
  STATUS current
  DESCRIPTION
"Specifies the maximum kilobyte lifetime to propose for a security
association to remain valid.

A value of zero indicates that there should be no maximum kilobyte
lifetime.  A non-zero value specifies the desired kilobyte
lifetime. This is consistent with [RFC3585].
```

```
When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecAhTransformEntry  7 }


--
--
-- The ipSecEspTransformSetTable
--

ipSecEspTransformSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecEspTransformSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies ESP transform sets. Within a transform set, the choices
are ORed with preference order. "
  ::= { ipSecEspTransform  1 }

ipSecEspTransformSetEntry OBJECT-TYPE
  SYNTAX IpSecEspTransformSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecEspTransformSetPrid }
  UNIQUENESS {
    ipSecEspTransformSetTransformSetId,
    ipSecEspTransformSetOrder
    }
  ::= { ipSecEspTransformSetTable 1 }

  IpSecEspTransformSetEntry ::= SEQUENCE {
     ipSecEspTransformSetPrid InstanceId,
     ipSecEspTransformSetTransformSetId TagId,
     ipSecEspTransformSetTransformId ReferenceId,
     ipSecEspTransformSetOrder IpSecOrderTC
}
```

```
ipSecEspTransformSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecEspTransformSetEntry  1 }

ipSecEspTransformSetTransformSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
```

```
"An ESP transform set is composed of one or more ESP transforms.
Transforms belonging to the same set have the same
TransformSetId."
  ::= { ipSecEspTransformSetEntry  2 }

ipSecEspTransformSetTransformId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecEspTransformEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in the ipSecEspTransformTable."
  ::= { ipSecEspTransformSetEntry  3 }

ipSecEspTransformSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"An integer that specifies the precedence order of the transform
identified by ipSecEspTransformSetTransformId within a transform
set. The transform set is identified by
ipSecEspTransformSetTransformSetId. Transforms within a set are
ORed with preference order."
  ::= { ipSecEspTransformSetEntry  4 }


--
--
-- The ipSecEspTransformTable
--

ipSecEspTransformTable OBJECT-TYPE
```

```
  SYNTAX SEQUENCE OF IpSecEspTransformEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies ESP transforms."
  ::= { ipSecEspTransform  2 }

ipSecEspTransformEntry OBJECT-TYPE
  SYNTAX IpSecEspTransformEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecEspTransformPrid }
  UNIQUENESS {
    ipSecEspTransformIntegrityTransformId,
    ipSecEspTransformCipherTransformId,
    ipSecEspTransformIntegrityKey,
    ipSecEspTransformCipherKey,
    ipSecEspTransformCipherKeyRounds,
    ipSecEspTransformCipherKeyLength,
    ipSecEspTransformUseReplayPrevention,
    ipSecEspTransformReplayPreventionWindowSize,
```

```
    ipSecEspTransformMaxLifetimeSeconds,
    ipSecEspTransformMaxLifetimeKilobytes
    }
  ::= { ipSecEspTransformTable 1 }

  IpSecEspTransformEntry ::= SEQUENCE {
     ipSecEspTransformPrid InstanceId,
     ipSecEspTransformIntegrityTransformId IpsecDoiAuthAlgorithm,
     ipSecEspTransformCipherTransformId IpsecDoiEspTransform,
     ipSecEspTransformIntegrityKey OCTET STRING,
     ipSecEspTransformCipherKey OCTET STRING,
     ipSecEspTransformCipherKeyRounds Unsigned16TC,
     ipSecEspTransformCipherKeyLength Unsigned16TC,
     ipSecEspTransformUseReplayPrevention TruthValue,
     ipSecEspTransformReplayPreventionWindowSize Unsigned32,
     ipSecEspTransformMaxLifetimeSeconds Unsigned32,
     ipSecEspTransformMaxLifetimeKilobytes Unsigned64
}

ipSecEspTransformPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
```

```
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecEspTransformEntry  1 }

ipSecEspTransformIntegrityTransformId OBJECT-TYPE
  SYNTAX IpsecDoiAuthAlgorithm
  STATUS current
  DESCRIPTION
"Specifies the transform ID of the ESP integrity algorithm to
propose."
  ::= { ipSecEspTransformEntry  2 }

ipSecEspTransformCipherTransformId OBJECT-TYPE
  SYNTAX IpsecDoiEspTransform
  STATUS current
  DESCRIPTION
"Specifies the transform ID of the ESP encryption algorithm to
propose."
  ::= { ipSecEspTransformEntry  3 }

ipSecEspTransformIntegrityKey OBJECT-TYPE
  SYNTAX OCTET STRING
  STATUS current
  DESCRIPTION
"When this ESP transform instance is used for a Static Action,
this attribute specifies the integrity key to be used. This
attribute MUST be ignored when this ESP transform instance is used
for a Negotiation Action."
  ::= { ipSecEspTransformEntry  4 }
```

```
ipSecEspTransformCipherKey OBJECT-TYPE
  SYNTAX OCTET STRING
  STATUS current
  DESCRIPTION
"When this ESP transform instance is used for a Static Action,
this attribute specifies the cipher key to be used. This attribute
MUST be ignored when this ESP transform instance is used for a
Negotiation Action."
  ::= { ipSecEspTransformEntry  5 }

ipSecEspTransformCipherKeyRounds OBJECT-TYPE
  SYNTAX Unsigned16TC
  STATUS current
  DESCRIPTION
"Specifies the number of key rounds for the ESP encryption
```

```
algorithm.  For encryption algorithms that use fixed number of key
rounds, this value is ignored."
  ::= { ipSecEspTransformEntry  6 }

ipSecEspTransformCipherKeyLength OBJECT-TYPE
  SYNTAX Unsigned16TC
  UNITS  "bits"
  STATUS current
  DESCRIPTION
"Specifies, in bits, the key length for the ESP encryption
algorithm. For encryption algorithms that use fixed-length keys,
this value is ignored."
  ::= { ipSecEspTransformEntry  7 }

ipSecEspTransformUseReplayPrevention OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"Specifies whether to enable replay prevention detection."
  ::= { ipSecEspTransformEntry  8 }

ipSecEspTransformReplayPreventionWindowSize OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "bits"
  STATUS current
  DESCRIPTION
"Specifies, in bits, the length of the sliding window used by the
replay prevention detection mechanism. The value of this property
is ignored if UseReplayPrevention is false. It is assumed that the
window size will take a value that is a power of 2."
  ::= { ipSecEspTransformEntry  9 }

ipSecEspTransformMaxLifetimeSeconds OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
```

```
"Specifies the maximum amount of time to propose for a security
association to remain valid.

A value of zero indicates that the default of 8 hours be used.  A
non-zero value indicates the maximum seconds lifetime. This is
consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
```

```
first lifetime to expire takes precedence."
  ::= { ipSecEspTransformEntry  10 }

ipSecEspTransformMaxLifetimeKilobytes OBJECT-TYPE
  SYNTAX Unsigned64
  UNITS  "kilobytes"
  STATUS current
  DESCRIPTION
"Specifies the maximum kilobyte lifetime to propose for a security
association to remain valid.

A value of zero indicates that there should be no maximum kilobyte
lifetime.  A non-zero value specifies the desired kilobyte
lifetime. This is consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecEspTransformEntry  11 }


--
--
-- The ipSecCompTransformSetTable
--

ipSecCompTransformSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecCompTransformSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IP COMP transform sets. Within a transform set, the
choices are ORed with preference order."
  ::= { ipSecCompTransform  1 }

ipSecCompTransformSetEntry OBJECT-TYPE
  SYNTAX IpSecCompTransformSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecCompTransformSetPrid }
  UNIQUENESS {
    ipSecCompTransformSetTransformSetId,
    ipSecCompTransformSetOrder
    }
  ::= { ipSecCompTransformSetTable 1 }
  IpSecCompTransformSetEntry ::= SEQUENCE {
     ipSecCompTransformSetPrid InstanceId,
     ipSecCompTransformSetTransformSetId TagId,
     ipSecCompTransformSetTransformId ReferenceId,
     ipSecCompTransformSetOrder IpSecOrderTC
}

ipSecCompTransformSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecCompTransformSetEntry  1 }

ipSecCompTransformSetTransformSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An IP COMP transform set is composed of one or more IP COMP
transforms. Transforms belonging to the same set have the same
TransformSetId."
  ::= { ipSecCompTransformSetEntry  2 }

ipSecCompTransformSetTransformId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecCompTransformEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in the ipSecCompTransformTable."
  ::= { ipSecCompTransformSetEntry  3 }

ipSecCompTransformSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"An integer that specifies the precedence order of the transform
identified by ipSecCompTransformSetTransformId within a transform
set. The transform set is identified by
ipSecCompTransformSetTransformSetId. Transforms within a set are
ORed with preference order."
  ::= { ipSecCompTransformSetEntry  4 }


--
--
-- The ipSecCompTransformTable
--

ipSecCompTransformTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecCompTransformEntry
  PIB-ACCESS install
```

```
  STATUS current
  DESCRIPTION
"Specifies IP COMP algorithms."
  ::= { ipSecCompTransform  2 }

ipSecCompTransformEntry OBJECT-TYPE
  SYNTAX IpSecCompTransformEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecCompTransformPrid }
  UNIQUENESS {
    ipSecCompTransformAlgorithm,
    ipSecCompTransformDictionarySize,
    ipSecCompTransformMaxLifetimeSeconds,
    ipSecCompTransformMaxLifetimeKilobytes
    }
  ::= { ipSecCompTransformTable 1 }

  IpSecCompTransformEntry ::= SEQUENCE {
     ipSecCompTransformPrid InstanceId,
     ipSecCompTransformAlgorithm IpsecDoiIpcompTransform,
     ipSecCompTransformDictionarySize Unsigned16TC,
     ipSecCompTransformMaxLifetimeSeconds Unsigned32,
     ipSecCompTransformMaxLifetimeKilobytes Unsigned64
}

ipSecCompTransformPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecCompTransformEntry  1 }

ipSecCompTransformAlgorithm OBJECT-TYPE
  SYNTAX IpsecDoiIpcompTransform
  STATUS current
  DESCRIPTION
"Specifies the transform ID of the IP COMP compression algorithm
to propose."
  ::= { ipSecCompTransformEntry  2 }

ipSecCompTransformDictionarySize OBJECT-TYPE
```

```
  SYNTAX Unsigned16TC
  STATUS current
  DESCRIPTION
"Specifies the log2 maximum size of the dictionary for the
compression algorithm.  For compression algorithms that have pre-
defined dictionary sizes, this value is ignored."
  ::= { ipSecCompTransformEntry  3 }

ipSecCompTransformMaxLifetimeSeconds OBJECT-TYPE
```

```
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
"Specifies the maximum amount of time to propose for a security
association to remain valid.

A value of zero indicates that the default of 8 hours be used.  A
non-zero value indicates the maximum seconds lifetime. This is
consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecCompTransformEntry  4 }

ipSecCompTransformMaxLifetimeKilobytes OBJECT-TYPE
  SYNTAX Unsigned64
  UNITS  "kilobytes"
  STATUS current
  DESCRIPTION
"Specifies the maximum kilobyte lifetime to propose for a security
association to remain valid.

A value of zero indicates that there should be no maximum kilobyte
lifetime.  A non-zero value specifies the desired kilobyte
lifetime. This is consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecCompTransformEntry  5 }


--
--
-- The ipSecIkeRuleTable
--
```

```
ipSecIkeRuleTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIkeRuleEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IKEv1 rules. This class is required only when
specifying:

- Multiple IKE phase one actions (e.g., with different exchange
modes) that are associated with one IPsec association. These
actions are to be tried in sequence till one success.

- IKE phase one actions that start automatically.

For each entry:
```

```
1. ipSecIkeRuleIfCapSetName must reference an existing capability
set name in frwkCapabilitySetTable [FRC3318] .

2. ipSecIkeRuleRoles must reference an existing Role Combination
in frwkRoleComboTable [RFC3318].

If any or both of these requirements is not satisfied, the entry
shall not be installed."
  ::= { ipSecIkeAssociation  1 }

ipSecIkeRuleEntry OBJECT-TYPE
  SYNTAX IpSecIkeRuleEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIkeRulePrid }
  UNIQUENESS {
    ipSecIkeRuleIfCapSetName,
    ipSecIkeRuleRoles,
    ipSecIkeRuleIkeActionSetId,
    ipSecIkeRuleActionExecutionStrategy,
    ipSecIkeRuleLimitNegotiation,
    ipSecIkeRuleAutoStart,
    ipSecIkeRuleIpSecRuleTimePeriodGroupId
    }
  ::= { ipSecIkeRuleTable 1 }

  IpSecIkeRuleEntry ::= SEQUENCE {
     ipSecIkeRulePrid InstanceId,
     ipSecIkeRuleIfCapSetName SnmpAdminString,
     ipSecIkeRuleRoles RoleCombination,
     ipSecIkeRuleIkeActionSetId TagReferenceId,
     ipSecIkeRuleActionExecutionStrategy INTEGER,
     ipSecIkeRuleLimitNegotiation INTEGER,
     ipSecIkeRuleAutoStart TruthValue,
     ipSecIkeRuleIpSecRuleTimePeriodGroupId TagReferenceId
}

ipSecIkeRulePrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecIkeRuleEntry  1 }

ipSecIkeRuleIfCapSetName OBJECT-TYPE
  SYNTAX SnmpAdminString
  STATUS current
  DESCRIPTION
"The interface capability set to which this IKE rule applies. The
interface capability name specified by this attribute must exist
```

```
in the frwkCapabilitySetTable [RFC3318] prior to association with
an instance of this class.

This attribute MUST be ignored if ipSecIkeRuleAutoStart is false."
  ::= { ipSecIkeRuleEntry  2 }

ipSecIkeRuleRoles OBJECT-TYPE
  SYNTAX RoleCombination
  STATUS current
  DESCRIPTION
"Specifies the role combination of the interface to which this IKE
rule should apply. There must exist an instance in the
frwkRoleComboTable [RFC3318] specifying this role combination,
together with the interface capability set specified by
ipSecIkeRuleIfName, prior to association with an instance of this
class.

This attribute MUST be ignored if ipSecIkeRuleAutoStart is false."
  ::= { ipSecIkeRuleEntry  3 }

ipSecIkeRuleIkeActionSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecIkeActionSetActionSetId }
  STATUS current
  DESCRIPTION
"Identifies a set of IKE actions to be associated with this rule."
  ::= { ipSecIkeRuleEntry  4 }

ipSecIkeRuleActionExecutionStrategy OBJECT-TYPE
  SYNTAX INTEGER {
    doAll(1),
    doUntilSuccess(2)
    }
  STATUS current
  DESCRIPTION
"Specifies the strategy to be used in executing the sequenced
actions in the action set identified by ipSecRuleIpSecActionSetId.

DoAll (1) causes the execution of all the actions in the action
set according to their defined precedence order. The precedence
order is specified by the ipSecActionSetOrder in
ipSecIkeActionSetTable.

DoUntilSuccess (2) causes the execution of actions according to
their defined precedence order until a successful execution of a
single action. The precedence order is specified by the
ipSecActionSetOrder in ipSecIkeActionSetTable."
  ::= { ipSecIkeRuleEntry  5 }

ipSecIkeRuleLimitNegotiation OBJECT-TYPE
  SYNTAX INTEGER {
    initiator(1),
    responder(2),
```

```
    both(3)
    }
  STATUS current
  DESCRIPTION
"Limits the negotiation method. Before proceeding with a phase 1
negotiation, this property is checked to determine if the
negotiation role of the rule matches that defined for the
negotiation being undertaken (e.g., Initiator, Responder, or
Both). If this check fails (e.g. the current role is IKE responder
while the rule specifies IKE initiator), then the IKE negotiation
is stopped. Note that this only applies to new IKE phase 1
negotiations and has no effect on either renegotiation or refresh
operations with peers for which an established SA already exists."
  ::= { ipSecIkeRuleEntry  6 }
```

```
ipSecIkeRuleAutoStart OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"Indicates if this rule should be automatically executed."
  ::= { ipSecIkeRuleEntry  7 }

ipSecIkeRuleIpSecRuleTimePeriodGroupId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecRuleTimePeriodSetRuleTimePeriodSetId }
  STATUS current
  DESCRIPTION
"Identifies a rule time period set, specified in
ipSecRuleTimePeriodSetTable, that is associated with this rule.

A value of zero indicates that this rule is always valid."
  ::= { ipSecIkeRuleEntry  8 }


--
--
-- The ipSecIkeActionSetTable
--

ipSecIkeActionSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIkeActionSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IKEv1 action sets."
  ::= { ipSecIkeAssociation  2 }

ipSecIkeActionSetEntry OBJECT-TYPE
  SYNTAX IpSecIkeActionSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIkeActionSetPrid }
```

```
  UNIQUENESS {
    ipSecIkeActionSetActionSetId,
    ipSecIkeActionSetOrder
    }
  ::= { ipSecIkeActionSetTable 1 }

  IpSecIkeActionSetEntry ::= SEQUENCE {
     ipSecIkeActionSetPrid InstanceId,
     ipSecIkeActionSetActionSetId TagId,
     ipSecIkeActionSetActionId ReferenceId,
     ipSecIkeActionSetOrder IpSecOrderTC
}

ipSecIkeActionSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecIkeActionSetEntry  1 }

ipSecIkeActionSetActionSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An IKE action set is composed of one or more IKE actions. Actions
belonging to the same set have the same ActionSetId."
  ::= { ipSecIkeActionSetEntry  2 }

ipSecIkeActionSetActionId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecIkeAssociationEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in the ipSecIkeAssociationTable."
  ::= { ipSecIkeActionSetEntry  3 }

ipSecIkeActionSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"Specifies the precedence order of the action within the action
set."
  ::= { ipSecIkeActionSetEntry  4 }


--
--
-- The ipSecIkeAssociationTable
--

ipSecIkeAssociationTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIkeAssociationEntry
```

```
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IKEv1 associations. "
  ::= { ipSecIkeAssociation  3 }

ipSecIkeAssociationEntry OBJECT-TYPE
  SYNTAX IpSecIkeAssociationEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIkeAssociationPrid }
  UNIQUENESS {
    ipSecIkeAssociationMinLiftetimeSeconds,
    ipSecIkeAssociationMinLifetimeKilobytes,
    ipSecIkeAssociationIdleDurationSeconds,
    ipSecIkeAssociationExchangeMode,
    ipSecIkeAssociationUseIkeIdentityType,
    ipSecIkeAssociationUseIkeIdentityValue,
    ipSecIkeAssociationIkePeerEndpoint,
    ipSecIkeAssociationPresharedKey,
    ipSecIkeAssociationVendorId,
    ipSecIkeAssociationAggressiveModeGroupId,
    ipSecIkeAssociationLocalCredentialId,
    ipSecIkeAssociationDoActionLogging,
    ipSecIkeAssociationIkeProposalSetId
    }
  ::= { ipSecIkeAssociationTable 1 }

  IpSecIkeAssociationEntry ::= SEQUENCE {
     ipSecIkeAssociationPrid InstanceId,
     ipSecIkeAssociationMinLiftetimeSeconds Unsigned32,
     ipSecIkeAssociationMinLifetimeKilobytes Unsigned64,
     ipSecIkeAssociationIdleDurationSeconds Unsigned32,
     ipSecIkeAssociationExchangeMode IpSecExchangeModeTC,
     ipSecIkeAssociationUseIkeIdentityType IpsecDoiIdentType,
     ipSecIkeAssociationUseIkeIdentityValue OCTET STRING,
     ipSecIkeAssociationIkePeerEndpoint ReferenceId,
     ipSecIkeAssociationPresharedKey OCTET STRING,
     ipSecIkeAssociationVendorId OCTET STRING,
     ipSecIkeAssociationAggressiveModeGroupId IkeGroupDescription,
     ipSecIkeAssociationLocalCredentialId TagReferenceId,
     ipSecIkeAssociationDoActionLogging TruthValue,
     ipSecIkeAssociationIkeProposalSetId TagReferenceId
}

ipSecIkeAssociationPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
```

```
  ::= { ipSecIkeAssociationEntry  1 }
```

```
ipSecIkeAssociationMinLiftetimeSeconds OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
"Specifies the minimum SA seconds lifetime that will be accepted
from a peer while negotiating an SA based upon this action.

A value of zero indicates that there is no minimum lifetime in
seconds enforced. This is consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecIkeAssociationEntry  2 }

ipSecIkeAssociationMinLifetimeKilobytes OBJECT-TYPE
  SYNTAX Unsigned64
  UNITS  "kilobytes"
  STATUS current
  DESCRIPTION
"Specifies the minimum kilobyte lifetime that will be accepted
from a negotiating peer while negotiating an SA based upon this
action.

A value of zero indicates that there is no minimum lifetime in
byte count enforced. This is consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecIkeAssociationEntry  3 }

ipSecIkeAssociationIdleDurationSeconds OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
"Specifies how long, in seconds, a security association may remain
unused before it is deleted.

A value of zero indicates that idle detection should not be used
for the security association (only the seconds and kilobyte
lifetimes will be used). This is consistent with [RFC3585]. "
  ::= { ipSecIkeAssociationEntry  4 }
```

```
ipSecIkeAssociationExchangeMode OBJECT-TYPE
  SYNTAX IpSecExchangeModeTC
  STATUS current
  DESCRIPTION
"Specifies the negotiation mode that the IKE server will use for
phase one."
  ::= { ipSecIkeAssociationEntry  5 }
```

```
ipSecIkeAssociationUseIkeIdentityType OBJECT-TYPE
  SYNTAX IpsecDoiIdentType
  STATUS current
  DESCRIPTION
"Specifies the type of IKE identity to use during IKE phase one
negotiation."
  ::= { ipSecIkeAssociationEntry  6 }

ipSecIkeAssociationUseIkeIdentityValue OBJECT-TYPE
  SYNTAX OCTET STRING
  STATUS current
  DESCRIPTION
"Specifies the ID payload value to be provided to the peer during
IKE phase one negotiation."
  ::= { ipSecIkeAssociationEntry  7 }

ipSecIkeAssociationIkePeerEndpoint OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecIkePeerEndpointEntry }
  STATUS current
  DESCRIPTION
"Pointer to a valid instance in the ipSecIkePeerEndpointTable to
indicate an IKE peer endpoint."
  ::= { ipSecIkeAssociationEntry  8 }

ipSecIkeAssociationPresharedKey OBJECT-TYPE
  SYNTAX OCTET STRING
  STATUS current
  DESCRIPTION
"This attribute specifies the preshared key or secret to use for
IKE authentication. This is the key for all the IKE proposals of
this association that set ipSecIkeProposalAuthenticationMethod to
presharedKey(1)."
  ::= { ipSecIkeAssociationEntry  9 }

ipSecIkeAssociationVendorId OBJECT-TYPE
  SYNTAX OCTET STRING
  STATUS current
  DESCRIPTION
"Specifies the value to be used in the Vendor ID payload.  It is a
hash value as defined in [RFC2408]  Section 3.16.

A zero length OCTET STRING means that Vendor ID payload will be
neither generated nor accepted. Otherwise, it means that a Vendor
ID payload will be generated (when acting as an initiator) or is
expected (when acting as a responder). "
  ::= { ipSecIkeAssociationEntry  10 }

ipSecIkeAssociationAggressiveModeGroupId OBJECT-TYPE
  SYNTAX IkeGroupDescription
  STATUS current
  DESCRIPTION
```

```
"Specifies the group ID to be used for aggressive mode. This
attribute is ignored unless the attribute
ipSecIkeAssociationExchangeMode is set to 4 (aggressive mode). "
  ::= { ipSecIkeAssociationEntry  11 }

ipSecIkeAssociationLocalCredentialId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecCredentialSetSetId }
  STATUS current
  DESCRIPTION
"Indicates a group of credentials. One of the credentials in the
group MUST be used when establishing an IKE association with the
peer endpoint."
  ::= { ipSecIkeAssociationEntry  12 }

ipSecIkeAssociationDoActionLogging OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"Specifies whether a log message is to be generated when the
negotiation is attempted (with the success or failure result)."
  ::= { ipSecIkeAssociationEntry  13 }

ipSecIkeAssociationIkeProposalSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecIkeProposalSetProposalSetId }
  STATUS current
  DESCRIPTION
"Identifies a set of IKE proposals that is associated with this
IKE association."
```

```
  ::= { ipSecIkeAssociationEntry  14 }


--
--
-- The ipSecIkeProposalSetTable
--

ipSecIkeProposalSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIkeProposalSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IKE proposal sets. Proposals within a set are ORed with
preference order. "
  ::= { ipSecIkeAssociation  4 }

ipSecIkeProposalSetEntry OBJECT-TYPE
  SYNTAX IpSecIkeProposalSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIkeProposalSetPrid }
```

```
  UNIQUENESS {
    ipSecIkeProposalSetProposalSetId,
    ipSecIkeProposalSetOrder
    }
  ::= { ipSecIkeProposalSetTable 1 }

  IpSecIkeProposalSetEntry ::= SEQUENCE {
     ipSecIkeProposalSetPrid InstanceId,
     ipSecIkeProposalSetProposalSetId TagId,
     ipSecIkeProposalSetProposalId ReferenceId,
     ipSecIkeProposalSetOrder IpSecOrderTC
}

ipSecIkeProposalSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecIkeProposalSetEntry  1 }

ipSecIkeProposalSetProposalSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An IKE proposal set is composed of one or more IKE proposals.
Proposals belonging to the same set has the same ProposalSetId. "
  ::= { ipSecIkeProposalSetEntry  2 }

ipSecIkeProposalSetProposalId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecIkeProposalEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in the ipSecIkeProposalTable."
  ::= { ipSecIkeProposalSetEntry  3 }

ipSecIkeProposalSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"An integer that specifies the precedence order of the proposal
identified by ipSecIkeProposalSetProposalId in a proposal set. The
proposal set is identified by ipSecIkeProposalSetProposalSetId.
Proposals within a set are ORed with preference order."
  ::= { ipSecIkeProposalSetEntry  4 }


--
--
-- The ipSecIkeProposalTable
--
```

```
ipSecIkeProposalTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIkeProposalEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IKEv1 proposals."
  ::= { ipSecIkeAssociation  5 }

ipSecIkeProposalEntry OBJECT-TYPE
  SYNTAX IpSecIkeProposalEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIkeProposalPrid }
  UNIQUENESS {
    ipSecIkeProposalMaxLifetimeSeconds,
    ipSecIkeProposalMaxLifetimeKilobytes,
    ipSecIkeProposalCipherAlgorithm,
    ipSecIkeProposalHashAlgorithm,
    ipSecIkeProposalAuthenticationMethod,
    ipSecIkeProposalPrfAlgorithm,
    ipSecIkeProposalIkeDhGroup
    }
  ::= { ipSecIkeProposalTable 1 }

  IpSecIkeProposalEntry ::= SEQUENCE {
     ipSecIkeProposalPrid InstanceId,
     ipSecIkeProposalMaxLifetimeSeconds Unsigned32,
     ipSecIkeProposalMaxLifetimeKilobytes Unsigned64,
     ipSecIkeProposalCipherAlgorithm IkeEncryptionAlgorithm,
     ipSecIkeProposalHashAlgorithm IkeHashAlgorithm,
     ipSecIkeProposalAuthenticationMethod IkeAuthMethod,
     ipSecIkeProposalPrfAlgorithm Unsigned16TC,
     ipSecIkeProposalIkeDhGroup IkeGroupDescription
}

ipSecIkeProposalPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecIkeProposalEntry  1 }

ipSecIkeProposalMaxLifetimeSeconds OBJECT-TYPE
  SYNTAX Unsigned32
  UNITS  "seconds"
  STATUS current
  DESCRIPTION
"Specifies the maximum amount of time to propose for a security
association to remain valid.
```

```
A value of zero indicates that the default of 8 hours be used.  A
non-zero value indicates the maximum seconds lifetime. This is
consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecIkeProposalEntry  2 }

ipSecIkeProposalMaxLifetimeKilobytes OBJECT-TYPE
```

```
  SYNTAX Unsigned64
  UNITS  "kilobytes"
  STATUS current
  DESCRIPTION
"Specifies the maximum kilobyte lifetime to propose for a security
association to remain valid.

A value of zero indicates that there should be no maximum kilobyte
lifetime.  A non-zero value specifies the desired kilobyte
lifetime. This is consistent with [RFC3585].

When both the LifetimeSeconds and LifetimeKilobytes are used, the
first lifetime to expire takes precedence."
  ::= { ipSecIkeProposalEntry  3 }

ipSecIkeProposalCipherAlgorithm OBJECT-TYPE
  SYNTAX IkeEncryptionAlgorithm
  STATUS current
  DESCRIPTION
"Specifies the encryption algorithm to propose for the IKE
association."
  ::= { ipSecIkeProposalEntry  4 }

ipSecIkeProposalHashAlgorithm OBJECT-TYPE
  SYNTAX IkeHashAlgorithm
  STATUS current
  DESCRIPTION
"Specifies the hash algorithm to propose for the IKE association."
  ::= { ipSecIkeProposalEntry  5 }

ipSecIkeProposalAuthenticationMethod OBJECT-TYPE
  SYNTAX IkeAuthMethod
  STATUS current
  DESCRIPTION
"Specifies the authentication method to propose for the IKE
association."
  ::= { ipSecIkeProposalEntry  6 }

ipSecIkeProposalPrfAlgorithm OBJECT-TYPE
  SYNTAX Unsigned16TC
  STATUS current
  DESCRIPTION
"Specifies the Psuedo-Random Function (PRF) to propose for the IKE
association. As indicated in [RFC2409], there are currently no
```

```
negotiable pseudo-random functions defined in this document.
Private use attribute values can be used for prf negotiation
```

```
between consenting parties. "
  ::= { ipSecIkeProposalEntry  7 }

ipSecIkeProposalIkeDhGroup OBJECT-TYPE
  SYNTAX IkeGroupDescription
  STATUS current
  DESCRIPTION
"The value of this property indicates the Diffie-Hellman group
number to propose for the IKE association.

The value of this property is to be ignored when doing aggressive
mode."
  ::= { ipSecIkeProposalEntry  8 }


--
--
-- The ipSecIkePeerEndpointTable
--

ipSecIkePeerEndpointTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIkePeerEndpointEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IKE peer endpoints."
  ::= { ipSecIkeAssociation  6 }

ipSecIkePeerEndpointEntry OBJECT-TYPE
  SYNTAX IpSecIkePeerEndpointEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIkePeerEndpointPrid }
  UNIQUENESS {
    ipSecIkePeerEndpointIdentityType,
    ipSecIkePeerEndpointIdentityValue,
    ipSecIkePeerEndpointIsNegated,
    ipSecIkePeerEndpointAddress,
    ipSecIkePeerEndpointCredentialSetId
    }
  ::= { ipSecIkePeerEndpointTable 1 }

  IpSecIkePeerEndpointEntry ::= SEQUENCE {
     ipSecIkePeerEndpointPrid InstanceId,
     ipSecIkePeerEndpointIdentityType IpsecDoiIdentType,
     ipSecIkePeerEndpointIdentityValue OCTET STRING,
     ipSecIkePeerEndpointIsNegated TruthValue,
     ipSecIkePeerEndpointAddress ReferenceId,
     ipSecIkePeerEndpointCredentialSetId TagReferenceId
}
```

```
ipSecIkePeerEndpointPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecIkePeerEndpointEntry  1 }

ipSecIkePeerEndpointIdentityType OBJECT-TYPE
  SYNTAX IpsecDoiIdentType
  STATUS current
  DESCRIPTION
"Specifies the type of identity that MUST be provided by the peer
in the ID payload during IKE phase one negotiation."
  ::= { ipSecIkePeerEndpointEntry  2 }

ipSecIkePeerEndpointIdentityValue OBJECT-TYPE
  SYNTAX OCTET STRING
  STATUS current
  DESCRIPTION
"Specifies the value to be matched with the ID payload provided by
the peer during IKE phase one negotiation.

The syntax may need to be converted for comparison. If the
ipSecIkePeerEndpointIdentityType is a DistinguishedName, the name
in the ipSecIkePeerEndpointIdentityValue
is represented by an ordinary string value, but this value must be
converted into a DER-encoded string before matching against the
values extracted from IKE ID payloads at runtime.  The same
applies to IPv4 & IPv6 addresses.

Different Wildcards wildcard mechanisms can be used as well as the
prefix notation for IPv4 addresses depending on the ID payload:

- an IdentityValue of *@example.com will match an user FQDN ID
payload of JDOE@EXAMPLE.COM

- an IdentityValue of *.example.com will match a FQDN ID payload
of WWW.EXAMPLE.COM

- an IdentityValue of cn=*,ou=engineering,o=company,c=us will
match a DER DN ID payload of cn=John Doe, ou=engineering,
o=company, c=us

- an IdentityValue of 192.0.2.0/24 will match an IPv4 address ID
```

```
payload of 192.0.2.10.

- an IdentityValue of 192.0.2.* will also match an IPv4 address ID
payload of 192.0.2.10.
```

```
The above wildcard mechanisms MUST be supported for all ID
payloads supported by the local IKE entity.  The character *
replaces 0 or multiple instances of any character."
  ::= { ipSecIkePeerEndpointEntry  3 }

ipSecIkePeerEndpointIsNegated OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"This attribute behaves like a logical NOT for the peer identity.
If the value of this attribute is 'true', the peer identity whose
type is specified by ipSecIkePeerEndpointIdentityType MUST not
match the vaule specified by ipSecIkePeerEndpointValue."
  ::= { ipSecIkePeerEndpointEntry  4 }

ipSecIkePeerEndpointAddress OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecAddressEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid entry in the ipSecAddressTable to specify
the endpoint address with which this PEP establishes IKE
association. The pointed address MUST be a single endpoint
address. This attribute is used only when the IKE association is
to be started automatically. Hence, the value of this attribute
MUST be zero if ipSecIkeRuleAutoStart is false."
  ::= { ipSecIkePeerEndpointEntry  5 }

ipSecIkePeerEndpointCredentialSetId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecCredentialSetSetId }
  STATUS current
  DESCRIPTION
"Identifies a set of credentials. Any one of the credentials in
the set is acceptable as the IKE peer credential."
  ::= { ipSecIkePeerEndpointEntry  6 }


--
```

```
--
-- The ipSecCredentialSetTable
--

ipSecCredentialSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecCredentialSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies credential sets.

For IKE peer credentials, any one of the credentials in the set is
acceptable as peer credential during IEK phase 1 negotiation. For
```

```
IKE local credentials, any one of the credentials in the set can
be used in IKE phase 1 negotiation."
  ::= { ipSecCredential  1 }

ipSecCredentialSetEntry OBJECT-TYPE
  SYNTAX IpSecCredentialSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecCredentialSetPrid }
  UNIQUENESS {
    ipSecCredentialSetSetId,
    ipSecCredentialSetCredentialId
    }
  ::= { ipSecCredentialSetTable 1 }

  IpSecCredentialSetEntry ::= SEQUENCE {
     ipSecCredentialSetPrid InstanceId,
     ipSecCredentialSetSetId TagId,
     ipSecCredentialSetCredentialId ReferenceId
}

ipSecCredentialSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecCredentialSetEntry  1 }

ipSecCredentialSetSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"A credential set is composed of one or more credentials.
Credentials belonging to the same set have the same
CredentialSetId."
  ::= { ipSecCredentialSetEntry  2 }

ipSecCredentialSetCredentialId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecCredentialEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in the ipSecCredentialTable."
  ::= { ipSecCredentialSetEntry  3 }


--
--
-- The ipSecCredentialTable
--
```

```
ipSecCredentialTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecCredentialEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies credentials."
  ::= { ipSecCredential  2 }

ipSecCredentialEntry OBJECT-TYPE
  SYNTAX IpSecCredentialEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecCredentialPrid }
  UNIQUENESS {
    ipSecCredentialCredentialType,
    ipSecCredentialFieldsId,
    ipSecCredentialCrlDistributionPoint
    }
  ::= { ipSecCredentialTable 1 }

  IpSecCredentialEntry ::= SEQUENCE {
     ipSecCredentialPrid InstanceId,
     ipSecCredentialCredentialType IpSecCredTypeTC,
     ipSecCredentialFieldsId TagReferenceId,
     ipSecCredentialCrlDistributionPoint OCTET STRING
}

ipSecCredentialPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecCredentialEntry  1 }

ipSecCredentialCredentialType OBJECT-TYPE
  SYNTAX IpSecCredTypeTC
  STATUS current
  DESCRIPTION
"Specifies the type of credential to be matched."
  ::= { ipSecCredentialEntry  2 }

ipSecCredentialFieldsId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecCredentialFieldsSetId }
  STATUS current
  DESCRIPTION
"Identifies a group of matching criteria to be used for the peer
credential. The identified criteria MUST all be satisfied."
  ::= { ipSecCredentialEntry  3 }

ipSecCredentialCrlDistributionPoint OBJECT-TYPE
```

```
  SYNTAX OCTET STRING
  STATUS current
  DESCRIPTION
"When credential type is certificate X509, this attribute
identifies the Certificate Revocation List (CRL) distribution
point for this credential."
  ::= { ipSecCredentialEntry  4 }


--
--
-- The ipSecCredentialFieldsTable
--

ipSecCredentialFieldsTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecCredentialFieldsEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies sets of credential sub-fields and their values to be
matched against. "
  ::= { ipSecCredential  3 }

ipSecCredentialFieldsEntry OBJECT-TYPE
  SYNTAX IpSecCredentialFieldsEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecCredentialFieldsPrid }
  UNIQUENESS {
    ipSecCredentialFieldsName,
    ipSecCredentialFieldsValue,
    ipSecCredentialFieldsIsNegated,
    ipSecCredentialFieldsSetId
    }
  ::= { ipSecCredentialFieldsTable 1 }

  IpSecCredentialFieldsEntry ::= SEQUENCE {
     ipSecCredentialFieldsPrid InstanceId,
     ipSecCredentialFieldsName SnmpAdminString,
     ipSecCredentialFieldsValue SnmpAdminString,
     ipSecCredentialFieldsIsNegated TruthValue,
     ipSecCredentialFieldsSetId TagId
}

ipSecCredentialFieldsPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecCredentialFieldsEntry  1 }
```

```
ipSecCredentialFieldsName OBJECT-TYPE
  SYNTAX SnmpAdminString
  STATUS current
  DESCRIPTION
"Specifies the sub-field of the credential to match with. This is
the string representation of a X.509 certificate attribute, e.g.
serialNumber,  issuerName, subjectName, etc.."
  ::= { ipSecCredentialFieldsEntry  2 }

ipSecCredentialFieldsValue OBJECT-TYPE
```

```
  SYNTAX SnmpAdminString
  STATUS current
  DESCRIPTION
"Specifies the value to match with for the sub-field identified by
ipSecCredentialFieldsName. A wildcard mechanism can be used in the
Value string. E.g., if the Name is subjectName then a Value of
cn=*,ou=engineering,o=foo,c=be will match successfully a
certificate whose subject attribute is cn=Jane Doe,
ou=engineering, o=foo, c=be.  The wildcard character * can be used
to represent 0 or several characters.

If the ipSecCredentialFieldsName corresponds to a
DistinguishedName, this value is represented by a string value.
However, an implementation must convert this string to a DER-
encoded string before matching against the values extracted from
credentials at runtime. "
  ::= { ipSecCredentialFieldsEntry  3 }

ipSecCredentialFieldsIsNegated OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"This attribute behaves like a logical NOT for the credential
field match. If the value of this attribute is 'true', the
credential field specified by ipSecCredentialFieldsName MUST not
match the vaule specified by ipSecCredentialFieldsValue."
  ::= { ipSecCredentialFieldsEntry  4 }

ipSecCredentialFieldsSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"Specifies the set this criteria belongs to. All criteria within a
set MUST all be satisfied."
  ::= { ipSecCredentialFieldsEntry  5 }


--
--
-- The ipSecSelectorSetTable
--

ipSecSelectorSetTable OBJECT-TYPE
```

```
  SYNTAX SEQUENCE OF IpSecSelectorSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IPsec selector sets."
  ::= { ipSecSelector  1 }

ipSecSelectorSetEntry OBJECT-TYPE
  SYNTAX IpSecSelectorSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecSelectorSetPrid }
  UNIQUENESS {
    ipSecSelectorSetSelectorSetId,
    ipSecSelectorSetOrder
    }
  ::= { ipSecSelectorSetTable 1 }

  IpSecSelectorSetEntry ::= SEQUENCE {
     ipSecSelectorSetPrid InstanceId,
     ipSecSelectorSetSelectorSetId TagId,
     ipSecSelectorSetSelectorId Prid,
     ipSecSelectorSetOrder IpSecOrderTC,
     ipSecSelectorSetIsNegated TruthValue
}

ipSecSelectorSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecSelectorSetEntry  1 }

ipSecSelectorSetSelectorSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An IPsec selector set is composed of one or more IPsec selectors.
Selectors belonging to the same set have the same SelectorSetId."
  ::= { ipSecSelectorSetEntry  2 }

ipSecSelectorSetSelectorId OBJECT-TYPE
  SYNTAX Prid
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in another class that describes
selectors. To use selectors defined in this IPsec PIB module, this
attribute MUST point to an instance in ipSecSelectorTable. This
attribute may also point to an instance in a selector or filter
PRC defined in other PIB modules."
  ::= { ipSecSelectorSetEntry  3 }
```

```
ipSecSelectorSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"An integer that specifies the precedence order of the selectors
identified by ipSecSelectorId within a selector set. The selector
set is identified by ipSecSelectorSetId. "
  ::= { ipSecSelectorSetEntry  4 }

ipSecSelectorSetIsNegated OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"If the value of this attribute is 'true', the filters pointed by
ipSecSelectorSetSelectorId SHALL be negated."
  ::= { ipSecSelectorSetEntry  5 }


--
--
-- The ipSecSelectorTable
--

ipSecSelectorTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecSelectorEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IPsec selectors. Each row in the selector table
represents multiple selectors. These selectors are obtained as
follows:

1. Substitute the ipSecSelectorSrcAddressGroupId with all the IP
addresses from the ipSecAddressTable whose ipSecAddressGroupId
matches the ipSecSelectorSrcAddressGroupId.

2. Substitute the ipSecSelectorDstAddressGroupId with all the IP
addresses from the ipSecAddressTable whose ipSecAddressGroupId
matches the ipSecSelectorDstAddressGroupId.

3. Substitute the ipSecSelectorSrcPortGroupId with all the ports
or ranges of port whose ipSecL4PortGroupId matches the
ipSecSelectorSrcPortGroupId.

4. Substitute the ipSecSelectorDstPortGroupId with all the ports
or ranges of port whose ipSecL4PortGroupId matches the
```

```
ipSecSelectorDstPortGroupId.

5. Construct all the possible combinations of the above four
fields. Then add to the combinations the ipSecSelectorProtocol,
ipSecSelectorDscp and ipSecSelectorFlowLabel attributes to form
all the selectors.
```

```
The relative order of the selectors constructed from a single row
is unspecified. "
  ::= { ipSecSelector  2 }

ipSecSelectorEntry OBJECT-TYPE
  SYNTAX IpSecSelectorEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecSelectorPrid }
  UNIQUENESS {
    ipSecSelectorSrcAddressGroupId,
    ipSecSelectorSrcPortGroupId,
    ipSecSelectorDstAddressGroupId,
    ipSecSelectorDstPortGroupId,
    ipSecSelectorProtocol,
    ipSecSelectorDscp,
    ipSecSelectorFlowLabel
    }
  ::= { ipSecSelectorTable 1 }

  IpSecSelectorEntry ::= SEQUENCE {
     ipSecSelectorPrid InstanceId,
     ipSecSelectorSrcAddressGroupId TagReferenceId,
     ipSecSelectorSrcPortGroupId TagReferenceId,
     ipSecSelectorDstAddressGroupId TagReferenceId,
     ipSecSelectorDstPortGroupId TagReferenceId,
     ipSecSelectorProtocol Unsigned32,
     ipSecSelectorDscp DscpOrAny,
     ipSecSelectorFlowLabel IPv6FlowLabelOrAny
}

ipSecSelectorPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
```

```
  ::= { ipSecSelectorEntry  1 }

ipSecSelectorSrcAddressGroupId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecAddressGroupId }
  STATUS current
  DESCRIPTION
"Indicates source addresses. All addresses in ipSecAddressTable
whose ipSecAddressGroupId matches this value are included as
source addresses.

A value of zero indicates wildcard address, i.e., any address
matches."
  ::= { ipSecSelectorEntry  2 }
```

```
ipSecSelectorSrcPortGroupId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecL4PortGroupId }
  STATUS current
  DESCRIPTION
"Indicates source layer 4 port numbers. All ports in ipSecL4Port
whose ipSecL4PortGroupId matches this value are included.

A value of zero indicates wildcard port, i.e., any port number
matches."
  ::= { ipSecSelectorEntry  3 }

ipSecSelectorDstAddressGroupId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecAddressGroupId }
  STATUS current
  DESCRIPTION
"Indicates destination addresses. All addresses in
ipSecAddressTable whose ipSecAddressGroupId matches this value are
included as destination addresses.

A value of zero indicates wildcard address, i.e., any address
matches."
  ::= { ipSecSelectorEntry  4 }

ipSecSelectorDstPortGroupId OBJECT-TYPE
  SYNTAX TagReferenceId
  PIB-TAG    { ipSecL4PortGroupId }
  STATUS current
  DESCRIPTION
"Indicates destination layer 4 port numbers. All ports in
```

```
ipSecL4Port whose ipSecL4PortGroupId matches this value are
included.

A value of zero indicates wildcard port, i.e., any port number
matches."
  ::= { ipSecSelectorEntry  5 }

ipSecSelectorProtocol OBJECT-TYPE
  SYNTAX Unsigned32 (0..255)
  STATUS current
  DESCRIPTION
"The layer-4 protocol Id to match against the IPv4 protocol number
or the IPv6 Next-Header number in the packet. A value of 255 means
match all. Note the protocol number of 255 is reserved by IANA,
and Next-Header number of 0 is used in IPv6."
  ::= { ipSecSelectorEntry  6 }

ipSecSelectorDscp OBJECT-TYPE
  SYNTAX DscpOrAny
  STATUS current
  DESCRIPTION
```

```
"The value that the DSCP in the packet can have and match this
filter. A value of -1 indicates that a specific DSCP value has not
been defined and thus all DSCP values are considered a match."
  ::= { ipSecSelectorEntry  7 }

ipSecSelectorFlowLabel OBJECT-TYPE
  SYNTAX IPv6FlowLabelOrAny
  STATUS current
  DESCRIPTION
"The flow identifier or flow label in an IPv6 packet header that
may be used to discriminate traffic flows.  The value of -1 is
used to indicate a wildcard, i.e. any value."
  ::= { ipSecSelectorEntry  8 }


--
--
-- The ipSecAddressTable
--

ipSecAddressTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecAddressEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
```

```
"This class allows the specification of a single IP address, a
subnet consisting of an IP address and the prefix length, an IP
address range, and a wild-card IP address.

If the address type is 'ipv4', 'ipv6', 'ipv4z' or 'ipv6z', to
specify a single IP address the values of ipSecAddressAddrMin and
ipSecAddressAddrMax MUST be the same and the
ipSecAddressAddrPrefixLength MUST have a value of 32 or greater
(128 or greater for 'ipv6' or 'ipv6z'). To specify a subnet, the
values of ipSecAddressAddrMin and ipSecAddressAddrMax MUST be the
same and the ipSecAddressAddrPrefixLength MUST have a value
between 0 and 32 (128 for 'ipv6' or 'ipv6z'). To specify an IP
address range, the values of ipSecAddressAddrMin and
ipSecAddressAddrMax MUST be different and the
ipSecAddressAddrPrefixLength MUST have a value of 32 (or 128 for
'ipv6' or 'ipv6z')

If the address type is 'dns', ipSecAddressAddrMin and
ipSecAddressAddrMax MUST contain the same 'dns' address. The
ipSecAddressAddrPrefixLength MUST be ignored. The mapping of the
address value to IPv4 or IPv6 addresses MUST be done by the PEP at
install time. A dns name may be mapped into multiple single IP
addresses. Each of them becomes a single row in the resulted
address table.

To specify a wild-card IP address, the
ipSecAddressAddrPrefixLength MUST be zero. "
  ::= { ipSecSelector  3 }
```

```
ipSecAddressEntry OBJECT-TYPE
  SYNTAX IpSecAddressEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecAddressPrid }
  UNIQUENESS {
    ipSecAddressAddressType,
    ipSecAddressAddrPrefixLength,
    ipSecAddressAddrMin,
    ipSecAddressAddrMax,
    ipSecAddressGroupId
    }
  ::= { ipSecAddressTable 1 }

  IpSecAddressEntry ::= SEQUENCE {
     ipSecAddressPrid InstanceId,
     ipSecAddressAddressType InetAddressType,
     ipSecAddressAddrPrefixLength InetAddressPrefixLength,
     ipSecAddressAddrMin InetAddress,
     ipSecAddressAddrMax InetAddress,
     ipSecAddressGroupId TagId
}

ipSecAddressPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecAddressEntry  1 }

ipSecAddressAddressType OBJECT-TYPE
  SYNTAX InetAddressType
  STATUS current
  DESCRIPTION
"Specifies the type of IP address.

While other types of addresses are defined in the InetAddressType
textual convention, an IP filter can only use IPv4 and IPv6
addresses directly to classify traffic. All other InetAddressTypes
require mapping to the corresponding Ipv4 or IPv6 address before
being used to classify traffic. Therefore, this object as such is
not limited to IPv4 and IPv6 addresses, i.e., it can be assigned
any of the valid values defined in the InetAddressType TC, but the
mapping of the address values to IPv4 or IPv6 addresses must be
done by the PEP at install time. "
  ::= { ipSecAddressEntry  2 }

ipSecAddressAddrPrefixLength OBJECT-TYPE
  SYNTAX InetAddressPrefixLength
  STATUS current
```

```
  DESCRIPTION
"The length of a mask for the matching of IP address. This
attribute is interpreted only if the InetAddressType is 'ipv4',
'ipv4z', 'ipv6' or 'ipv6z'.

Masks are constructed by setting bits in sequence from the most-
significant bit downwards for ipSecAddressAddrPrefixLength bits
length. All other bits in the mask, up to the  number needed to
fill the length of the address ipSecAddressAddrMin are cleared to
```

```
zero. A zero bit in the mask then means that the corresponding bit
in the address always matches.

In IPv4 addresses, a length of 0 indicates a match of any address.
When ipSecAddressAddrMin and ipSecAddressAddrMax have the same
value, a length of 32 or greater indicates a match of a single
host address, and a length between 0 and 32 indicates the use of a
CIDR Prefix. When ipSecAddressAddrMin and ipSecAddressAddrMax have
different values, this attribute MUST have a value of 32 to
indicate an IP address range.

In IPv6 addresses, a length of 0 indicates a match of any address.
When ipSecAddressAddrMin and ipSecAddressAddrMax have the same
value, a length of 128 or greater indicates a match of a single
host address, and a length between 0 and 128 indicates the use of
a CIDR Prefix. When ipSecAddressAddrMin and ipSecAddressAddrMax
have different values, this attribute MUST have value of 128 in
order to indicate an IP address range."
  ::= { ipSecAddressEntry  3 }

ipSecAddressAddrMin OBJECT-TYPE
  SYNTAX InetAddress
  STATUS current
  DESCRIPTION
"Specifies an IP address. The type of the address is specified by
the ipSecAddressAddressType attribute. If the address type is
'ipv4', 'ipv6', 'ipv4z' or 'ipv6z' then, the attribute
ipSecAddressAddrPrefixLength indicates the number of bits that are
relevant."
  ::= { ipSecAddressEntry  4 }

ipSecAddressAddrMax OBJECT-TYPE
  SYNTAX InetAddress
  STATUS current
  DESCRIPTION
"If a range of addresses is used then this specifies the ending
address. The type of the address is specified by the
ipSecAddressAddressType attribute.

To specify a single IP addres or a subnet, this attribute MUST be
the same as that of ipSecAddressAddrMin.

When ipSecAddressAddressType is 'dns', this attribute MUST contain
the same DNS address as ipSecAddressAddrMin"
```

```
  ::= { ipSecAddressEntry  5 }
```

```
ipSecAddressGroupId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"Specifies the group this IP address, address range or subnet
address belongs to."
  ::= { ipSecAddressEntry  6 }


--
--
-- The ipSecL4PortTable
--

ipSecL4PortTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecL4PortEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies layer four port numbers."
  ::= { ipSecSelector  4 }

ipSecL4PortEntry OBJECT-TYPE
  SYNTAX IpSecL4PortEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecL4PortPrid }
  UNIQUENESS {
    ipSecL4PortPortMin,
    ipSecL4PortPortMax,
    ipSecL4PortGroupId
    }
  ::= { ipSecL4PortTable 1 }

  IpSecL4PortEntry ::= SEQUENCE {
     ipSecL4PortPrid InstanceId,
     ipSecL4PortPortMin InetPortNumber,
     ipSecL4PortPortMax InetPortNumber,
     ipSecL4PortGroupId TagId
}

ipSecL4PortPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecL4PortEntry  1 }

ipSecL4PortPortMin OBJECT-TYPE
```

```
  SYNTAX InetPortNumber
  STATUS current
  DESCRIPTION
"Specifies a layer 4 port or the first layer 4 port number of a
range of ports. The value of this attribute must be equal or less
than that of ipSecL4PortPortMax.

A value of zero indicates any port matches."
  ::= { ipSecL4PortEntry  2 }

ipSecL4PortPortMax OBJECT-TYPE
  SYNTAX InetPortNumber
  STATUS current
  DESCRIPTION
"Specifies the last layer 4 port in the range. If only a single
port is specified, the value of this attribute must be equal to
that of ipSecL4PortPortMin. Otherwise, the value of this attribute
MUST be greater than that specified by ipSecL4PortPortMin.

If ipSecL4PortPortMin is zero, this attribute MUST be ignored."
  ::= { ipSecL4PortEntry  3 }

ipSecL4PortGroupId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"Specifies the group this port or port range belongs to."
  ::= { ipSecL4PortEntry  4 }


--
--
-- The ipSecIpsoFilterSetTable
--

ipSecIpsoFilterSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIpsoFilterSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IP Security Options (IPSO) filter sets. Each set
contains an ordered list of IPSO filters. Please refer to
[RFC1108] for details on IPSO."
  ::= { ipSecSelector  5 }

ipSecIpsoFilterSetEntry OBJECT-TYPE
```

```
  SYNTAX IpSecIpsoFilterSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIpsoFilterSetPrid }
  UNIQUENESS {
    ipSecIpsoFilterSetFilterSetId,
```

```
    ipSecIpsoFilterSetOrder
    }
  ::= { ipSecIpsoFilterSetTable 1 }

  IpSecIpsoFilterSetEntry ::= SEQUENCE {
     ipSecIpsoFilterSetPrid InstanceId,
     ipSecIpsoFilterSetFilterSetId TagId,
     ipSecIpsoFilterSetFilterId ReferenceId,
     ipSecIpsoFilterSetOrder IpSecOrderTC,
     ipSecIpsoFilterSetIsNegated TruthValue
}

ipSecIpsoFilterSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecIpsoFilterSetEntry  1 }

ipSecIpsoFilterSetFilterSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An IPSO filter set is composed of one or more IPSO filters.
Filters belonging to the same set have the same FilterSetId."
  ::= { ipSecIpsoFilterSetEntry  2 }

ipSecIpsoFilterSetFilterId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecIpsoFilterEntry }
  STATUS current
  DESCRIPTION
"A pointer to a valid instance in the ipSecIpsoFilterTable."
  ::= { ipSecIpsoFilterSetEntry  3 }

ipSecIpsoFilterSetOrder OBJECT-TYPE
  SYNTAX IpSecOrderTC
  STATUS current
  DESCRIPTION
"An integer that specifies the precedence order of the filter
identified by ipSecIpsoFilterSetFilterId within a filter set. The
filter set is identified by ipSecIpsoFilterSetFilterSetId."
  ::= { ipSecIpsoFilterSetEntry  4 }

ipSecIpsoFilterSetIsNegated OBJECT-TYPE
  SYNTAX TruthValue
  STATUS current
  DESCRIPTION
"If the value of this attribute is 'true', the filter pointed by
ipSecIpsoFilterSetFilterId SHALL be negated."
  ::= { ipSecIpsoFilterSetEntry  5 }
```

```
--
--
-- The ipSecIpsoFilterTable
--

ipSecIpsoFilterTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIpsoFilterEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies IP Security Options (IPSO) filters. Please refer to
[RFC1108] for details on IPSO."
  ::= { ipSecSelector  6 }

ipSecIpsoFilterEntry OBJECT-TYPE
  SYNTAX IpSecIpsoFilterEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIpsoFilterPrid }
  UNIQUENESS {
    ipSecIpsoFilterMatchConditionType,
    ipSecIpsoFilterClassificationLevel,
    ipSecIpsoFilterProtectionAuthority
    }
  ::= { ipSecIpsoFilterTable 1 }

  IpSecIpsoFilterEntry ::= SEQUENCE {
     ipSecIpsoFilterPrid InstanceId,
     ipSecIpsoFilterMatchConditionType INTEGER,
     ipSecIpsoFilterClassificationLevel IpSecIpsoClassificationTC,
     ipSecIpsoFilterProtectionAuthority IpSecIpsoProtectionTC
}

ipSecIpsoFilterPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecIpsoFilterEntry  1 }

ipSecIpsoFilterMatchConditionType OBJECT-TYPE
  SYNTAX INTEGER {
    classificationLevel(1),
    protectionAuthority(2)
    }
  STATUS current
  DESCRIPTION
"Specifies the IPSO header field to be matched."
  ::= { ipSecIpsoFilterEntry  2 }
```

```
ipSecIpsoFilterClassificationLevel OBJECT-TYPE
  SYNTAX IpSecIpsoClassificationTC
  STATUS current
  DESCRIPTION
"Specifies the value for classification level to be matched
against. This attribute MUST be ignored if
ipSecIpsoFilterMatchConditionType is not 1 (classificationLevel)."
  ::= { ipSecIpsoFilterEntry  3 }

ipSecIpsoFilterProtectionAuthority OBJECT-TYPE
  SYNTAX IpSecIpsoProtectionTC
  STATUS current
  DESCRIPTION
"Specifies the value for protection authority to be matched
against. This attribute MUST be ignored if
ipSecIpsoFilterMatchConditionType is not 2 (protectionAuthority).
"
  ::= { ipSecIpsoFilterEntry  4 }


--
--
-- The ipSecRuleTimePeriodTable
--
```

```
ipSecRuleTimePeriodTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecRuleTimePeriodEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies the time periods during which a policy rule is valid.
The values of the first five attributes in a row are ANDed
together to determine the validity period(s). If any of the five
attributes is not present, it is treated as having value always
enabled.  "
  ::= { ipSecPolicyTimePeriod  1 }

ipSecRuleTimePeriodEntry OBJECT-TYPE
  SYNTAX IpSecRuleTimePeriodEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecRuleTimePeriodPrid }
  UNIQUENESS {
    ipSecRuleTimePeriodTimePeriod,
    ipSecRuleTimePeriodMonthOfYearMask,
    ipSecRuleTimePeriodDayOfMonthMask,
    ipSecRuleTimePeriodDayOfWeekMask,
    ipSecRuleTimePeriodTimeOfDayMask,
    ipSecRuleTimePeriodLocalOrUtcTime
    }
  ::= { ipSecRuleTimePeriodTable 1 }
```

```
  IpSecRuleTimePeriodEntry ::= SEQUENCE {
     ipSecRuleTimePeriodPrid InstanceId,
     ipSecRuleTimePeriodTimePeriod TimePeriodTC,
     ipSecRuleTimePeriodMonthOfYearMask MonthOfYearTC,
     ipSecRuleTimePeriodDayOfMonthMask DayOfMonthTC,
     ipSecRuleTimePeriodDayOfWeekMask DayOfWeekTC,
     ipSecRuleTimePeriodTimeOfDayMask TimeOfDayTC,
     ipSecRuleTimePeriodLocalOrUtcTime LocalOrUtcTimeTC
}

ipSecRuleTimePeriodPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index to uniquely identify an instance of this class"
  ::= { ipSecRuleTimePeriodEntry  1 }
```

```
ipSecRuleTimePeriodTimePeriod OBJECT-TYPE
  SYNTAX TimePeriodTC
  STATUS current
  DESCRIPTION
"Identifies an overall range of calendar dates and times over
which a policy rule is valid."
  ::= { ipSecRuleTimePeriodEntry  2 }

ipSecRuleTimePeriodMonthOfYearMask OBJECT-TYPE
  SYNTAX MonthOfYearTC
  STATUS current
  DESCRIPTION
"Specifies months of a year during which a policy is valid."
  ::= { ipSecRuleTimePeriodEntry  3 }

ipSecRuleTimePeriodDayOfMonthMask OBJECT-TYPE
  SYNTAX DayOfMonthTC
  STATUS current
  DESCRIPTION
"Specifies days of a month during which a policy is valid."
  ::= { ipSecRuleTimePeriodEntry  4 }

ipSecRuleTimePeriodDayOfWeekMask OBJECT-TYPE
  SYNTAX DayOfWeekTC
  STATUS current
  DESCRIPTION
"Specifies days of a week during which a policy is valid."
  ::= { ipSecRuleTimePeriodEntry  5 }

ipSecRuleTimePeriodTimeOfDayMask OBJECT-TYPE
  SYNTAX TimeOfDayTC
  STATUS current
  DESCRIPTION
"Specifies a range of times in a day during which a policy is
valid."
  ::= { ipSecRuleTimePeriodEntry  6 }
```

```
ipSecRuleTimePeriodLocalOrUtcTime OBJECT-TYPE
  SYNTAX LocalOrUtcTimeTC
  STATUS current
  DESCRIPTION
"Indicates whether the times represented in this class represent
local times or UTC times.  There is no provision for mixing of
local times and UTC times:  the value of this property applies to
all of the other time-related properties."
```

```
  ::= { ipSecRuleTimePeriodEntry  7 }


--
--
-- The ipSecRuleTimePeriodSetTable
--

ipSecRuleTimePeriodSetTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecRuleTimePeriodSetEntry
  PIB-ACCESS install
  STATUS current
  DESCRIPTION
"Specifies time period sets. The ipSecRuleTimePeriodTable can
specify only a single time period within a day. This class enables
the specification of multiple time periods within a day by
grouping them into one set. "
  ::= { ipSecPolicyTimePeriod  2 }

ipSecRuleTimePeriodSetEntry OBJECT-TYPE
  SYNTAX IpSecRuleTimePeriodSetEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecRuleTimePeriodSetPrid }
  UNIQUENESS {
    ipSecRuleTimePeriodSetRuleTimePeriodSetId,
    ipSecRuleTimePeriodSetRuleTimePeriodId
    }
  ::= { ipSecRuleTimePeriodSetTable 1 }

  IpSecRuleTimePeriodSetEntry ::= SEQUENCE {
     ipSecRuleTimePeriodSetPrid InstanceId,
     ipSecRuleTimePeriodSetRuleTimePeriodSetId TagId,
     ipSecRuleTimePeriodSetRuleTimePeriodId ReferenceId
}

ipSecRuleTimePeriodSetPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index to uniquely identify an instance of this class"
  ::= { ipSecRuleTimePeriodSetEntry  1 }
```

```
ipSecRuleTimePeriodSetRuleTimePeriodSetId OBJECT-TYPE
  SYNTAX TagId
  STATUS current
  DESCRIPTION
"An integer that uniquely identifies an ipSecRuleTimePeriod set. "
  ::= { ipSecRuleTimePeriodSetEntry  2 }

ipSecRuleTimePeriodSetRuleTimePeriodId OBJECT-TYPE
  SYNTAX ReferenceId
  PIB-REFERENCES    {ipSecRuleTimePeriodEntry }
  STATUS current
  DESCRIPTION
"An integer that identifies an ipSecRuleTimePeriod, specified by
ipSecRuleTimePeriodPrid in the ipSecRuleTimePeriodTable, that is
included in this set."
  ::= { ipSecRuleTimePeriodSetEntry  3 }


--
--
-- The ipSecIfCapsTable
--

ipSecIfCapsTable OBJECT-TYPE
  SYNTAX SEQUENCE OF IpSecIfCapsEntry
  PIB-ACCESS notify
  STATUS current
  DESCRIPTION
"Specifies capabilities that may be associated with an interface
of a specific type. The instances of this class are referenced by
the frwkCapabilitySetCapability attribute of the
frwkCapabilitySetTable [RFC3318]."
  ::= { ipSecIfCapability  1 }

ipSecIfCapsEntry OBJECT-TYPE
  SYNTAX IpSecIfCapsEntry
  STATUS current
  DESCRIPTION
"Specifies an instance of this class"
  PIB-INDEX { ipSecIfCapsPrid }
  UNIQUENESS {
    ipSecIfCapsDirection,
    ipSecIfCapsMaxIpSecActions,
    ipSecIfCapsMaxIkeActions
    }
  ::= { ipSecIfCapsTable 1 }

  IpSecIfCapsEntry ::= SEQUENCE {
     ipSecIfCapsPrid InstanceId,
     ipSecIfCapsDirection INTEGER,
     ipSecIfCapsMaxIpSecActions Unsigned16TC,
     ipSecIfCapsMaxIkeActions Unsigned16TC
}
```

```
ipSecIfCapsPrid OBJECT-TYPE
  SYNTAX InstanceId
  STATUS current
  DESCRIPTION
"An integer index that uniquely identifies an instance of this
class."
  ::= { ipSecIfCapsEntry  1 }

ipSecIfCapsDirection OBJECT-TYPE
  SYNTAX INTEGER {
    in(1),
    out(2),
    bi-directional(3)
    }
  STATUS current
  DESCRIPTION
"Specifies the direction for which this capability applies."
  ::= { ipSecIfCapsEntry  2 }

ipSecIfCapsMaxIpSecActions OBJECT-TYPE
  SYNTAX Unsigned16TC
  STATUS current
  DESCRIPTION
"Specifies the maximum number of actions an IPsec action set may
contain. IPsec action sets are specified by the
ipSecActionSetTable.

A value of zero indicates that there is no maximum limit."
  ::= { ipSecIfCapsEntry  3 }

ipSecIfCapsMaxIkeActions OBJECT-TYPE
  SYNTAX Unsigned16TC
  STATUS current
  DESCRIPTION
"Specifies the maximum number of actions an IKE action set may
contain. IKE action sets are specified by the
ipSecIkeActionSetTable.

A value of zero indicates that there is no maximum limit."
  ::= { ipSecIfCapsEntry  4 }


--
--
-- Conformance Section
```

```
--

ipSecPolicyPibCompliances
    OBJECT IDENTIFIER ::= { ipSecPolicyPibConformance 1 }

ipSecPolicyPibConformanceGroups
    OBJECT IDENTIFIER ::= { ipSecPolicyPibConformance 2 }
```

```
ipSecPolicyPibCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
"        Compliance statement"
    MODULE --this module
        MANDATORY-GROUPS {
             ipSecSaGroup,
             ipSecIkeGroup,
             ipSecSelectorGroup,
             ipSecIfCapsGroup
        }

    GROUP ipSecIkeRuleGroup
        DESCRIPTION
"This group is mandatory if any of the following is supported: 1)
multiple IKE phase one actions (e.g., with different exchange
modes) are associated with an IPsec rule. These actions are to be
tried in sequence till one success; 2) IKE phase one actions that
start automatically."

    GROUP ipSecIkeActionSetGroup
        DESCRIPTION
"This group is mandatory if any of the following is supported: 1)
multiple IKE phase one actions (e.g., with different exchange
modes) are associated with an IPsec rule. These actions are to be
tried in sequence till one success; 2) IKE phase one actions that
start automatically."

    GROUP ipSecIpsoFilterSetGroup
        DESCRIPTION
"This group is mandatory if IPSO filter is supported."

    GROUP ipSecIpsoFilterGroup
        DESCRIPTION
"This group is mandatory if IPSO filter is supported."

    GROUP ipSecRuleTimePeriodGroup
        DESCRIPTION
```

```
"This group is mandatory if policy scheduling is supported."

    GROUP ipSecRuleTimePeriodSetGroup
        DESCRIPTION
"This group is mandatory if policy scheduling is supported."

    OBJECT ipSecRuleIpSecIpsoFilterSetId
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecRuleLimitNegotiation
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
```

```
"              Support of this attribute is optional"

    OBJECT ipSecRuleAutoStart
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecRuleIpSecRuleTimePeriodGroupId
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecActionSetDoActionLogging
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecActionSetDoPacketLogging
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecAssociationMinLifetimeSeconds
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecAssociationMinLifetimeKilobytes
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"
```

```
    OBJECT ipSecAssociationIdleDurationSeconds
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecAssociationUseKeyExchangeGroup
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecAssociationGranularity
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecAhTransformUseReplayPrevention
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecAhTransformReplayPreventionWindowSize
```

```
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecEspTransformCipherKeyRounds
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecEspTransformCipherKeyLength
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecEspTransformUseReplayPrevention
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecEspTransformReplayPreventionWindowSize
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecCompTransformDictionarySize
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkeAssociationMinLiftetimeSeconds
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkeAssociationMinLifetimeKilobytes
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkeAssociationIdleDurationSeconds
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkeAssociationPresharedKey
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkeAssociationVendorId
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"
```

```
    OBJECT ipSecIkeAssociationAggressiveModeGroupId
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkeAssociationLocalCredentialId
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkeAssociationDoActionLogging
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkeProposalPrfAlgorithm
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIkePeerEndpointAddress
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecIfCapsMaxIkeActions
    PIB-MIN-ACCESS not-accessible
    DESCRIPTION
"              Support of this attribute is optional"

    OBJECT ipSecRuleActionExecutionStrategy
    SYNTAX INTEGER {
      doAll(1)
      }
    DESCRIPTION
"              Support of doUntilSuccess(2) is not required"

    OBJECT ipSecStaticActionAction
    SYNTAX INTEGER {
      byPass(1),
      discard(2),
      preConfiguredTransport(4),
      preConfiguredTunnel(5)
      }
    DESCRIPTION
"              Support of ikeRejection(3) is not required"

    ::= { ipSecPolicyPibCompliances 1 }

ipSecSaGroup OBJECT-GROUP
    OBJECTS {
       ipSecRulePrid,
```

```
       ipSecRuleIfCapSetName,
       ipSecRuleRoles,
       ipSecRuleDirection,
       ipSecRuleIpSecSelectorSetId,
       ipSecRuleIpSecIpsoFilterSetId,
       ipSecRuleIpSecActionSetId,
       ipSecRuleActionExecutionStrategy,
       ipSecRuleOrder,
       ipSecRuleLimitNegotiation,
       ipSecRuleAutoStart,
       ipSecRuleIpSecRuleTimePeriodGroupId,
       ipSecActionSetPrid,
       ipSecActionSetActionSetId,
       ipSecActionSetActionId,
       ipSecActionSetDoActionLogging,
       ipSecActionSetDoPacketLogging,
       ipSecActionSetOrder,

       ipSecStaticActionPrid,
       ipSecStaticActionAction,
       ipSecStaticActionTunnelEndpointId,
       ipSecStaticActionDfHandling,
       ipSecStaticActionSpi,
       ipSecStaticActionLifetimeSeconds,
       ipSecStaticActionLifetimeKilobytes,
       ipSecStaticActionSaTransformId,

       ipSecNegotiationActionPrid,
       ipSecNegotiationActionAction,
       ipSecNegotiationActionTunnelEndpointId,
       ipSecNegotiationActionDfHandling,
       ipSecNegotiationActionIpSecAssociationId,
       ipSecNegotiationActionKeyExchangeId,

       ipSecAssociationPrid,
       ipSecAssociationMinLifetimeSeconds,
       ipSecAssociationMinLifetimeKilobytes,
       ipSecAssociationIdleDurationSeconds,
       ipSecAssociationUsePfs,
       ipSecAssociationUseKeyExchangeGroup,
       ipSecAssociationDhGroup,
       ipSecAssociationGranularity,
       ipSecAssociationProposalSetId,

       ipSecProposalSetPrid,
       ipSecProposalSetProposalSetId,
       ipSecProposalSetProposalId,
       ipSecProposalSetOrder,

       ipSecProposalPrid,
       ipSecProposalEspTransformSetId,
       ipSecProposalAhTransformSetId,
```

```
       ipSecProposalCompTransformSetId,

       ipSecAhTransformSetPrid,
       ipSecAhTransformSetTransformSetId,
       ipSecAhTransformSetTransformId,
       ipSecAhTransformSetOrder,

       ipSecAhTransformPrid,
       ipSecAhTransformTransformId,
       ipSecAhTransformIntegrityKey,
       ipSecAhTransformUseReplayPrevention,
       ipSecAhTransformReplayPreventionWindowSize,
       ipSecAhTransformMaxLifetimeSeconds,
       ipSecAhTransformMaxLifetimeKilobytes,

       ipSecEspTransformSetPrid,
       ipSecEspTransformSetTransformSetId,
       ipSecEspTransformSetTransformId,
       ipSecEspTransformSetOrder,

       ipSecEspTransformPrid,
       ipSecEspTransformIntegrityTransformId,
       ipSecEspTransformCipherTransformId,
       ipSecEspTransformIntegrityKey,
       ipSecEspTransformCipherKey,
       ipSecEspTransformCipherKeyRounds,
       ipSecEspTransformCipherKeyLength,
       ipSecEspTransformUseReplayPrevention,
       ipSecEspTransformReplayPreventionWindowSize,
       ipSecEspTransformMaxLifetimeSeconds,
       ipSecEspTransformMaxLifetimeKilobytes,

       ipSecCompTransformSetPrid,
       ipSecCompTransformSetTransformSetId,
       ipSecCompTransformSetTransformId,
       ipSecCompTransformSetOrder,

       ipSecCompTransformPrid,
       ipSecCompTransformAlgorithm,
       ipSecCompTransformDictionarySize,
       ipSecCompTransformMaxLifetimeSeconds,
       ipSecCompTransformMaxLifetimeKilobytes
       }
    STATUS current
    DESCRIPTION
"This group specifies IPsec phase two rules"
    ::= { ipSecPolicyPibConformanceGroups  1 }

ipSecIkeGroup OBJECT-GROUP
    OBJECTS {
       ipSecIkeAssociationPrid,
       ipSecIkeAssociationMinLiftetimeSeconds,
       ipSecIkeAssociationMinLifetimeKilobytes,
       ipSecIkeAssociationIdleDurationSeconds,
       ipSecIkeAssociationExchangeMode,
       ipSecIkeAssociationUseIkeIdentityType,
       ipSecIkeAssociationUseIkeIdentityValue,
       ipSecIkeAssociationIkePeerEndpoint,
       ipSecIkeAssociationPresharedKey,
       ipSecIkeAssociationVendorId,
       ipSecIkeAssociationAggressiveModeGroupId,
       ipSecIkeAssociationLocalCredentialId,
       ipSecIkeAssociationDoActionLogging,
       ipSecIkeAssociationIkeProposalSetId,

       ipSecIkeProposalSetPrid,
       ipSecIkeProposalSetProposalSetId,
       ipSecIkeProposalSetProposalId,
       ipSecIkeProposalSetOrder,

       ipSecIkeProposalPrid,
       ipSecIkeProposalMaxLifetimeSeconds,
       ipSecIkeProposalMaxLifetimeKilobytes,
       ipSecIkeProposalCipherAlgorithm,
       ipSecIkeProposalHashAlgorithm,
       ipSecIkeProposalAuthenticationMethod,
       ipSecIkeProposalPrfAlgorithm,
       ipSecIkeProposalIkeDhGroup,

       ipSecIkePeerEndpointPrid,
       ipSecIkePeerEndpointIdentityType,
       ipSecIkePeerEndpointIdentityValue,
       ipSecIkePeerEndpointIsNegated,
       ipSecIkePeerEndpointAddress,
       ipSecIkePeerEndpointCredentialSetId,

       ipSecCredentialSetPrid,
       ipSecCredentialSetSetId,
       ipSecCredentialSetCredentialId,

       ipSecCredentialPrid,
       ipSecCredentialCredentialType,
       ipSecCredentialFieldsId,
       ipSecCredentialCrlDistributionPoint,

       ipSecCredentialFieldsPrid,
       ipSecCredentialFieldsName,
       ipSecCredentialFieldsValue,
       ipSecCredentialFieldsIsNegated,
       ipSecCredentialFieldsSetId
```

```
       }
    STATUS current
    DESCRIPTION
"This group specifies IPsec phase one rules (IKEv1)"
    ::= { ipSecPolicyPibConformanceGroups  2 }
```

```
ipSecSelectorGroup OBJECT-GROUP
    OBJECTS {
       ipSecSelectorSetPrid,
       ipSecSelectorSetSelectorSetId,
       ipSecSelectorSetSelectorId,
       ipSecSelectorSetOrder,
       ipSecSelectorSetIsNegated,

       ipSecSelectorPrid,
       ipSecSelectorSrcAddressGroupId,
       ipSecSelectorSrcPortGroupId,
       ipSecSelectorDstAddressGroupId,
       ipSecSelectorDstPortGroupId,
       ipSecSelectorProtocol,
       ipSecSelectorDscp,
       ipSecSelectorFlowLabel,

       ipSecAddressPrid,
       ipSecAddressAddressType,
       ipSecAddressAddrPrefixLength,
       ipSecAddressAddrMin,
       ipSecAddressAddrMax,
       ipSecAddressGroupId,

       ipSecL4PortPrid,
       ipSecL4PortPortMin,
       ipSecL4PortPortMax,
       ipSecL4PortGroupId
       }
    STATUS current
    DESCRIPTION
"This group specifeis IPsec selectors"
    ::= { ipSecPolicyPibConformanceGroups  3 }

ipSecIfCapsGroup OBJECT-GROUP
    OBJECTS {
       ipSecIfCapsPrid,
       ipSecIfCapsDirection,
       ipSecIfCapsMaxIpSecActions,
       ipSecIfCapsMaxIkeActions
       }
    STATUS current
    DESCRIPTION
"This group spedifies IPsec interface capabilities"
    ::= { ipSecPolicyPibConformanceGroups  4 }

ipSecIkeRuleGroup OBJECT-GROUP
    OBJECTS {
       ipSecIkeRulePrid,
       ipSecIkeRuleIfCapSetName,
       ipSecIkeRuleRoles,
       ipSecIkeRuleIkeActionSetId,
       ipSecIkeRuleActionExecutionStrategy,
```

```
       ipSecIkeRuleLimitNegotiation,
       ipSecIkeRuleAutoStart,
       ipSecIkeRuleIpSecRuleTimePeriodGroupId
       }
    STATUS current
    DESCRIPTION
"Objects from the ipSecIkeRuleTable."
    ::= { ipSecPolicyPibConformanceGroups  5 }

ipSecIkeActionSetGroup OBJECT-GROUP
    OBJECTS {
       ipSecIkeActionSetPrid,
       ipSecIkeActionSetActionSetId,
       ipSecIkeActionSetActionId,
       ipSecIkeActionSetOrder
       }
    STATUS current
    DESCRIPTION
"Objects from the ipSecIkeActionSetTable."
    ::= { ipSecPolicyPibConformanceGroups  6 }

ipSecIpsoFilterSetGroup OBJECT-GROUP
    OBJECTS {
       ipSecIpsoFilterSetPrid,
       ipSecIpsoFilterSetFilterSetId,
       ipSecIpsoFilterSetFilterId,
       ipSecIpsoFilterSetOrder,
       ipSecIpsoFilterSetIsNegated
       }
    STATUS current
    DESCRIPTION
```

```
"Objects from the ipSecIpsoFilterSetTable."
    ::= { ipSecPolicyPibConformanceGroups  7 }

ipSecIpsoFilterGroup OBJECT-GROUP
    OBJECTS {
       ipSecIpsoFilterPrid,
       ipSecIpsoFilterMatchConditionType,
       ipSecIpsoFilterClassificationLevel,
       ipSecIpsoFilterProtectionAuthority
       }
    STATUS current
    DESCRIPTION
"Objects from the ipSecIpsoFilterTable."
    ::= { ipSecPolicyPibConformanceGroups  8 }

ipSecRuleTimePeriodGroup OBJECT-GROUP
    OBJECTS {
       ipSecRuleTimePeriodPrid,
       ipSecRuleTimePeriodTimePeriod,
       ipSecRuleTimePeriodMonthOfYearMask,
       ipSecRuleTimePeriodDayOfMonthMask,
       ipSecRuleTimePeriodDayOfWeekMask,
```

```
       ipSecRuleTimePeriodTimeOfDayMask,
       ipSecRuleTimePeriodLocalOrUtcTime
       }
    STATUS current
    DESCRIPTION
"Objects from the ipSecRuleTimePeriodTable."
    ::= { ipSecPolicyPibConformanceGroups  9 }

ipSecRuleTimePeriodSetGroup OBJECT-GROUP
    OBJECTS {
       ipSecRuleTimePeriodSetPrid,
       ipSecRuleTimePeriodSetRuleTimePeriodSetId,
       ipSecRuleTimePeriodSetRuleTimePeriodId
       }
    STATUS current
    DESCRIPTION
"Objects from the ipSecRuleTimePeriodSetTable."
    ::= { ipSecPolicyPibConformanceGroups  10 }

END
```

6. Security Considerations

This document defines an IPsec PIB for configuring IPsec policies on

IPsec enabled devices. As IPsec provides security services, it is critical that IPsec configuration data be protected at least as strongly as the desired IPsec policy.

The ipSecEspTransformTable, ipSecAhTransformTable contain authentication and encryption keys for static IPsec security associations. These two attributes are ignored for IPsec security associations that are dynamically established. The ipSecIkeAssociationTable contains an optional pre-shared key for IKE authentication. Malicious access of the above PRCs can compromise the keys. As a result, they MUST NOT be observed by third parties.

In addition, the PRCs in this PIB may contain information that may be sensitive from a business perspective, in that they may represent a customer's service contract or the filters that the service provider chooses to apply to a customer's traffic. All the tables except the ipSecIfCapsTable have a PIB-ACCESS clause of install. Malicious altering of the these PRCs may affect the IPsec behavior of the device being provisioned. Malicious access of the above PRCs also exposes policy information concerning how the device is provisioned.

The ipSecIfCapsTable has a PIB-ACCESS clause of notify. Malicious access of the this PRC exposes information concerning the device being provisioned.

The authentication and integrity of configuration information is of utmost importance to the security of a network. Administrators SHOULD carefully consider the potential threat environment involving

PDP and PEP data exchange. At a minimum, PDP's and PEP's SHOULD authenticate one another and SHOULD use a transport protocol that supports data integrity and authentication. Administrators SHOULD also carefully consider the importance of confidentiality of their configuration information, because it may reveal private or confidential information about customer access, business relationships, keys, etc. If these are concerns to the organization, then confidentiality SHOULD be used to transport the information. Administrators SHOULD use IPSEC or TLS between PDP and PEP as described in [5] and [15] to provide necessary protections.

7. RFC Editor Considerations

Normatively references [23][24]are Internet drafts. Please use their corresponding RFC numbers prior to publishing of this document as a RFC.

8. IANA Considerations

This document describes the ipSecPolicyPib Policy Information Base (PIB) module for registration under the "pib" branch registered with IANA. IANA has assigned PIB number <tbd> for it under the "pib" branch.

IANA Considerations for SUBJECT-CATEGORIES follow the same requirements as specified in [RFC2748] IANA Considerations for COPS Client Types. The IPsec PIB defines a new COPS Client Type. The IANA has assigned a COPS client type XXXXX (tbd) as described in [RFC2748] IANA Considerations. IANA has updated the registry (http://www.iana.org/assignments/cops-parameters) for COPS Client Types as a result.

The authors suggest the use of "ipSec" as the name of the ClientType.

9. Normative References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

3. S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

4. F. Dawson, D. Stenerson, "Internet Calendaring and Scheduling Core Object Specification (iCalendar) ", RFC 2445, November 1998.

5. J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

6. K. Chan, D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith, R. Yavatkar, "COPS Usage for Policy Provisioning", RFC 3084, March 2001.

7. D. Piper, "The Internet IP Security Domain of Interpretation

for ISAKMP", RFC 2407, November 1998.

8. S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP) ", RFC 2406, November 1998.

9. M. Fine, K. McCloghrie, J. Seligson, K. Chan, S. Hahn, A. Smith, F. Reichmeyer "Framework Policy Information Base", RFC 3318, March 2003.

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

11. A. Shacham, R. Monsour, R. Pereira, M. Thomas, "IP Payload Compression Protocol (IPComp) ", RFC 2393, August 1998.

12. J. Jason, L. Rafalow, E. Vyncke "IPsec Configuration Policy Model", RFC 3585, August 2003.

13. A. Westerinen, et al "Terminology for Policy-Based Management", RFC 3198, November 2001.

14. K. McCloghrie, M. Fine, J. Seligson, K. Chan, S. Chan, A. Smith, F. Reichmeyer, "Structure of Policy Provisioning Information", RFC 3159, August 2001.

15. K. McCloghrie, D. Perkins, J. Schoenwaelder, J. Case, M. Rose, S. Waldbusser, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

16. K. McCloghrie, D. Perkins, J. Schoenwaelder, J. Case,M. Rose, S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

17. F. Baker, K. Chan, A. Smith, "Management Information Base for the Differentiated Services Architecture", RFC 3289, May 2002.

18. M. Daniele, B. Haberman, S. Routhier, J. Schoenwaelder, "Textual Conventions for Internet Network Addresses.", RFC 3291, May 2002.

19. D. Harrington, R. Presuhn, B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", RFC 3411, December 2002.

20. B. Wijnen, "Textual Conventions for Ipv6 Flow Label", RFC 3595, September 2003.

21. S. Kent, "U.S. Department of Defense Security Options for the Internet Protocol", RFC 1108, November 1991.

22. B. Moore, E. Ellesson, J. Strassner, A. Westerinen, "Policy Core Information Model -- Version 1 Specification", RFC 3060, February 2001.

23. M. Baer, R. Charlet, W. Hardaker, R. Story, C. Wang, "IPsec Security Policy IPsec Action MIB", draft-ietf-ipsp-ipsecaction-mib-00.txt, January 2004.

24. M. Baer, R. Charlet, W. Hardaker, R. Story, C. Wang, " IPsec Security Policy IKE Action MIB", draft-ietf-ipsp-ikeaction-mib-00.txt, January 2004.

10. Informative References

25. J. Walker, A. Kulkarni, "COPS Over TLS", draft-ietf-rap-cops-tls-04.txt, June 2002.

11. Author's Addresses

Man Li
Nokia
5 Wayside Road,
Burlington, MA 01803
Phone: +1 781 993 3923
Email: man.m.li@nokia.com

David Arneson
Email: dla@mediaone.net

Avri Doria
ETRI
161 Gajeong-dong, Yuseong-gu
Deajeon 305-350 Korea
Email: avri@acm.org

Jamie Jason
Intel Corporation
MS JF3-206
2111 NE 25th Ave.
Hillsboro, OR 97124
Phone: +1 503 264 9531
Email: jamie.jason@intel.com

Cliff Wang
SmartPipes Inc.

Suite 300, 565 Metro Place South
Dublin, OH 43017
Phone: +1 614 923 6241
Email: CWang@smartpipes.com

Markus Stenberg
SSH Communications Security Corp.
Fredrikinkatu 42
FIN-00100 Helsinki, Finland
Phone: +358 20 500 7466
Email: fingon@iki.fi

12. IPR Disclosure Acknowledgement

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in according with RFC 2668.

13. Full Copyright Statement